Get started

With Microsoft Agent 365 in Microsoft 365 admin center

Microsoft

What is Microsoft Agent 365?

Agent 365 is the control plane that gives IT and security leaders confidence to move from agent experimentation to enterprise-scale operations. It delivers a comprehensive framework to observe, secure, and govern agents across the organization, and empowers IT along with Security practitioners to stay in control as agents get embedded into business processes. Agent 365 extends the existing management, security, and governance processes and solutions you use for employees to agents, embedding purpose-built controls for agents directly into Microsoft Admin Center for agent management, and Microsoft Security solutions – Defender, Entra, and Purview for agent security and governance.

Who is this guide for

Microsoft 365 admins responsible for agent discovery, lifecycle management, and governance within the admin center.

This guide highlights key steps to get started. For a comprehensive end to end deployment of Agent 365 visit Microsoft Agent 365 documentation | Microsoft Learn.

Prerequisites

- A Microsoft 365 tenant with access to agent management features.
- Admin permissions to manage agents in the Microsoft 365 admin center.
- Premium Agent 365 features require an Agent 365 license.

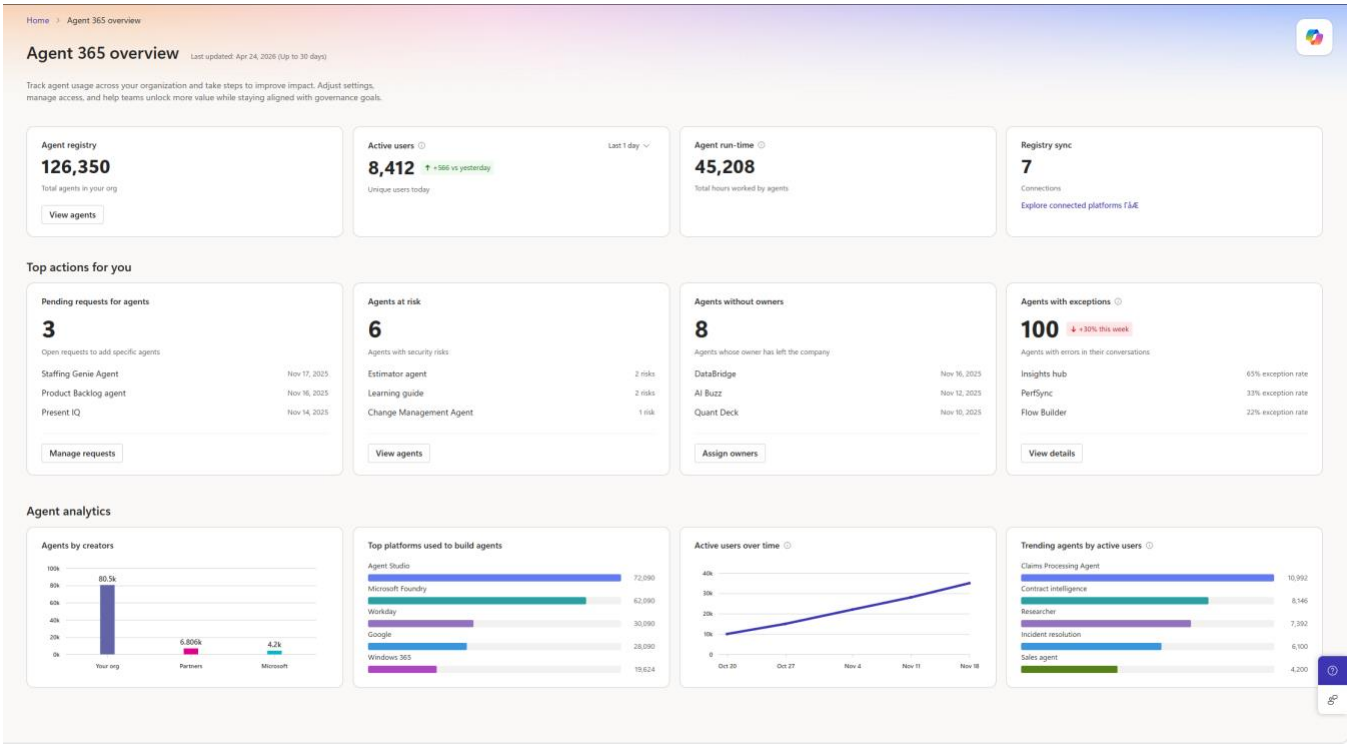
Table of Contents

View agent analytics (Overview)

Goal: Identify and act on critical governance tasks by using actionable insights from the Agent overview dashboard to maintain compliance, mitigate risk, and ensure agents are properly managed across the organization.

1. Navigate to Microsoft 365 admin center and sign in.
2. From the left navigation, go to **Agents > Overview.**
3. Review the **Agent overview dashboard,** which provides a centralized, up to 30-day snapshot of agent usage and health.
4. Analyse **key metrics (hero metrics),** including:
   - **Active users** – Unique users interacting with agents.
   - **Total sessions** – Completed agent interactions.
   - **Agent run-time** – Total time agents are used.
   - **Exception rate** – Percentage of sessions completed without errors.
5. Identify **trends, high-impact agents, and governance signals,** including alerts, exceptions, and areas requiring admin attention. [learn.microsoft.com]
6. **Act directly from the dashboard,** such as approving requests, managing agents with alerts, or addressing exceptions surfaced in the overview.

Validate: Agent overview dashboard provides a centralized control plane to track usage, assess agent health and reliability, surface governance signals, and take action across your agent ecosystem. Learn more about Agent Overview

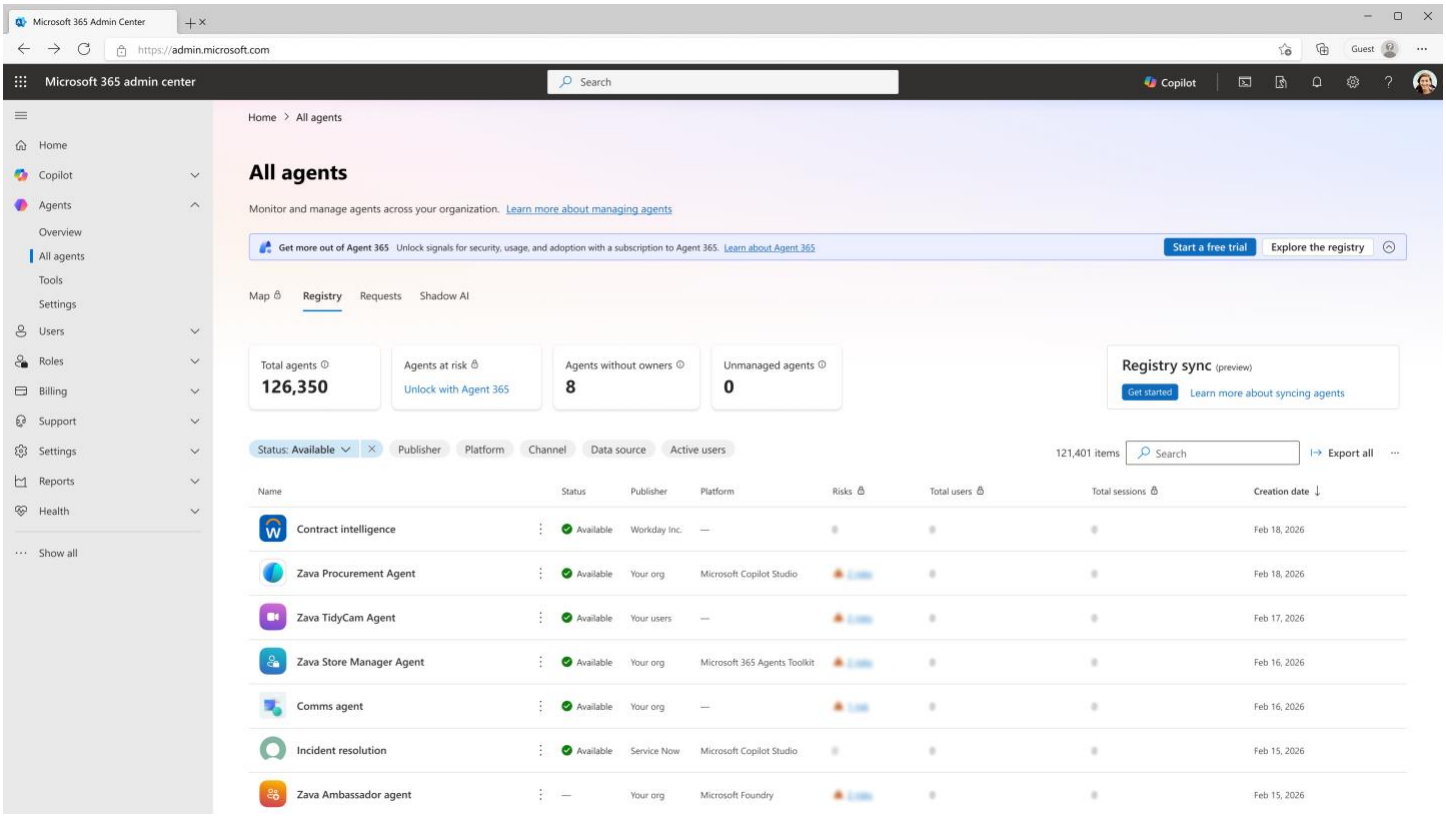


Discover agents (Agent Registry)

Goal: Get a complete inventory of agents in your tenant and understand how to explore them.

1. Navigate to https://admin.microsoft.com and sign in.
2. In the left navigation, select **Agents > All agents > Registry > explore all agents.**
3. Review the **full agent inventory** surfaced in the registry.
4. Use **Filters** to explore agents by **Status, Publisher Type, Channel, Platform,** and **Data source.** For example, filter by Publisher Type to identify Microsoft, external partner, and internally created agents.

Validate: You can see a centralized list of agents in your tenant and can filter views. Learn more about Agent Registry.

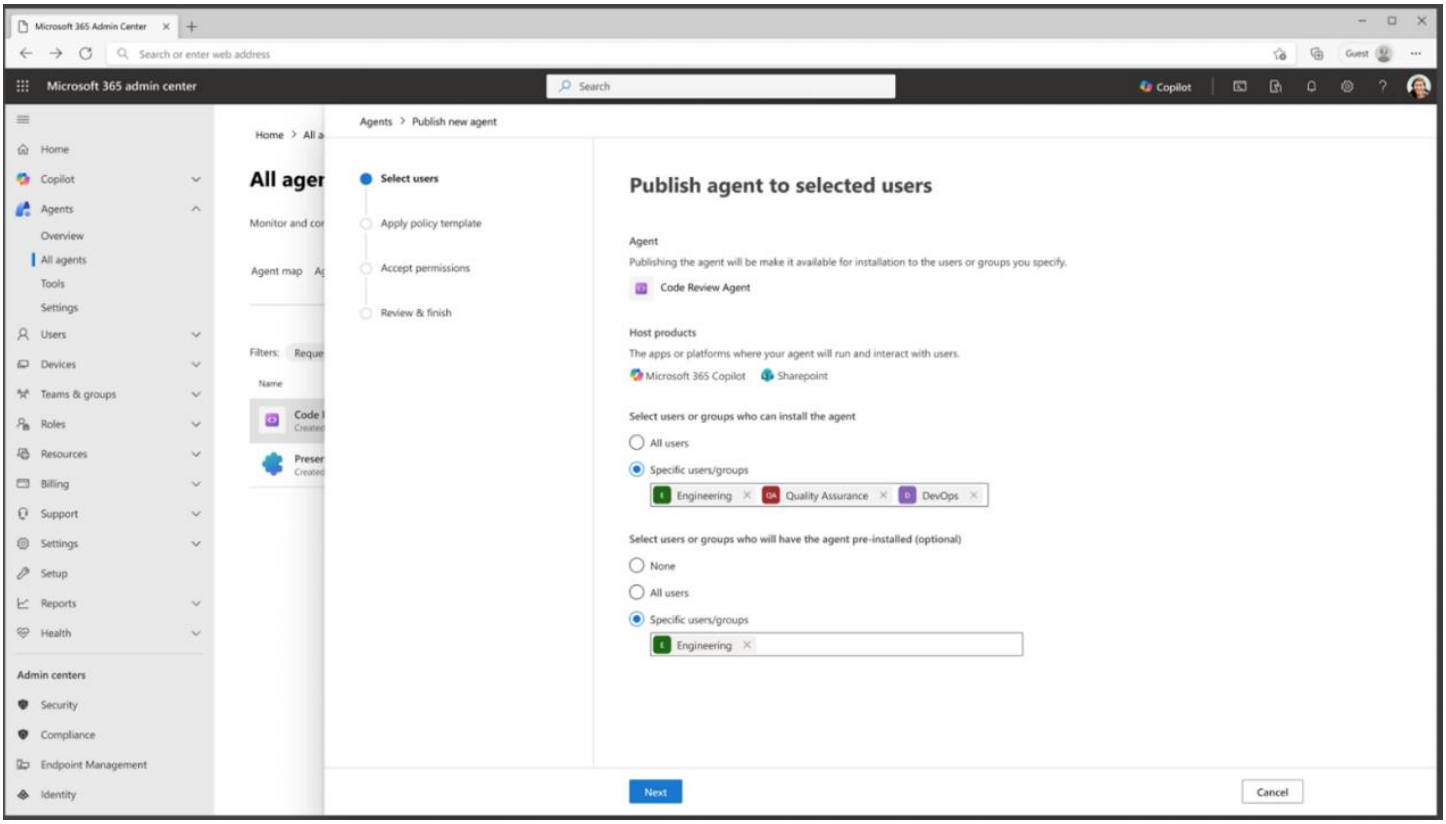


Review and publish agents

Goal: Review requested agents and approve or reject agents, then define which users can access them.

1. Navigate to https://admin.microsoft.com and sign in with an admin account.
2. Go to **Agents > All agents > Requests.**
3. Select an agent request, then choose **Publish to store.**
4. On **Publish agent to selected users,** select who can install the agent (for example, **All users** or a pilot group), then select **Next.**
5. On **Apply security template,** select the template you, then select **Next.**
6. Complete **Review permissions,** then select Publish and Done.

Validate: The agent appears in the registry with the expected published/deployment state. Learn more about Publishing agents.

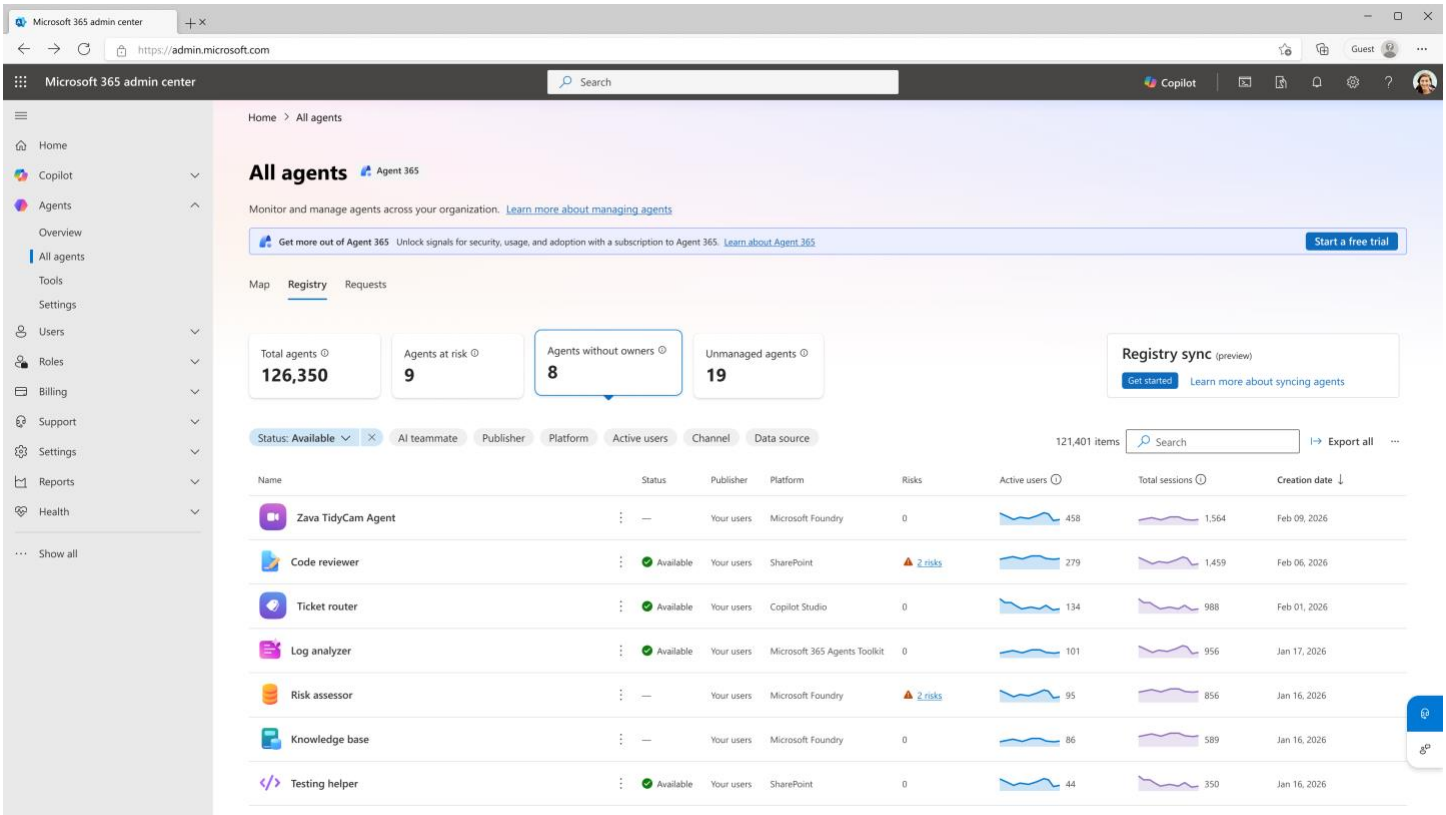


Review ownerless agents

Goal: Identify agents without owners and determine appropriate governance actions (assign or review).

1. Navigate to https://admin.microsoft.com and sign in with an admin account.
2. Go to **Agents** > **All agents** > **Registry,** then filter or identify ownerless agents.
3. Open and ownerless agent to review details such as status, publisher, platform, and last updated.
4. Confirm whether the agent requires ownership assignment or further action.
5. Close the agent details pane when finished.

Validate: You can identify ownerless agents and review key details to determine appropriate governance actions. Learn more about Ownerless shared agent management.

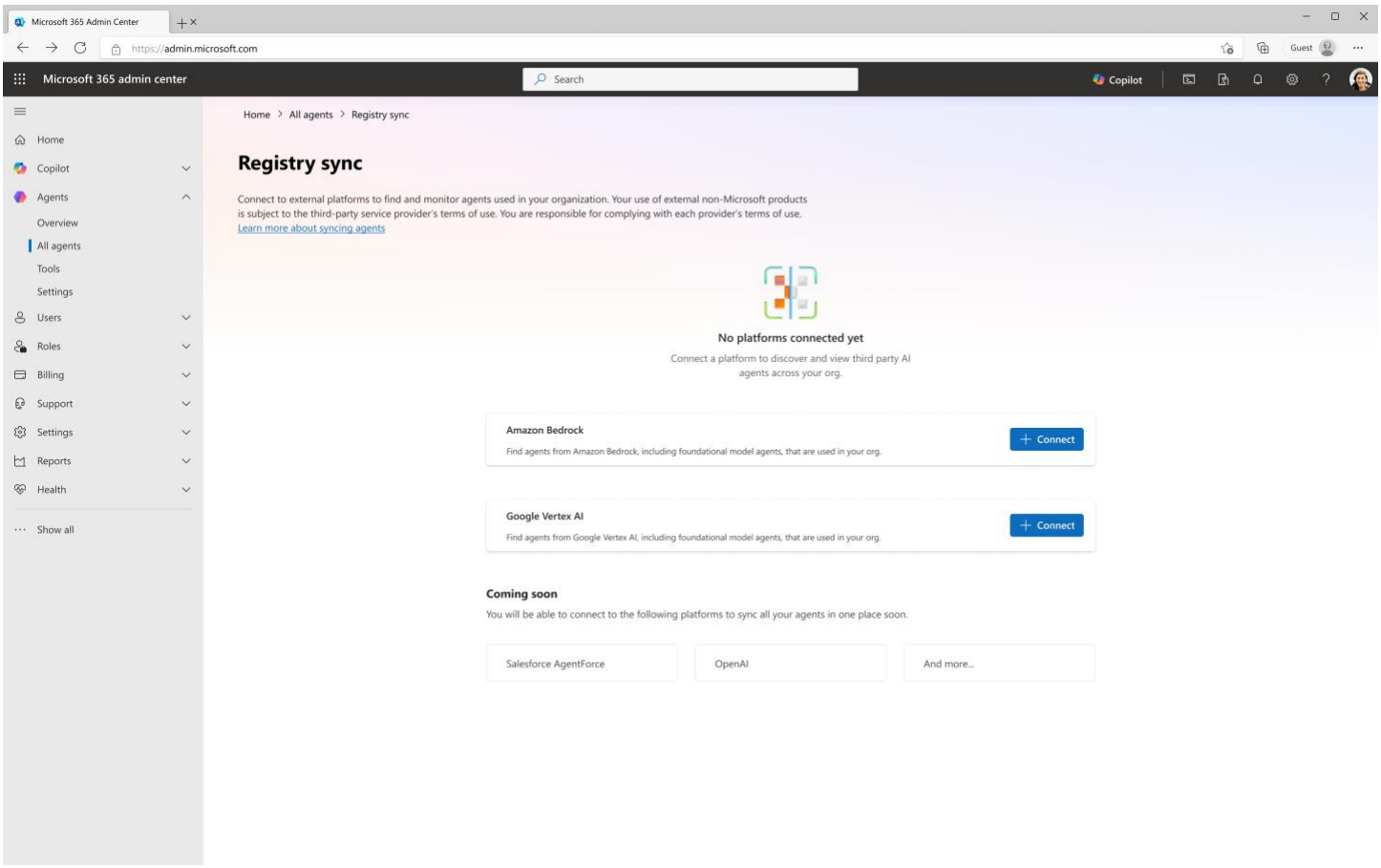


Connect external platforms (Registry sync)

Goal: Connect external platforms to discover and include third-party agents in the Agent Registry.

1. Navigate to https://admin.microsoft.com and sign in.
2. Go to **Agents > All agents > Registry sync.**
3. Review **available platforms** (for example, Amazon Bedrock, Google Vertex AI).
4. Select Connect for a platform you want to onboard.
5. Follow the connection flow to authorize and establish integration.
6. Return to the Agent Registry to review imported agents.

Validate: You can connect external platforms and ensure agents from those platforms are visible in the registry.

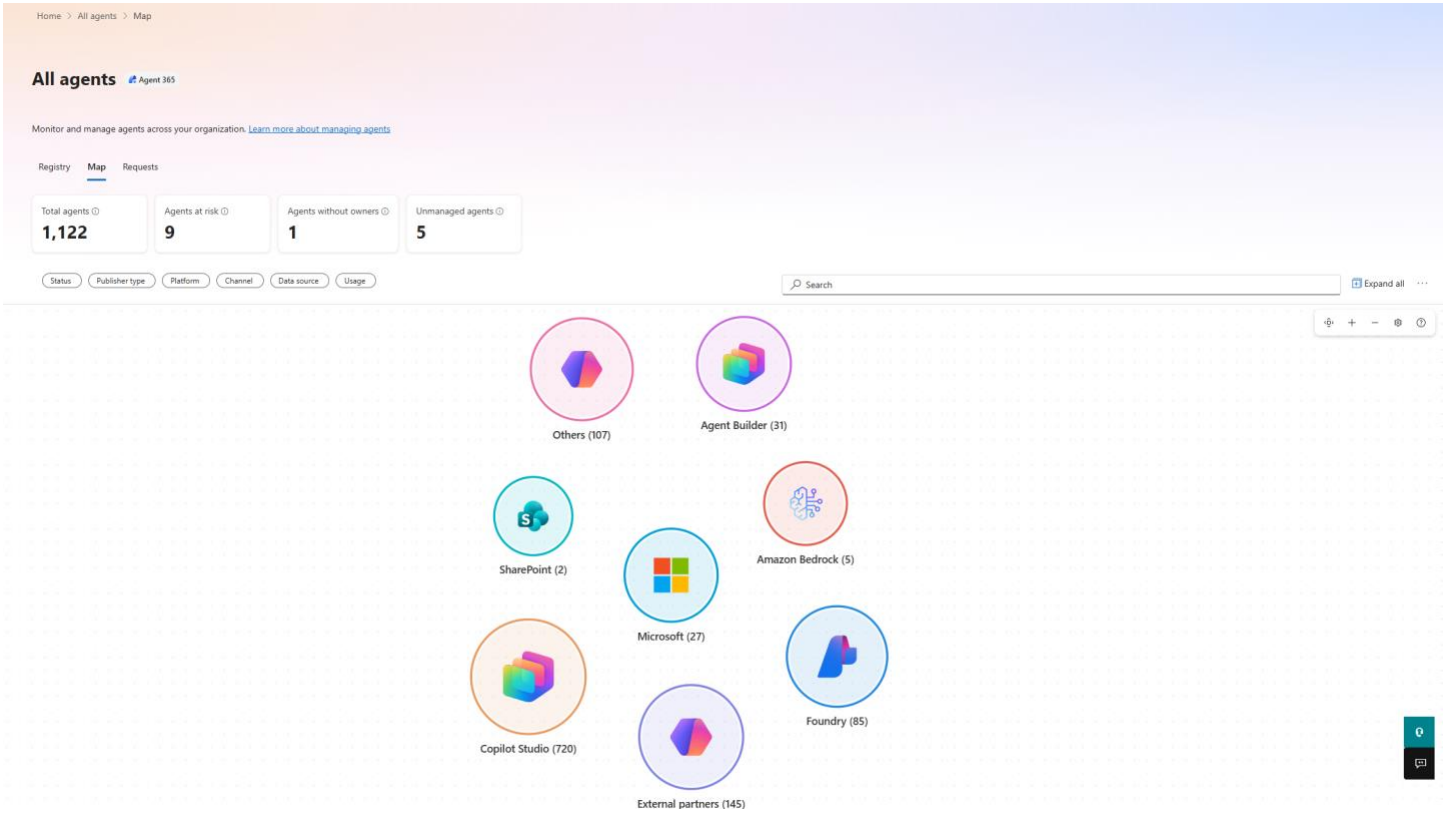


Visualize agent relationships (Agent map)

Goal: Understand how agents are organized and connected across your environment and explore how they relate to one another as part of a broader ecosystem.

1. Navigate to https://admin.microsoft.com and sign in.
2. Go to **Agents** > **All agents,** then select **Map** (if available).
3. Review the map to see agents grouped by platform or publisher, and explore clusters (for example, Microsoft or external partners).
4. Zoom or pan to focus on specific groups, then select an agent to open its details panel.

Validate: You can open an agent's details panel directly from the map and understand how agents are grouped and connected across your environment, including how they relate to other agents. Learn more about Agent map.

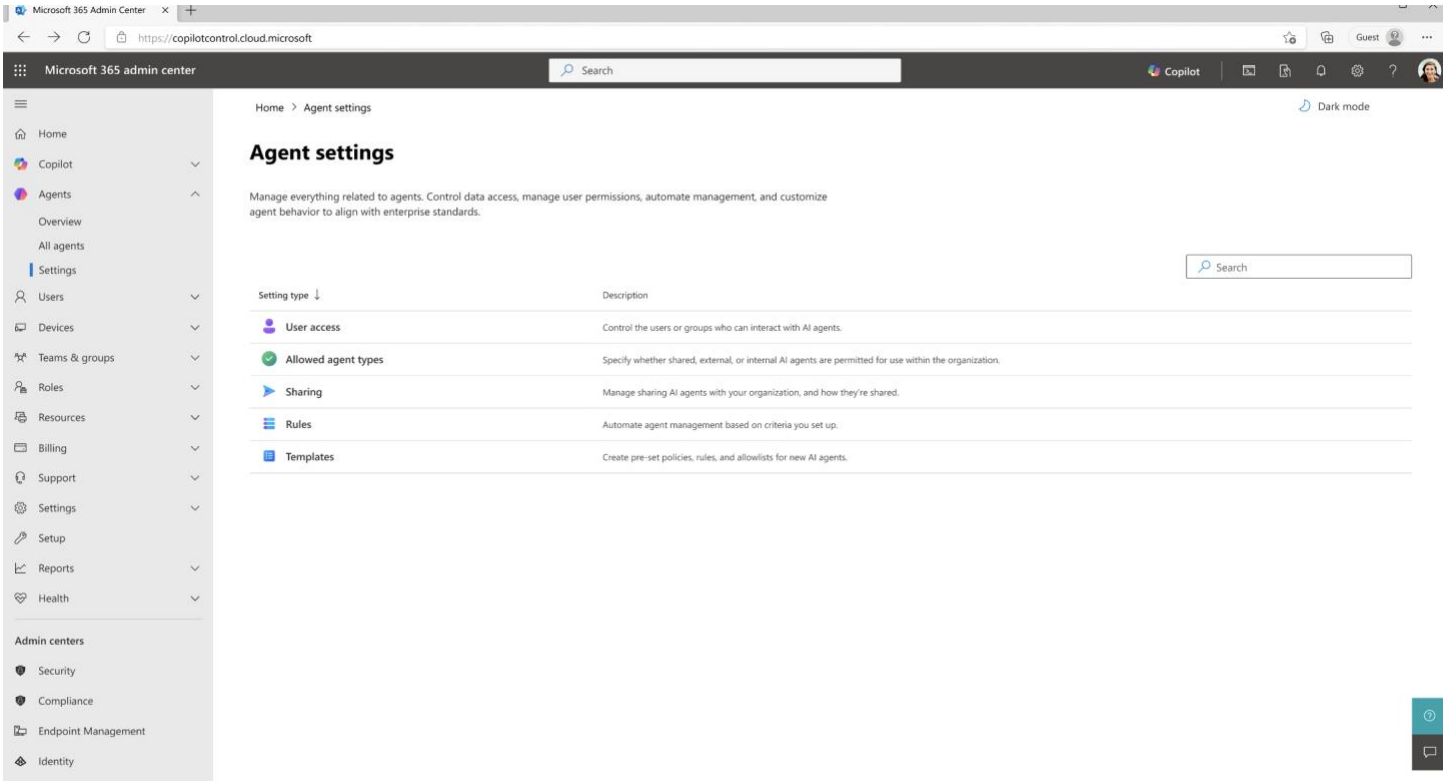


Configure agent settings

Goal: Configure governance, access, and policy settings to control how agents are used across your organization.

1. Navigate to https://admin.microsoft.com and sign in.
2. Go to Agents > **Settings**.
3. Review available settings, including:
   - **Allowed agent types** – Control which agents users can view and install (Microsoft, internal, or external)
   - **Sharing** – Control who can share agents and how broadly they can be shared.
   - **Templates** – Define and apply default governance and security policies for new agents.
   - **User access** – Control which users or groups can access and use agents.
4. Select a setting (for example, Allowed agent types or Sharing) and review current configuration.
5. Update settings as needed to align with your organization's governance and access requirements.
6. Save changes to apply updates across your tenant.

Validate: You can control which agents are available, how they are shared, and how governance policies are applied across your organization. Learn more about agent settings.

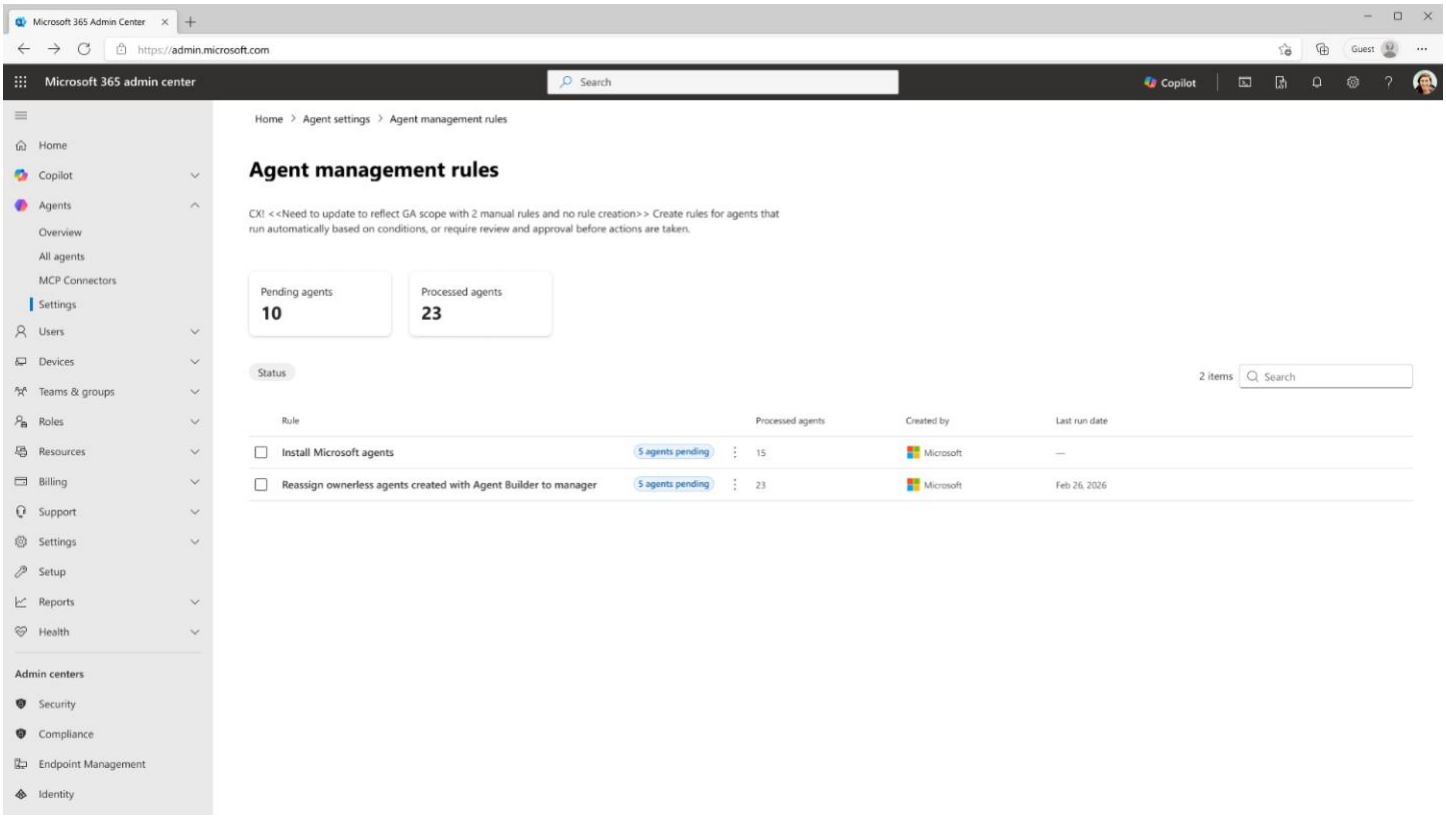


Manage agents at scale with agent management rules

Goal: Apply governance and lifecycle controls across agents using rule-based bulk actions to reduce manual effort and maintain consistency.

1. Navigate to https://admin.microsoft.com and sign in.
2. Go to **Agents** > **Settings** > **Agent management rules.** Agent Management Rules currently support the following governance scenarios:
   - Install Microsoft agents
   - Reassign ownerless agents created with Agent Builder to manage
3. Review available rules and select a rule.
4. Define rule conditions to identify applicable agents.
5. Preview impacted agents before execution.
6. Run the rule to apply governance actions across selected agents.

Validate: You can identify agents that meet defined conditions and apply governance actions in bulk, ensuring consistent compliance, ownership accountability, and deployment across your organization.

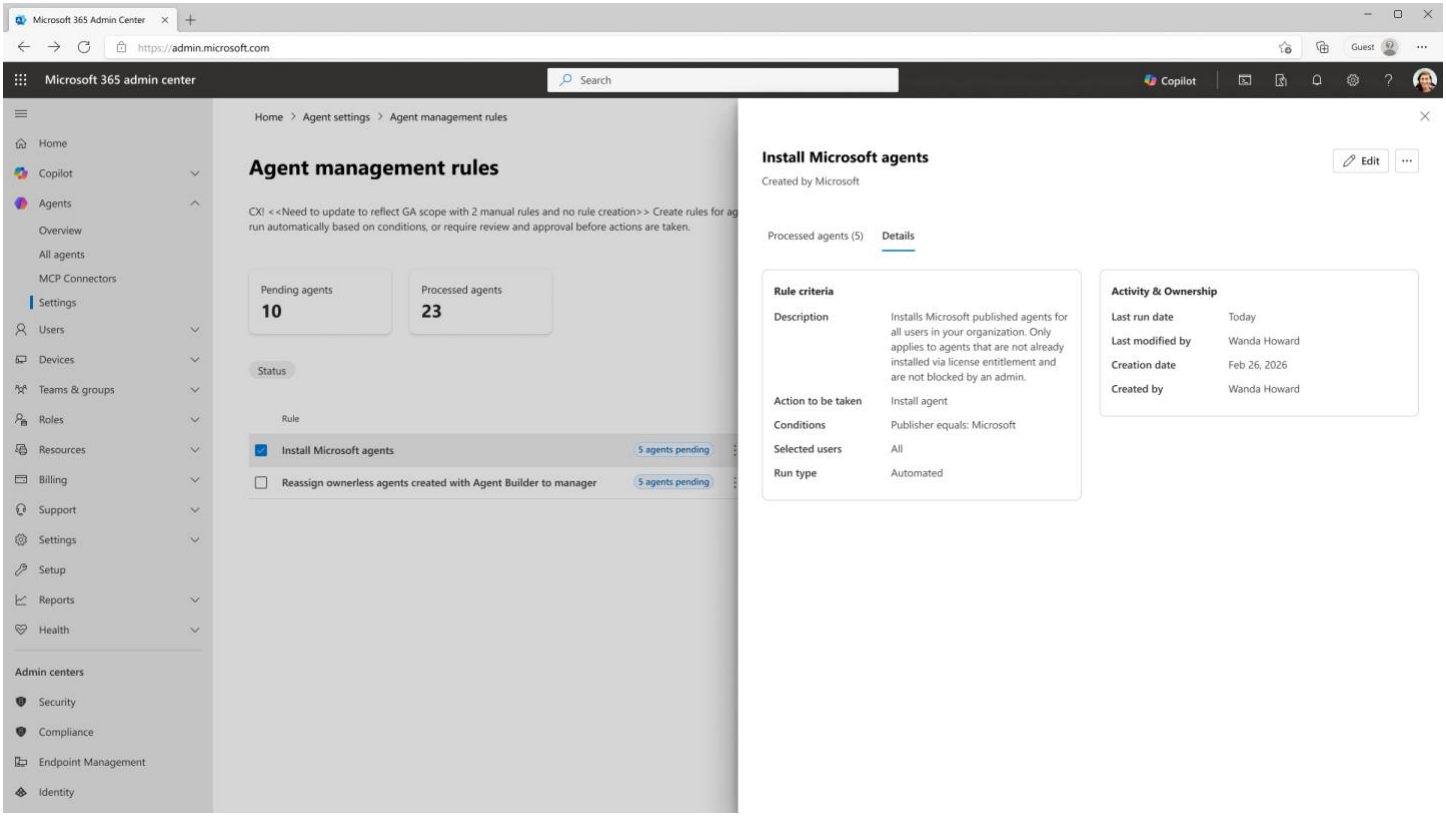


Install Microsoft agents at scale with agent management rules

Goal: Identify and install Microsoft (1P) agents across your tenant using a bulk action.

1. Navigate to https://admin.microsoft.com and sign in.
2. Go to **Agents** > **Settings** > **Agent management rules.**
3. Select the **Install Microsoft agents rule.**
4. Identify Microsoft published agents within the tenant.
5. Review eligible agents prior to installation.
6. Install selected agents for all users through a single bulk action.

Validate: Microsoft agents appear as installed and are readily available for end-users in the organization.



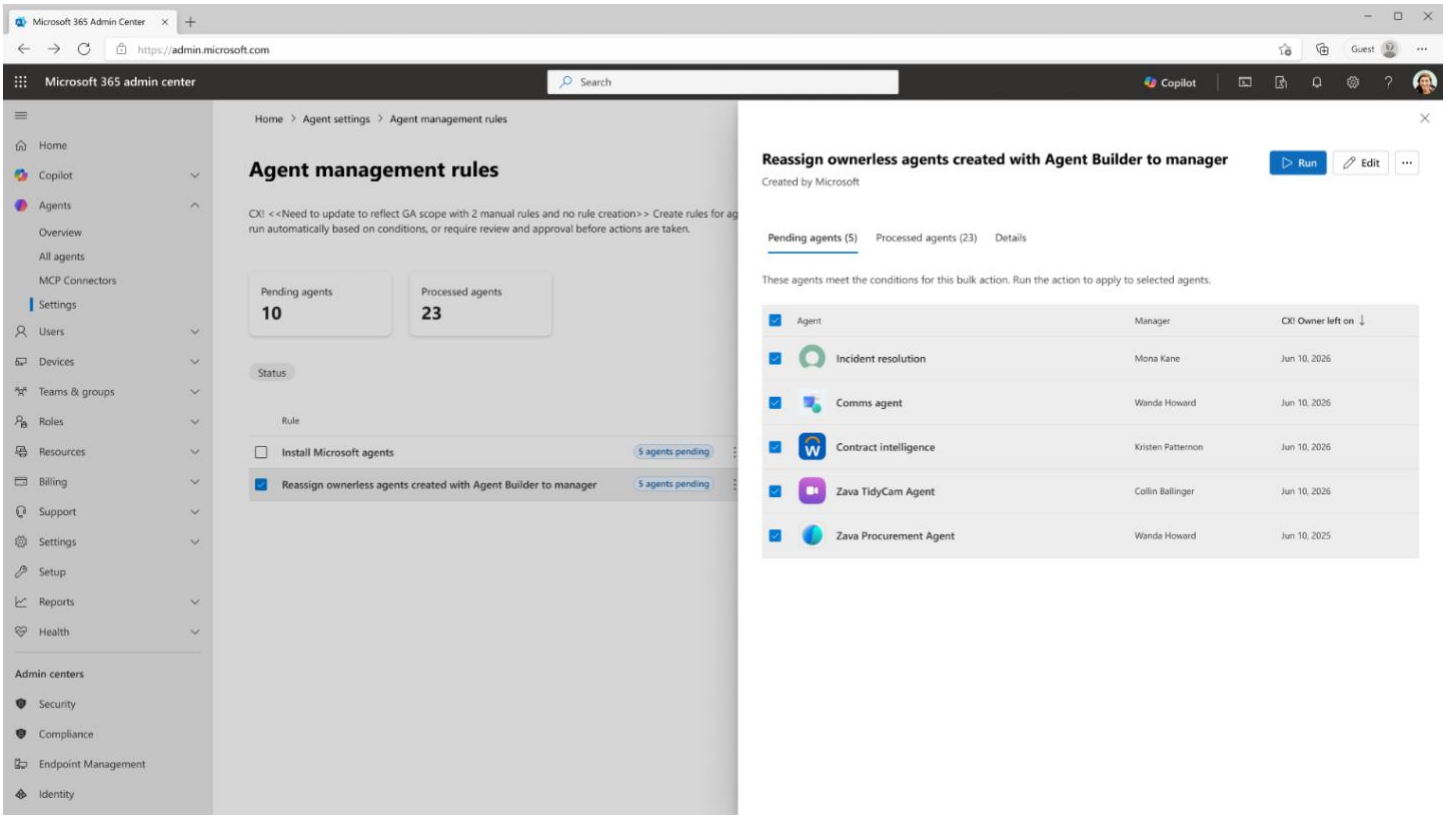
Reassign ownerless agents at scale with agent management rules

Goal: Reassign ownership of agents that no longer have a valid owner to maintain governance and accountability.

1. Navigate to https://admin.microsoft.com and sign in.
2. Go to **Agents > Settings > Agent management rules.**
3. Select the **Reassign ownerless agents rule.**
4. Identify agents that do not have a valid owner.
5. Review impacted agents prior to reassignment.
6. Run the rule to transfer ownership to the manager of the previous owner based on Microsoft Entra ID hierarchy.

Note: This rule is only supported for agents created using Microsoft 365 Copilot Agent Builder.

Validate: Ownerless agents are reassigned, ensuring continued ownership, accountability, and lifecycle governance.



Create and apply an agent security template

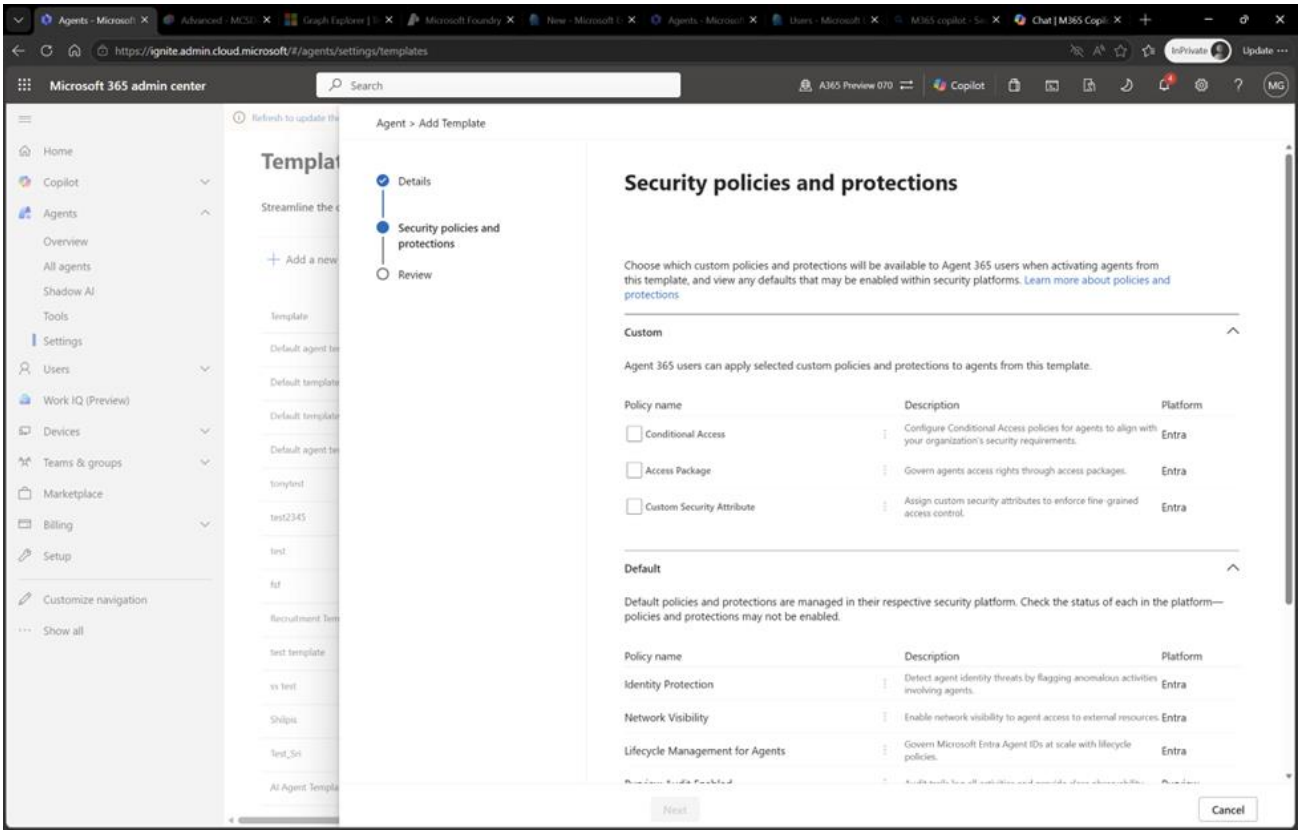
Goal: Define reusable governance controls and apply them consistently when publishing agents.

1. Navigate to https://admin.microsoft.com and sign in with an admin account.
2. Go to **Agents** > **Settings** > **Templates.**
3. Select **Add a new template.**
4. For **What agents can use this template?** Choose the appropriate scope (example: **No instances** while you're authoring).
5. Enter a **Template name** and description, then select **Next**.
6. On **Security policies and protections,** select the controls you want to bundle (for example, a Conditional Access policy, an access package, and a custom security attribute value), then select **Next**.
7. Select **Save template**, then **Finish**.

Validate: The new template appears in the template list and can be selected during agent publishing. Learn more about agent templates.

Note: To create a template, ensure the following prerequisites are met:

1. Create all required policies in Entra before creating a template.
2. Ensure both Global Admin and AI Admin have the Attribute Definition Administrator role for custom security attributes.
3. AI Admin can create and apply access packages but doesn't have privileges for Conditional Access.

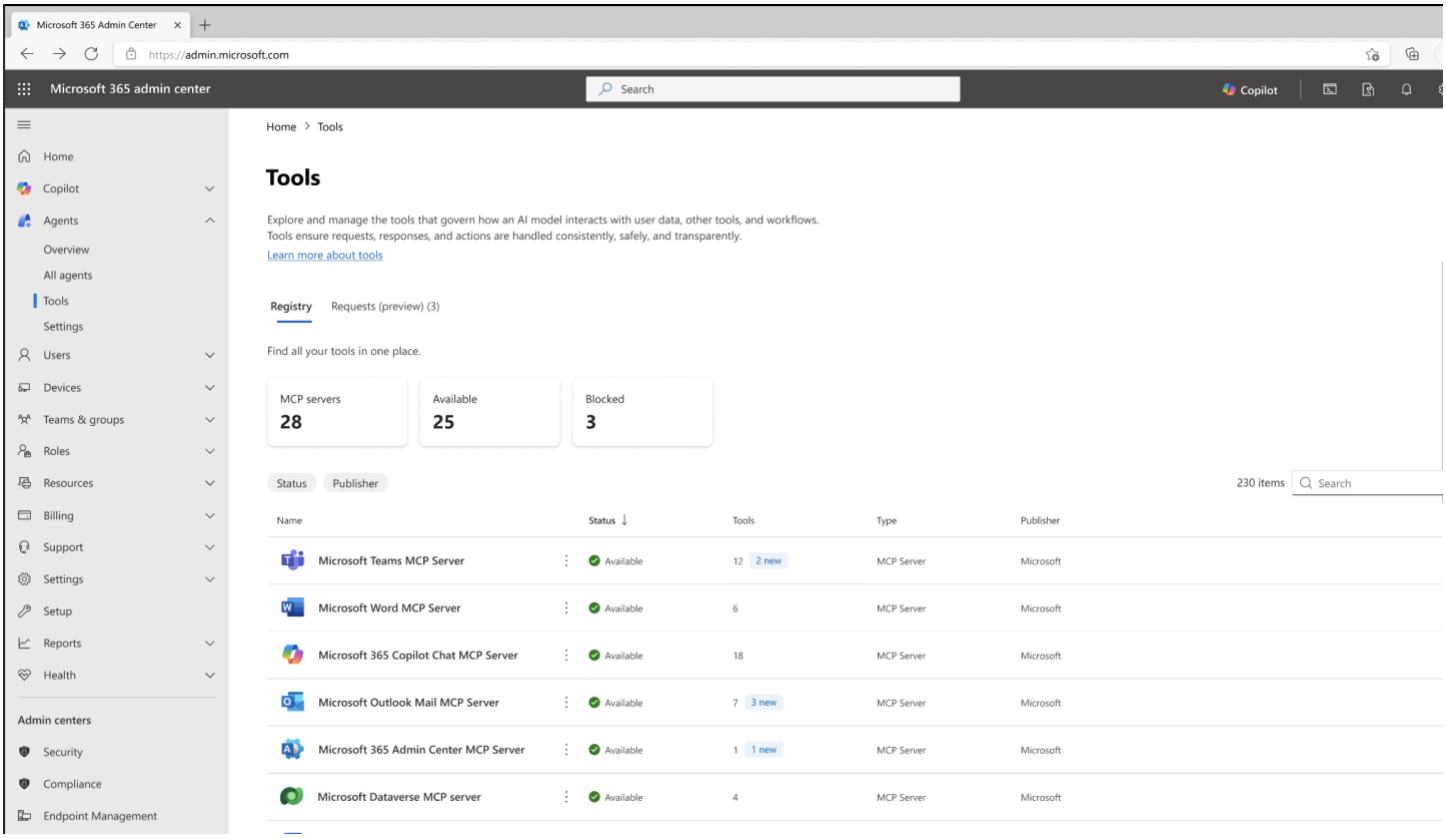


Explore agent tools

Goal: Access and use available tools to manage, extend, and operate agents across your tenant.

1. Navigate to https://admin.microsoft.com and sign in.
2. Go to **Agents >Tools.**
3. Review available tools, which represent services agents can use (for example, Teams, Outlook Mail, SharePoint, OneDrive, and Calendar).
4. View tool details, including status (Available or Blocked), type, and publisher.
5. Use filters to explore tools by status, type, or publisher.
6. Select a tool to block or unblock access based on your organization's requirements.

Validate: You can view and control which tools agents can use to interact with apps, data, and workflows across your organization. Learn more about agent tools.

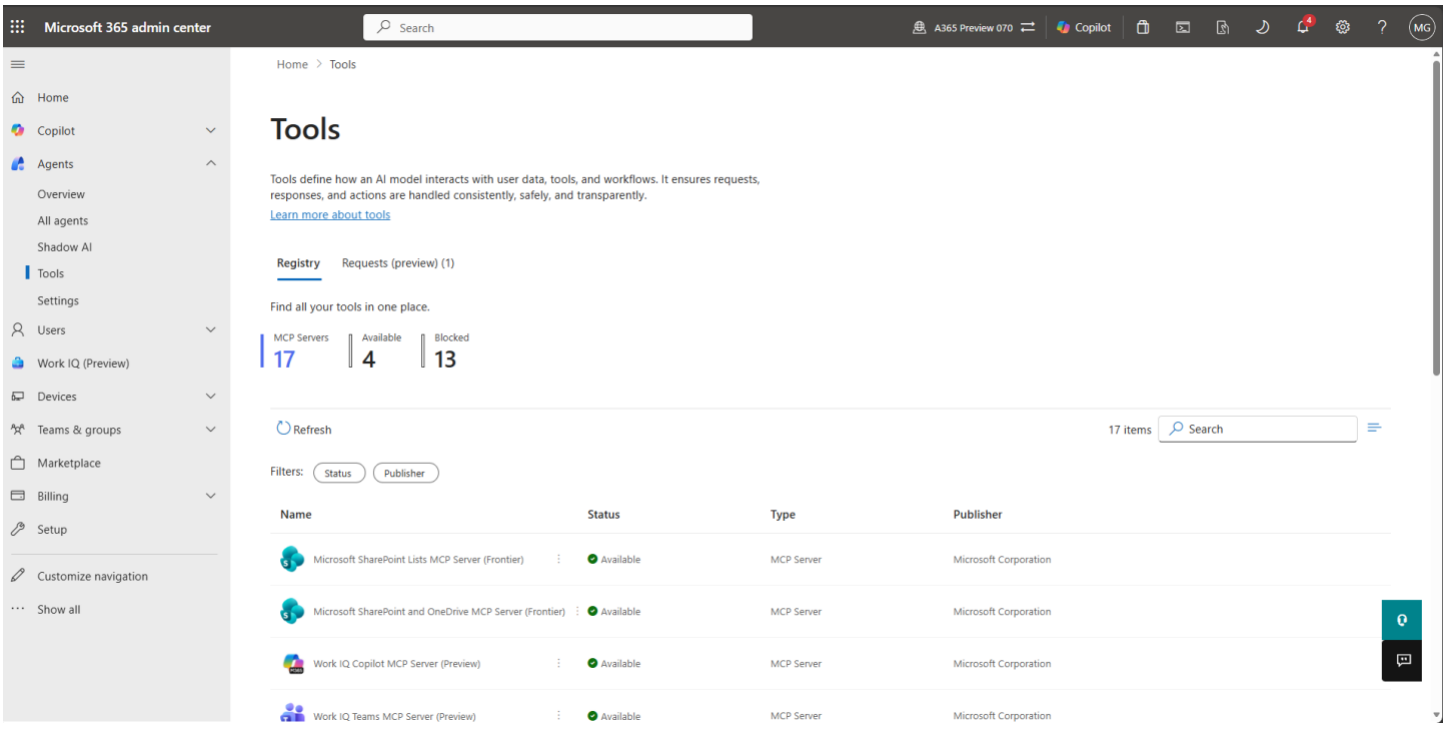


Bring your Own MCP server (Preview)

Goal: Enable organizations to register and govern custom MCP servers with Agent 365, ensuring centralized review, approval, and visibility.

1. Navigate to the Microsoft 365 Admin Center.
2. Go to **Agents** > **Tools** and select the **Requests** tab.
3. Pending requests display the following details for each server:
   - Server name
   - Publisher
   - Requested by
   - Requested date
4. Validate server details and declared tools for compliance and accuracy.
5. Select Approve to add the server to the organizational registry or Reject to deny the request.
6. Upon approval, complete required Entra permission consent for the MCP server.

Validate: Approved MCP servers are available for use in agent-building surfaces and governed through the centralized registry.



View Shadow AI (Preview)

Goal: Review unmanaged AI agents used within your tenant and take action to govern them.

1. Navigate to https://admin.microsoft.com and sign in.
2. Go to Agents > Shadow AI.
3. View a list of available shadow agents that can be detected and blocked.
4. Take action by applying security policies to monitor and or block shadow Agents
5. View a list of which managed devices these agents are running on within your organization.

Validate: You can view, monitor and block shadow agents within your tenant.