Copilot Studio FAQ

Last updated: 9/4/2025
Microsoft will continuously update this document on a regular cadence.

Contents

Top Questions

1. What is Copilot Studio?

Microsoft Copilot Studio is a powerful platform for building secure, scalable, and intelligent agents that work across Microsoft 365 and line-of-business systems. Copilot Studio offers two ways to build AI agents: a lite experience (integrated into the Microsoft 365 Copilot app) and a full experience (a standalone Copilot Studio application). Both experiences enable you to create agents, but they serve different needs. Technical details here: https://aka.ms/copilotstudiodocs

2. Why does Copilot Studio offer both lite and full experiences for building agents?

Copilot Studio supports diverse user needs. The lite experience is ideal for quick, simple agents, while the full experience enables robust solutions with deeper control and application life-cycle management and governance. Together, they ensure flexibility and scalability for all users.

3. What's the difference between Copilot Studio and Copilot Chat?

Copilot Chat provides free and secure AI chat as a foundational and standardized user experience, with access to agents (some agent capabilities are pay-as-you-go) that will be critical to transforming business processes while simplifying AI management and security. This allows organizations of any size to begin using Copilot and agents within their workflow.

4. Are Copilot Studio and Azure AI Foundry essentially the same thing?

Microsoft Copilot Studio and Azure AI Foundry share a goal of enabling custom AI agents, but they are not the same. Copilot Studio is a fully managed SaaS offering – a low-code, turnkey agent platform where Microsoft handles the infrastructure and you build agents through a graphical interface. In contrast, Azure AI Foundry is a PaaS solution for pro developers, offering a code-first approach with deep integration into developer tools like Visual Studio Code and GitHub.

5. How much will building an agent cost?

There are many different variables to take into account when creating an agent. To help add clarity, Microsoft will be releasing a public-facing agent consumption estimator for Copilot Studio. This tool allows your organization to project monthly consumption of custom engine agents and see how things would be zero-rated for M365 Copilot. The plan is to update this estimator on a regular cadence and eventually expand it to other agent scenarios. To test drive the estimator visit: aka.ms/copilotstudioestimator

Build 2025 Announcements

Delivering the best new tools in the agent toolbox

- **Computer use tool in Copilot Studio** *(Frontier)*
  This new capability gives agents the ability to perform enterprise tasks on user interfaces across both desktop and web applications. With AI vision and understanding, automate repetitive tasks using Computer Using Agent (CUA) technology for tasks such as data transfer, document processing, market research, and compliance monitoring. Run them at scale them on virtual machines hosted by Microsoft to accelerate deployment, simplify management, and reduce costs.

- **Code interpreter in Copilot Studio** *(paid public preview)*
  Allows agents to write and run Python code to perform complex tasks such as processing files, calculating math, and generating images of graphs.

- **Dataverse for agents** *(generally available)*
  Store business data on Dataverse, the operational database for individual or teams of agents built in Copilot Studio, to optimize for speed and seamless interactions. Additionally, Dataverse and uploaded files will have increased efficiency and search capabilities like image extraction, multi-language support and ability to query embedded tabular files.

- **Solution Workspace** *(generally available on 5/30)*
  Enables makers to define business requirements and use AI to generate process map (PP), design solution architecture including pages, dashboards, data tables & MCS agents

- **Agent feed** *(public preview)*
  Provides a hub for business users to manage and monitor agents, with an activity feed for updates and guidance when human input is needed (PP). Makers can set up agents to suggest actions (EAP) and end-users can build automations (EAP).

- **Tools enhancements** *(preview)*
  Tools enhancements across Microsoft's existing set of supported tools and actions provide agents and apps with the ability to do more. Examples of Tools are Prompts, document generation, deep reasoning prompts, agent flows, connectors, REST APIs, and more.

Creating agentic systems

- **Model Context Protocol** *(generally available)*
  Model Context Protocol (MCP) in Copilot Studio streamlines AI integration with apps, APIs, and data sources, enabling faster, scalable intelligent agents. MCP connectors automate updates between agents and knowledge servers, ensuring accuracy. Makers can also use SDK support to build MCP servers, publish connectors, and integrate tools seamlessly. This boosts efficiency, reduces complexity, and fosters responsive innovation.

- **Agent orchestration** *(paid public preview on June 9)*
  Agent orchestration allows multiple agents, including those built in Copilot Studio, Azure Agent Service or M365 Agents SDK, to work together, distribute work across multiple steps and deliver more comprehensive experiences. Additionally, Microsoft announced native support for open standards including A2A in Copilot Studio and Azure AI Foundry, starting with public preview. With these capabilities, agents built on Microsoft's platforms will be able to discover peer agents, negotiate tasks and complete work together while honoring the identity, governance and safety controls that protect every Microsoft AI workload.

- **Dynamics 365 MCP Servers** *(public preview)*
  Dynamics 365 MCP servers for ERP, Sales, Customer Service and Business Central enhance agent intelligence by securely exposing data, actions and tools making them more context rich to execute processes autonomously.

- **Agent Store** *(generally available)*
  Features agents from Microsoft, partners, and customer organizations. It offers immersive and personalized discovery and engagement across Microsoft 365 Copilot endpoints, including Copilot Chat, recommending agents based on usage signals. End users can quickly find and utilize agents, conduct searches, and share with colleagues to boost collaboration and productivity, ultimately getting more done.

Pro-code dev tools and integrations

- **Microsoft 365 Agents Toolkit for Visual Studio** *(generally available)*
  Streamlines the development of enterprise-grade, agents by integrating AI tools like the Microsoft 365 Agents SDK and Azure AI Foundry, along with seamless project scaffolding, testing and publishing in Visual Studio. TypeSpec for Copilot is also now natively integrated in the toolkit.

- **Microsoft 365 Agents SDK** *(now generally available)*
  Enables building enterprise-grade, scalable, multichannel agents and offers flexibility for advanced needs,

customization with Azure AI Foundry, easy integration with Copilot Studio and Visual Studio, and the capability to publish across multiple platforms with over 10 messaging channels. The SDK also includes enhanced Power Platform connectors.

- **Microsoft 365 Copilot APIs** *(public preview)*
  A suite of enterprise-ready APIs that enable developers to build fast, context-aware, secure and compliant generative AI experiences with Microsoft 365 data – powered by search, retrieval, chat, and compliance capabilities. The Retrieval API is in preview.

- **Enhanced Power Platform connector SDK** *(preview)*
  Allows developers to build enhanced Power Platform connectors faster than before with the new SDK. These enhanced Power Platform connectors consume structured data in a structured format which is easy for agents to read, understand, and reason upon your enterprise data sources.

- **Bring your own model to Copilot Studio** *(preview)*
  Allows agents built in Microsoft Copilot Studio to access the Azure catalog of 1,900+ AI models, enabling makers to call industry-specific fine-tuned models for use, whether it is for scenario specific prompts or summarization in agents within your agents built in Copilot Studio. BYOM to prompts is in *public preview* & BYOM to answers/summarization is in *private preview*.

- **Microsoft 365 Copilot Tuning** *(limited EAP)*
  Copilot Tuning, available through an Early Access Program in June, lets qualifying organizations use their own data to train Copilot's LLM to power agents that can perform domain-specific tasks, including document summarization, Q&A generation and document generation. Agents typically rely on retrieval augmented generation (RAG) to supplement LLM responses in real time. As a result, they often provide generalized responses to tasks. With Copilot Tuning, the organization's data is directly embedded into the underlying model.

New features

- **GPT-5 model** *(public preview)*
  GPT-5 is a combination of models that enables your agent to understand your instructions and prompts and choose the best way for the agent to respond. For simple or routine prompts and instructions, the GPT-5 Chat model will be used, prioritizing speed and straightforward responses. For complex or more open-ended agent steps, the new GPT-5 Reasoning model will be used, applying deeper reasoning to plan and generate output. GPT-5 will be available as an option both for agent models (settings page) as well as for custom prompt tools. Read the announcement, learn more about the early release cycle environments, and agent model selection.

- **Deep reasoning** *(public preview)*
  Solve more complex business processes by integrating advanced models with agents. Break down complex problems into smaller, manageable steps and solve them through explicit logical reasoning. Unlike general-purpose language models, reasoning models are specifically trained to show their work and follow a more structured thought process. These models are particularly effective in scenarios that require structured problem-solving, such as market analysis, supply chain management, and legal contract review. They provide clear delineation between reasoning steps, making it easier to detect errors and understand the decision-making process.

- **Agent flows** *(generally available)*

Agent flows in Copilot Studio offer structured, rules-based workflows designed for repetitive business processes requiring consistency and control. Ideal for tasks like routing or compliance, they employ predefined sequences of actions to ensure predictable outcomes. These flows can operate independently or integrate as actions within existing agents, using prebuilt or custom connectors to enhance efficiency and standardize processes across organizations. By automating repeatable workflows, agent flows help businesses save time while maintaining high levels of accuracy and reliability.

- **Advanced approvals in agent flows** *(public preview)*
  Advanced approvals in agent flows, organizations can create multi-stage processes with distinct steps and decision-makers at each point. You can also build in conditional logic, allowing workflows to automatically adapt based on outcomes, criteria, or business rules—making complex approval chains more robust. '

- **Tools and prompts** *(generally available)*
  The Tools menu is a new centralized place where makers can create, manage, and assign reusable functionality across agents. Available inside the tools menu, the Prompts tool allows makers to easily create custom prompts inside Copilot Studio, either at the app level or within an agent or topic. Inside the tool, you'll find out-of-the-box templates to help you instruct the model effectively, or you can write the prompt from scratch.

- **Open web search** *(public preview)*
  Open web search gives your agents the ability to surface high-quality, real-time information from the web when configured knowledge sources fall short. This new capability helps your agents deliver relevant responses in broader, more open-ended scenarios like research, content creation, and competitive analysis—without requiring makers to anticipate every possible data source in advance. Connecting agents to publicly available information through open web search significantly expands their ability to provide accurate and up-to-date answers. Whether enhancing internal knowledge with the latest technological advancements or empowering end-users with richer, more flexible responses, this integration ensures your agents stay relevant and valuable. This can help to increase usage, drive higher satisfaction rates, and create greater impact.

- **Agent catalog** *(preview)*
  On the "Create" page in Copilot Studio, admins will now see available agents under the "Built by Microsoft" heading and can click on an agent to install it. By accessing the whole agent installation process inside Copilot Studio, it's faster and easier to create the agents you need, empowering teams to more efficiently deploy, manage, and scale properly configured agents across your organization and processes.

- **Other new features:**
  - Autonomous agents and generative orchestration support in Analytics
  - ROI analysis of Copilot Studio agents with Viva Insights
  - Copilot Studio support for customer managed keys
  - New Copilot connectors: Guru, GitLab, Asana, 15Five, Miro, Trello, Zendesk, Smartsheet, Seismic Content
  - Bring your own knowledge (BYOK) with Azure AI Search

Terminology

Recent naming updates

FROM	TO
Custom copilots	Agents

Copilot for M365	M365 Copilot
Extensions	Agents
Copilot agents	Agents
Business Chat	Copilot Chat
Azure AI Studio	Azure AI Foundry
Microsoft Graph connectors	Copilot connectors
Power Automate workflows	Agent flows
Agent Builder	Copilot Studio lite

Definitions for common terms

CONCEPT	DEFINITION
Agents	Agents are programs that use AI to automate and execute business processes, working alongside or on behalf of a person, team or organization.
Orchestrator	The critical component of an agent that oversees and synchronizes its operations, ensuring that various workflows, actions, and knowledge sources work together seamlessly.
Sydney	An orchestration system powering Microsoft 365 Copilot and Copilot Studio lite.
Samba	A managed orchestration within Copilot Studio for agents built in the full Copilot Studio experience.
Large language model	Advanced AI models trained on vast amounts of data to understand and generate human-like language, enabling tasks like text generation, translation, and summarization.
Managed models	Pre-built models integrated within products that cannot be trained or modified at the underlying level. While you cannot alter the core model, you can configure settings related to the output.
Custom models	A tailored AI model that can be trained, modified, and deployed according to user-defined parameters. You can create, manage, and optimize these models in Azure AI foundry.
Knowledge	Repositories of information that agents can access to provide accurate and relevant responses, such as databases, documents, or external APIs.
Grounding	Process of linking abstract knowledge in AI systems to specific, real-world content to increase the accuracy of AI agent comprehension.
Tenant graph grounding	Grounding with up-to-date, context-aware knowledge from Microsoft 365 and external data, offering built-in security and inheriting data access governance policies.

Web grounding	Dynamically generated responses based on the web as a knowledge source.
Actions	Steps that an agent can take in response to user input, such as calling an API, displaying a message, or performing a task.
Agent actions (i.e. "autonomous" actions)	AI-led orchestration for triggers, topics, agent flows, text & generative AI tools, Power Platform premium connectors and custom connectors to automate complex business processes. Not available in Copilot Studio lite.
Autonomous agent	An agent capable of performing tasks independently without continuous human intervention, often using AI to make decisions and adapt to new situations.
Conversational/interactive agent	An AI-powered agent designed to engage in natural language conversations with users, providing information, assistance, or performing tasks.
Agent flows	Fixed automation pathways, built in Copilot Studio, that don't rely on agent reasoning and orchestration at every step and follow a predefined sequence of actions.
Cloud flows	Flows built in Power Automate that are triggered either automatically, instantly or via a schedule.
Text & generative AI tools	Specialized tools that extend agents capabilities by teaching them to perform specific tasks, leveraging a combination of AI prompt engineering, model configuration, code execution, and knowledge retrieval.
Triggers	A mechanism that initiates specific actions or responses from an autonomous agent based on defined conditions or events. Event triggers allow agents to perform actions or call topics autonomously in response to events external to the agent, such as the creation of an item in SharePoint, the completion of a task in Planner etc., helping automate workflows.
Declarative agent	An agent that leverages the Microsoft 365 orchestrator, follows predefined rules and logic to perform tasks, often used for structured and predictable workflow.
Custom engine agent	An agent built with custom logic and capabilities tailored to specific business needs, often integrating with proprietary systems.

Agents & Agent Types

1. What is an agent?

Agents use AI to automate and execute business processes, working alongside or on behalf of a person, team, or organization. Makers can build agents that work on behalf of individuals, teams, or functions. These range from simple prompt-and-response agents to more advanced agents that complete tasks for a human without being prompted. Agents are available out-of-the-box with prebuilt, configurable templates, or they can be built from scratch. An agent consists of knowledge, tools, autonomous capabilities, orchestrator, and foundation models.

2. How do Copilot and agents work together?

Copilot is for every employee; agents are for every business process. Copilot is the UI for AI. While there could be millions of agents, each person only has one Copilot. The Copilot interface is the organizing layer that lets people interact with agents. The Copilot interface lets you retrieve information about your work, prompt agents to complete tasks, or see notifications from agents that are working on your behalf. Agents are extensions of Copilot. Makers can create numerous agents to make Copilot more robust and useful. Makers create these agents in Copilot Studio using low code or natural language. In Copilot Studio, you can write a prompt to build an agent, add data sources, and publish to your channel or channels (including SharePoint, WhatsApp, Slack, and more).

3. How are agents different from chatbots?

The term chatbot has been used in the industry for a long time. Agents are the next step in conversational AI technology and bring in a layer of generative AI with language models. These agents are also not just "chat" enabled – they now have autonomous capabilities.

4. What's the difference between pre-built agents and custom agents?

- **Prebuilt agents:** Pick from a variety of pre-built agents designed to automate common business tasks in the Agent Store in Copilot Chat or the Copilot Studio Agent Library. These agents can be published across various channels, including D365, Copilot Chat, Copilot Studio, or even on your own website and mobile applications.
  Examples: Store Operations, Awards & Recognition, Employee Self-Service

- **Templates:** Copilot Studio offers templates that help you quickly turn ideas into working agents – perfect for exploring new use cases or solving business challenges without starting from scratch.
  Examples: Safe travels, Team navigator, Benefit

5. What is the Agent Store?

Features prebuilt agents from Microsoft, partners (ISVs), and customer organizations. It offers immersive and personalized discovery and engagement across Microsoft 365 Copilot endpoints, including Copilot Chat, recommending agents based on usage signals. End users can quickly find and utilize agents, conduct searches, and share with colleagues to boost collaboration and productivity, ultimately getting more done. Easily select from an assortment of agents that span multiple business functions and deploy them immediately or customize them further by incorporating your organization's knowledge.

6. What is the Copilot Studio agent catalogue?

On the "Create" page in Copilot Studio, admins will now see available prebuilt agents under the "Built by Microsoft" heading and can click on an agent to install it. By accessing the whole agent installation process inside Copilot Studio, it's faster and easier to create the agents you need, empowering teams to more efficiently deploy, manage, and scale properly configured agents across your organization and processes.

7. What is the difference between 1st party and 3rd party agents?

1st party agents are created by Microsoft, or by customers using Microsoft tools. They can be found in the agent store or Copilot Studio agent catalog. 3rd party agents are created by partners/ISVs and are available for download from the Agent Store.

8. What are Dynamics 365 agents?

Learn more about them here

9. **What are SharePoint agents?**

Learn more about them here

10. **What are role-based agents for M365 Copilot?**

    Learn more about them here

11. **How are agents built?**

Copilot Studio is a low-code tool for creating, managing and connecting agents to Microsoft 365 Copilot, your website and apps.

- **Create an Agent**: Set up an agent to assist with product knowledge and order management on your website.
- **Ground in Data**: Use generative answers to enable multi-turn chat over real-time data from various sources, including your public website.
- **Design Critical Topics**: For areas like account management, use visual authoring or natural language to design specific conversational flows before proceeding to generative AI.
- **Add Actions**: Enable your agent to automate key business processes using 1500+ data connectors (e.g., SAP, Workday, Salesforce), custom connectors, agent flows, prompts and skills to handle complex queries dynamically.
- **Custom Development**: Use Azure models and services with Copilot Studio for a hybrid approach combining low-code and custom pro-code integration.
- **Publish**: Make your agent available on multiple channels (websites, Microsoft Teams, social apps, etc.) and enable escalation to tools like Dynamics 365, Genesys, and Salesforce for human assistance.
- **Monitor & Secure**: Review agent performance with the built-in analytics dashboard and secure/manage it with governance features from the central admin center.

12. **Can you build voice-enabled agents with Copilot Studio?**

Yes, Copilot Studio supports interactive voice response (IVR) capabilities, including speech and dual-tone multi-frequency (DTMF) input, context variables, call transfer, and speech and DTMF customization. Makers can also now add generative AI to an IVR system. Voice in Copilot Studio lets organizations deploy agents that users can speak to – this can reduce escalations to people and save time. It also lets users use the modality that is most convenient for them, to increase usage and value. Learn more about voice-enabled agents here.

13. **Can agents I build in Copilot Studio analyze images?**

    Yes, you can allow users of your agent to upload images, which your agent can then analyze and use to provide responses.

14. **What is a "task agent"?**

Task agents can do things like answer questions or complete basic tasks, like scheduling a meeting, sending an invite, closing a ticket, etc.

Copilot Studio overview

1. **Is Copilot Studio the same as Power Virtual Agents?**

Yes. Power Virtual Agents capabilities and features became part of Copilot Studio in 2023.

2. **Is Copilot Studio still part of the Microsoft Power Platform?**

Yes, Copilot Studio is built upon the foundations of Power Virtual Agents and the broader Microsoft Conversational AI ecosystem. Copilot Studio provides new ways to build your own agents with the latest generative AI and autonomous capabilities. Copilot Studio continues to live within the Power Platform, including its integrations across Power Apps, Power Pages, Power Automate etc. It enables makers to leverage the same Power Platform data connectors, Dataverse and the Power Platform admin center.

3. Is there more information about where data resides when using generative AI?
Please visit our Learn page to understand regional availability and data movement.

4. How does Copilot Studio approach responsible AI?
Generative AI within Copilot Studio is designed to align with Microsoft responsible AI principles, including fairness, reliability and safety, privacy and security, inclusiveness, transparency, and accountability. Learn more here.

5. How is Copilot Studio different from competitor offerings?
It is connected to the Microsoft ecosystem, including Microsoft Graph, Fabric, D365, M365, and Azure. It integrates and improves agents in Microsoft 365 so people using Microsoft 365 Copilot can use agents that help them be more productive. With the integration into Azure AI Search, you can use existing investments to power your agents. Copilot Studio also works well with the other low-code tools in Power Platform and benefits from Microsoft's robust security and governance capabilities.

Orchestration

1. What is Classic orchestration? Is "Classic Orchestration" topic-based?

Classic orchestration allows makers to trigger Topics in Copilot Studio, which allow them to define the conversation using the powerful authoring capabilities to define conversation using the available nodes, such as question, condition and message nodes. Makers provide example trigger phrases for each topic. Trigger phrases are used to generate a traditional natural language model which is then used to evaluate which topic to trigger when a user query is received. Agents using classic mode can fallback to available knowledge sources, using generative answers, when no suitable topics are available, with the agent searching across knowledge sources and generating an answer to a user query.

2. What is Generative orchestration?

With generative mode, makers can add knowledge, actions and topics – when more granular control is needed – and can combine one or more of these components to answer a user's query. When an action is selected, the agent can generate conversation to prompt the end user for missing inputs before the action is called. Once all knowledge, actions and topics have been called, the agent can generate a contextual response for the user.

Knowledge

1. What is Knowledge?
Knowledge allows your agents to provide richer, more contextual responses. By leveraging enterprise data, agents can reason over a broader set of information, delivering more accurate and relevant answers.

2. What knowledge sources are currently available in Copilot Studio?
Dataverse provides an end-to-end experience for discovering, adding, and managing knowledge sources. From custom data to Microsoft Graph, Dataverse to public websites, agents can be grounded in a wide variety of sources. Technical details can be found here: aka.ms/copilotstudioknowledge.

Copilot Studio supports many internal and external knowledge sources, providing a broad range of enterprise content for agents to access and reference:

- OneDrive, SharePoint, and Teams data
- Azure SQL, Azure AI Seach, Microsoft Fabric, Microsoft Graph, and Dataverse

- Unstructured data from Salesforce, ServiceNow, and Zendesk
- Structured data from platforms like Snowflake, Databricks, and SAP

3. Will agents connect to 3rd party technology?

Yes. Using advanced knowledge tuning in Copilot Studio, makers can add new sources of knowledge (including documents, 3rd party databases, etc.) to tailor the agent to various business scenarios. Makers can designate authoritative knowledge sources to match specific instructions ensuring the agent uses reliable sources of knowledge.

4. What are the new knowledge sources available in Copilot Studio (as of Build 2025)?

Knowledge from Microsoft Azure AI Search is generally available as of May 2025. Agents can now reference this data more effectively, whether the goal is analyzing sales pipeline trends, identifying churn risks, or supporting role-specific insights across business systems.

OneDrive files and folders, SharePoint Lists, and Teams chats and channels are all now supported. Outside this internal data, agents can now employ unstructured data from platforms like Salesforce, ServiceNow, and Zendesk, as well as structured data from platforms like Snowflake, Databricks, and SAP.

5. Do the same restrictions for knowledge sources exist? I believe it was 4 public sites, 4 private, 4 files.

The limits currently apply to knowledge sources when an agent is using classic orchestration. Agents using generative orchestration can use all knowledge sources that have been added to the agent. When more knowledge sources have been added than can be supported in a single query, the descriptions of each knowledge source are used to filter down to the most relevant knowledge sources before they are searched across.

Tools

1. What are Tools in Copilot Studio?

At Build 2025, Microsoft announced the public preview of Tools in Copilot studio. Tools is a one-stop shop for best-in-class features which enable extensibility for your Agents, including seamless integrations with internal and external systems. This results in significantly improving task quality and speed and generating substantial business value.

2. What defines a Tool in Copilot Studio?

There are three criteria for a Tool:

First and foremost, a Tool must enable an agent to do something in external system. Unlike simply reading data from an external source, a Tool must be able to facilitate actions such as updating or creating information on a third-party system. This ability to enact change is a fundamental characteristic of a Tool.

Secondly, a Tool should be versatile enough to be used across multiple agents. One of the key advantages of the Tools page is that it allows makers to view these capabilities at an environment level, promoting the reuse of tools where possible.

Lastly, Tools must be easy to create and integrate into an agent. Microsoft's goal is to ensure that makers can easily add tools to their agents. We will be demonstrating three types of tools later on, showcasing this experience.

3. Where can I find Tools in Copilot Studio?

Makers can access the new Tools tile on the left nav bar in Copilot Studio. Clicking on the tile will open the tools homepage where makers can select from six new tool types. To learn more about each of the different tool types see the next section.

4. What are the Tool types that are available?

- Prompts enable makers to create their own unique AI capabilities, to build intelligent agents, flow and apps.

- Agent Flows allow makers to automate sets of business-specific tasks.
- Custom Connectors and REST APIs provide makers with the ability to connect to third-party systems that aren't available as prebuilt connectors.
- Computer Use tool allows agents to browse the web and utilize reasoning capabilities to perform actions within a web browser.
- Model Context Protocol allows users to connect with existing knowledge servers and data sources directly within Copilot Studio.

5. How do prompts work?

Prompts provide structured instructions that guide large language models (LLMs) to perform specific tasks. This technique, known as instruction tuning, allows businesses to optimize AI-generated responses for more precise, relevant, and useful outputs. With Prompts, you can also ground models in your enterprise data—respecting runtime user permissions and data policies—so they can securely draw insights from internal resources. By clarifying directives, instruction tuning reduces ambiguity and enhances consistency across automated and agentic workflows.

Autonomy

1. Can makers build agents with autonomous capabilities today?

Yes, autonomous capabilities are now generally available.

2. How are the new autonomous capabilities different to what you can build as a custom agent today?

Instead of a user prompting an agent to do something every time they need it, they can design an agent to act automatically in response to events (e.g. when an email arrives, add the sender to the database). These actions can automate and manage intricate, complex business processes with greater independence and reduced human involvement.

3. Are these new autonomous agent capabilities included in Microsoft 365 Copilot?

Yes, you can technically deploy autonomous agents to Copilot. However, they logically will not function as prescribed since they do not use human chat-based triggers.

4. How do autonomous agents create dynamic plans and what is their thought process?

Each business process can have different paths. Agents create dynamic plans on the fly to handle tasks based on the set of guidelines provided by the maker. Their thought process lets users view key details, steps, and systems involved. This provides insight into why the agent chose a particular method, its reasoning, and the context used, along with detailed steps including variables and outputs, which are critical for debugging.

5. How does Microsoft differentiate event-based triggers in agents vs. agent flows?

An agent reacts to triggers based on its natural language instructions and language model. This means it can react differently depending on the situation and its behavior can be tweaked by altering its instructions.

Model Context Protocol

1. What is Model Context Protocol (MCP)?

MCP is a standard protocol designed to enhance the integration between AI apps and agents. It standardizes how agents communicate with each other, ensuring seamless and scalable process for developers and users within the Copilot Studio Ecosystem.

2. How does MCP benefit Copilot Studio users?

MCP streamlines the interaction between AI apps and agents, enabling faster deployment, smoother integration, and more reliable performance. It allows Copilot Studio to scale more effectively while delivering improved capabilities to end-users, all while reducing the complexity of managing multiple data sources and APIs.

3. What are the key features of MCP in Copilot Studio?

- **Interoperability:** Ensures smooth communication across agents and AI apps with standardized protocols.
- **Scalability:** Easily integrates new data sources and knowledge servers into the Copilot Studio environment. Actions and knowledge are dynamically added to the agent as functionality evolves.
- **Enhanced Customization:** Provides more flexibility for developers to create tailored AI interactions.

4. How will MCP impact the user experience in Copilot Studio?

MCP reduces the friction of integrating new data sources and knowledge servers, leading to smoother workflows and quicker time to value for users. It will enhance the overall user experience by ensuring that interactions between AI apps and agents are more observable, reliable, and easier to manage.

5. How do I get started with MCP in Copilot Studio?

You can get started by reviewing the official documentation for MCP integration in Copilot Studio at https://aka.ms/mcsmcp. It provides detailed guidance on capabilities and information on how to configure, deploy, and utilize MCP within your existing projects.

6. Is there any additional cost associated with using MCP in Copilot Studio?

Currently, MCP support is included as part of the Copilot Studio offering. Any changes or updates to pricing will be communicated as part of regular service announcements.

7. Are there any prerequisites for using MCP in Copilot Studio?

You will also need to have Generative orchestration enabled for your agent.

8. How does MCP support security and data privacy?

MCP servers are made available to Copilot Studio using connector infrastructure. This means they can employ enterprise security and governance controls such as Virtual Network integration, Data Loss Prevention controls, multiple authentication methods.

9. Where can I find more detailed documentation on MCP support in Copilot Studio?

Comprehensive documentation on MCP is available here, where you can access integration guides, best practices, and troubleshooting tips.

10. What are the available resources on MCP support in Copilot Studio?

- Announcement: https://aka.ms/mcs-mcp
- Extend your agent with Model Context Protocol
- Connect to an existing Model Context Protocol (MCP) server
- Copilot Studio MCP Catalog

Agent Flows in Copilot Studio

1. When were agent flows announced?

Agent flows in Copilot Studio were announced 25 March 2025. Agent flows in Copilot Studio become generally available on 31 March 2025.

2. Is there still a place for Power Automate?

Yes! Agent flows are additive to your agents! Power Automate remains a key part of the Power Platform as Microsoft's end-to-end hyperautomation platform. Power Automate will continue to be *the destination* for complex enterprise automation infused with artificial intelligence, delivered through desktop flows (RPA) for UI automation, cloud flows for API automation, and process mining for continuous improvement.

3. How are agent flows different than topics?

Both topics and agent flows are deterministic pathways for automation. While topics are optimized for managing conversational flows and can be enhanced with actions for automation behind the scenes of the conversation, agent flows are optimized for business process automation and have more comprehensive automation abilities for non-conversational processes

4. Can an agent flows be used across multiple agents?

Yes, once you build an agent flow, you can add that agent flow as an action to any of your agents, allowing you to reuse common tasks that are applicable across departmental scenarios and scale them across your organization.

5. Can I add AI powered actions to agent flows?

Yes. You can add intelligent actions to both your agent and your agent flows for document processing, decision making, simplification of complex steps, and more. This allows you to infuse intelligence into your processes at every level from agent to flow, striking the optimal balance of autonomy, intelligence, and speed.

6. What is the difference between agent flows in MCS, and cloud flows in Power Automate?

For Power Automate customers who are experienced in building flows in Power Automate, agent flows provide similar maker experiences designed to expedite the work of professional developers and empower business users to engage in automation.

Agent flows, however, are unique in that they are…

- Optimized for use in Copilot Studio – natively integrated to offer seamless maker experiences that simplify and accelerate agent development.
- Billed directly through Copilot Studio based on consumption without requiring individual licensing – helping organizations seamlessly scale process transformation enterprise wide in one solution.
- Equipped with advanced new features exclusive to Copilot Studio like recently announced advanced approvals for complex workflow management.

7. "When do I use agent flows in Copilot Studio, and when do I use Power Automate?"

These products are individually valuable and designed to work together to help you achieve your most strategic business outcomes through automation.

- **Copilot Studio:** If you are transforming your business process agents and AI, Copilot studio and agent flows are designed to provide an integrated experience and business model to enable this transformation.
- **Power Automate:** If you are an automation team that wants to perform automation to reduce costs and repetitive work by automating on-premises and legacy systems without APIs, start with Power Automate.

8. Can I migrate my existing cloud flows in Power Automate to Copilot Studio as agent flows?

Yes. You can migrate existing solution-based cloud flows to agent flows. You can simply go to the flow detail page in Power Automate and edit the plan for this flow to "Copilot Studio", after which they will be visible under the "Flows" tab in Copilot Studio and run on the Copilot Studio meter.

9. Will my Power Automate licenses cover agent flows?

Agent flows are billed in Copilot Studio based on usage and are not included in Power Automate licensing.

SharePoint

1. **With these SharePoint improvements, do organizations need M365 Copilot in place before it can be used?**

Find answers to licensing questions in the Copilot Studio and Agents Licensing FAQ.

2. **Can you please Clarify if a SharePoint agent will have access to the semantic index created for the tenant?**

Agents in SharePoint use the semantic index for M365 Copilot, so they do support semantic index.

3. **Is generative answers in Copilot Studio when reasoning over SharePoint (Not M365 Copilot agents), will it use Semantic index like what agents are doing?**

You will have the ability to toggle on Semantic index for SharePoint. Enabling Semantic index will cost extra. This can be enabled by turning on the "enhanced search results" toggle.

4. **Can I choose my own LLM models? If so, then how?**

Yes, through an Azure AI integration

5. **For the lexicon-based SharePoint search support for up to 512 MB files, does it need M365 Copilot in place before I can use it in Copilot Studio?**

No, lexical grounding of SharePoint only requires Copilot Studio capacity.

6. **Will there be any vectorization within Copilot studio or integration to a vector DB?**

Different Knowledge Sources will offer vectorization. Organizations can also ground against 1st and 3rd party vector DB.

7. **How is Microsoft improving the quality of answers from SharePoint?**

Microsoft is updating the backend integration with graph data entities to be able to improve search results. but as mentioned previously, the quality of the search results is license dependent.

Azure Integrations

Note: See the Azure AI Foundry FAQ for more information

1. **What is "BYOM"?**

Bring Your Own Model from Azure AI Foundry enables makers to use the 1900+ Azure AI Foundry Models in their agents built with Microsoft Copilot Studio, enabling the use of industry-specific & fine-tuned models, whether it is for scenario specific prompts or summarization in agents built in Copilot Studio. BYOM to prompts is in public preview & BYOM to answers/summarization is in private preview.

2. **What is Bring your own Knowledge?**

Microsoft also announced the GA of Bring your own Knowledge from Azure AI Search to Copilot Studio. This will allow you to use the vectorized indices built using Azure AI Search as a source of knowledge for custom RAG operations in your agents. It's generally available.

3. **Can agents built with Copilot Studio interact with agents built with Azure AI Foundry?**

Yes, agent orchestration is available in preview. This multi-agent solution allows Copilot Studio agents to talk to other agents built in Copilot Studio, Azure AI Foundry Agents, Fabric or Microsoft 365 Agents SDK, exchanging data, collaborating on tasks, and distributing work, enabling cross-platform orchestration.

M365 Copilot Extensibility

Note: See the M365 Copilot FAQ agent for more information

1. **What are the ways to build or extend an agent for Microsoft 365 Copilot, and when should I use which approach?**

Microsoft offers a **spectrum of tools** for creating or integrating agents into Copilot, suitable for different skill sets and needs:

- **Copilot Studio & Copilot Studio lite (Low-Code/No-Code):** Copilot Studio lite is a built-in tool in Microsoft 365 Copilot and Copilot Studio is a SaaS tool for business users and makers. Both provide a friendly interface to create *agents*. You can start by simply describing in natural language what the agent should do (its instructions/behavior). You can then refine it by adding pre-built **tools or connectors** (for example, allow the agent to call an internal API, or use a knowledge base) and setting its knowledge sources or triggers. Copilot Studio is great for **quickly building FAQ agents, workflow helpers, or other agents** without writing code. Use this when you need a solution fast or when the person building it isn't a developer. It's "start simple" – e.g., create an HR policy Q&A agent or a project onboarding helper in a morning.

- **Azure AI Foundry (Pro-Code for Custom Models and AI services):** For organizations that want to use more advanced techniques, such as custom AI models or complex logic, Azure AI offers Azure AI Foundry and related tools. Copilot Studio and Azure AI Foundry are tightly integrated, for example makers in **Copilot Studio can use models from Azure AI Foundry or knowledge with Azure AI Search** to power low-code agents. Developers can also build sophisticated AI services (using Azure OpenAI Service, cognitive services, or other ML models) and then use the **M365 Agents SDK** to integrate these into Copilot. This approach is suitable when you have data scientists or developers building bespoke models or when the solution needs deep customization beyond what a declarative agent can do. Essentially, you build your AI on Azure (leveraging its full flexibility – different model choices, fine-tuning, etc.), then connect it to Copilot Chat with the **M365 Agents SDK** so it appears as an agent available to users. This is more effort, but yields powerful custom agents (for example, an agent that plans complex operations, or uses proprietary algorithms).

- **Visual Studio/Visual Studio Code via Microsoft 365 Agents Toolkit (Pro-code for building declarative and custom engine agents):** The Microsoft 365 Agents Toolkit is an extension in Visual Studio and Visual Studio Code designed for organizations with code-first developers. It facilitates the creation of agents using either a simple declarative approach or custom engine agents that incorporate custom logic and models from Azure AI Foundry and other providers by utilizing the Microsoft 365 Agents SDK. Additionally, the toolkit enables developers to create applications for the Microsoft 365 ecosystem, including agents for Microsoft 365 Copilot and Teams.

- **Microsoft 365 Agents SDK (Integration of Existing Agents):** The SDK is also the route to take if you already have an agent or service built on other non-Microsoft service and want to bring it to Microsoft 365 Copilot. It's a pro-code approach as well, but focused on *integration* rather than building new logic. Use this if your main challenge is "I have something running outside Copilot, and I want it in Copilot." Developers are encouraged to use the Microsoft 365 Agents Toolkit along with the SDK but it can be used separately.

In practice, these approaches can complement each other. For example, a team might **start with Copilot Studio** to prototype an agent using out-of-the-box connectors and basic prompts (this requires no code). If they hit limitations or want to add a custom model, a developer can then step in to use the **Azure AI Foundry + Copilot Studio** to enhance that agent with more sophisticated capabilities or integrate the Azure AI Foundry agent with the Microsoft 365 Agents SDK to bring it to Microsoft 365 Copilot. Copilot's platform is open-ended: from simple point-and-click agent creation to full-code solutions. The key is to pick the approach that matches your team's skills and the complexity of the use case.

Tip: It often makes sense to *start simple and iterate*. Many organizations begin with a minimal viable agent in Copilot Studio to address a single use-case (fast deployment), and then as value is proven, they scale up to more complex integrations or additional tools for that agent.

Approach	**Audience**	**Interface**	**Use Case**	**Customization Level**	**Integration with M365 Copilot**	**Best For**
Copilot Studio & Copilot Studio lite	Business users, makers	Low-code/no-code UI in M365 Copilot or standalone Copilot Studio	FAQ bots, onboarding helpers, workflow agents	Low to moderate (via connectors, HTTP requests, plugins)	Native (via Copilot Studio lite and Teams channel)	Fast prototyping, non-dev teams, internal tools
Azure AI Foundry	Data scientists, developers	Azure portal, SDKs, APIs	Custom AI models, advanced logic, proprietary algorithms	High (custom models, fine-tuning, Azure OpenAI, Cognitive Services)	Via M365 Agents SDK or as a backend to Copilot Studio agents	Deep AI customization, model-driven agents
M365 Agents Toolkit (VS/VS Code)	Developers	Pro-code IDE (Visual Studio / VS Code)	Declarative or custom engine agents, SDK-based apps	High (code-first, SDK integration, plugin logic)	Full support via SDK and toolkit	Building scalable, production-grade agents
M365 Agents SDK	Developers	SDK (IDE agnostic)	Custom engine agents & wrapping existing agents/services for M365 Copilot	High (integration-focused, not logic-building)	Direct integration into M365 Copilot	Building new & reusing existing bots, APIs, or services

Copilot Studio lite

1. **Where can I find Copilot Studio lite documentation?**

See: Use Copilot Studio lite to Build Agents | Microsoft Learn

2. **What is the Copilot Studio lite experience?**

The lite experience of Copilot Studio in Copilot Chat allows users to quickly create simple, conversational agents tailored to their work needs—no coding or full Copilot Studio required. It's ideal for internal FAQs, onboarding, or team-specific guidance. Agents are managed using Microsoft 365 admin tools for sharing, visibility, and lifecycle control.

3. **How should I choose between the lite and full Copilot Studio experiences?**
   Microsoft developed a decision framework to guide organizations based on:
   - **Audience** – Who will use the agent?
   - **Deployment scope** – How broadly will it be shared?
   - **Functionality** – What tasks will it perform?
   - **Governance needs** – Is lifecycle management required?

   A new article outlines this framework and governance principles in detail.

4. **If the lite experience in Copilot Studio meets my needs, why would I use the full experience?**

The lite experience is scoped for simpler use cases. The full experience unlocks richer functionality, deeper control, and governance capabilities—ideal for complex, scalable, enterprise-grade agent solutions.

5. **Is Copilot Studio part of Microsoft 365 Copilot?**

Yes. Copilot Studio is part of the Microsoft 365 Copilot ecosystem. Most agent-building scenarios are included in the $30 per user/month license.

6. **Why is Copilot Studio retiring the "agent builder" term?**
   - The term caused confusion, often implying a separate product.
   - It was limiting—both lite and full experiences involve building agents.
   - Consolidating under "Copilot Studio" clarifies that all users build agents within the same product.

7. **What changes are coming to Copilot Studio to reflect this is a unified product?**

(Confidential – not for external sharing)

- A more intuitive lite experience for quick agent creation.
- A seamless path to graduate agents from lite to full for deeper customization.

8. **When will references to "agent builder" be removed from Copilot Studio documentation?**

Updates are rolling out across marketing materials and Microsoft Learn starting early September, with completion expected by end of October.

9. **How does someone create a new agent using the lite experience?**

In Copilot Chat, click "Create agent" and describe what you want the agent to do using natural language. Copilot will generate the agent for you. You can also start with templates like Career Coach or Idea Coach. Add knowledge sources (e.g., SharePoint, websites, files), and share the agent with a group or the entire company via Teams, Outlook, or other Microsoft 365 experiences. You can further customize agents in the full Copilot Studio editor.

10. **What are the required fields for building an agent in Copilot Chat?**

See: Use Copilot Studio lite to Build Agents | Microsoft Learn

11. **Where can I use agents created with the lite experience?**

Agents created with lite can be used directly in Copilot Chat by chatting or @mentioning them. They can also be shared via email or Teams links.

12. **Can you share an example of an agent you would create in SharePoint or Copilot Chat and how it would be useful for an employee?**

A sales team preparing for a customer engagement could work with an agent that is an expert on that particular customer's situation, or a finance team managing quarterly budget planning could work with an agent that is an expert on the company's budget policies to forecast information.

13. **Can you provide examples of how different roles within an organization can benefit from agents?**

- **Marketing lead** – create a product launch assistant to enable a large, cross-functional team to quickly filter and reason over the various marketing documents to understand key dates, deliverables, and KPIs *(content creation, data-driven insights, time efficiencies)*
- **Sales lead** – create a conversation companion, where the agent uses customer details and interactions to suggest pertinent questions and content, optimizing conversations and engagement *(time efficiency, increase customer face time, real time assistance)*
- **HR coordinator** - creates an onboarding assistant that guides new employees through company policies and provides them with instant, relevant answers *(streamline information, reduce tasks and redundancy)*
- **HR hiring** – upload resumes to a SharePoint site and receive ratings on how they match up to the job criteria *(reduce task redundancy, support advanced analysis and strategic decision making)*
- **Engineering manager** – create a field incident report agent to enable engineers to analyze the types of issues coming in from the field and help provide analysis on what product issues should be prioritized *(data-driven insights)*
- **Sales** – create a customer story agent enabling a user to filter through the case studies on unique parameters such as customer profile and challenges *(time efficiencies, increased sales productivity and efficiency, time for deeper personalization)*

14. How does the lite experience interact with Microsoft 365 Copilot?

Copilot Studio lite extends Microsoft 365 Copilot by grounding data from sources like SharePoint, public websites, and specific documents. These agents are designed for specific purposes, teams, or projects to enhance collaboration and knowledge sharing. Like other Microsoft apps, they can be shared via a link.

15. Where is Copilot Studio lite available, and what languages does it support?

See: Copilot Studio lite regional availability and language support | Microsoft Learn

16. How much will it cost for employees without a M365 Copilot license to use agents?

Find answers to licensing questions in the Copilot Studio and Agents Licensing FAQ.

17. When will I be able to integrate a custom engine agent into M365 Copilot?

This capability is now generally available.

18. How do instruction limits work?

Instructions guide the agent's behavior and are limited to 8,000 characters. They function like system prompts and can include task definitions, tone, and fallback behaviors. Best practices include keeping them clear, specific, and concise.

19. What types of information can be added to an agent's knowledge base, and how do permissions work?

See: Use Copilot Studio lite to Build Agents | Microsoft Learn

Permissions are enforced end-to-end—agents only show content users can already access in Microsoft 365.

- When a user interacts with an agent, the agent will only surface content from knowledge sources that the user has permission to access.
- If a document/site/email is added to an agent's knowledge base but the end user does not have access to that document, the agent will not use or reference that content in its responses.
- This ensures that agents do not leak or expose information beyond what users are already authorized to see.

Note that if you **upload** a document during agent setup, it becomes accessible to anyone using that agent. To keep Microsoft 365 permission controls when sharing agents, select documents from the knowledge drop-down rather than uploading them.

20. What are the limitations for public websites?

See: Use Copilot Studio lite to Build Agents | Microsoft Learn

21. What file types are supported from SharePoint?

See: Use Copilot Studio lite to Build Agents | Microsoft Learn

22. How are knowledge sources refreshed?

Unless a static file is manually uploaded to the agent, knowledge sources are not statically ingested or archived at the time of configuration—they are dynamically referenced at runtime. This means that when a user interacts with an agent, the agent retrieves the most current version of the content from the linked source (e.g., SharePoint, OneDrive, or public websites).

If the underlying document or site is updated, the agent will reflect those changes in future responses. This dynamic grounding ensures that agents always use the latest available information, provided the user has access to the content.

However, this also means:

- If a document is deleted or permissions change, the agent may no longer be able to retrieve it.
- There is no versioning or snapshotting of the knowledge source at the time of agent creation.

23. How can users share agents created with the lite experience?

Agents can be shared with individuals or security groups via the Copilot Chat interface. Admins can manage sharing in the Microsoft 365 Admin Center. Bulk sharing is not supported.

24. Can agents be shared using Microsoft 365 groups?

Not currently. Sharing is limited to individuals, the entire organization, or security groups.

25. Can users be allowed to create agents but not share them?

Admins can control who can build and use agents via the Microsoft 365 Admin Center (Copilot > Settings > Extensions). However, sharing cannot be disabled independently.

26. Can you block the ability to create agents?

Yes, but this also blocks the ability to use agents.

27. Can you allow some users to create agents and others to only use them?

No. If a user has access to agents, they can both create and use them.

28. What governance controls are available?

- Build/use agents: Admins can control who can build and use agents in Copilot Chat by configuring settings in the Microsoft 365 admin center. Navigate to Copilot > Settings > Extensions.
- Content Permission Policies: Agents in Copilot Chat adhere to the same underlying permissions model used across Microsoft 365 services. Admins can apply content permission policies to ensure users have access to appropriate content.
- Pay-as-You-Go Controls: While setting a maximum spend cap for groups of users is not currently supported, admins can set consumption alerts for each environment to monitor and manage spend levels.

- Agent Availability: Admins can manage the availability of agents in the store tenant-wide by viewing available, deployed, or blocked apps, making agents available to specific users or groups, blocking or unblocking agents for the entire organization, and deploying or removing agents for the entire organization or specific users or groups.
- Review Process: User-created agents built using Copilot Studio and submitted to IT for approval will appear under 'Requested Apps' within the Integrated Apps section of the Microsoft 365 admin center.
- Risky activities: By leveraging Purview's Insider Risk Management, admins can detect risky user activities. They can also detect prompts containing non-compliant content with Communication Compliance.
- Data retention, data sensitivity, and eDiscovery: Purview's controls are built-in so data controls apply, such data lifecycle management, Data Security Posture Management (DSPM), and eDiscovery.

29. Can admins review and publish agents to the tenant catalog?

Yes, via the Integrated Apps section of the Microsoft 365 Admin Center.

30. Can the management of agents change over time?

This is not currently supported in lite.

31. How does data flow and residency work in the lite experience, and what data does it store?

Copilot Studio lite stores agent metadata within Microsoft-managed infrastructure aligned to your organization's Microsoft 365 environment geography. It uses Microsoft 365 and Copilot Studio services, inheriting the same compliance, security, and data residency commitments. Specifically:

- **Agent metadata:** Name, description, and instructions, are stored in Microsoft-managed infrastructure aligned to the organization's Microsoft 365 geography.
- **Knowledge sources:** SharePoint content and documents added as part of the agent's knowledge are governed by the tenant's existing permissions; data remains in its original location.
- **Chat history:** Not stored in the lite experience—chat interactions are handled by Microsoft 365 Copilot in accordance with its data handling policies.

32. What product terms apply to users as they build and use Copilot Studio lite agents?

Copilot Studio lite is a feature of Copilot Studio and it operates as an extension of Copilot Chat. Because it is part of Copilot Chat, users agree to both the Copilot Studio and Copilot Chat terms when they use the lite experience.

33. Why can't agents be switched from Declarative Agent (DA) to Custom Engine Agent (CEA)?

This is a known limitation. Microsoft is exploring improvements.

34. Can agents built in Copilot Studio be integrated into Copilot Chat?

Yes, this is now generally available.

35. Can agents built with the lite experience be extended with Azure AI Foundry?

No. Only agents built at copilotstudio.microsoft.com can.

Bring your own agent or model

36. **My organization's AI model is very domain-specific (fine-tuned on our data). Can that be used with Copilot?**

Absolutely. There are two main ways to leverage a domain-specific model with Copilot:

1. **Integrate the Model as a Custom Agent:** If you have a model (say fine-tuned on your proprietary data or an AI hosted in Azure/GCP) that gives unique results, you can integrate it via the **Microsoft 365 Agents SDK**. If the model is hosted on Azure AI Foundry you can also use it **directly from Copilot Studio.** Essentially, your model stays where it is (with all its special training intact); your Microsoft 365 Copilot agent will call it. This corresponds to creating a custom agent in Copilot whose function is to query your model. The model's outputs are then returned to the user through Copilot Chat via your agent. It's effective when your model is a key differentiator (e.g., it "talks in your company's voice" or has expert knowledge). Copilot is model-agnostic in this sense – it can work with **your fine-tuned model via agents you create** just as well as with Microsoft's base models.

2. **Fine-Tuning Microsoft's Copilot (Preview feature):** Microsoft has introduced the ability to fine-tune the Copilot's underlying models with tenant data for large organizations. As of now, fine-tuning is in **private preview for tenants with 5k+ seats**. This means selected organizations can have Microsoft's AI model adapt to their corporate data/style, after which Copilot (and any agents running on it) will inherently respond in.

37. **I've already built my own agent solution outside of the Microsoft 365 ecosystem. Why should I integrate it with Microsoft 365 Copilot instead of using it on its own?**

Integrating your solution with Copilot adds incremental value rather than replacing what you've built. Here's why it's **"better together"**:

- **Single Pane of Glass for Users:** Your users likely spend much of their day in Microsoft 365 (Copilot, Teams, Outlook, etc.). By surfacing your agent in Copilot, users can invoke it right in their flow of work without switching contexts. This drives higher utilization and satisfaction, since the agent becomes available whenever and wherever they're already working.

- **Multi-Agent Capabilities:** Copilot's interface is designed for handling multiple agents. Users can easily **switch between agents mid-conversation** and have Copilot coordinate among them. For instance, a user could get an answer from your custom agent and then ask Copilot to summarize or further drill down using another tool – all in one chat thread. This kind of rich hand-off and collaboration is not typically possible when your agent exists in isolation.

- **End-to-End Productivity Vision:** Copilot is part of Microsoft's broader AI vision – integrating your solution means it becomes part of an **end-to-end AI workflow** for users. For example, a sales employee might use Copilot to draft an email, then consult your custom agent (through Copilot) for a compliance check, then continue – all steps working in concert. Without integration, that flow would be broken across separate tools. Copilot provides the glue that can bind separate AI capabilities into a coherent workflow.

- **No Need to Abandon Your Investment:** Integration doesn't mean replacement. Think of it as *amplifying* your agent's reach and abilities, not starting over. You keep your intellectual property and unique functionality, but leverage Microsoft's UI and ecosystem to make it more accessible and powerful. In short, your homegrown agent can **coexist with Copilot, benefiting from Copilot's UI and ecosystem while retaining your agent's unique strengths**.

In summary, using Copilot as the front-end for an existing solution can enhance its adoption and utility while reducing the friction by integrating with a platform that users are already familiar with – Copilot.

38. Can I bring my existing “homegrown” agent or model into Copilot without rebuilding it from scratch?

Yes – Microsoft has designed Copilot’s extensibility so that you can **“bring your own agent”** rather than starting over. There are a couple of integration approaches depending on how your agent is built:

- **Using the M365 Agents SDK (Full Integration):** If you have a custom AI application (whether running on Azure, another cloud, or on-premises), you can use the Microsoft 365 **Agents SDK** to integrate it into Copilot Chat **as a native agent**. This SDK provides libraries and tools in languages like C#, JavaScript, and Python to connect your agent’s logic and APIs into the Copilot environment. Essentially, you wrap your existing agent so that Copilot can invoke it. *Your core code and model remain the same* – the SDK is just the connector. This method gives you full control over your agent’s branding, logic, and data access within Copilot. From the user’s perspective, your agent will appear as any other agent within Copilot (with whatever name and icon you choose), and when invoked it will execute your existing logic.

- **Lightweight Integration via Copilot Studio (API Wrapping):** If you prefer not to use a full SDK or your agent already exposes a RESTful API, Copilot Studio allows you to **register external APIs as actions/tools** that Copilot agents can call. In practice, you could ”wrap” your homegrown agent behind a REST API and then use Copilot Studio’s low-code interface to create a new declarative agent that simply calls your API whenever needed. This approach means you **don’t need to rebuild the underlying agent at all** – you’re just creating a thin wrapper so Copilot can talk to it.

- **Connecting Copilot Studio agents with other agents**: Copilot Studio also allows you to connect your Copilot Studio agent with other agents, dedicated to handling steps of your workflow. Currently, Copilot Studio supports connecting to other Copilot Studio agents. Support for connecting to Azure AI Foundry and SDK-based agents is on the roadmap. Copilot Studio also supports the *Model Context Protocol (MCP)* which can also be used to connect an external agent service to Copilot as a tool, again with minimal recoding. In short, if your agent can be called via an endpoint, Copilot can be set up to call it.

Whichever route, the guiding principle is that you **reuse your existing agent’s capabilities**. You are not throwing away the work you’ve done – you’re *bringing it directly to Copilot or integrating* it with other agents and tools. This preserves your investment and even extends its value (by plugging it into new interfaces and data sources).

Finally, note that integration can be phased. Some organizations might start by integrating a subset of their agent’s functionality as a proof of concept (via a simple API call) and later do a deeper SDK integration for full functionality and finer control. The flexibility is there to choose the path that best fits your technical constraints and timeline.

39. My organization already has an agent or AI model, what is the guidance to bring it to Microsoft 365 Copilot?

Organizations vary in how they want to combine their solutions with Copilot. Below are common scenarios and the recommended approach for each:

Scenario	Guidance	Complexity
My organization has a pro-code, homegrown AI agent (e.g., built on Azure AI Foundry, or non-Microsoft) and wants it available in Copilot’s UI.	If your organization needs Foundry tools (RAG, Code Interpreter, multi-modal) at run-time, then keep Foundry (or 3rd party) as the “brains”; M365 Agents SDK only surfaces it into Copilot Chat as a native agent. This preserves full functionality and control.	Medium to High. Organizations will have to do low to high refactoring depending on your needs.

	If an organization is open to full refactor, re-implement logic directly in the M365 Agents SDK using SK/LangChain.	
My organization has a homegrown AI agent but wants to limit which parts of it are exposed in Copilot.	If full integration is not desired, your organization can a) expose an API endpoint from the agent and call it with custom logic in a new agent via the M365 Agents SDK b) expose an API endpoint from the agent and call it via a new Copilot Studio agent (via tools/REST API) or via the M365 Agents Toolkit for declarative agents.	Low to Medium. Direct API call
My organization's custom agent has a strong internal brand – we want to keep its name/identity while using Copilot.	Copilot allows **branding customization** for integrated agents. Coexist by surfacing the solution as a Copilot agent with a custom name and logo. (In Copilot Studio, you can set the agent's appearance to use your branding.) The agent runs within Copilot but retains its distinct identity.	Low
I want to use my own AI model because it reflects my industry or company knowledge ("it talks like us").	Two approaches: (a) **Fine-tune** Copilot's base model with your organization's data – available in private preview for >5k seat tenants (GA expected post-summer); or (b) use Copilot Studio/Azure AI Foundry's Model Catalog to integrate the custom model into Copilot for <5k seat organizations. Either way, the goal is to have Copilot respond in the organization's own style and context.	Medium to High

Each scenario above shows that **Copilot + Agents** is flexible: organizations can either build new agents, bring existing ones, or integrate specific AI models. The general advice is to **use the native SDK integration when possible** (for full functionality and UI richness), and reserve the lighter or partial methods for cases where full integration isn't feasible. Microsoft's strategy is to enable *coexistence*, not forced replacement: whatever your organization has already invested in AI can likely be incorporated into the Copilot ecosystem in some form

40. What are the most common objections and concerns to building and connecting agents to M365 Copilot?

- **"This sounds complex – I don't have resources to do another AI project."**

  Response: Emphasize that integration can be very lightweight to start. With Copilot Studio's no-code tools, a basic integration can be done quickly by a power user (not every solution requires a full dev team). Also, much of the heavy lifting (security, UI, scaling) is handled by Copilot's platform – your team doesn't need to build those pieces. Start small (maybe integrate one capability of your agent) and scale up. Microsoft and partners also provide guidance, sample code, and even a decision tree to help choose the simplest path. In short, the initial step can be quick and low-effort, delivering value without a massive project.

- **"Is it secure and compliant to connect our agent? What about sensitive data?"**

  Response: Copilot and Microsoft 365 are built with enterprise-grade security. Any agent integrated into Copilot can enforce the same Data Loss Prevention (DLP) policies and sensitivity labels as the rest of M365. Admins have full visibility and control – they can govern which agents are available, to whom, and what data they can access. Copilot Studio agents interactions grounded on Dataverse can be logged and audited through Microsoft Purview. In practice, your agent, when running via Copilot, is subject to your organization's compliance rules (no less secure than any other app in M365). Furthermore, if your agent needs to handle highly sensitive data internally, you can architect the integration such that only minimal information passes through Copilot (e.g., the agent can receive a query, do a secure lookup in your system, and return an answer – without exposing raw data). This way, no sensitive documents need to be duplicated into Copilot; your agent keeps them in its original repository. The bottom line: integration doesn't compromise security – it extends your existing security framework to the agent within Copilot underscoring the need for secure agent design from your organization.

- **"Will the integrated solution scale for our whole organization? We have thousands of users."**

  Response: Yes, assuming your agent's backend is also hosted to scale, which for example Azure can support. When you integrate with Copilot, you inherit Microsoft's cloud scale, in this case to access your agent's front-end. When you bring an agent to M365 Copilot you control the backend and its resources. For agents built directly on Copilot (Copilot Studio agents / declarative agents built with the M365 Agents Toolkit) they run on Microsoft's Azure infrastructure, built to handle enterprise workloads. Whether 100 users or 100,000 users start using the agent, the backend can scale accordingly. In either case, you benefit from scale reach as this drastically reduces rollout friction. If your agent today is limited to a subset of users due to deployment constraints, putting it in Copilot can actually increase its reach with minimal effort. It's akin to publishing an app to a store that everyone already has access to.

- **"Will using an external agent via Copilot be slow or laggy? And will it slow down our deployment timelines?"**

  Response: Performance: Copilot is optimized for fast interactive use, and that applies to integrated agents too. In many cases, the latency added by routing through Copilot is negligible). Deployment speed: As mentioned, building integration can be done quickly for a basic version. The seller guide's mantra is "go from idea to working agent in minutes-hours, not weeks". Once integrated, rolling it out through the tenant is faster than a standalone solution because it's just an update to Copilot's available agents – no separate software for IT to deploy. So both in development and in end-user experience, using Copilot + agent is designed to be fast.

- **"We invested in our own AI to differentiate against the field – why align with Microsoft's Copilot strategy?"**

  Response: By integrating, you're not giving up your differentiation – you're amplifying it. Your unique AI continues to exist and provide value, now with a broader audience and enriched by Microsoft's ecosystem. Strategically, this alignment ensures your solution stays current with the latest AI advancements. Microsoft is investing billions in Copilot and related AI; by plugging in, you ride that wave (as opposed to trying to keep up alone). For example, consider user expectations: as Copilot becomes a common interface for work tasks, having your AI present there keeps your organization at the cutting edge of user experience. It shows you are integrating with the best and not creating information silos. Finally, Microsoft's vision is not to replace all agents with Copilot, but to create an ecosystem ("the UI for AI"). In that vision, your solution has a first-class place at the table.

- **Agent might not have user's chat history or context when called. "If Copilot calls (@) our agent, will it know what the user already asked?"**

Response: Copilot can pass along relevant context to your agent. Additionally, you can implement multi-turn memory or session state in your agent. For example, your agent can maintain its own conversation memory via an ID, or Copilot's call can include conversation history snippets. Using retrieval (RAG) techniques to fetch past interactions is another way to give your agent context of prior chat turns. In practice, many integrations use a combination of Copilot-provided context + the agent's internal memory plugin to preserve continuity.

- **My organization's agent output might get altered by Copilot (reformatted or reprocessed). "We have careful wording; will Copilot change it?"**

  Response: By default, Copilot will present the agent's answer as-is. If using a declarative agent (calling external agent via API), there is a risk it could run the output through GPT again. To prevent any unwanted reprocessing (which could be problematic for legal/sensitive content), you can enforce that the agent's response is final. Use **DLP policies in your backend** to block unwanted content and configure the agent instructions, disabling any fallback to a generalized response. If using a custom engine agent directly, Copilot will present the agent's answer as-is.

  Uploading files or large data to our agent via Copilot is clunky. "Users might want to feed a document to the agent – how to handle that in Copilot?"
  Native file upload to custom agent is in roadmap. As a workarounds you can use **Power Automate flows** to extract file content from a SharePoint/Dataverse location and pipe it to your agent. Or your agent could expose a custom **API endpoint** that Copilot (or the user) calls with a file link, and the agent then fetches the file from the link. Another approach is to **wrap your agent as a REST API** within a Copilot Studio agent or M365 Agents Toolkit declarative agent that does handle files (since Copilot can ingest files for its own analysis). In short, it's possible, but may require an extra integration step.

- **I can't store certain data outside my environment (data residency requirements). "Our agent's knowledge base can't be duplicated to the cloud."**

  Response: The integration can be designed so that **Copilot does not store your data**. For instance, your agent can keep all its knowledge (documents, indexes) on your servers. When Copilot queries it, only the query and answer traverse the cloud – the source data stays put. If needed, use techniques like passing only vector embeddings or document IDs, so Copilot never sees the full text. Essentially, Copilot becomes a conduit, and your agent remains the sole holder of the sensitive content. This way, you satisfy requirements that no second storage of the data exists – Copilot just "asks" your system and relays the answer

Microsoft 365 Agents SDK & Toolkit

1. Why is it called the Microsoft 365 Agents SDK?

Microsoft 365 Copilot makes agents more personal for your organization, and agents make Microsoft 365 Copilot more capable. As a developer, you can build agents for Microsoft 365 Copilot and beyond with the Microsoft 365 Agents Software Development Kit (SDK). With the Agents SDK, you can build agents with the preferred tools of your choice. From Azure AI Foundry services, Semantic Kernel, Copilot Studio, or your own, you can build agents that extend Microsoft 365 Copilot or your own apps in Teams, web, Slack, Messenger, or 10+ other messaging channels. You are in control—whether you use low code or pro code, you can build agents that fit your and your organization's needs.

2. Is the M365 Agents SDK available today?

Microsoft 365 Agents SDK is in public preview, enabling developers to have continuity between Copilot Studio and Visual Studio.

3. What is the purpose of the M365 Agents Toolkit?

The Microsoft 365 Agents Toolkit simplifies the development process for building, debugging, and deploying enterprise-grade agents. Debug and test in M365 Copilot, Teams, web, and in the Agent Playground – then deploy using smart defaults for Azure. Get started using the templates combined with the Microsoft 365 Agents SDK to develop scalable and intelligent agents.

4. When should my organization consider leveraging Microsoft 365 Agents Toolkit?

If you decide to choose pro code to build agents for Microsoft 365 Copilot / Copilot Chat, the toolkit is your first choice.

5. What are M365 Copilot APIs?

Microsoft 365 Copilot APIs are a set of developer-first building blocks (Search, Retrieval, Chat, and Activity APIs) that power enterprise-grade generative AI experiences using Microsoft 365 data. They enable fast, secure, and compliant access to content across SharePoint, Teams, Outlook, and more, without requiring data egress or custom pipelines.

With these APIs, developers can create low-latency search, build grounded RAG workflows, integrate Copilot into custom apps, and monitor usage responsibly.

Agents for Power Platform

1. What is the Copilot Studio lite experience in Power Apps?

Copilot Studio lite in Power Apps enables makers to build agents for their app from within Power Apps Studio, using the lightweight Copilot Studio experience. The app-specific agents will leverage the logic, knowledge and actions already existing in the apps to execute tasks autonomously. The users of the apps will then be able to oversee the actions that the agents took in the app and act where agents hit roadblocks to complete.

2. Can I build agents in Power Pages?

At Ignite 2024, Microsoft introduced the ability to build agents in Power Pages websites—powerful autonomous agents designed for external use cases. Secured by Power Pages' role-based access control and authentication, these agents enable users to create workflows for external channels while maintaining robust security. The integration supports both authentication (choice of Identity Provider) and authorization layers (web roles and permissions), ensuring comprehensive security. Additionally, it simplifies the creation of agents in Microsoft Copilot Studio, based on existing complex Power Pages forms and other components through studio integration.

3. Are Power Platform copilots now rebranded as agents?

If they are the embedded copilots that help you to navigate the app, no. If they are the agents that you build in Copilot Studio, yes.

Power Platform Admin Center

Note: See the Agent Governance FAQ for more information

1. What are the newest security features and why are they important?

- Dynamics 365/Power Platform Managed Security is a comprehensive solution designed to safeguard enterprise data and business processes in the age of AI.

- It brings together advanced security capabilities including threat detection, data protection, access management, compliance, and security posture management capabilities to enable organizations to address rapidly evolving cyber security challenges.
- Power Platform admin center Security page enables security administrators to confidently and easily navigate the complex security landscape with easy-to-use, scalable security experiences, improved tools, automation, and intelligent insights that help detect, address, and prevent security risks. These comprehensive security capabilities empower admins to ensure the highest standards of data protection and regulatory compliance for their organizations.

2. Is the Agent orchestrator the Semantic Kernel, or the traditional Power Automate automation? Can automations be asynchronous or does it need to be synchronous? Is the variable added any Rest API interface. Finally, does the orchestrator use the user identify of the requestor or can a "service account be specified"?

The orchestrator used by the agent depends on the type of agent that has been created. Agents that are created to extend M365, or customized SharePoint agents, utilize the same orchestrator as the native M365 Copilot. Custom agents utilize a native generative orchestrator within Copilot Studio. When adding actions to an agent, makers can determine the type of authentication to be used, with the default being end-user authentication, where end users provide a connection for an action when an action is first called. When author authentication is configured for an action, the maker defines the connection that will be used whenever that action is called.

Pricing and Licensing

1. Will new features be included in the pricing of Copilot Studio?

Any features in limited early access preview or public preview do not have licensing information available. Please see the pricing and licensing section for other questions.

2. If I have a M365 Copilot license, and my org has disabled Copilot Studio unless requested, can I still build agents in M365 Copilot using the no-code options? Or does Studio need to be enabled/turned on?

Agents can still be created via the embedded experience in Copilot for M365 or via SharePoint. If Copilot Studio has been disabled unless requested, agents that have the option to be customized with Copilot Studio can only be done so if Copilot Studio is available for the user.

Agent cost controls

Estimating & Managing Agent Costs

1. What tools are available to estimate agent message volume and enable cross-chargeback processes?

You can now estimate message consumption volumes for your agents using Copilot Studio agent usage estimator. Organizations can use it to project the monthly message consumption volume per custom engine agent based on factors such as agent traffic, type, orchestrator, knowledge sources and other capabilities and inclusive of zero-rated usage for features included for M365 Copilot licensed users.

Organizations can enable cross-chargeback processes as follows:

Microsoft 365 admin center (MAC):

- Departmental billing and charge back can be accomplished using the pay-as-you-go (PAYG) billing policies. Set up Microsoft 365 Copilot pay-as-you-go for IT admins | Microsoft Learn. You can create a billing policy for each department (HR, Finance, Engineering) or any other group of users in your organization, and enable PAYG for consumptive billing for enabled Copilot services (such as M365 Copilot Chat, SharePoint agents, Copilot tuning, Copilot APIs etc.). This setup enables seamless cross-chargeback based on actual consumption, ensuring accurate cost attribution and reducing administrative overhead.

- Going forward, organizations will be able to set budgets at a billing policy (user group) level, which will help admins manage and track PAYG costs for a set of users. Additionally, organizations will soon be able to apply unused message capacity packs towards billing policies for Copilot services from within MAC.

Power Platform admin center (PPAC):

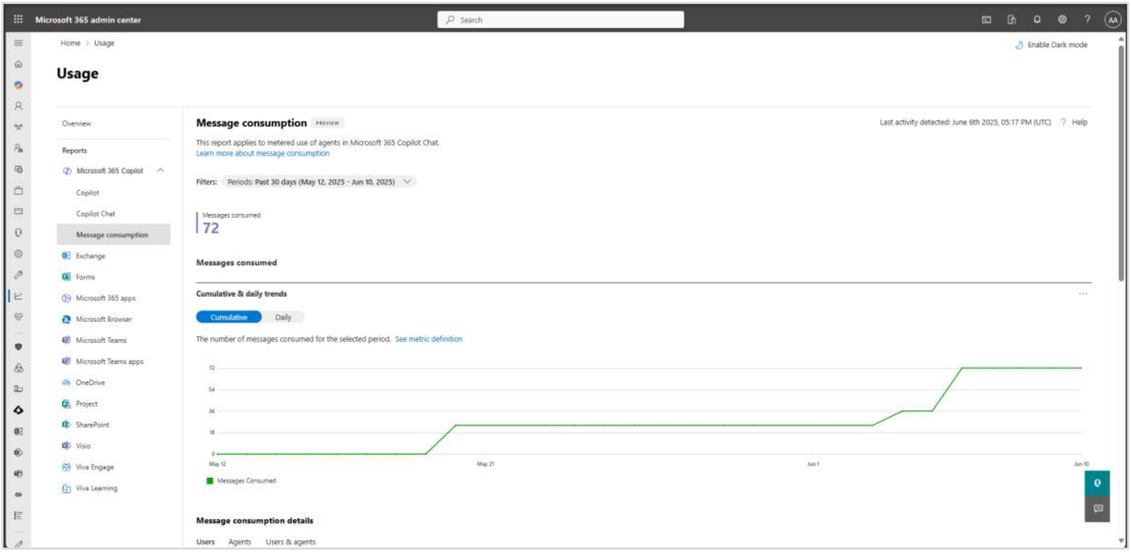
- Pre-paid message pack: Organizations can allocate pre-paid message capacity to specific environments—often aligned with departments or business units. Once capacity is assigned, it becomes fully isolated, ensuring other environments cannot consume from it. This isolation supports chargeback models and cost accountability by allowing each team to manage its own usage.
- Pay-as-you-go: Organizations can enable pay-as-you-go (PAYG) for individual environments or a group of environments. Any usage within these environments is billed directly to the Azure subscription associated with the billing plan, enabling seamless cross-chargeback based on actual consumption. PPAC also supports tracking consumption at the granularity of environment, which can be used by organizations for departmental cross charging. Note that consumption will draw from message capacity first before incurring usage costs on a pay-as-you-go basis.

2. How can organizations manage budgets efficiently with agent cost prediction tools?

Organizations can manage budgets efficiently with agent cost prediction tools by following a comprehensive lifecycle approach to agent cost management. This involves several key stages:

1. **Estimating Initial Costs:** Before deploying AI agents, it's crucial to estimate their potential costs. This helps in aligning budgets, managing stakeholder expectations, and avoiding surprises after deployment. Tools like the Copilot Studio Agent Consumption Estimator can assist in estimating monthly message consumption volumes that organizations can use to then compare costs for different billing models.
2. **Setting Up Billing Models:** Selecting the appropriate billing model is essential. Options include prepaid message packs, pay-as-you-go (PAYG) billing, and M365 Copilot licenses. Each model offers flexibility based on usage patterns and financial predictability. Users with and M365 Copilot license are not subject to metered usage of agents.
3. **Tracking and Analyzing Usage:** Once agents are in use, ongoing tracking and analysis of actual costs are critical. Tools like the Microsoft 365 admin center (MAC) and Power Platform admin center (PPAC) provide detailed visibility into agent-related message usage, enabling administrators to monitor consumption, analyze trends, and forecast future spending.

In M365 admin center, admins can view message consumption in the Reports section under Microsoft 365 Copilot > Message Consumption.



Last activity detected: June 6th 2025, 05:17 PM (UTC)

This report applies to metered use of agents in Microsoft 365 Copilot Chat.
Learn more about message consumption

Filters: Periods: Past 30 days (May 12, 2025 - Jun 10, 2025)

Messages consumed
72

Messages consumed

Cumulative & daily trends

The number of messages consumed for the selected period. See metric definition

Message consumption details

Billing & PAYG Processes

3. Can administrators set limits or controls on Pay-as-you-go (PAYG) spending for M365 Copilot Chat users without a full license, particularly when agents are created or shared using SharePoint as a knowledge base in Copilot Studio lite?

In Microsoft 365 admin center (MAC), admins can:

- Define department-level billing policies (Already GA)
- Set budgets with alerts at thresholds (Coming in July)
- Apply notifications when thresholds are reached (Coming in July)

With integration with Azure Cost Management, admins can:

- Monitor Pay-As-You-Go billing by meter and resource.
- Establish alerts for budget thresholds.

In Power Platform admin center (PPAC), admins can:

- Enable governance and department level cost management by configuring a billing plan at the environmental level to activate Pay-as-you-go
- Monitor Pay-as-you-go consumption per environment
- Coming Soon (Preview in July)
  - Define monthly consumption limits for each Copilot Studio agent - whether the environment uses Prepaid or PAYG.
  - Take specific actions:
    - Search for specific agents
    - Set usage caps directly
    - Enforce monthly limits — in Prepaid environments, within the allocated pool; in PAYG environments, with flexible thresholds and overages billed accordingly
    - Turn off agents from this interface
    - Configure guardrails — such as notifications or auto-disabling agents once they reach 100% of their assigned limit
  - Get a centralized view of all agents across the tenant in Licensing Hub, showing:
    - Configured message limits (if set)
    - Month-to-date usage

    - Associated environments
    - Current usage status (within limit, nearing limit, or over limit)

4. Can I set limits to the PAYG plan?

In Microsoft 365 admin center (MAC), you can enable

- **Billing Policies with Budget Limits.** Admins can define billing policies scoped to departments or Entra ID groups. Each policy can include a dollar limit, which helps prevent overspending. Once defined thresholds are reached, notification emails will be sent to the specified users. Usage can be monitored or restricted depending on the configuration
- **Agent-Level Controls.** Global Admin, AI Admin and Billing admin will be able to apply PAYG billing policies at the agent level, enabling fine-grained control over which agents incur costs. This is particularly useful for managing declarative agents in Copilot Chat or SharePoint scenarios

In Power Platform admin center (PPAC), Users have the capability to set an alert in Azure cost management. Currently, in PPAC, there is no direct method to establish a limit per pay-as-you-go plan. It will be possible to set a limit per agent, thereby allowing better control over each agent's usage.

5. Can I use Prepaid Message Packs to create agents in the lite experience and Copilot Studio or is a PAYG plan needed?

Yes, you can use Message Packs (prepaid licensing) to create agents using both Copilot Studio and the lite experience—a PAYG plan is not required for this capability.

Prepaid message packs (Message Packs) are a valid licensing path for agent creation, and organizations do not need to activate PAYG unless they prefer that model for flexibility or scaling purposes.

6. Can I set limits to the PAYG plan in Microsoft 365 admin center?

Yes, organizations using the Pay-As-You-Go (PAYG) plan in Microsoft 365 admin center can set limits to manage and control your spending.

Microsoft provides several mechanisms for setting budget and spending limits within PAYG billing policies:

- Hard Limits: These suspend services once the defined budget is exceeded, preventing further charges (These limits are coming to MAC in a subsequent release). Hard limits are available in public preview in the Power Platform admin center.
- Soft Limits: These trigger email notifications when usage reaches custom thresholds (e.g., 70%, 90%). These Limits are planned will be available in July 2026.

These controls are especially useful for large organizations with distributed cost centers, as they help maintain transparency and accountability across departments or user groups.

There capabilities will allow admins to:

- Define and enforce budget limits per billing policy directly in the Microsoft 365 admin center.
- Configure reset frequencies (monthly, quarterly, yearly).
- Set up email alerts at customizable thresholds (e.g., 80%, 90%, 100%) to notify mail-enabled security groups

7. What happens if a user is added to two or more different billing policies?

If a user is added to two or more different billing policies, the billing policy to which the user was first assigned will take precedence.

8. Is group level billing for MAC only available for PAYG or also in message pack too?

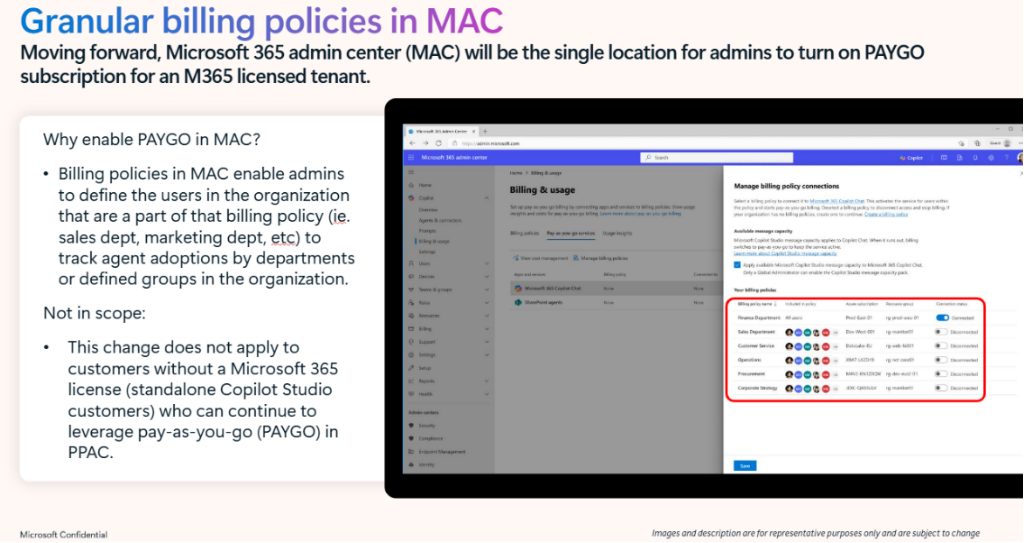
Currently, group-level billing for MAC (Microsoft 365 admin center) is available only for PAYG (Pay-As-You-Go) accounts. Efforts are underway to enhance this functionality so that unused message capacity from message packs can also be applied toward a billing policy within the Microsoft 365 admin center.

9. What happens if I have PAYG billing plans in Copilot Studio and billing policies with PAYG policies configured in Microsoft 365 admin center at the same time? PPAC focuses on PAYG in the environment, while MAC focuses on a group of users. Should my organization set up both, or is one sufficient?

If you have both Pay-As-You-Go (PAYG) billing plans configured in Copilot Studio and billing policies with PAYG options set up in the Microsoft admin center (MAC), you only need to configure one—setting up both is not required.

The key distinction is that:

- Power Platform admin center (PPAC) manages PAYG at the environment level
- Microsoft 365 admin center (MAC) for licensed Microsoft 365 Copilot users applies PAYG billing to a specified group of users (see below)



Granular billing policies in MAC

Moving forward, Microsoft 365 admin center (MAC) will be the single location for admins to turn on PAYGO subscription for an M365 licensed tenant.

Why enable PAYGO in MAC?

- Billing policies in MAC enable admins to define the users in the organization that are a part of that billing policy (ie. sales dept, marketing dept, etc) to track agent adoptions by departments or defined groups in the organization.

Not in scope:

- This change does not apply to customers without a Microsoft 365 license (standalone Copilot Studio customers) who can continue to leverage pay-as-you-go (PAYGO) in PPAC.

Manage billing policy connections

Select a billing policy to connect it to Microsoft 365 Copilot Chat. This activates the service for users within the policy and starts pay-as-you-go billing. Deselect a billing policy to disconnect access and stop billing. If your organization has no billing policies, create one to continue. Create a billing policy

Available message capacity

Microsoft Copilot Studio message capacity applies to Copilot Chat. When it runs out, billing switches to pay-as-you-go to keep the service active.
Learn more about Copilot Studio message capacity

☑ Apply available Microsoft Copilot Studio message capacity to Microsoft 365 Copilot Chat.
Only a Global Administrator can enable the Copilot Studio message capacity pack.

Your billing policies

Billing policy name ↓	Included in policy	Azure subscription	Resource group	Connection status
Finance Department	All users	Prod-East-01	rg-prod-weu-01	Connected
Sales Department		Dev-West-001	rg-monitor01	Disconnected
Customer Service		DataLake-EU	rg-web-fe001	Disconnected
Operations		X9A7-LK2D19	rg-net-core01	Disconnected
Procurement		M4V2-KN1Z0QW	rg-dev-eus2-01	Disconnected
Corporate Strategy		JEXC-QA93UEV	rg-monitor01	Disconnected

Microsoft Confidential

Images and description are for representative purposes only and are subject to change

For declarative agents, if a PAYG billing plan is established through MAC, all related billing events will be processed via the MAC configuration and will not be billed again through any PAYG setup in PPAC. This ensures there is no double-billing and clarifies which billing policy takes precedence.

10. When should I use Microsoft 365 admin center vs Power Platform admin center to set up and management PAYG billing for Microsoft 365 Copilot?

Microsoft 365 admin center: Recommended for most Microsoft 365 customers. MAC is becoming the centralized hub for managing PAYG billing across Copilot services, including Copilot Chat and SharePoint agents.

Microsoft 365 admin center: Best suited for Microsoft 365 licensed customers who need a single pane of glass for billing, usage, and agent management.

- You want to manage PAYG billing by user groups or departments (e.g., Sales, Marketing).
- You need billing policies that map to Azure subscriptions and resource groups.
- You want to track usage and costs by department or group.
- You want to enforce spending limits, receive alerts, and integrate with Azure Cost Management.

Power Platform admin center: Best suited for standalone Copilot Studio customers or those managing billing at the environment level.

Use PPAC when:

- You are not using Microsoft 365 licenses (e.g., standalone Copilot Studio customers).
- You want to manage PAYG per environment rather than by user group.
- You need to create billing plans that link environments to Azure subscriptions.
- You want to set monthly consumption limits for each agent and configure guardrails like auto-disabling agents at 100% usage.

PPAC offers more granular control over Copilot Studio agent-level usage, including message limits, usage status, and the ability to turn off agents directly.

Agent Controls

11. Are there plans to make MAC agent controls more granular? (For example, separate toggle for creating agents, using agents, and sharing agents)

For context, agents that are created from the lite experience and SharePoint are end-user facing agents and are managed with the M365 Copilot Controls on MAC. End-user created agents can only include custom prompts and instructions and define the knowledge sources within the set that the user already has access to.

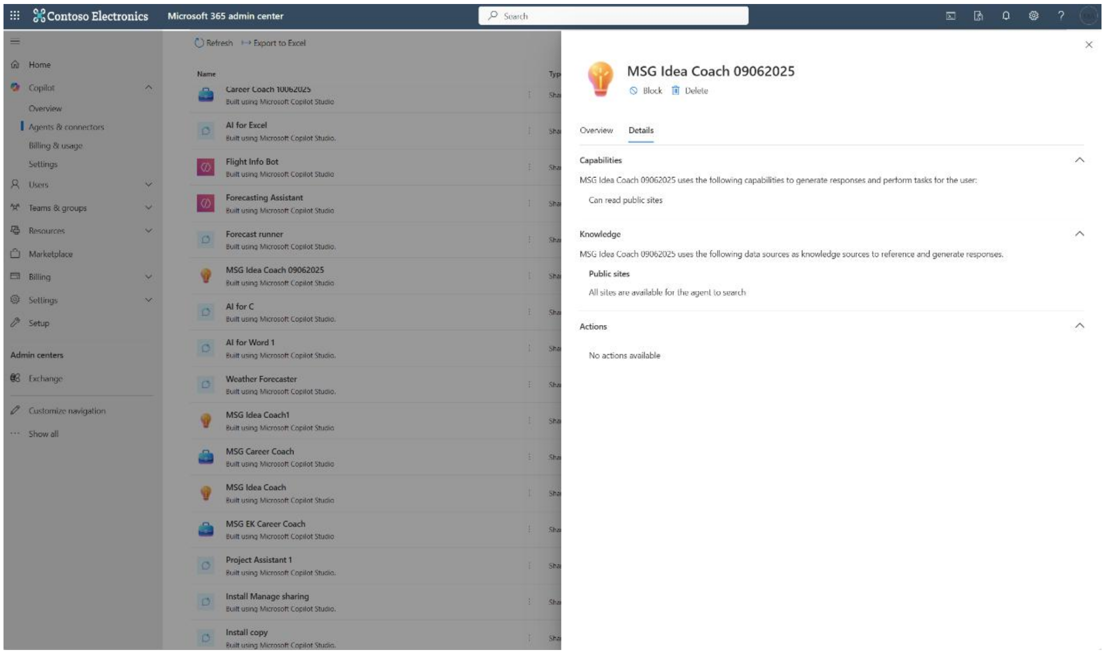
Microsoft does not have separate controls for the end-user created agents because they are not any more than customized and smaller scoped Copilot Chat which is already governed with the copilot controls. If the user is assigned with M365 Copilot licenses, then they are eligible to use the Copilot Chat and create an agent from Copilot Studio lite.

For creating from Copilot Studio or Pro-dev tools, the user will need to be in admin managed environments, because maker/pro-dev created agents can access more resources than Copilot itself and require additional governance. In short, create and use is governed together with Copilot controls for end-user facing agents in a similar way to file management.

The inventory and lifecycle of end-user created agents can be managed from MAC, and MAC admin can monitor agents’ usage and block any agent if it is needed. The lifecycle management gestures on MAC also includes orphan agent identification, owners’ assignment, delete of the agent and soon Microsoft will enable rule-based management for governance in bulk.

12. Is it possible for organizations to have more control over the data sources available during agent creation, for example, by having the option to disable features like 'upload files'?

Yes, organizations can have more control over the data sources available during agent creation, including the option to disable features like 'upload files'. Administrators can manage who can create agents and what data sources they can access by configuring permissions and roles within the Power Platform admin center (PPAC) and Microsoft 365 admin center (MAC).



Name
Career Coach 10062025 Built using Microsoft Copilot Studio
AI for Excel Built using Microsoft Copilot Studio.
Flight Info Bot Built using Microsoft Copilot Studio
Forecasting Assistant Built using Microsoft Copilot Studio
Forecast runner Built using Microsoft Copilot Studio.
MSG Idea Coach 09062025 Built using Microsoft Copilot Studio
AI for C Built using Microsoft Copilot Studio.
AI for Word 1 Built using Microsoft Copilot Studio.
Weather Forecaster Built using Microsoft Copilot Studio.
MSG Idea Coach1 Built using Microsoft Copilot Studio
MSG Career Coach Built using Microsoft Copilot Studio
MSG Idea Coach Built using Microsoft Copilot Studio
MSG EK Career Coach Built using Microsoft Copilot Studio
Project Assistant 1 Built using Microsoft Copilot Studio.
Install Manage sharing Built using Microsoft Copilot Studio.
Install copy Built using Microsoft Copilot Studio.

MSG Idea Coach 09062025

Capabilities

MSG Idea Coach 09062025 uses the following capabilities to generate responses and perform tasks for the user:

Can read public sites

Knowledge

MSG Idea Coach 09062025 uses the following data sources as knowledge sources to reference and generate responses.

Public sites

All sites are available for the agent to search

Actions

No actions available

13. Is there a way to disable the creation of agents in the lite experience while still allowing agent usage? I want to allow the usage of agents built by Microsoft and block new agent creation.

At present, it is not possible to disable the creation of agents in the lite experience while still allowing users to use agents created by Microsoft or others. The current system links both creation and usage permissions under a single control. However, this distinction between creation and usage controls has been recognized as an important feature request and is under consideration for potential future updates.

14. Is there a way to block an agent from a subset of users so they can't see it but still have it available to others?

In the Agents & Connectors section, administrators can navigate to the Agent inventory, select a specific agent, and then choose 'Users' to manage who has access to that agent. By removing certain users or groups from this list, admins can restrict access so that only approved individuals can see and use the agent.

Governance & Reporting

15. How does Microsoft talk to organizations about Microsoft's governance strategy, what's in place today and what's coming next?

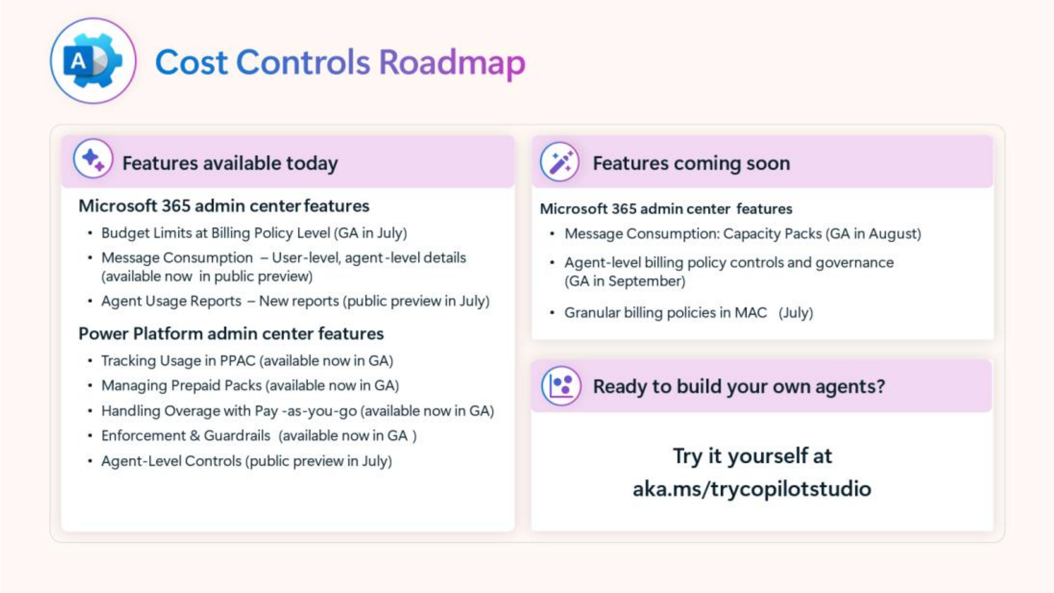
What's in place today

- Agent Visibility & Inventory
  - The Copilot Control System (CCS) in the Microsoft 365 admin center provides a centralized view of all agents, including those created by end users.
  - The "Shared Agents" tab helps identify unofficial agents by showing metadata like publishing status, data sources, and deployment method.
- Access & Creation Controls
  - Admins can manage who can create agents by assigning licenses only to approved users or groups (e.g., "Copilot Studio Makers").

    - Role-based access and environment-level permissions in Power Platform admin center (PPAC) help restrict agent development and publishing.
- Usage & Cost Management
    - MAC admins can set per-user quotas, agent-level message limits, and budget thresholds to control consumption.
    - PAYG and Prepaid billing models can be scoped to environments (via PPAC) or user groups (via MAC). PPAC admin can track Copilot Studio message usage (GA) and manage prepaid capacity packs (GA)
    - PPAC admins have Pay-as-you-go (PAYG) support (GA) and can address overages using Pay-G or available tenant capacity (GA)
- Blocking & Enforcement
    - Agents that violate policy or overconsume resources can be blocked via MAC, preventing further use without deletion.

Coming Soon

- Agent-Level Cost Controls
    - Soon, MAC admins will be able to set monthly message limits per agent, with usage status indicators (e.g., within limit, nearing limit, over limit) and auto-disable options.
    - Soon, PPAC admins will be able to set agent-level message limits and have the option to turn off individual agents (Preview in July)
- Support for Prepaid Packs
    - Prepaid message capacity will be assignable by department or group through billing policies in MAC—enabling more granular control before PAYG charges kick in.
- Budget Enforcement
    - MAC admins will be able to define billing policy budgets with reset frequencies and email alerts at thresholds like 80%, 90%, and 100%.
    - For agents managed in PPAC, publish & runtime enforcement will start in Aug to ensure that agents in overage do not exceed set capacity limits.
- Improved Reporting
    - The Message Consumption Report in MAC will offer near real-time alerts and detailed breakdowns by user, agent, and agent-user pair.



Cost Controls Roadmap

Features available today

Microsoft 365 admin center features

- Budget Limits at Billing Policy Level (GA in July)
- Message Consumption – User-level, agent-level details (available now in public preview)
- Agent Usage Reports – New reports (public preview in July)

Power Platform admin center features

- Tracking Usage in PPAC (available now in GA)
- Managing Prepaid Packs (available now in GA)
- Handling Overage with Pay -as-you-go (available now in GA)
- Enforcement & Guardrails (available now in GA)
- Agent-Level Controls (public preview in July)

Features coming soon

Microsoft 365 admin center features

- Message Consumption: Capacity Packs (GA in August)
- Agent-level billing policy controls and governance (GA in September)
- Granular billing policies in MAC (July)

Ready to build your own agents?

Try it yourself at
aka.ms/trycopilotstudio

16. What user-level consumption-based reporting is available to help organizations manage internal chargeback processes and ensure billing methods support agent usage in Copilot chat?

User-level consumption-based reporting is essential for managing internal chargeback processes and ensuring billing methods support agent usage in Copilot chat. Here are the key tools and features available:

1. **Microsoft 365 admin center (MAC)**: The MAC, through the Copilot Control System (CCS), provides tools for tracking, analyzing, and forecasting agent-related costs across Microsoft 365 Copilot Chat. Admins can monitor usage patterns, identify high-cost agents or users, and manage consumption proactively. The "Shared Agents" tab in the Integrated Apps experience allows admins to view metadata about each agent, search for agents by name or function, and identify agents deployed via public store, direct upload, or internal development.

   User-Level Message Consumption Reporting

   These reports include:

   - Cumulative and daily trends
   - Usage details per user, agent, user-agent pair, and billing policy
   - Exportable CSVs showing messages consumed per user
   - Alerts for high hsage: near-real-time alerts for users who exceed thresholds (e.g., 2,000 billed messages in 30 days, equivalent to ~$20). Admins are prompted to assign a Copilot license if usage justifies it.
2. **Power Platform admin center (PPAC)**: The PPAC offers detailed visibility into agent-related message usage across environments. Key tracking features include environment-level monitoring, billing policy views, and capacity summary dashboards. Admins can track message consumption by environment, product, agent, and feature, and analyze costs through consumption drilldowns and Azure Cost Management integration.
3. **Azure Cost Management**: The Azure portal provides features for tracking, analyzing, and forecasting agent costs. Administrators can search for specific agents, monitor their consumption patterns, and use tools like the Azure Consumption API and Azure Graph API to pull detailed usage and billing data. This enables the creation of custom dashboards or portals for real-time metrics and cost analysis.

These tools and features help organizations maintain financial control, optimize usage, and ensure that billing methods align with agent consumption patterns.

17. Is there a consolidated report that includes all agents created in Copilot Studio and Copilot Studio lite?

Agents & connectors in the Microsoft 365 admin center (MAC) a centralized inventory of all agents in the tenant. This includes:

- Agents created using Copilot Studio
- Agents built with Copilot Studio lite
- Agents created by end users

This view allows administrators to:

- See metadata for each agent (e.g., capabilities, data sources, publishing status)
- Search by agent name or function
- Identify deployment method (e.g., public store, internal development, direct upload)

This section effectively consolidates visibility across both Copilot Studio and lite experience agents

18. How can third-party agents be incorporated into the reporting and governance framework?

Yes, third party agents can be managed and measured in Microsoft 365 admin center using the same tools for all other agents in M365 Copilot. For management, third party agents can be governed via Agents & connectors in the

Microsoft 365 admin center. For measurement, third party agents usage can be viewed in Agents usage report, planned for release in July 2025.

19. Where can I view how many messages a specific agent consumes?

You can view how many messages a specific agent consumes using the tools available in both the Microsoft 365 admin center (MAC) and the Power Platform admin center (PPAC), depending on where the agent is deployed and how it's billed.

In Microsoft 365 admin center (MAC): For agents used in Microsoft 365 Copilot Chat, the Message Consumption Report (currently in Preview) provides:

- Per-agent message consumption: View how many messages each agent has consumed.
- Per-user and agent-user pair metrics: Understand which users are driving the most usage for each agent.
- Time series data: See cumulative and daily usage trends.
- Alerts: Get notified when users exceed thresholds (e.g., 2,000 messages in 30 days) with links to detailed usage per agent

This applies to all declarative agents in Microsoft 365 Copilot and Copilot Chat.

In Power Platform admin center (PPAC): For agents built in Copilot Studio, PPAC provides:

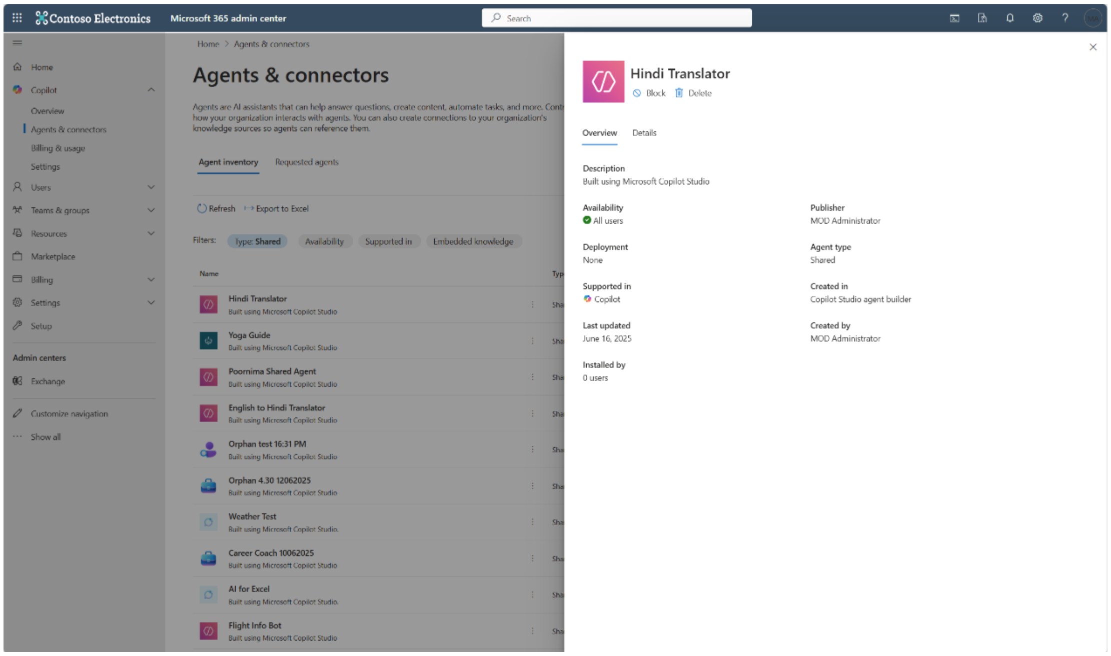
- Consumption drilldowns: Track message usage by agent, user, or agent-user pair.
- Capacity summary dashboards: View usage by environment and agent.
- Custom reporting: Download reports showing usage per agent to support internal chargebacks or optimization.
- Coming soon: A new Licensing Hub will allow admins to:
  - Set and monitor monthly message limits per agent.
  - View month-to-date usage and status indicators (e.g., within limit, nearing limit, over limit).
  - Search for agents and enforce usage caps or auto-disable them when limits are reached.

20. Do SharePoint agents, or declarative agents (DAs) or custom engine agents (CEAs), published in SharePoint require PAYG for users who are not licensed with M365 Copilot?

Yes, starting in July 2025, SharePoint agents can be onboarded as a Microsoft 365 Copilot PAYG service via M365 admin center > Copilot > Billing and usage > Pay-as-you-go services. Once enabled, users without an M365 Copilot license will be able to use SharePoint agents on a PAYG basis. Similarly, users enabled with agents can access and use DAs and CEAs, in SharePoint on a PAYG basis. Yes, coming in Sept, SP agents will be able to use message packs.

21. How can administrators obtain a comprehensive overview of all agents created using Copilot Studio lite (excluding those created directly through Copilot Studio), including details about their functions and capabilities?

This is currently available in the Agents and Connectors page in MAC. Select Type=shared and click on an agent to view the details of the agent.



Agents & connectors

Agents are AI assistants that can help answer questions, create content, automate tasks, and more. Contr how your organization interacts with agents. You can also create connections to your organization's knowledge sources so agents can reference them.

Name	Typ
Hindi Translator Built using Microsoft Copilot Studio	Sha
Yoga Guide Built using Microsoft Copilot Studio	Sha
Poornima Shared Agent Built using Microsoft Copilot Studio	Sha
English to Hindi Translator Built using Microsoft Copilot Studio	Sha
Orphan test 16:31 PM Built using Microsoft Copilot Studio	Sha
Orphan 4.30 12062025 Built using Microsoft Copilot Studio	Sha
Weather Test Built using Microsoft Copilot Studio.	Sha
Career Coach 10062025 Built using Microsoft Copilot Studio	Sha
AI for Excel Built using Microsoft Copilot Studio.	Sha
Flight Info Bot Built using Microsoft Copilot Studio	Sha

Hindi Translator

Description
Built using Microsoft Copilot Studio

Availability
All users

Publisher
MOD Administrator

Deployment
None

Agent type
Shared

Supported in
Copilot

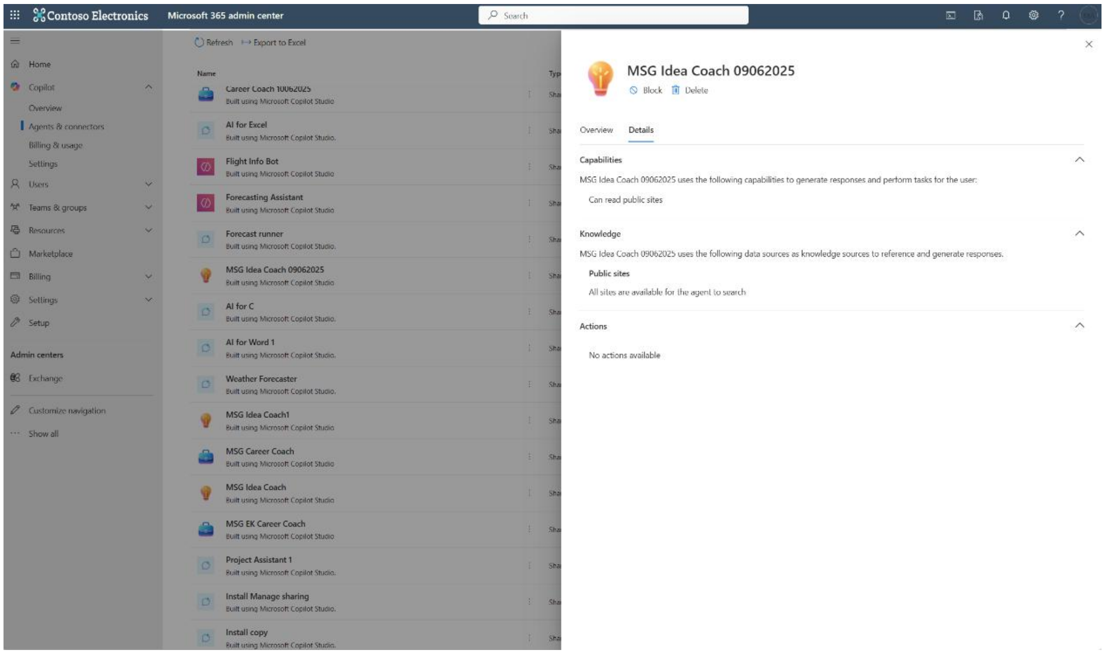
Created in
Copilot Studio agent builder

Last updated
June 16, 2025

Created by
MOD Administrator

Installed by
0 users

Click on the details tab to view the details about Capabilities, Knowledge sources and Actions.



Name	Typ
Career Coach 10062025 Built using Microsoft Copilot Studio	Sha
AI for Excel Built using Microsoft Copilot Studio.	Sha
Flight Info Bot Built using Microsoft Copilot Studio	Sha
Forecasting Assistant Built using Microsoft Copilot Studio	Sha
Forecast runner Built using Microsoft Copilot Studio.	Sha
MSG Idea Coach 09062025 Built using Microsoft Copilot Studio	Sha
AI for C Built using Microsoft Copilot Studio.	Sha
AI for Word 1 Built using Microsoft Copilot Studio.	Sha
Weather Forecaster Built using Microsoft Copilot Studio.	Sha
MSG Idea Coach1 Built using Microsoft Copilot Studio	Sha
MSG Career Coach Built using Microsoft Copilot Studio	Sha
MSG Idea Coach Built using Microsoft Copilot Studio	Sha
MSG EK Career Coach Built using Microsoft Copilot Studio	Sha
Project Assistant 1 Built using Microsoft Copilot Studio.	Sha
Install Manage sharing Built using Microsoft Copilot Studio.	Sha
Install copy Built using Microsoft Copilot Studio.	Sha

MSG Idea Coach 09062025

Capabilities

MSG Idea Coach 09062025 uses the following capabilities to generate responses and perform tasks for the user:

Can read public sites

Knowledge

MSG Idea Coach 09062025 uses the following data sources as knowledge sources to reference and generate responses.

Public sites

All sites are available for the agent to search

Actions

No actions available

22. Is there a way to monitor the usage and activity of specific shared agents, created with Copilot Studio lite?

Administrators can track and manage agents through the Integrated Apps experience in the Microsoft 365 admin center (MAC). A dedicated "Shared Agents" tab provides a centralized inventory of all agents in the tenant, including those created by end users that haven’t been published to the IT Catalog. This tab allows admins to view metadata about each agent, search for agents by name or function, and identify agents deployed via public store, direct upload, or internal development.

23. Will third-party agents be incorporated into the CCS reporting and management framework?

Admins can track and manage agents through the Integrated Apps experience in MAC. A dedicated "Shared Agents" tab provides a centralized inventory of all agents in the tenant, including third-party agents created by end users that haven't been published to the IT Catalog.

24. In terms of control, providing my organization does not use M365 and I only want to use free Copilot Chat, what can I control?

For organizations who choose not to use Microsoft 365 (M365) and only wish to utilize the free Copilot Chat, the control over data sources, agent creation, and usage monitoring will be restricted compared to the full M365 environment.

25. Is there a native feature to block agent creation to only specific environments?

Administrators can control who can create agents by:

- Assigning Copilot Studio licenses only to users in a designated Microsoft Entra security group (e.g., "Copilot Studio Makers").
- Granting access only to environments where agents can be developed and deployed by assigning that security group to the Copilot Studio author setting in the Power Platform admin center (PPAC).

This setup ensures that only authorized users can create agents, and only within the environments explicitly configured for development and deployment. It effectively blocks agent creation in all other environments unless access is granted.

Additionally, environment roles (e.g., Maker, Admin) can be used to further restrict access to Copilot Studio functionality, and publishing approvals can be enabled to control how agents are released to business units or regions.

26. How can I restrict which user groups or individuals are allowed to create, share, or use agents in Copilot Studio lite in M365 Copilot Chat?

Admins can configure agent usage and creation with a single control in the Microsoft 365 admin center under Copilot > Settings > Agents. Here, admins can select: all users, no users, or a combination of specific users or groups. Limiting usage to specific groups allows for: controlled rollout, better visibility into consumption, and departmental or regional adoption management.

27. Can I see agents made in the lite experience by users in Agent & connectors section?

Agents created using Copilot Studio lite (in Microsoft 365 Copilot Chat) can be viewed and managed through the Microsoft 365 admin center under Copilot > Agents & connectors and filter by "Shared agents." Limiting usage

28. What admin roles are required to manage billing in Microsoft 365 admin center vs Power Platform admin center?

- M365 admin center is for Global Administrators and Billing Administrators
- Power Platform admin center is for Global Administrators, Power Platform Administrators, and Environment Administrators

These admins, in their respective admin centers, have the ability to do certain things such as:

- Allocate capacity
- Create a billing plan
- Edit a billing plan
- Link a billing plan (to an environment or PAYG service)