

Get started

*With Microsoft Agent 365 in
Microsoft 365 admin center*



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

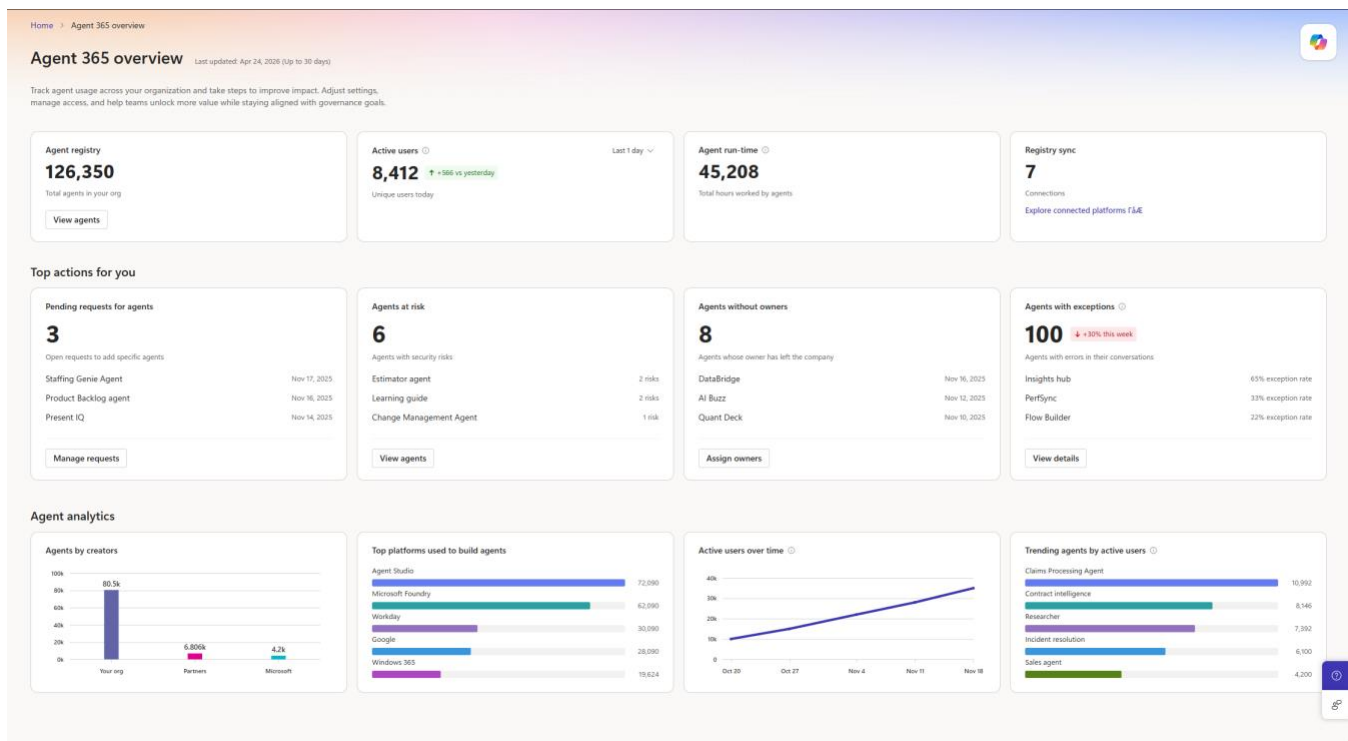
View agent analytics (Overview)	4
Discover agents (Agent Registry)	5
Review and publish agents	6
Review ownerless agents	7
Connect external platforms (Registry sync).....	8
Visualize agent relationships (Agent map).....	9
Configure agent settings	10
Manage agents at scale with agent management rules	11
Install Microsoft agents at scale with agent management rules	12
Reassign ownerless agents at scale with agent management rules	13
Create and apply an agent security template	14
Explore agent tools	15
Bring your Own MCP server (Preview)	16
View Shadow AI (Preview).....	17

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](#).

The screenshot shows the Microsoft 365 Admin Center interface for the Agent Registry. The left sidebar contains navigation options like Home, Copilot, Agents, Overview, All agents, Tools, Settings, Users, Roles, Billing, Support, Reports, and Health. The main content area is titled 'All agents' and includes a search bar and a 'Registry sync' button. Below this, there are summary cards for 'Total agents' (126,350), 'Agents at risk' (0), 'Agents without owners' (8), and 'Unmanaged agents' (0). A filter bar allows selection by Status (Available), Publisher, Platform, Channel, Data source, and Active users. The main table lists agents with columns for Name, Status, Publisher, Platform, Risks, Total users, Total sessions, and Creation date. The table includes agents like Contract intelligence, Zava Procurement Agent, Zava TidyCam Agent, Zava Store Manager Agent, Comms agent, Incident resolution, and Zava Ambassador agent.

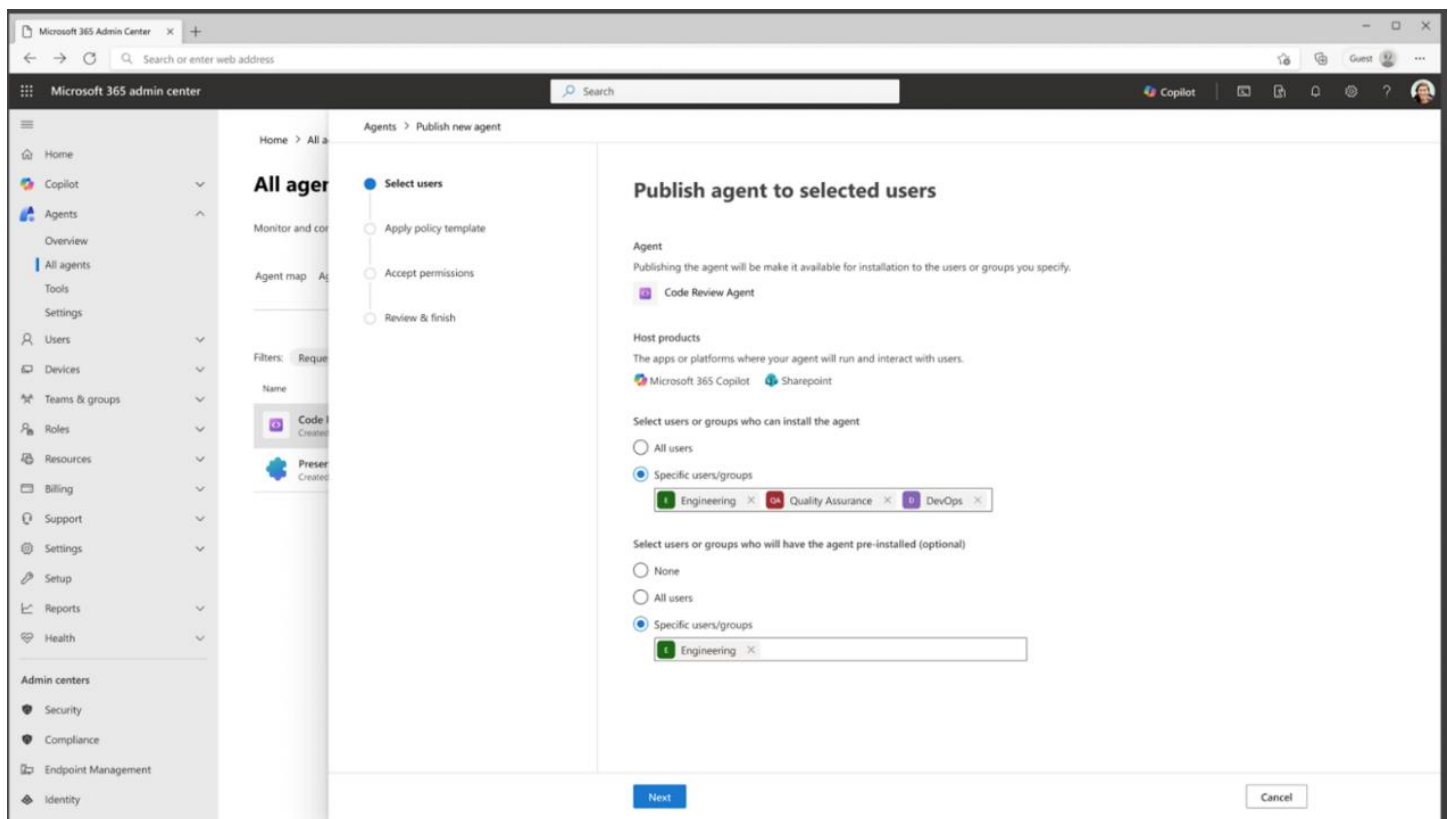
Name	Status	Publisher	Platform	Risks	Total users	Total sessions	Creation date
Contract intelligence	Available	Workday Inc.	—	0	0	0	Feb 18, 2026
Zava Procurement Agent	Available	Your org	Microsoft Copilot Studio	0	0	0	Feb 18, 2026
Zava TidyCam Agent	Available	Your users	—	0	0	0	Feb 17, 2026
Zava Store Manager Agent	Available	Your org	Microsoft 365 Agents Toolkit	0	0	0	Feb 16, 2026
Comms agent	Available	Your org	—	0	0	0	Feb 16, 2026
Incident resolution	Available	Service Now	Microsoft Copilot Studio	0	0	0	Feb 15, 2026
Zava Ambassador agent	—	Your org	Microsoft Foundry	0	0	0	Feb 15, 2026

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](#).

The screenshot shows the Microsoft 365 Admin Center interface. The main content area is titled 'All agents' and includes a summary of agent statistics. The 'Agents without owners' category is highlighted with a red box, showing 8 agents. Below the summary is a table of agents with columns for Name, Status, Publisher, Platform, Risks, Active users, Total sessions, and Creation date. The table lists several agents, including Zava TidyCam Agent, Code reviewer, Ticket router, Log analyzer, Risk assessor, Knowledge base, and Testing helper.

Name	Status	Publisher	Platform	Risks	Active users	Total sessions	Creation date
Zava TidyCam Agent	—	Your users	Microsoft Foundry	0	458	1,564	Feb 09, 2026
Code reviewer	Available	Your users	SharePoint	2 risks	279	1,459	Feb 06, 2026
Ticket router	Available	Your users	Copilot Studio	0	134	988	Feb 01, 2026
Log analyzer	Available	Your users	Microsoft 365 Agents Toolkit	0	101	956	Jan 17, 2026
Risk assessor	—	Your users	Microsoft Foundry	2 risks	95	856	Jan 16, 2026
Knowledge base	—	Your users	Microsoft Foundry	0	86	589	Jan 16, 2026
Testing helper	Available	Your users	SharePoint	0	44	350	Jan 16, 2026

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.

Microsoft 365 Admin Center

Home > All agents > Registry sync

Registry sync

Connect to external platforms to find and monitor agents used in your organization. Your use of external non-Microsoft products is subject to the third-party service provider's terms of use. You are responsible for complying with each provider's terms of use. [Learn more about syncing agents](#)

No platforms connected yet

Connect a platform to discover and view third party AI agents across your org.

Amazon Bedrock

Find agents from Amazon Bedrock, including foundational model agents, that are used in your org. [+ Connect](#)

Google Vertex AI

Find agents from Google Vertex AI, including foundational model agents, that are used in your org. [+ Connect](#)

Coming soon

You will be able to connect to the following platforms to sync all your agents in one place soon.

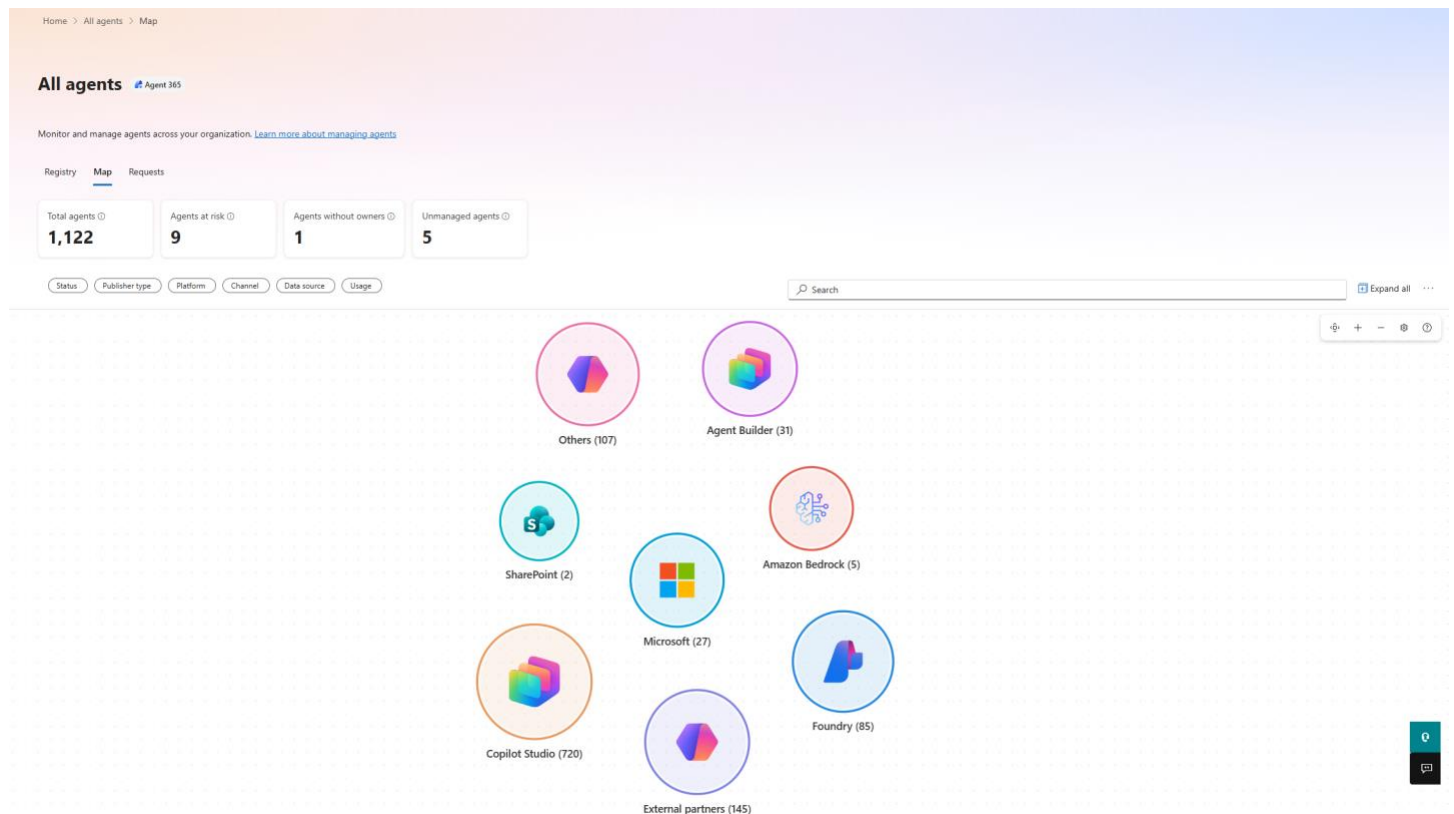
Salesforce AgentForce OpenAI And more...

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](#).

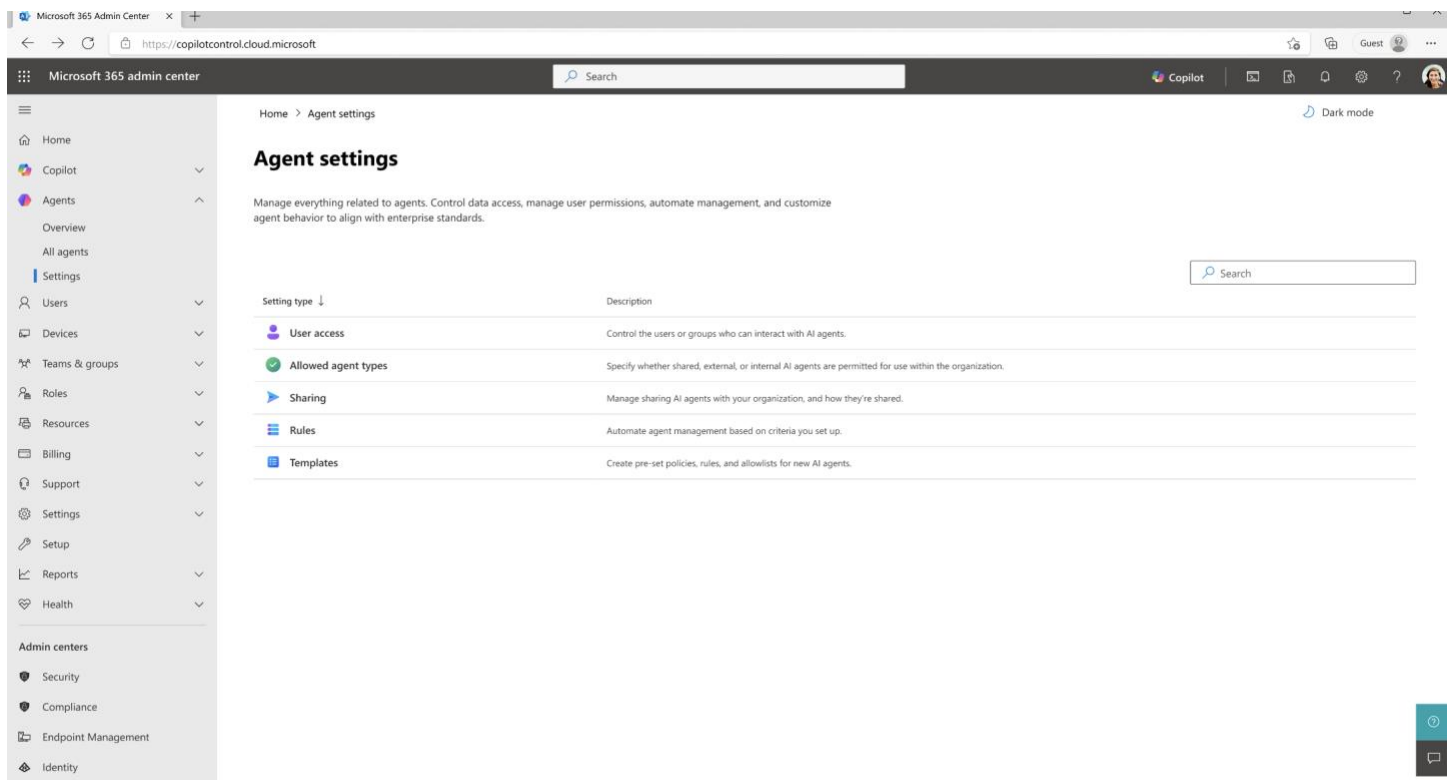


Configure agent settings

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](#).



The screenshot displays the Microsoft 365 Admin Center interface. The left-hand navigation pane includes sections for Home, Copilot, Agents, Users, Devices, Teams & groups, Roles, Resources, Billing, Support, Settings, Setup, Reports, Health, Admin centers, Security, Compliance, Endpoint Management, and Identity. The main content area is titled "Agent settings" and contains a table of settings. The table has two columns: "Setting type" and "Description".

Setting type	Description
User access	Control the users or groups who can interact with AI agents.
Allowed agent types	Specify whether shared, external, or internal AI agents are permitted for use within the organization.
Sharing	Manage sharing AI agents with your organization, and how they're shared.
Rules	Automate agent management based on criteria you set up.
Templates	Create pre-set policies, rules, and allowlists for new AI agents.

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.

Microsoft 365 Admin Center

Home > Agent settings > Agent management rules

Agent management rules

CX! <<Need to update to reflect GA scope with 2 manual rules and no rule creation>> Create rules for agents that run automatically based on conditions, or require review and approval before actions are taken.

Pending agents: **10** | Processed agents: **23**

Status: [Filter] | 2 items [Search]

Rule	Processed agents	Created by	Last run date
<input type="checkbox"/> Install Microsoft agents	5 agents pending 15	Microsoft	—
<input type="checkbox"/> Reassign ownerless agents created with Agent Builder to manager	5 agents pending 23	Microsoft	Feb 26, 2026

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.

The screenshot shows the Microsoft 365 Admin Center interface. The main content area displays the 'Agent management rules' page. On the left, there is a navigation pane with options like Home, Copilot, Agents, Overview, All agents, MCP Connectors, Settings, Users, Devices, Teams & groups, Roles, Resources, Billing, Support, Settings, Setup, Reports, Health, Admin centers, Security, Compliance, and Endpoint Management. The main area shows 'Agent management rules' with a summary of 'Pending agents: 10' and 'Processed agents: 23'. Below this, there are two rules listed: 'Install Microsoft agents' (selected) and 'Reassign ownerless agents created with Agent Builder to manager'. A modal window titled 'Install Microsoft agents' is open, showing details for the selected rule. The modal includes a 'Details' tab and the following information:

Rule criteria	
Description	Installs Microsoft published agents for all users in your organization. Only applies to agents that are not already installed via license entitlement and are not blocked by an admin.
Action to be taken	Install agent
Conditions	Publisher equals: Microsoft
Selected users	All
Run type	Automated

Activity & Ownership	
Last run date	Today
Last modified by	Wanda Howard
Creation date	Feb 26, 2026
Created by	Wanda Howard

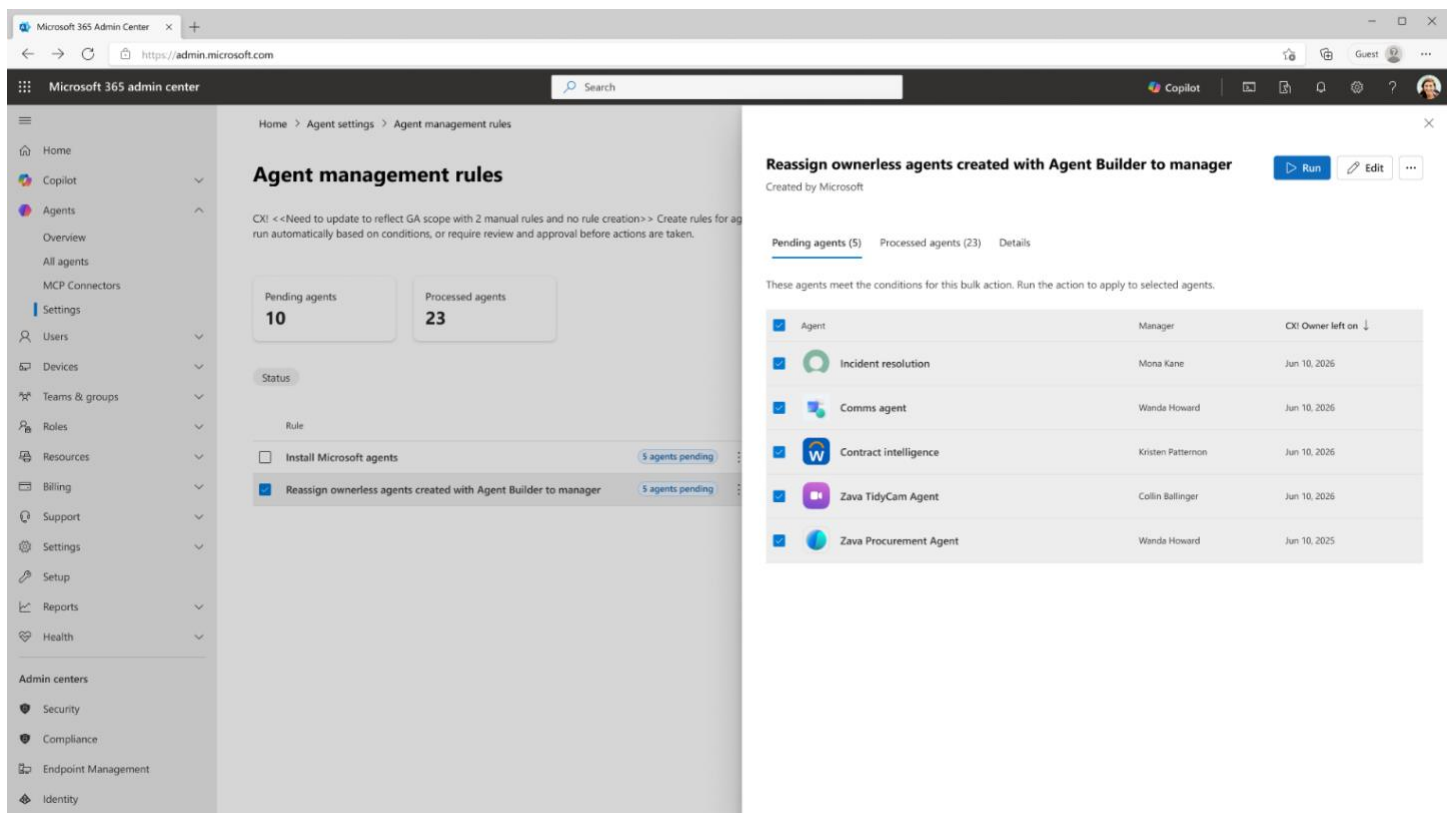
Reassign ownerless agents at scale with agent management rules

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.



The screenshot shows the Microsoft 365 Admin Center interface. The main content area is titled 'Agent management rules' and displays a rule named 'Reassign ownerless agents created with Agent Builder to manager'. The rule is currently pending for 5 agents. A table below the rule lists the affected agents, their managers, and the date of the action.

Agent	Manager	CXI Owner left on
Incident resolution	Mona Kane	Jun 10, 2025
Comms agent	Wanda Howard	Jun 10, 2025
Contract intelligence	Kristen Patternon	Jun 10, 2025
Zava TidyCam Agent	Collin Balingier	Jun 10, 2025
Zava Procurement Agent	Wanda Howard	Jun 10, 2025

Create and apply an agent security template

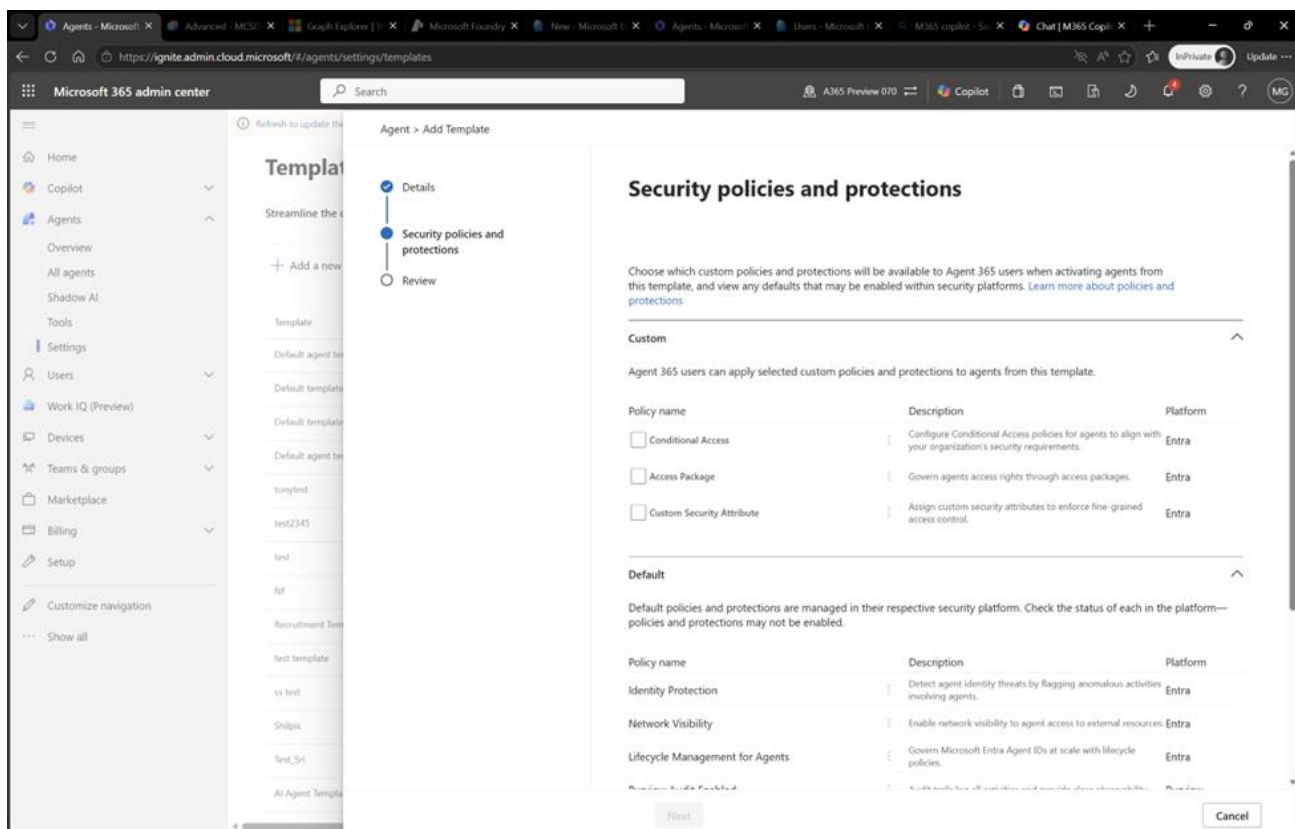
Goal: Define reusable governance controls and apply them consistently when publishing agents.

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](#).

Microsoft 365 Admin Center

Home > Tools

Tools

Explore and manage the tools that govern how an AI model interacts with user data, other tools, and workflows. Tools ensure requests, responses, and actions are handled consistently, safely, and transparently. [Learn more about tools](#)

Registry Requests (preview) (3)

Find all your tools in one place.

MCP servers: 28 Available: 25 Blocked: 3

Status Publisher 230 items Search

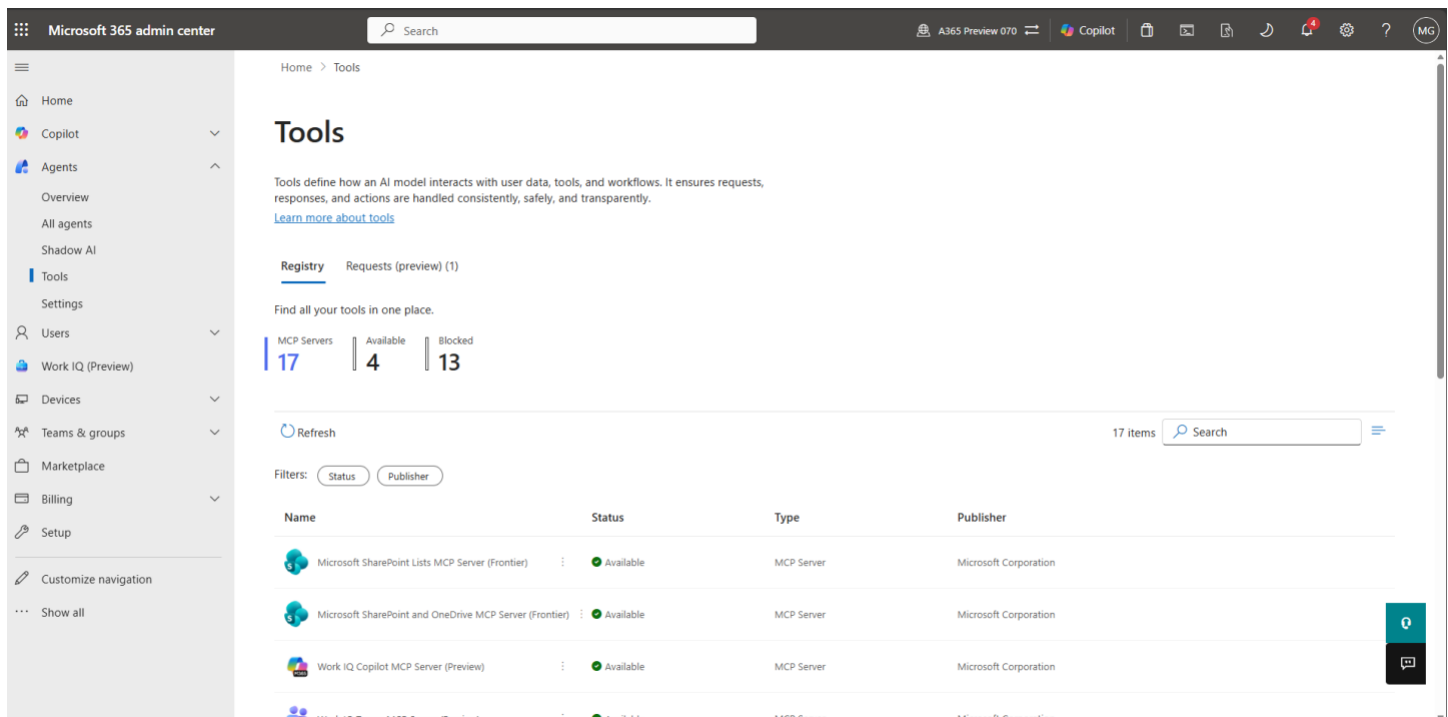
Name	Status	Tools	Type	Publisher
Microsoft Teams MCP Server	Available	12 2 new	MCP Server	Microsoft
Microsoft Word MCP Server	Available	6	MCP Server	Microsoft
Microsoft 365 Copilot Chat MCP Server	Available	18	MCP Server	Microsoft
Microsoft Outlook Mail MCP Server	Available	7 3 new	MCP Server	Microsoft
Microsoft 365 Admin Center MCP Server	Available	1 1 new	MCP Server	Microsoft
Microsoft Dataverse MCP server	Available	4	MCP Server	Microsoft

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.



The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar contains navigation options: Home, Copilot, Agents, Tools (selected), Settings, Users, Work IQ (Preview), Devices, Teams & groups, Marketplace, Billing, Setup, and Customize navigation. The main content area is titled 'Tools' and includes a description of tools and a link to 'Learn more about tools'. Below this, there are two tabs: 'Registry' (selected) and 'Requests (preview) (1)'. A summary bar shows 'Find all your tools in one place.' with counts: MCP Servers (17), Available (4), and Blocked (13). A 'Refresh' button and a search bar are present. Below the summary, there are filters for 'Status' and 'Publisher'. A table lists MCP Servers with columns for Name, Status, Type, and Publisher.

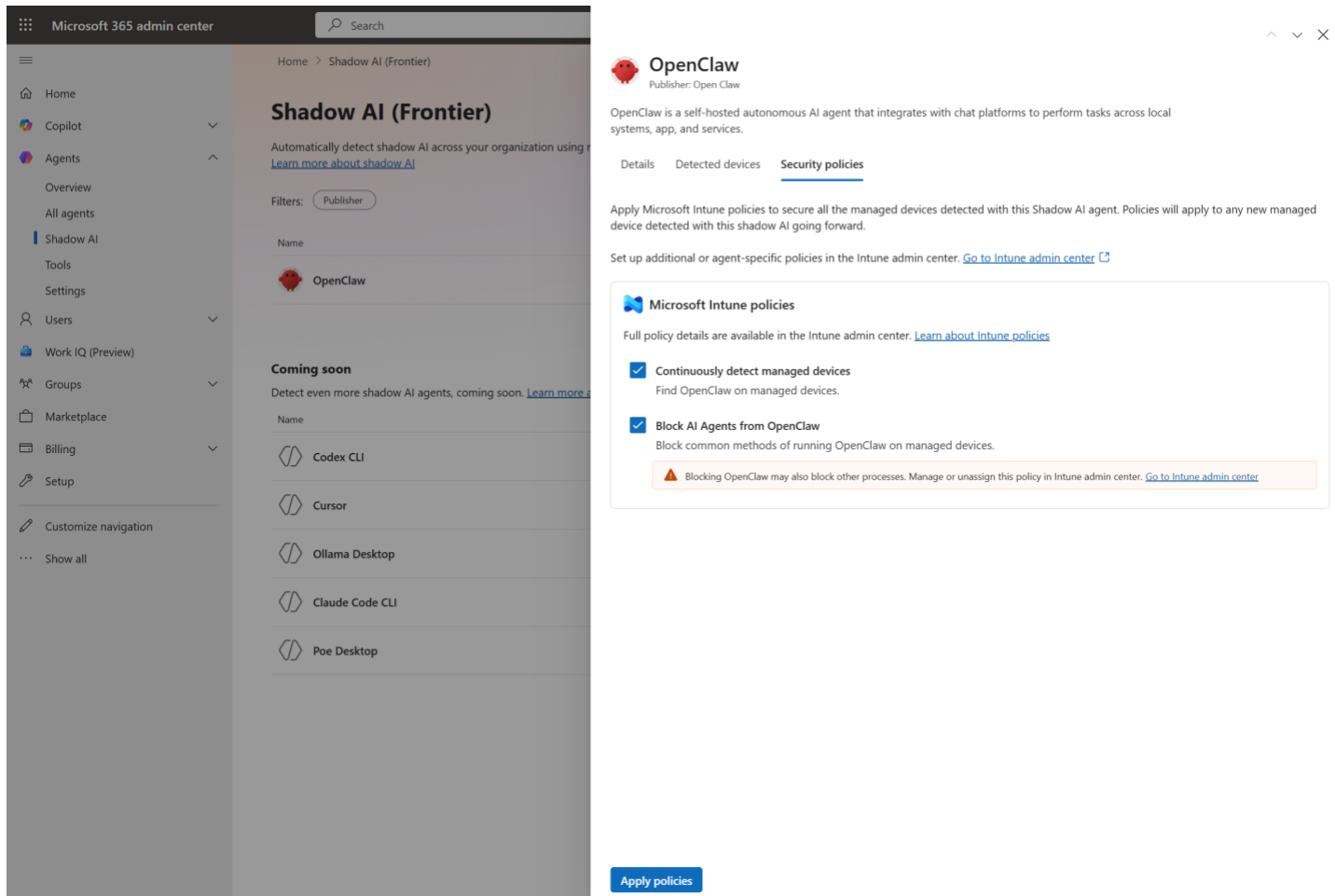
Name	Status	Type	Publisher
Microsoft SharePoint Lists MCP Server (Frontier)	Available	MCP Server	Microsoft Corporation
Microsoft SharePoint and OneDrive MCP Server (Frontier)	Available	MCP Server	Microsoft Corporation
Work IQ Copilot MCP Server (Preview)	Available	MCP Server	Microsoft Corporation
Work IQ Teams MCP Server (Preview)	Available	MCP Server	Microsoft Corporation

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.



The screenshot shows the Microsoft 365 admin center interface. The left sidebar contains navigation options like Home, Copilot, Agents, Shadow AI, Tools, Settings, Users, Work IQ (Preview), Groups, Marketplace, Billing, Setup, and Customize navigation. The main content area is titled 'Shadow AI (Frontier)' and shows a list of shadow AI agents. The 'OpenClaw' agent is selected, and its details are shown on the right. The 'Security policies' tab is active, displaying two policies: 'Continuously detect managed devices' and 'Block AI Agents from OpenClaw'. A warning message states: 'Blocking OpenClaw may also block other processes. Manage or unassign this policy in Intune admin center. [Go to Intune admin center](#)'.