How to manage agents with Agent 365

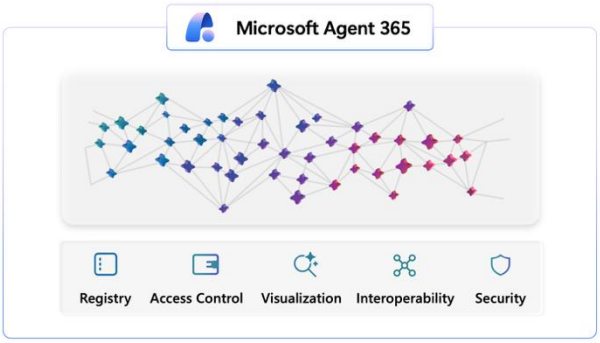
Canonical Guide | Level 150
Primary audience: Internal field teams looking to help customers get started or to directly adopt A365
Secondary Audience: Admins looking to use A365 to manage and govern agents for their organization, and agent developers looking to adopt A365 SDKs.
Goal: Establish a unified and precise narrative for A365 and related concepts and upload to Seismic

---

What is Microsoft Agent 365?

Agent 365 is the control plane for agents. It extends the infrastructure that customers use for managing users, leverages familiar tools and capabilities, and adapts these for AI agents. Agent 365 brings Microsoft security and compliance solutions, including Defender, Entra, and Purview, to register, protect, and govern agents. It also gives agents the ability to securely collaborate using Microsoft's suite of productivity tools such as Outlook, Word, Excel.

With Agent 365, organizations don't need to reinvent the wheel because the fastest path to confidently deploying agents is by managing these agents in the same way that they manage and secure users. Agent 365 delivers an **agent registry**, **access control**, **visualization**, **interoperability**, **security.**



Agent 365 is compatible with all agents, whether they are built on Microsoft agent creation platforms like M365 Copilot Agent Builder, Copilot Studio, Foundry, or built on external agent creation platforms. With built-in governance, observability, and compliance features, Agent 365 ensures organizations can confidently deploy, manage, and automate business processes.

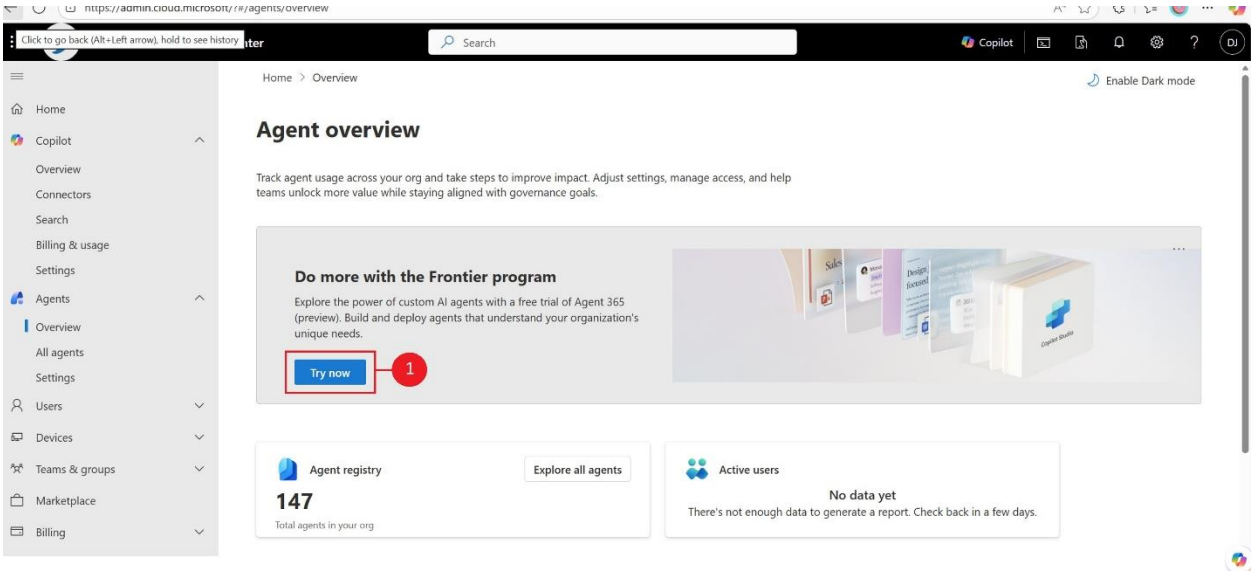
Get access

To get early access, organizations need to be in the Frontier program. See Getting started guide. Customers interested in A365's data and tools capabilities require a Microsoft Modern commerce agreement (where offered).

Detailed steps to get started:
Start: go to Microsoft 365 Admin Center (MAC)

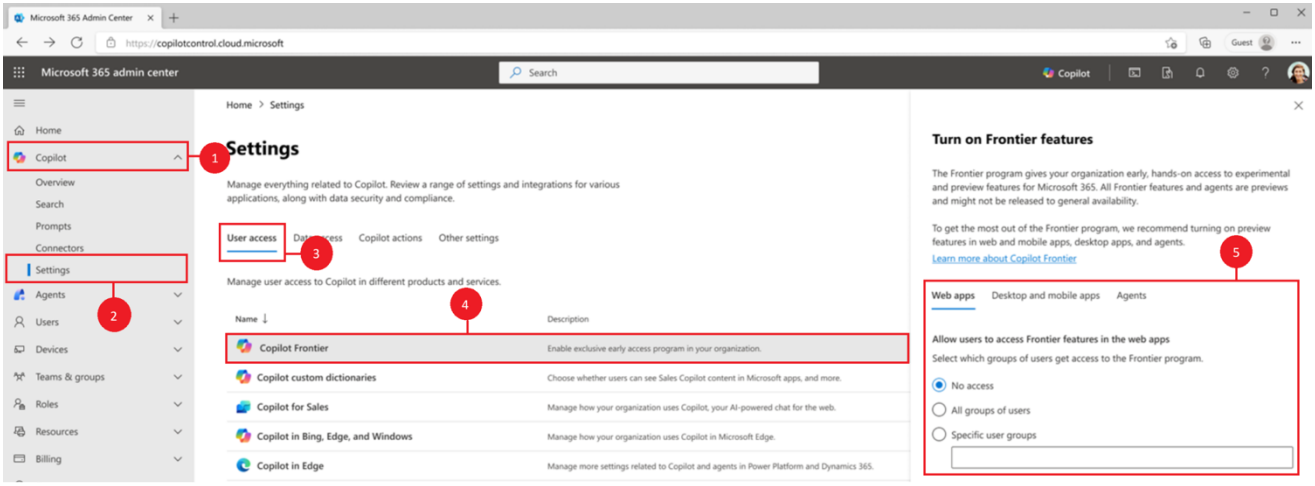
If you are already enrolled in the Frontier program

1. click "Try now" on the Agent overview page and accept terms.

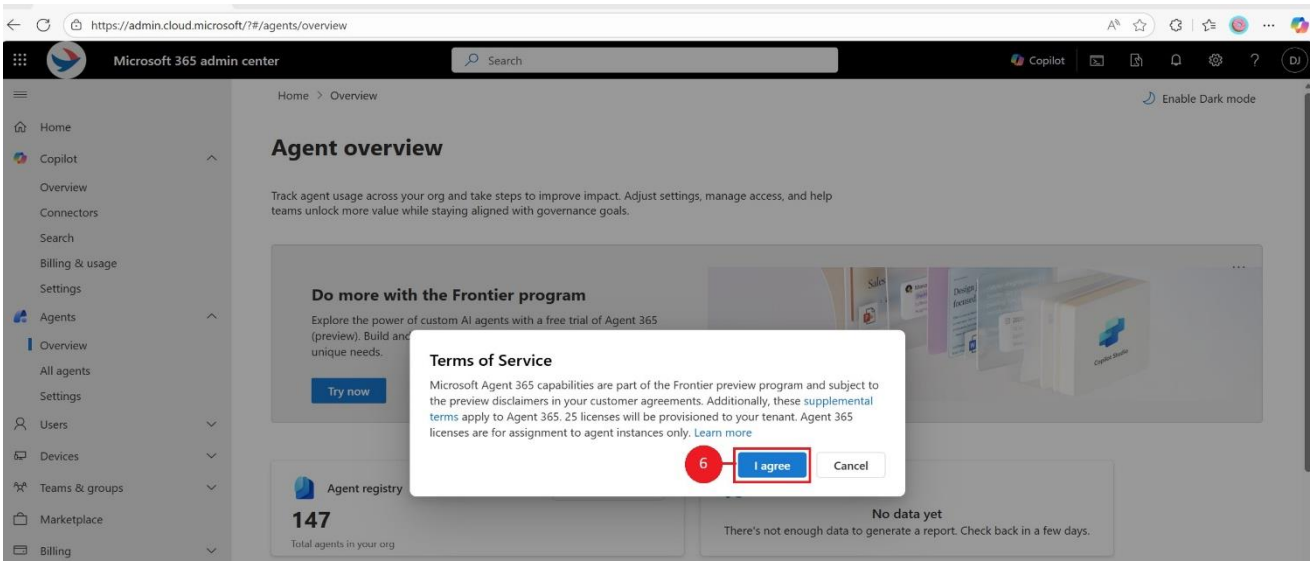


<u>If not already in the Frontier program</u>

1. Select Copilot
2. Select Settings
3. Under User access,
4. Select Copilot Frontier
5. Choose the groups to grant access.



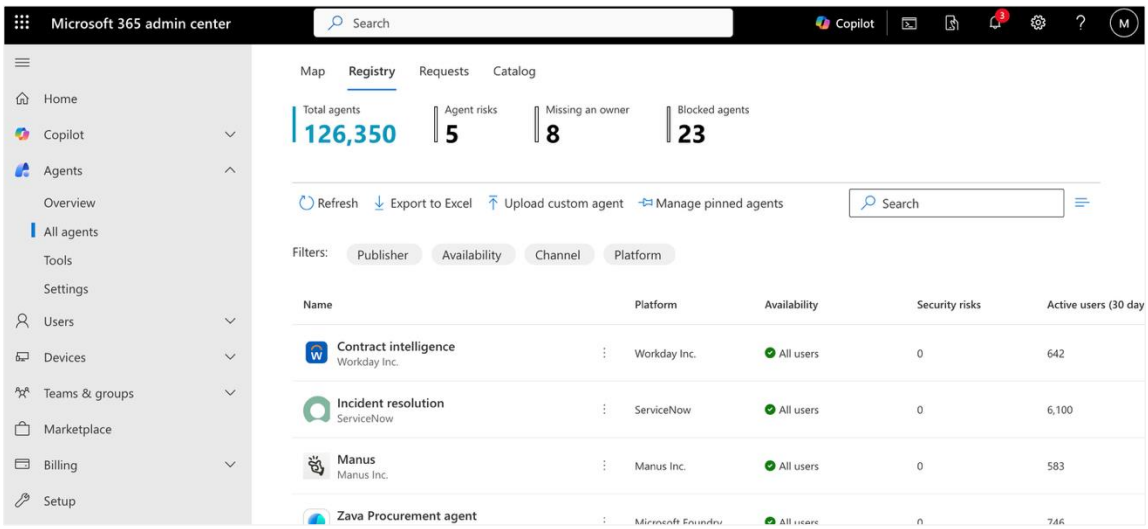
6. Then go to Agent Overview, click “Try now” and accept terms



What's possible

Primary persona: IT Admin

As an IT admin, you can engage with Agent 365 by starting on Microsoft 365 Admin Center (MAC).



Agent Registry, Access Control, Visualization, Security

- **View agent registry**: in the MAC's Left Side Navigation, go to `Agents > All Agents`. This view shows all A365-enabled agents in the company, with details such as # of agents created or agents by creation platforms.

  At Ignite, the agents that will light up are all agents published to the M365 channel (i.e. agents built with M365 Agent Builder SDK, MCS lite & full, Foundry, Partner-center published, SharePoint, LOB agents), as well as all agents with **Microsoft Entra Agent ID**.

- **View agent details and manage access**: Entra Agent ID consolidates agents into a single registry surfaced in MAC. Here, you get a centralized view for managing each agent.

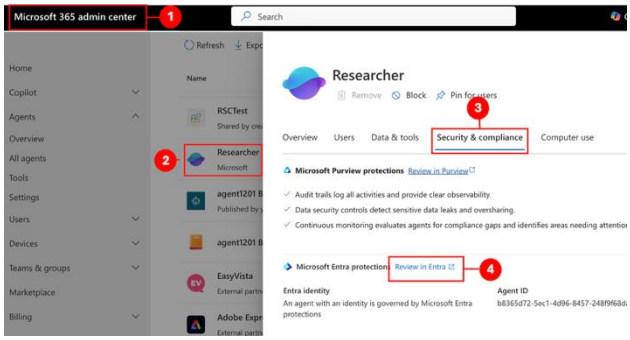
    - Select `View Details` to view a detailed list of all instances created under that agent.
        i. Manage individual instances: Access and update settings for each instance.
        ii. Review security and compliance status: Ensure every instance meets organizational standards.
        iii. Apply and customize licenses: Assign licenses and configure options at the instance-level.
- **Activate agent:** You can activate agents so that specific users, groups, or the entire tenant can add and use Agent 365 agents securely, within governance policies you set.
    - In the MAC, go to `Agents > All Agents`
    - Select the agent you want to activate
    - Select `Activate`
    - Select users that can add the activated template agent.
    - Apply a `policy template`.
    - Accept `permissions`.
    - Select `Review and finish`.
- **Block and unblock agents** - You can block or unblock agents for the entire organization. Blocking an agent turns off all instances created under that agent. These instances remain inactive until the IT admin unblocks the agent.
    - In the MAC, go to `Agents > All Agents`
    - Choose an agent from the list of agents.
    - Select `Block`.
    - Decide whether to block or unblock the agent for everyone.
- **Delete agent instances** - Admins can delete an agent instance from the MAC.
    - In the MAC, go to `Agents > All agents`.
    - Choose the agent that owns the instance you want to delete.
    - A pane is displayed, showing all instances associated with that agent.
    - Select `View Details` to see all instances created by that agent.
    - Select the instance you want to delete, then select `Delete`.
    - Confirm deletion.
    - Notify the hiring manager of deletion.
    - Provide access to the instance's OneDrive and Outlook data for 30 days. After 30 days, all instance accounts and data are permanently deleted. Audit logs are kept.

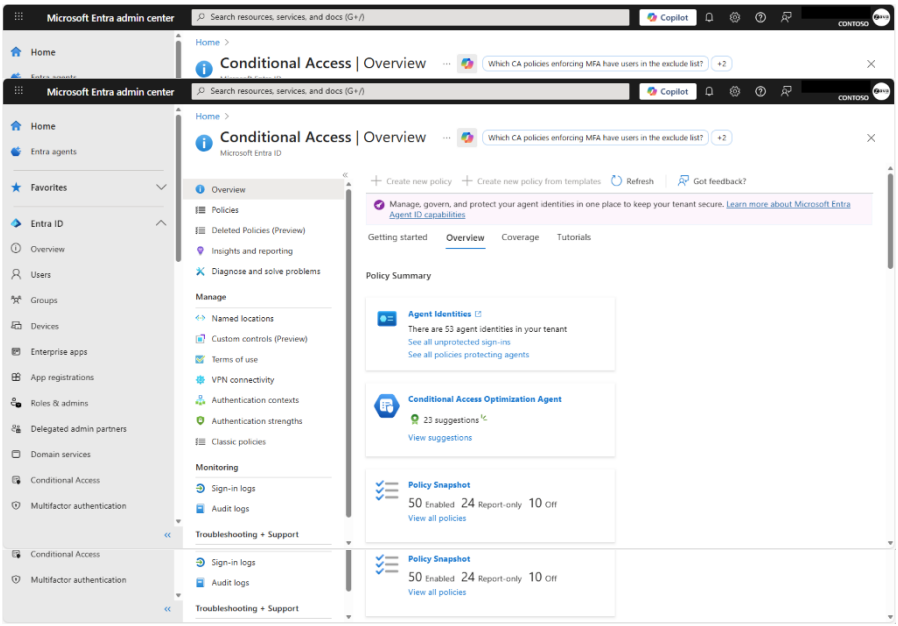
Primary personas: Security worker, IT Admin

As organizations adopt AI agents to automate workflows and boost productivity, securing these agents has become a critical concern. Unlike traditional applications, AI agents operate autonomously, interact with sensitive data, and execute tasks across multiple systems - making them high-value targets for intentional attacks and also vulnerable to unintentional compromise. Microsoft Agent 365 provides a unified control plane for all AI agents in your organization, and integrates with Microsoft's security platforms including Entra, Purview, and Defender.

Visibility, Identity Management, Access Control with Microsoft Entra Agent ID: Microsoft Entra Agent ID extends security capabilities to agents through conditional access policies, identity protection, identity governance, and network-level controls. Entra agent ID ensures that for A365 Data and Tools access, agents are controlled by a least-privileged approach, requesting just-in-time scoped tokens for exactly the resources the agent needs. To view an agent's Entra details:

1. In the MAC's left side navigation, `Agents > All Agents`.
2. Click on the relevant agent
3. Click on `Security & compliance`
4. Click on `Review in Entra`



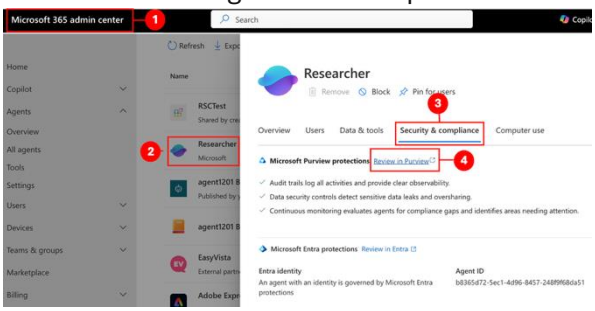


In the Entra admin portal, admins can easily monitor granular agent activity and limit agents' access to on the resources they need, and prevent agent compromise with risk-based conditional access policies. Learn more

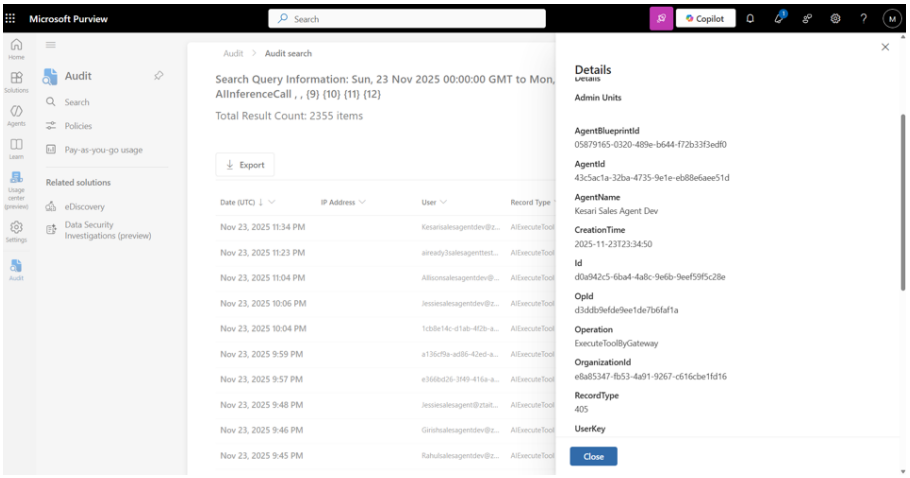
Data security with Microsoft Purview: Purview supports secure by default capabilities including audit trails that log agent activities, data security controls to detect sensitive data in agent interactions, compliance monitoring to evaluate agents for gaps and identify opportunity areas.

With secure by default capabilities, IT admins in MAC can understand the agent's aggregated activities, sensitive data interactions, and AI baseline assessment. These insights can be expanded upon engagement with the data security admin through the Microsoft Purview portal. To view an agent's Purview protections,

1. In the MAC's left side navigation, `Agents => All Agents`.
2. Then click on the relevant agent
3. Click on `Security & compliance`



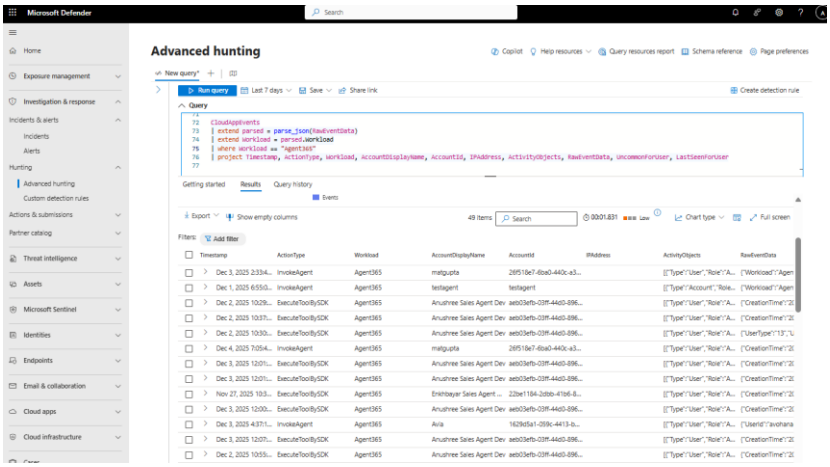
4. Click on `Review in Purview`



In the Purview admin portal, admins can easily monitor agent activity through unified audit trails. These logs provide visibility into key actions, including agent invocations, tool executions, and inference calls, helping ensure compliance and security. Learn more

Threat protection with Microsoft Defender: Agent 365 provides observability in Defender across all agent activities, allowing security teams to monitor and trace behaviors from a centralized location. Microsoft Defender provides out-the-box threat detections in case of malicious activities and allows customers to create custom detections on agent activities. Learn more

1. In the MAC's left side navigation, `Agents => All Agents`.
2. Then click on the relevant agent
3. Click on `Security & compliance`
4. Click on `Review in Defender`



In the Microsoft Defender admin portal, you can investigate and respond to threat incidents involving AI agents. Learn more

Primary persona: Agent Developer

Interoperability (Data & Tools)

Agent 365 tooling servers are enterprise-grade Model Context Protocol (MCP) servers that give agents safe, governed access to business systems such as Microsoft Outlook, Teams, SharePoint,

OneDrive, Dataverse, and more. Builders can use these servers from the Agent 365 SDK, Copilot Studio, or pro-code frameworks to add deterministic, auditable "tools" to any agent. Key features

- Centralized governance: IT admins manage MCP servers in the MAC, allowing or blocking servers across the organization.
- Enterprise grade security: Scoped permissions with Entra Agent ID, policy enforcement, and runtime observability ensure agents operate within compliance boundaries.
- Agent notifications: the Notification Module enables developers to build agents that can respond to events and notifications from Microsoft 365 applications. With notifications support, agents can receive and process alerts when users interact with them through email, document comments, or other collaborative scenarios.
- Continuous evaluation: All MCP servers undergo rigorous testing across diverse datasets and models, measuring: Accuracy, Latency, Reliability
- Integrated developer experience: Tooling infrastructure is built into Agent 365 SDK, Foundry SDK, and Copilot Studio. Learn more

To meet the minimum bar of A365 enablement, an agent needs to be (1) part of the A365 registry and needs to be (2) observable. Not all agents will require advanced M365 data and tools capabilities. As a result, integration with A365 data and tools is not required.

How to enable an agent to be Agent 365 compatible

1. Agent 365 SDK

Use the **Agent 365 SDK** to extend agents built using any agent SDK or platform, with enterprise grade identity, observability, notifications, security, and governed access to Microsoft 365 data.

Agents have unique identities. People invoke them using common gestures (such as @mentions) in apps that enterprise users typically operate in (such as Teams, Word, Outlook, and more). They demonstrate observable behaviors that build trust, take auditable actions, and do so via secure access to tools and data.

With the Agent 365 SDK, agents can:

- Use Entra-backed Agent Identity with their own user resources like mailbox for secure authentication and controlled access to tools and data.
- Receive and respond to notifications from Teams, Outlook, Word comments, and emails—just like a human participant in Microsoft 365 apps.
- Gain full observability via Open Telemetry, enabling audited, traceable agent interactions, inference events, and tool usage.
- Invoke governed Model Context Protocol (MCP) servers to access Microsoft 365 workloads (for example, Mail, Calendar, SharePoint, Teams) under admin control.
- Function within an ITapproved blueprint system, ensuring each agent instance inherits compliance, governance, and security policies.

Learn more about the Agent 365 SDK.

2. Agent 365 CLI

Agent 365 CLI is the command-line backbone for Agent 365 throughout the agent development lifecycle - automating setup, identity, configuration, MCP integration, publishing, and Azure deployment for enterprise-ready agents.

With the Agent 365 CLI, developers can:

- Create agent blueprints and all supporting resources required by them.
- Manage out-of-box and custom MCP servers, permissions, and tooling for agents.
- Deploy agent code to Azure.
- Publish agent application packages to Microsoft Admin Center.
- Clean up agent blueprints, identities, and other Azure resources created by the CLI.

Learn more about the Agent 365 CLI

FAQ

Is Agent 365 an AI agent or an agent creation tool?

Agent 365 itself is *not* an AI agent nor a tool to build agents – rather, it is the infrastructure layer that secures, governs, and augments agents. Agent 365 is analogous to how IT is currently securing, managing and controlling users in their M365 environment. Once you have an AI agent, Agent 365 helps you wrap the agent with an identity, security policies, compliance controls, administrative oversight, as well as Microsoft 365 app access.

- A365 is agent-agnostic; it's compatible with Microsoft agents and agents built by other organizations.
- A365 is agent creation platform-agnostic; it is compatible with agents built using Microsoft tools and platforms like Copilot Studio, Foundry, Agent SDK and third-party creation tools and platforms like Claude SDK and the Manus AI agent.

Who is Agent 365 designed for?

Agent 365 is designed for organizations that are adopting AI agents and need to securely manage them at scale. The solution primarily speaks to IT leaders (CIOs, CTOs, CISOs) responsible for enabling new technology while protecting the enterprise.

What is the business model and pricing structure for Agent 365?

The business model has not been announced. Microsoft aims to gather feedback and information before finalizing packaging and pricing to ensure this new offering will meet the dynamic needs of customers and a rapidly evolving agent landscape.

When will A365 be GA?

We do not have a date yet, though we hope to GA in the first half of CY26.

How does Agent 365 differentiate from other agent management solutions?

Microsoft's advantage with Agent 365 comes from the broad integration of identity, security, and productivity apps under one roof. Unlike point solutions, Agent 365 is built on top of Microsoft Entra Agent ID, which is a part of our unified identity platform for all users, and the Microsoft 365 productivity platform that organizations already use. It uniquely enables AI agents to have an identity in your corporate directory and integrate with your everyday tools and security policies. For example, third-party "AI agent management" products might offer logging or monitoring, but they lack tight integration with Office apps, or they require complex connector setups for identity. Agent 365's differentiation is that it owns the identity layer (Entra agent ID), offers deep native integration with agent development platforms, and provides out-of-the-box access to the world's most widely used productivity suite (M365). Additionally, Microsoft brings to bear its comprehensive security stack: Purview, Defender, Entra, all extended to agents with purpose-built capabilities in Agent 365. In summary, Agent 365 offers a single-source, end-to-end solution for enterprise agent management that others cannot match: it covers identity, apps, data, and security in one package

Resources

Team	PoCs
Agent 365 PG LT	• A365 Product Owner: Nirav Shah • A365 Control System: Ray Smith, Satish Krishnan, Scott Rosemund • A365 Data & Tools: James Oleinik, Gio Della-Libera • A365 Foundations: Mauktik Gandhi • A365 Ecosystem: Monica Ugwi
Security PG	• Neta Haiby, Moran Gutman, Assaf Yatziv (Defender), Diana Smetters (Entra)
CxE	• Saurabh Pant, Nasos K.
PMM	• Irina Nechaeva, Caroline Stanford, Richard Riley
Field Enablement	• Michelle Lancaster, Sachin Gupta

- Office Hours: Weds - alternating 9:00a & 5:00p PST
- Learn site: aka.ms/A365mslearn
- Microsoft Agent 365 Pitch deck & demos: Pitch Deck - Agent 365.pptx, Ignite demos
- Provide Feedback to Agent 365 PG: aka.ms/ Agent365Feedback
- Agent 365 Seismic

Appendix

- Agent 365 Field Advisory document
- Agent 365 Field FAQ