



Microsoft Copilot for Admins:

<https://admin.cloud.microsoft/>

software **one**



Ondrej Vysek

Unlocking Infinite Possibilities Through
Technology | SoftwareOne | Microsoft MVP



The Risks We Don't Fully Understand Yet





What is Microsoft 365 Copilot



Copilot Control System (CCS)



Microsoft 365 Copilot MAC walkthrough



Data Discovery Configuration



Security Best Practices



Copilot Data Privacy and Security

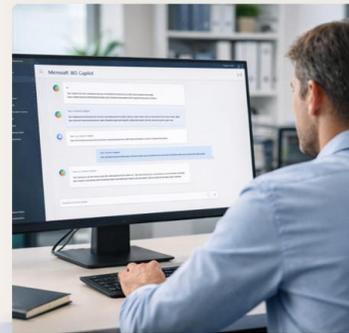


Reporting & Monitoring



Microsoft 365 Copilot for admin center

[Copilot in Microsoft 365 Admin Centers](#)

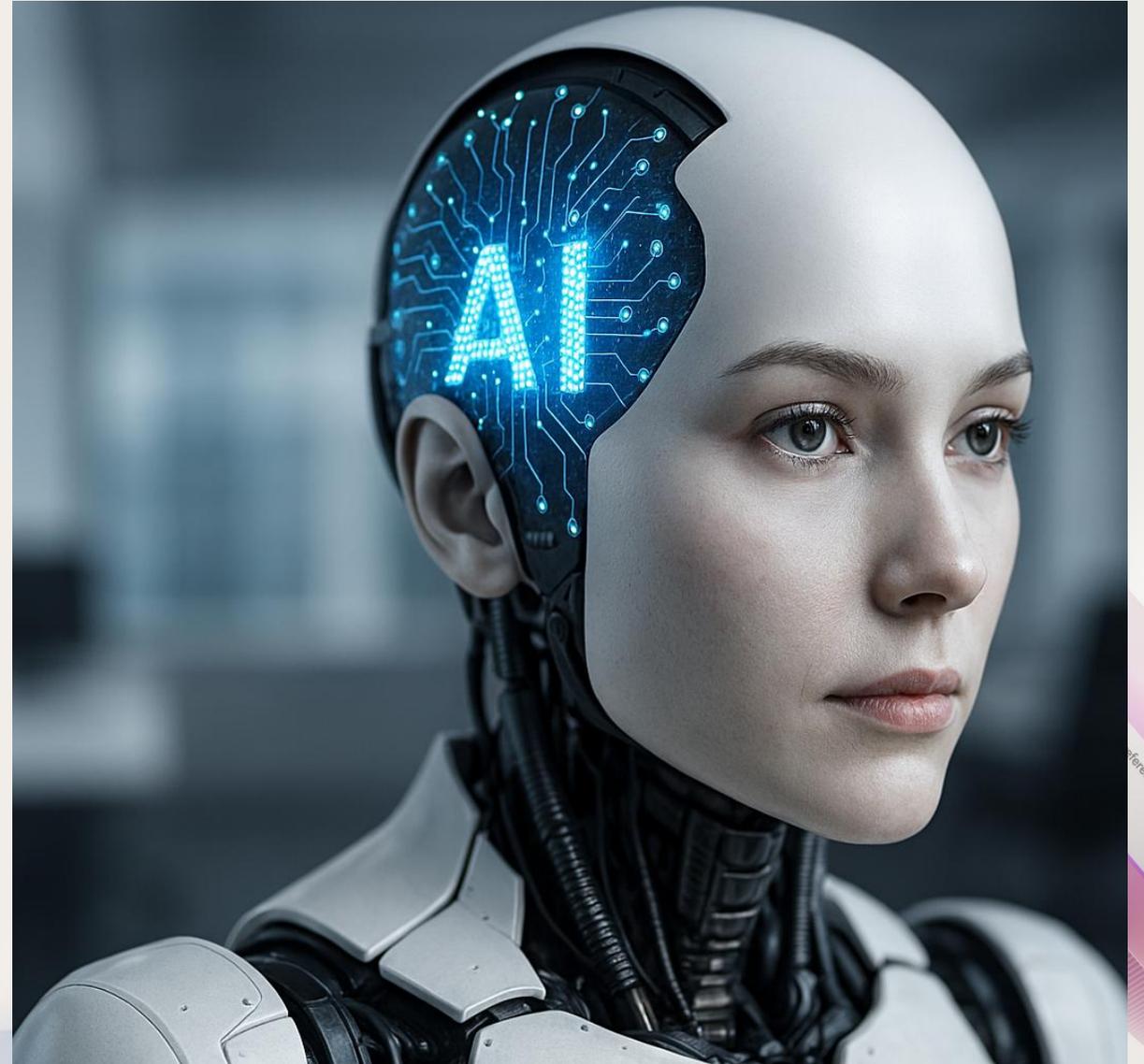


M365 Copilot Agents





What is Microsoft 365 Copilot





Microsoft 365 Copilot

Copilot Chat

- Secure AI chat and agents with web access
- AI-powered creation (standard access)
- Ability to work with open files in Microsoft 365 apps

- Custom agents based on your data, pay-as-you-go
- Standard access to GPT-5



Microsoft 365 Copilot license

- AI chat s Work IQ
- Search with AI
- AI Notebooks
- AI-powered creation (priority access)
- GPT-5 Priority Access
- **Copilot in Microsoft 365 apps**
Enhanced capabilities and editing directly in the app

- Comprehensive approach to agents
- Pre-built Microsoft agents
- Advanced analysts and research agents for deeper analysis
- Custom agents based on your data
- Advanced management and analytics

Powered by Work IQ



Copilot Control System (CCS)



Copilot Control System



Copilot + Agents



Security & Governance

- Data security
- AI security
- Compliance & privacy



Management Controls

- Licensing & metering
- Customization



Measurement & Reporting

- Impact & ROI metrics
- Robust prebuilt reports
- Custom reporting included

Tools to secure and govern your Copilot use



Address oversharing concerns

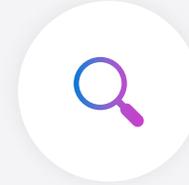
- Gain visibility into overshared content
- Remediate excessive permissions
- Prevent Copilot from processing sensitive files

Secure



Protect against data loss and insider risks

- Get alerts and reports of risky behavior and AI use
- Protect sensitive files and interactions
- Dynamically apply security policies based on risky actions



Govern AI use to meet regulations & policies

- Inspect interaction content and audit logs
- Investigate for compliance and ethical violations
- Enforce lifecycle policies and legal holds

Govern



Microsoft 365 Copilot MAC walkthrough



Network requirements

- Most features can be managed in Microsoft 365 admin center (MAC)
- Microsoft doesn't recommend and cannot support attempts to manage Microsoft 365 Copilot Chat and related settings through network-level restrictions
- M365 Copilot is deeply integrated with applications, such network-level restrictions can lead to unpredictable results

[Microsoft 365 URLs and IP address ranges - Microsoft 365 Enterprise](#)



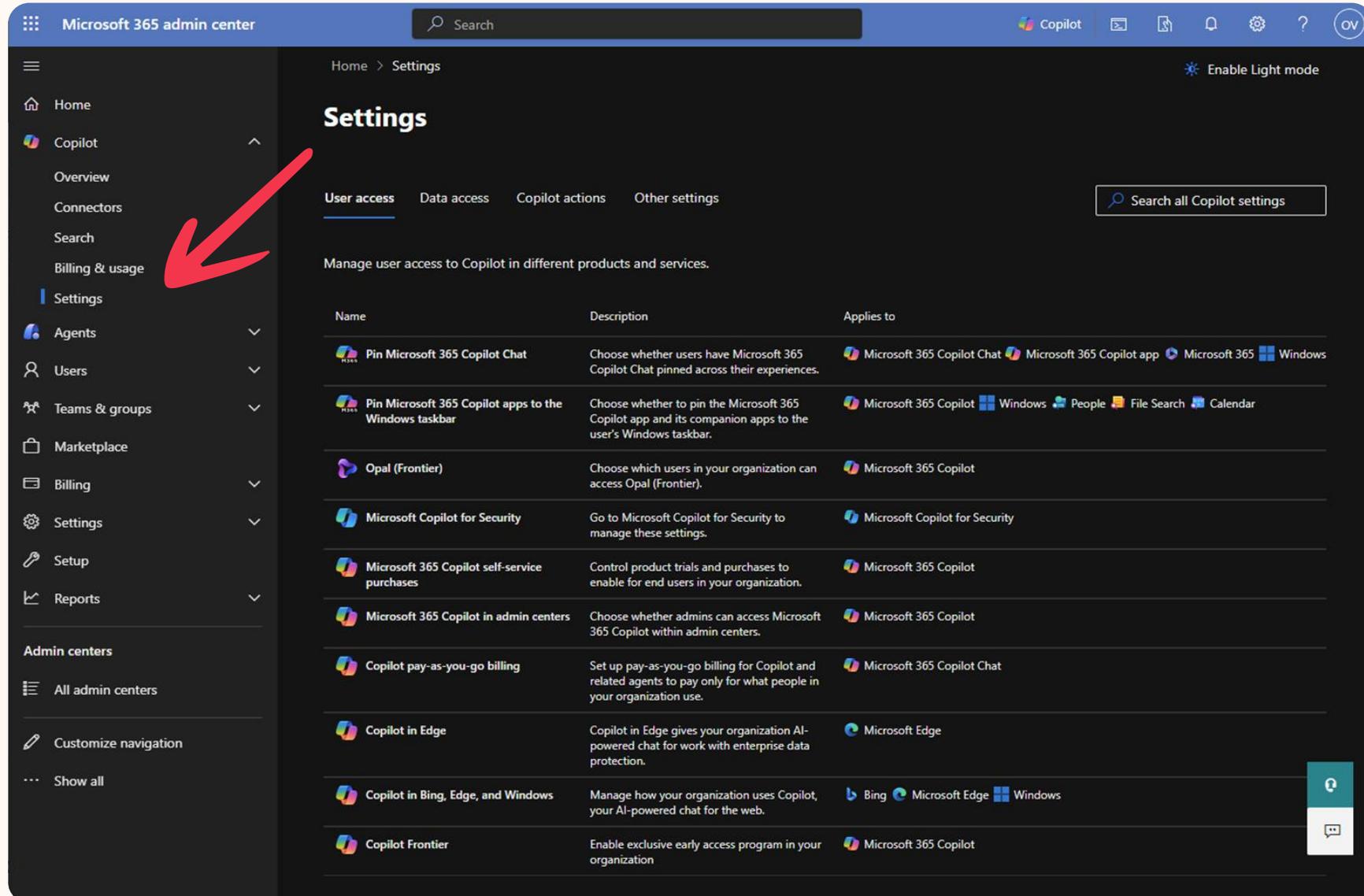
Where to start

- Common Settings under the Copilot Section
- Detailed Agent Settings -> Agent365
- Specialized features are set in the product Admin portals (Defender, Purview, Entra, Power Platform)

The screenshot shows the Microsoft 365 admin center interface. The left sidebar contains navigation options: Home, Copilot, Overview (selected), Connectors, Search, Billing & usage, Settings, Agents, Users, Teams & groups, Marketplace, Billing, Settings, Setup, Reports, Admin centers, All admin centers, Customize navigation, and Show all. The main content area is titled 'Copilot Control System' and includes tabs for Overview, Security, Health, and Discover. Below the tabs, there are four key success metrics: 'Optimize Copilot license assignment' (Active user rate: 50%), 'Encourage users to make Copilot a daily habit' (AI adoption score: 0/100), 'Highlight Copilot's business impact' (Copilot assisted hours: --), and 'Leverage user feedback to increase delight' (Promoters: --). At the bottom, there are sections for 'Adoption by app' (Enabled users: 2, Active users: 1, Active users rate: 50.0%) and 'Copilot licenses' (M365 Copilot Special Benefi: 2/5 assigned, 3 available). The page is last updated on January 6, 2026 (UTC).

Copilot Settings #1: User Access

- Common Settings under the Copilot Section



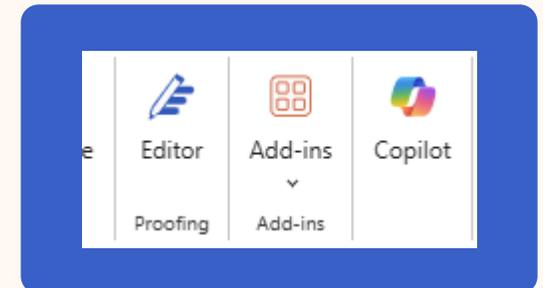
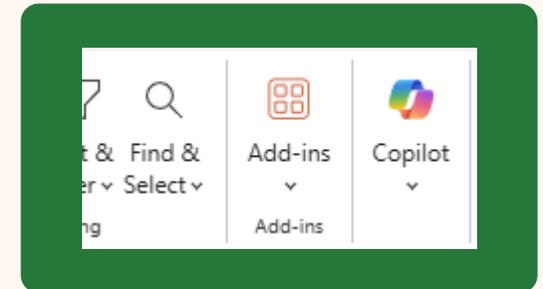
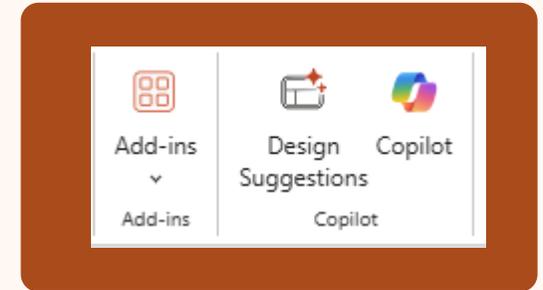
The screenshot displays the Microsoft 365 admin center interface. The left-hand navigation pane is visible, with the 'Settings' option highlighted and a red arrow pointing to it. The main content area shows the 'Settings' page for Copilot, with the 'User access' tab selected. Below the tab, there is a table listing various Copilot settings and their descriptions.

Name	Description	Applies to
Pin Microsoft 365 Copilot Chat	Choose whether users have Microsoft 365 Copilot Chat pinned across their experiences.	Microsoft 365 Copilot Chat, Microsoft 365 Copilot app, Microsoft 365, Windows
Pin Microsoft 365 Copilot apps to the Windows taskbar	Choose whether to pin the Microsoft 365 Copilot app and its companion apps to the user's Windows taskbar.	Microsoft 365 Copilot, Windows, People, File Search, Calendar
Opal (Frontier)	Choose which users in your organization can access Opal (Frontier).	Microsoft 365 Copilot
Microsoft Copilot for Security	Go to Microsoft Copilot for Security to manage these settings.	Microsoft Copilot for Security
Microsoft 365 Copilot self-service purchases	Control product trials and purchases to enable for end users in your organization.	Microsoft 365 Copilot
Microsoft 365 Copilot in admin centers	Choose whether admins can access Microsoft 365 Copilot within admin centers.	Microsoft 365 Copilot
Copilot pay-as-you-go billing	Set up pay-as-you-go billing for Copilot and related agents to pay only for what people in your organization use.	Microsoft 365 Copilot Chat
Copilot in Edge	Copilot in Edge gives your organization AI-powered chat for work with enterprise data protection.	Microsoft Edge
Copilot in Bing, Edge, and Windows	Manage how your organization uses Copilot, your AI-powered chat for the web.	Bing, Microsoft Edge, Windows
Copilot Frontier	Enable exclusive early access program in your organization	Microsoft 365 Copilot

Copilot Settings #1: User Access

The screenshot shows the Microsoft 365 admin center interface. The left sidebar contains a navigation menu with items like Home, Copilot, Overview, Connectors, Search, Billing & usage, Settings, Agents, Users, Teams & groups, Marketplace, Billing, Settings, Setup, and Reports. A red arrow points to the 'Agents' item. The main content area is titled 'Settings' and has tabs for 'User access', 'Data access', 'Copilot actions', and 'Other settings'. The 'User access' tab is active, showing a table of settings for Copilot Chat and other services. A modal window titled 'Pin Microsoft 365 Copilot Chat' is open on the right, showing options to pin Copilot Chat in Microsoft 365 apps and on the Windows taskbar.

Name	Description
Pin Microsoft 365 Copilot Chat	Choose whether users have Microsoft 365 Copilot Chat pinned across their experience.
Pin Microsoft 365 Copilot apps to the Windows taskbar	Choose whether to pin the Microsoft 365 Copilot app and its companion apps to the user's Windows taskbar.
Opal (Frontier)	Choose which users in your organization can access Opal (Frontier).
Microsoft Copilot for Security	Go to Microsoft Copilot for Security to manage these settings.
Microsoft 365 Copilot self-service purchases	Control product trials and purchases to enable for end users in your organization.
Microsoft 365 Copilot in admin centers	Choose whether admins can access Microsoft 365 Copilot within admin centers.
Copilot pay-as-you-go billing	Set up pay-as-you-go billing for Copilot and related agents to pay only for what people in your organization use.
Copilot in Edge	Copilot in Edge gives your organization AI-powered chat for work with enterprise data protection.
Copilot in Bing, Edge, and Windows	Manage how your organization uses Copilot for your AI-powered chat for the web.
Copilot Frontier	Enable exclusive early access program in your organization.



Copilot Settings #1: User Access

The screenshot displays the Microsoft 365 Admin Center interface. The left sidebar contains navigation options: Home, Copilot, Overview, Connectors, Search, Billing & usage, Settings, Agents, Users, Teams & groups, Marketplace, Billing, Settings, Setup, Reports, Admin centers, All admin centers, Customize navigation, and Show all. The main content area is titled 'Settings' and includes a search bar and tabs for 'User access', 'Data access', 'Copilot actions', and 'Other settings'. The 'User access' tab is active, showing a table of settings to manage user access to Copilot products. A red arrow points to the setting 'Pin Microsoft 365 Copilot apps to the Windows taskbar'. A modal window on the right provides details for this setting, including a description and configuration options.

Name	Description
Pin Microsoft 365 Copilot Chat	Choose whether users have Microsoft 365 Copilot Chat pinned across their experience.
Pin Microsoft 365 Copilot apps to the Windows taskbar	Choose whether to pin the Microsoft 365 Copilot app and its companion apps to the user's Windows taskbar.
Opal (Frontier)	Choose which users in your organization can access Opal (Frontier).
Microsoft Copilot for Security	Go to Microsoft Copilot for Security to manage these settings.
Microsoft 365 Copilot self-service purchases	Control product trials and purchases to enable for end users in your organization.
Microsoft 365 Copilot in admin centers	Choose whether admins can access Microsoft 365 Copilot within admin centers.
Copilot pay-as-you-go billing	Set up pay-as-you-go billing for Copilot and related agents to pay only for what people in your organization use.
Copilot in Edge	Copilot in Edge gives your organization AI-powered chat for work with enterprise data protection.
Copilot in Bing, Edge, and Windows	Manage how your organization uses Copilot your AI-powered chat for the web.
Copilot Frontier	Enable exclusive early access program in your organization.

Pin Microsoft 365 Copilot apps to the Windows Taskbar

The Microsoft 365 Copilot apps provides users with a new AI first way of working to boost productivity and streamline workflows. Pin the Microsoft 365 Copilot app and its companion apps to the Windows taskbar to make them easier to find and use.

This setting applies to Intune-managed Windows 10 and 11 devices that have the Microsoft 365 Copilot apps installed.

[Learn more about this setting](#)

Choose how users pin on the Windows taskbar

Pin the Microsoft 365 Copilot and its companion apps to the Windows taskbar (recommended)

Customize

Pin the Microsoft 365 companion apps to the Windows taskbar ⓘ

Do not pin the Microsoft 365 Copilot app and its companion apps to the Windows taskbar

Save

Copilot Settings #1: User Access

The screenshot displays the Microsoft 365 admin center interface. The left-hand navigation pane includes sections for Home, Copilot, Agents, Users, Teams & groups, Marketplace, Billing, Settings, Setup, and Reports. A red arrow points to the 'Settings' menu item. The main content area is titled 'Settings' and shows the 'User access' tab selected. Below this, a table lists various Copilot settings. A right-hand panel is open, showing the configuration for 'Microsoft 365 Copilot self-service trials and purchases', with the 'Allow' option selected.

Microsoft 365 admin center

Home > Settings

Settings

User access | Data access | Copilot actions | Other settings

Manage user access to Copilot in different products and services.

Name	Description
Pin Microsoft 365 Copilot Chat	Choose whether users have Microsoft 365 Copilot Chat pinned across their experience.
Pin Microsoft 365 Copilot apps to the Windows taskbar	Choose whether to pin the Microsoft 365 Copilot app and its companion apps to the user's Windows taskbar.
Opal (Frontier)	Choose which users in your organization can access Opal (Frontier).
Microsoft Copilot for Security	Go to Microsoft Copilot for Security to manage these settings.
Microsoft 365 Copilot self-service purchases	Control product trials and purchases to enable for end users in your organization.
Microsoft 365 Copilot in admin centers	Choose whether admins can access Microsoft 365 Copilot within admin centers.
Copilot pay-as-you-go billing	Set up pay-as-you-go billing for Copilot and related agents to pay only for what people in your organization use.
Copilot in Edge	Copilot in Edge gives your organization AI-powered chat for work with enterprise data protection.
Copilot in Bing, Edge, and Windows	Manage how your organization uses Copilot for your AI-powered chat for the web.
Copilot Frontier	Enable exclusive early access program in your organization.

Microsoft 365 Copilot self-service trials and purchases

Give users the flexibility to acquire this product without an administrator's help. This can help admins understand and manage the demand.

[Go to self-service settings for other products](#)
[Learn which products offer self-service trials](#)

- Allow**
Users can try or buy this product on their own.
- Allow trials only**
Users can try this product for free, but cannot buy it themselves. When the trial ends, it does not convert to a paid subscription, but users might be able to request a paid license from an admin.
- Do not allow**
No self-service purchases are allowed for this product, but in some cases, free trials might still be available, and users might be able to request a paid license from an admin.

Save

Copilot Settings #1: User Access

The screenshot displays the Microsoft 365 admin center interface. The left-hand navigation pane includes sections for Home, Copilot, Agents, Users, Teams & groups, Marketplace, Billing, Settings, Setup, Reports, and Admin centers. A red arrow points to the 'Settings' option in the left pane. The main content area is titled 'Settings' and has a breadcrumb 'Home > Settings'. Below this, there are tabs for 'User access', 'Data access', 'Copilot actions', and 'Other settings'. The 'User access' tab is active, showing a list of settings. A red arrow points to the 'Microsoft 365 Copilot in admin centers' setting in this list. A modal window is open on the right, titled 'Microsoft 365 Copilot in admin centers'. It contains the following text: 'Microsoft 365 Copilot is available in admin centers to help IT admins streamline their workflows with AI. Microsoft 365 Copilot only provides users with information they already have permission to see based on their admin role.' Below this, it states: 'This setting affects users with an admin role who use Microsoft 365 Copilot in the Microsoft 365 admin center, Exchange admin center, SharePoint admin center, and Microsoft Teams admin center. After changing this setting, please allow a couple of hours for changes to take effect.' There is a link: 'Learn more about Microsoft 365 Copilot in admin centers'. Two radio button options are present: 'Allow for all admins (recommended)' (which is selected) and 'Block for all admins'. The 'Block for all admins' option includes the text: 'No one in your organization can use Microsoft 365 Copilot in admin centers.' and a link: 'Manage security groups'. A 'Save' button is at the bottom of the modal. A red arrow also points to the 'Copilot' icon in the top right header of the admin center.

Microsoft 365 admin center

Home > Settings

Settings

User access | Data access | Copilot actions | Other settings

Manage user access to Copilot in different products and services.

Name	Description
Pin Microsoft 365 Copilot Chat	Choose...
Pin Microsoft 365 Copilot apps to the Windows taskbar	Choose Windows...
Opal (Frontier)	Choose...
Microsoft Copilot for Security	Go to...
Microsoft 365 Copilot self-service purchases	Control...
Microsoft 365 Copilot in admin centers	Choose...
Copilot pay-as-you-go billing	Set up organization...
Copilot in Edge	Copilot...
Copilot in Bing, Edge, and Windows	Manag...
Copilot Frontier	Enable...

Microsoft 365 Copilot in admin centers

Microsoft 365 Copilot is available in admin centers to help IT admins streamline their workflows with AI. Microsoft 365 Copilot only provides users with information they already have permission to see based on their admin role.

This setting affects users with an admin role who use Microsoft 365 Copilot in the Microsoft 365 admin center, Exchange admin center, SharePoint admin center, and Microsoft Teams admin center. After changing this setting, please allow a couple of hours for changes to take effect.

[Learn more about Microsoft 365 Copilot in admin centers](#)

Allow for all admins (recommended)

You can still block specific admins from using Microsoft 365 Copilot in admin centers by adding them to a security group with this exact name: CopilotForM365AdminExclude

[Manage security groups](#)

Block for all admins

No one in your organization can use Microsoft 365 Copilot in admin centers.

[Save](#)

Copilot Settings #1: User Access

The image shows two screenshots of the Microsoft 365 admin center interface. The left screenshot displays the 'Settings' page for Copilot, with a red arrow pointing to the 'Admin centers' section in the left-hand navigation pane. The right screenshot shows the 'Billing & usage' page, with a red arrow pointing to the 'Billing & usage' option in the left-hand navigation pane.

Microsoft 365 admin center - Settings

Home > Settings

Settings

User access | Data access | Copilot actions | Other settings

Manage user access to Copilot in different products and services.

Name	Description
Pin Microsoft 365 Copilot Chat	Choose whether users have Microsoft 365 Copilot Chat pinned across their experiences.
Pin Microsoft 365 Copilot apps to the Windows taskbar	Choose whether to pin the Microsoft 365 Copilot app and its companion apps to the user's Windows taskbar.
Opal (Frontier)	Choose which users in your organization can access Opal (Frontier).
Microsoft Copilot for Security	Go to Microsoft Copilot for Security to manage these settings.
Microsoft 365 Copilot self-service purchases	Control product trials and purchases to enable for end users in your organization.
Microsoft 365 Copilot in admin centers	Choose whether admins can access Microsoft 365 Copilot within admin centers.
Copilot pay-as-you-go billing	Set up pay-as-you-go billing for Copilot and related agents to pay only for what people in your organization use.
Copilot in Edge	Copilot in Edge gives your organization AI-powered chat for work with enterprise data protection.
Copilot in Bing, Edge, and Windows	Manage how your organization uses Copilot, your AI-powered chat for the web.
Copilot Frontier	Enable exclusive early access program in your organization.

Microsoft 365 admin center - Billing & usage

Home > Billing & usage

Billing & usage

Set up pay-as-you-go billing by connecting apps and services to billing policies. View usage insights and costs for pay-as-you-go billing. [Learn more about pay-as-you-go billing](#)

Billing policies | Pay-as-you-go services

[View cost management](#) | [Manage billing policies](#)

Service	Billing policy	Connected to
Microsoft 365 Copilot Chat	None	None
SharePoint agents	None	None

Copilot Settings #1: User Access

The image displays two screenshots of the Microsoft 365 admin center interface, illustrating the navigation path to Copilot settings.

Left Screenshot: Microsoft 365 admin center - Settings

- Home > Settings
- Settings (selected)
- User access (selected)
- Table of settings:

Name	Description
Pin Microsoft 365 Copilot Chat	...
Pin Microsoft 365 Copilot apps to the Windows taskbar	...
Opal (Frontier)	...
Microsoft Copilot for Security	...
Microsoft 365 Copilot self-service purchases	...
Microsoft 365 Copilot in admin centers	...
Copilot pay-as-you-go billing	...
Copilot in Edge	...
Copilot in Bing, Edge, and Windows	...
Copilot Frontier	...

Right Screenshot: Microsoft Edge for Business

- Home > Microsoft Edge for Business
- Microsoft Edge for Business (selected)
- Navigation menu: Overview, Configuration policies, Site lists, Connectors, Copilot (selected), Monitoring dashboard
- Section: Copilot in Edge
- Text: Manage how users in your organization interact with Microsoft 365 Copilot Chat, an AI-powered web chat that protects your company and personal data. [Learn more about Copilot.](#)
- Settings:

- Copilot Mode **Preview** (Select)
- Agent Mode **Coming soon** (Select sites >)
- Access to browser context (Select)
- Copilot icon in the toolbar (Select)
- Copilot search box (Select)
- AI-generated text and editing (Select)

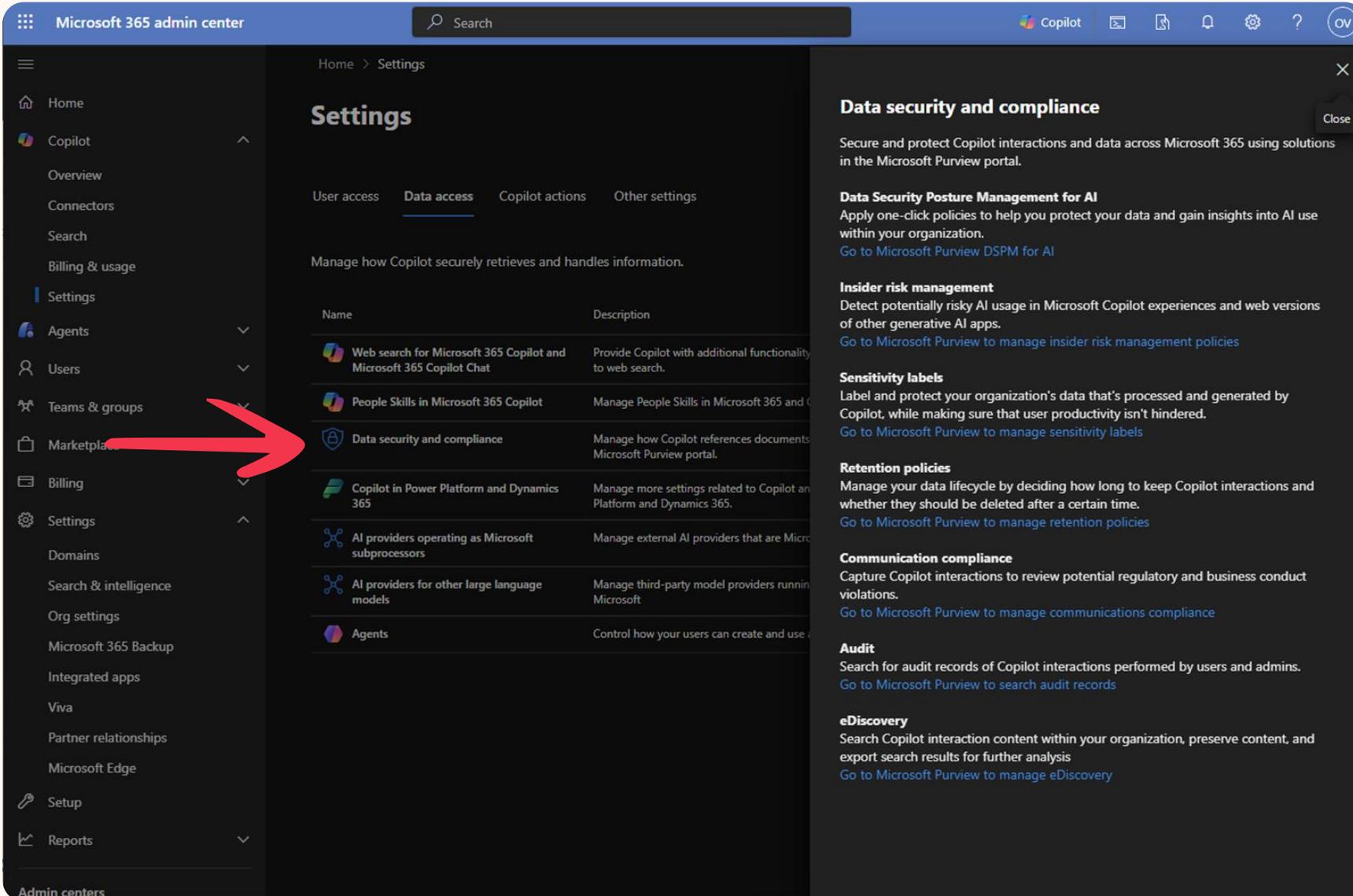
Copilot Settings #1: User Access

The screenshot displays the Microsoft 365 admin center interface. The left-hand navigation pane includes sections for Home, Copilot, Agents, Users, Teams & groups, Marketplace, Billing, Settings, Domains, Search & intelligence, Org settings, Microsoft 365 Backup, Integrated apps, Viva, Partner relationships, Microsoft Edge, Setup, and Reports. A red arrow points to the 'Settings' menu item. The main content area is titled 'Settings' and contains a sub-section for 'User access'. Below this, a table lists various Copilot settings:

Name	Description
Pin Microsoft 365 Copilot Chat	Choose whether users have Microsoft 365 Copilot across their experiences.
Pin Microsoft 365 Copilot apps to the Windows taskbar	Choose whether to pin the Microsoft 365 Copilot companion apps to the user's Windows taskbar.
Opal (Frontier)	Choose which users in your organization can access Copilot in the Opal (Frontier) program.
Microsoft Copilot for Security	Go to Microsoft Copilot for Security.
Microsoft 365 Copilot self-service purchases	Control product trials and purchases to enable Copilot in your organization.
Microsoft 365 Copilot in admin centers	Choose whether admins can access Microsoft 365 Copilot in admin centers.
Copilot pay-as-you-go billing	Set up pay-as-you-go billing for Copilot and restrict it only for what people in your organization use.
Copilot in Edge	Copilot in Edge gives your organization AI-powered search with enterprise data protection.
Copilot in Bing, Edge, and Windows	Manage how your organization uses Copilot, Copilot for the web.
Copilot Frontier	Enable exclusive early access program in your organization.

On the right side of the interface, there is a panel titled 'Turn on Frontier features'. It includes a description of the Frontier program and a section for 'Web apps' where users can select access levels: 'No access', 'All users', and 'Specific users'. The 'Specific users' option is selected, and a list of users is shown, including 'Copilot Chat'. A red arrow points to the 'Opal (Frontier)' setting in the table, and another red arrow points to the 'Specific users' radio button.

Copilot Settings #2: Data Access – Data Security and Compliance



The screenshot displays the Microsoft 365 Admin Center interface. The left-hand navigation pane includes sections for Home, Copilot, Agents, Users, Teams & groups, Marketplaces, Billing, Settings, Domains, Search & intelligence, Org settings, Microsoft 365 Backup, Integrated apps, Viva, Partner relationships, Microsoft Edge, Setup, and Reports. The main content area is titled 'Settings' and has a breadcrumb 'Home > Settings'. Below this, there are tabs for 'User access', 'Data access', 'Copilot actions', and 'Other settings', with 'Data access' currently selected. A descriptive text reads: 'Manage how Copilot securely retrieves and handles information.' Below this is a table with two columns: 'Name' and 'Description'. A red arrow points to the 'Data security and compliance' entry in the table. To the right of the table, a detailed panel for 'Data security and compliance' is open, showing various sub-sections such as 'Data Security Posture Management for AI', 'Insider risk management', 'Sensitivity labels', 'Retention policies', 'Communication compliance', 'Audit', and 'eDiscovery'. Each sub-section includes a brief description and a link to the Microsoft Purview portal.

Name	Description
Web search for Microsoft 365 Copilot and Microsoft 365 Copilot Chat	Provide Copilot with additional functionality to web search.
People Skills in Microsoft 365 Copilot	Manage People Skills in Microsoft 365 and Copilot.
Data security and compliance	Manage how Copilot references documents in the Microsoft Purview portal.
Copilot in Power Platform and Dynamics 365	Manage more settings related to Copilot in Power Platform and Dynamics 365.
AI providers operating as Microsoft subprocessors	Manage external AI providers that are Microsoft subprocessors.
AI providers for other large language models	Manage third-party model providers running on Microsoft.
Agents	Control how your users can create and use Copilot agents.

Data security and compliance

Secure and protect Copilot interactions and data across Microsoft 365 using solutions in the Microsoft Purview portal.

Data Security Posture Management for AI

Apply one-click policies to help you protect your data and gain insights into AI use within your organization.
[Go to Microsoft Purview DSPM for AI](#)

Insider risk management

Detect potentially risky AI usage in Microsoft Copilot experiences and web versions of other generative AI apps.
[Go to Microsoft Purview to manage insider risk management policies](#)

Sensitivity labels

Label and protect your organization's data that's processed and generated by Copilot, while making sure that user productivity isn't hindered.
[Go to Microsoft Purview to manage sensitivity labels](#)

Retention policies

Manage your data lifecycle by deciding how long to keep Copilot interactions and whether they should be deleted after a certain time.
[Go to Microsoft Purview to manage retention policies](#)

Communication compliance

Capture Copilot interactions to review potential regulatory and business conduct violations.
[Go to Microsoft Purview to manage communications compliance](#)

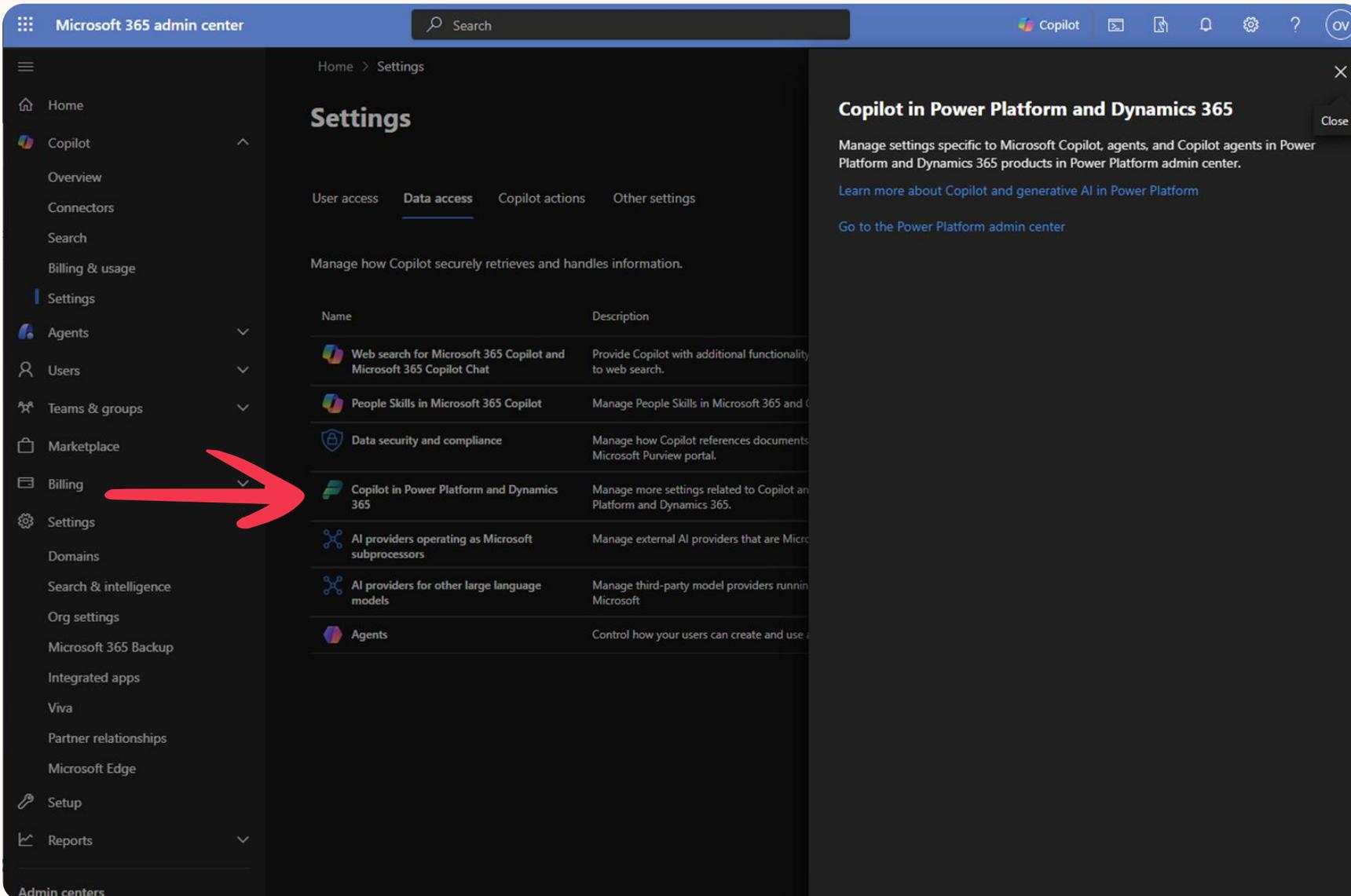
Audit

Search for audit records of Copilot interactions performed by users and admins.
[Go to Microsoft Purview to search audit records](#)

eDiscovery

Search Copilot interaction content within your organization, preserve content, and export search results for further analysis
[Go to Microsoft Purview to manage eDiscovery](#)

Copilot Settings #2: Data Access - PowerPlatform



The screenshot displays the Microsoft 365 admin center interface. The left-hand navigation pane includes sections for Home, Copilot, Connectors, Search, Billing & usage, Settings, Agents, Users, Teams & groups, Marketplace, Billing, Domains, Search & intelligence, Org settings, Microsoft 365 Backup, Integrated apps, Viva, Partner relationships, Microsoft Edge, Setup, and Reports. A red arrow points to the 'Settings' menu item. The main content area is titled 'Settings' and shows the 'Data access' tab selected. Below this, a table lists various Copilot settings. The 'Copilot in Power Platform and Dynamics 365' setting is highlighted. A right-hand pane is open, titled 'Copilot in Power Platform and Dynamics 365', providing instructions on how to manage these settings.

Name	Description
Web search for Microsoft 365 Copilot and Microsoft 365 Copilot Chat	Provide Copilot with additional functionality to web search.
People Skills in Microsoft 365 Copilot	Manage People Skills in Microsoft 365 and Copilot.
Data security and compliance	Manage how Copilot references documents: Microsoft Purview portal.
Copilot in Power Platform and Dynamics 365	Manage more settings related to Copilot in Power Platform and Dynamics 365.
AI providers operating as Microsoft subprocessors	Manage external AI providers that are Microsoft subprocessors.
AI providers for other large language models	Manage third-party model providers running on Microsoft.
Agents	Control how your users can create and use Copilot agents.

Copilot Settings #2: Data Access – Anthropic subprocessor

Microsoft 365 admin center

Home > Settings

Settings

User access | **Data access** | Copilot actions | Other settings

Manage how Copilot securely retrieves and handles information.

Name	Description
Web search for Microsoft 365 Copilot and Microsoft 365 Copilot Chat	Provide Copilot with additional functionality to web search.
People Skills in Microsoft 365 Copilot	Manage People Skills in Microsoft 365 and Copilot.
Data security and compliance	Manage how Copilot references documents in Microsoft Purview portal.
Copilot in Power Platform and Dynamics 365	Manage more settings related to Copilot in Power Platform and Dynamics 365.
AI providers operating as Microsoft subprocessors	Manage external AI providers that are Microsoft subprocessors.
AI providers for other large language models	Manage third-party model providers running on Microsoft.
Agents	Control how your users can create and use agents.

AI providers operating as Microsoft subprocessors

Manage whether your organization can use other AI model providers operating as subprocessors for Microsoft in your Copilot experiences. These models can operate in facilities outside of Microsoft.

[Learn more about AI subprocessors](#)

Available subprocessors for your organization

Anthropic

Disabled by default
Anthropic as a Microsoft subprocessor will be available for use effective January 7, 2026.

Terms and conditions

Microsoft offers an optional capability to use Anthropic AI models to enhance Copilot and generative AI experiences in Microsoft Online Services. Anthropic operates as a Microsoft subprocessor for these experiences. Your Microsoft [Product Terms](#) and [Data Protection Addendum](#) apply to your use of Anthropic AI models from within Microsoft Online Services unless otherwise documented in [Anthropic as a Subprocessor](#).

Note: Anthropic AI models operating within Microsoft Online Services are not in scope for EU Data Boundary commitments.

By enabling the use of Anthropic AI models, you acknowledge and agree to the above terms.

Select your preference

Enable Anthropic as a Microsoft subprocessor subject to the above terms

Disable Anthropic as a Microsoft subprocessor

Save

Copilot Settings #2: Data Access – 3rd party model providers

The screenshot displays the Microsoft 365 Admin Center interface. The left-hand navigation pane includes sections for Home, Copilot, Agents, Users, Teams & groups, Marketplace, Billing, Settings, Domains, Search & indexing, Org settings, Microsoft 365 Backup, Integrated apps, Viva, Partner relationships, Microsoft Edge, Setup, and Reports. The main content area is titled 'Settings' and has a breadcrumb 'Home > Settings'. Under the 'Settings' heading, there are tabs for 'User access', 'Data access', 'Copilot actions', and 'Other settings'. The 'Data access' tab is selected, showing a description: 'Manage how Copilot securely retrieves and handles information.' Below this is a table with two columns: 'Name' and 'Description'. The table lists several settings, with 'AI providers for other large language models' highlighted by a red arrow. This setting's description is 'Manage third-party model providers running on Microsoft'. To the right of the main content, a modal window titled 'AI providers for other large language models' is open. It contains the text 'Allow users to connect to other large language models (LLM).', a link to 'Learn more about connecting to other large language models (LLMs)', and a section titled 'Available model providers for your organization'. Under this section, 'Anthropic' is listed as an available provider. A sub-modal window for 'Anthropic' is also open, showing its description as 'AI safety and research company.' and a 'Legal terms' section. The legal terms text states: 'Microsoft is providing you with an optional capability to access Anthropic services from within a Microsoft Online Service. Learn more. Anthropic services operate outside of Microsoft. By clicking the Allow provider button below, you agree on behalf of your organization that a) you are bound by, and must use the Anthropic services only in accordance with, the Anthropic Commercial Terms of Service and Anthropic Data Processing Addendum, and b) you are electing to share your organization's data with Anthropic and egress data from Microsoft. Your Microsoft customer agreements (including the Product Terms and Microsoft's Data Protection Addendum) do not apply to your use of Anthropic services from within a Microsoft Online Service, and Microsoft's data residency, audit and compliance requirements, service level agreements, and Customer Copyright Commitment do not apply to your use of Anthropic services.' Below the legal terms is a checkbox labeled 'I have read and agree to the Terms and Conditions.' and an 'Allow provider' button.

Name	Description
Web search for Microsoft 365 Copilot and Microsoft 365 Copilot Chat	Provide Copilot with additional functionality to web search.
People Skills in Microsoft 365 Copilot	Manage People Skills in Microsoft 365 and Copilot.
Data security and compliance	Manage how Copilot references documents: Microsoft Purview portal.
Copilot in Power Platform and Dynamics 365	Manage more settings related to Copilot in Power Platform and Dynamics 365.
AI providers operating as Microsoft subprocessors	Manage external AI providers that are Microsoft subprocessors.
AI providers for other large language models	Manage third-party model providers running on Microsoft.
Agents	Control how your users can create and use agents.

Copilot Settings #2: Data Access – Agents

The screenshot displays the Microsoft 365 Admin Center interface. The left-hand navigation pane includes categories like Home, Copilot, Agents, Users, Teams & groups, Marketplace, Billing, Settings, Domains, Search & intelligence, Org settings, Microsoft 365 Backup, Integrated apps, Viva, Partner relationships, Microsoft Edge, Setup, and Reports. A red arrow points to the 'Agents' item in the 'Settings' category.

The main content area is titled 'Settings' and shows the 'Data access' tab selected under the 'Agents' section. It contains a table of agents and a configuration panel on the right.

Name	Description
Web search for Microsoft 365 Copilot and Microsoft 365 Copilot Chat	Provide Copilot to web search
People Skills in Microsoft 365 Copilot	Manage Peop
Data security and compliance	Manage how Microsoft Pur
Copilot in Power Platform and Dynamics 365	Manage more Platform and
AI providers operating as Microsoft subprocessors	Manage exter
AI providers for other large language models	Manage third Microsoft
Agents	Control how y

Agents

Agents are AI assistants that can help answer questions, create content, automate tasks, and more. Use these settings to control how your users interact with agents.

Data processed by non-Microsoft services is not subject to Microsoft agreements. Please consult your internal policies before allowing access.

[Manage all agents](#)

Choose who can access agents

- All users
- No users
- Specific users/groups

Search for users or groups to add

Choose who can share agents with anyone in the organization

Users who are restricted from sharing with anyone can still share their agents with individual users and security groups.

- All users
- No users
- Specific users

Search for users or groups to add

Save

Copilot Settings #3: Copilot Actions

The screenshot shows the Microsoft 365 admin center interface. The left sidebar contains navigation options: Home, Copilot, Overview, Connectors, Search, Billing & usage, Settings (selected), Agents, Users, Teams & groups, Marketplace, Billing, Domains, Search & intelligence, Org settings, Microsoft 365 Backup, Integrated apps, Viva, Partner relationships, Microsoft Edge, Setup, and Reports. The main content area is titled 'Settings' and has a breadcrumb 'Home > Settings'. Below this, there are tabs for 'User access', 'Data access', 'Copilot actions' (selected), and 'Other settings'. A search box for 'Search all Copilot settings' is present. The main heading is 'Settings' and the sub-heading is 'Choose how Copilot responds to user prompts to comply with organizational policies.' Below this is a table with four rows of settings.

Name	Description	Applies to
Copilot video generation	Manage whether users can create generative AI videos with Copilot.	Video content generated by AI across Microsoft 365
Copilot in Teams meetings	Go to the Microsoft Teams admin center to change how Copilot is used in meetings.	Copilot in Microsoft Teams
Copilot image generation	Manage whether users can generate images with Copilot	Designer integrations across Copilot
Copilot AI disclaimer	Choose how prominently the AI disclaimer is shown to users in Microsoft 365 Copilot.	AI disclaimer font settings integrated across Microsoft 365

Copilot Settings #3: Copilot Actions - Teams

The image displays two side-by-side screenshots of administrative interfaces. The left screenshot shows the Microsoft 365 admin center with the 'Settings' page open to 'Copilot actions'. A red arrow points to 'Copilot in Teams meetings'. The right screenshot shows the Microsoft Teams admin center with the 'Recording & transcription' settings page open. Two red arrows point to the 'Require participant agreement for recording, transcription, and Copilot' toggle (which is turned 'On') and the 'Copilot' dropdown menu (set to 'On with saved transcript required').

Microsoft 365 admin center

- Home
- Copilot
 - Overview
 - Connectors
 - Search
 - Billing & usage
 - Settings
 - Agents
 - Users
 - Teams & groups
 - Marketplace
 - Billing
 - Settings
 - Domains
 - Search & intelligence
 - Org settings
 - Microsoft 365 Backup
 - Integrated apps
 - Viva
 - Partner relationships
 - Microsoft Edge
 - Setup
 - Reports

Microsoft Teams admin center

- Content sharing
- Content protection Premium
- Recording & transcription
 - Recording and transcription settings let you control how these features are used in a Teams meeting. [Learn more about recording and transcription settings](#)
 - Meeting recording On
 - Find related settings at [Voice > Calling policies](#) and [Meetings > Live events policies](#)
 - Require participant agreement for recording, transcription, and Copilot On
 - Store recordings outside of your country or region Off
 - Transcription On
 - Find related settings at [Voice > Calling policies](#), [Meetings > Live events policies](#), and [Voice > Voicemail policies](#)
 - Recordings and transcriptions automatically expire On
 - Default expiration time: 120
 - Live captions: Not enabled, but users can enable
 - Real-time-text (RTT) On
 - Copilot On with saved transcript required
- Audio & video

Save **Cancel**

Copilot Settings #3: Copilot Actions - Disclaimer

The image shows a sequence of three screenshots from the Microsoft 365 Admin Center, illustrating the process of configuring the Copilot AI disclaimer.

Left Screenshot: The 'Settings' page is shown with the 'Copilot actions' tab selected. A red arrow points to the 'Copilot AI disclaimer' option in the left-hand navigation pane.

Middle Screenshot: The 'Copilot actions' settings page is displayed. A table lists various Copilot actions, with a red arrow pointing to the 'Copilot AI disclaimer' entry.

Name	Description
Copilot video generation	Manage whether users can create generated content with Copilot.
Copilot in Teams meetings	Go to the Microsoft Teams admin center to manage whether Copilot is used in meetings.
Copilot image generation	Manage whether users can generate images with Copilot.
Copilot AI disclaimer	Choose how prominently the AI disclaimer is shown to users in Microsoft 365 Copilot.

Right Screenshot: The 'Copilot AI disclaimer' configuration window is shown. It includes options for font weight (Standard or Bold), a field for a tooltip URL (containing 'https://url.to.internal.policy'), and a preview section. A red arrow points to the preview area, which shows two examples of the disclaimer: one with standard font weight and one with bold font weight.

Copilot Settings #4: Other Settings

The screenshot shows the Microsoft 365 admin center interface. The top navigation bar includes the Microsoft 365 admin center logo, a search bar, and various utility icons (Copilot, mail, print, notifications, settings, help, and user profile). The left sidebar contains a navigation menu with categories like Home, Copilot, Agents, Users, Teams & groups, Marketplace, Billing, Settings, Domains, Search & intelligence, Org settings, Microsoft 365 Backup, Integrated apps, Viva, Partner relationships, Microsoft Edge, Setup, and Reports. The main content area is titled 'Settings' and shows the 'Other settings' tab selected. Below the tabs is a search bar for Copilot settings and a heading 'Find more settings that can assist your organization's use of Copilot.' A table lists two settings: 'Copilot diagnostic logs' and 'Copilot Custom Dictionary'.

Microsoft 365 admin center

Home > Settings

Enable Light mode

Settings

User access Data access Copilot actions **Other settings**

Search all Copilot settings

Find more settings that can assist your organization's use of Copilot.

Name	Description	Applies to
Copilot diagnostic logs	Send diagnostic logs for Copilot on behalf of individual users who are having issues.	Microsoft 365 Copilot
Copilot Custom Dictionary	Manage custom dictionaries for your organization.	Copilot in Microsoft Teams Microsoft Teams

Admin centers

Copilot Settings #5: <https://config.office.com>

The screenshot displays the Microsoft 365 Apps admin center interface. The left-hand navigation pane includes sections for Home, Cloud Update, Overview, Current, Monthly Enterprise, Customization, Device Configuration, Policy Management (selected), Health, Inventory, Learn More, and Setup. The main content area is titled 'Configure Settings' and shows a progress indicator with 'Basics' and 'Scope' completed, and 'Policies' in progress. Below the progress indicator, summary statistics are shown: Total 7, Security Baseline 0, Accessibility Baseline 0, and Configured 5. A table lists 7 policies with columns for Policy, Platform, Application, Status, and Area. The policies are: 'Adjust responsible AI protections for Microsoft 365 Copilot' (Configured), 'Create and view Copilot Pages and Copilot Notebooks' (Configured), 'Allow web search in Copilot' (Configured), 'Pin Microsoft 365 Copilot Chat' (Configured), 'Copilot AI Disclaimer' (Not configured), 'Enable code previews for AI-generated content in Microsoft 365 ...' (Configured), and 'Multiple account access to Copilot for work documents' (Not configured). At the bottom of the page are 'Back', 'Next', and 'Cancel' buttons.

Microsoft 365 Apps admin center

Home / Policy Management

Configure Settings

Select policy settings for this configuration

Total 7 | Security Baseline 0 | Accessibility Baseline 0 | Configured 5

7 Policies Filter Search

Policy	Platform	Application	Status	Area
Adjust responsible AI protections for Microsoft 365 Copilot	Windows +3	Office	✓ Configured	None
Create and view Copilot Pages and Copilot Notebooks	Windows +3	Office	✓ Configured	None
Allow web search in Copilot	Windows +3	Office	✓ Configured	None
Pin Microsoft 365 Copilot Chat	Windows +3	Office	✓ Configured	None
Copilot AI Disclaimer	Windows +3	Office	Not configured	None
Enable code previews for AI-generated content in Microsoft 365 ...	Windows +3	Office	✓ Configured	None
Multiple account access to Copilot for work documents	Windows +3	Office	Not configured	None

Back Next Cancel

Copilot Settings #6: Service Health

Microsoft 365 admin center

Home > Service health

Service health

Overview Issue history Reported issues

View the issues and health status of all services that are available with your current subscriptions. [Learn more](#)

[Report an issue](#) [Customize](#)

Active issues Microsoft is working on

Issue title
Users may be unable to use the AI features in the Create module of Microsoft Copilot (Microsoft 365)

Service status

Service	Status
Microsoft Copilot (Microsoft 365)	1 advisory
Microsoft 365 Copilot Chat	Healthy
Microsoft Copilot (Power Platform)	Healthy

Customize

Page view Email

Show health status for these services only *

- Basic Mobility and Security
- Dynamics 365 Apps
- Exchange Online
- Microsoft 365 Copilot Chat
- Microsoft 365 apps
- Microsoft 365 for the web
- Microsoft 365 suite
- Microsoft Bookings
- Microsoft Clipchamp
- Microsoft Copilot (Microsoft 365)
- Microsoft Copilot (Power Platform)
- Microsoft Dataverse
- Microsoft Defender XDR
- Microsoft Entra
- Microsoft Forms
- Microsoft Intune
- Microsoft OneDrive

Save

Copilot Settings #6: Message Center

The screenshot shows the Microsoft 365 admin center interface. The top navigation bar includes the Microsoft 365 admin center logo, a search bar, and various utility icons like Copilot, mail, documents, notifications, settings, and help. The left sidebar contains navigation options such as Home, Copilot, Agents, Users, Teams & groups, Marketplace, Billing, Settings, Setup, Reports, Health, Service health, Windows release health, Message center, Product feedback, Network connectivity, Software updates, Admin centers, All admin centers, Customize navigation, and Show all.

The main content area is titled "Message center" and includes a breadcrumb "Home > Message center". Below the title is a descriptive paragraph: "Each message gives you a high-level overview of a planned change and how it may affect your users, and links out to more detailed information to help you prepare. [Learn more about managing changes](#)".

There are two tabs: "Inbox" (selected) and "Archive". Below the tabs are "Preferences" and "Planner syncing" options. A "Filters" section includes buttons for "Service", "Tag", "Message state", "Relevance", "Status for your org", and "Platform".

The message list shows several entries, each with a checkbox, a message title, a star icon, and a service tag. The visible titles are:

- Message title
- (Updated) Microsoft 365 Copilot for Android: Preview and chat with Word, Excel, and PowerPoint files in the Copilot app
- (Updated) Microsoft 365 Copilot: RSVP to meetings directly in Copilot chat
- (Updated) Microsoft Purview | Compliance Manager - AI Powered Regulatory Templates
- (Updated) New request and approval experience for Microsoft agents in the Microsoft 365 admin center
- (Updated) Microsoft 365 Copilot: "Hey Copilot" to start voice in Copilot on Windows devices
- (Updated) Microsoft 365 Copilot: Generate text for a PowerPoint slide using slide context

The "Preferences" panel is open on the right, showing two tabs: "Custom View" (selected) and "Email". The text below the tabs reads: "You can customize which messages show up in the list either by selecting the service or tag." Under the heading "Show messages for these services", there is a list of services with checkboxes:

- Basic Mobility & Security
- Dynamics 365 Apps
- Exchange Online
- General announcement
- Microsoft 365 Apps
- Microsoft 365 Copilot
- Microsoft 365 Copilot Chat
- Microsoft 365 for the web
- Microsoft 365 suite
- Microsoft Bookings
- Microsoft Clipchamp
- Microsoft Copilot (Power Platform)
- Microsoft Dataverse
- Microsoft Defender XDR

A "Save" button is located at the bottom of the preferences panel.

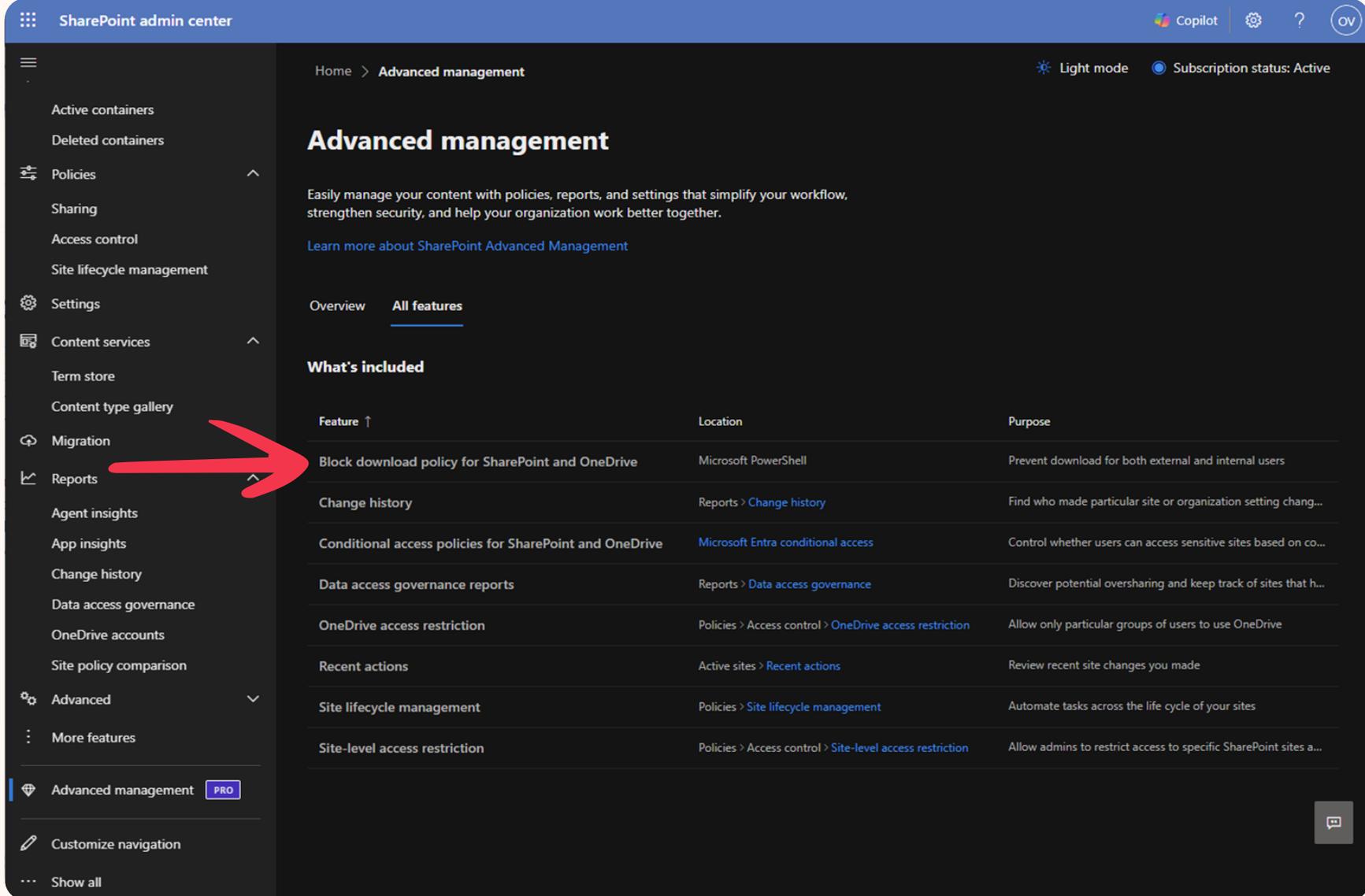


Data Discovery Configuration



Copilot Settings: SharePoint Advanced Management

- At least one Copilot License – you have access
- Strong Copilot Readiness toolkit
- Tenant-wide visibility and content insights
- Copilot-ready data governance and quality control



The screenshot displays the SharePoint Admin Center interface. The top navigation bar includes the 'SharePoint admin center' title, a 'Copilot' icon, and a 'Subscription status: Active' indicator. The left-hand navigation pane lists various administrative areas, with 'Advanced management' highlighted in blue and marked with a 'PRO' badge. A red arrow points to the 'Reports' link in this pane. The main content area is titled 'Advanced management' and provides an overview of content management tools. Below the overview, there is a table titled 'What's included' with columns for 'Feature', 'Location', and 'Purpose'.

Feature ↑	Location	Purpose
Block download policy for SharePoint and OneDrive	Microsoft PowerShell	Prevent download for both external and internal users
Change history	Reports > Change history	Find who made particular site or organization setting changes
Conditional access policies for SharePoint and OneDrive	Microsoft Entra conditional access	Control whether users can access sensitive sites based on conditions
Data access governance reports	Reports > Data access governance	Discover potential oversharing and keep track of sites that have been accessed
OneDrive access restriction	Policies > Access control > OneDrive access restriction	Allow only particular groups of users to use OneDrive
Recent actions	Active sites > Recent actions	Review recent site changes you made
Site lifecycle management	Policies > Site lifecycle management	Automate tasks across the life cycle of your sites
Site-level access restriction	Policies > Access control > Site-level access restriction	Allow admins to restrict access to specific SharePoint sites and OneDrive accounts

Copilot Settings: SharePoint – Site Level Restrictions

The image displays two overlapping screenshots of the SharePoint Admin Center interface. The left screenshot shows the 'Access control' section in the left-hand navigation pane, with a red arrow pointing to it. The right screenshot shows the 'Active sites' list with the 'DEMO' site selected, and the 'Settings' tab for that site. A red arrow points to the 'Restrict content from Microsoft 365 Copilot' setting, which is currently set to 'On'. Other settings visible include 'Email', 'Privacy', 'External file sharing', 'Sensitivity label', 'Restricted site access', and 'Version history limit'. The 'DEMO' site is identified as a 'Private group'.

SharePoint admin center

Access control
Use these settings to restrict how users are allowed to access content.

- Unmanaged devices
Restrict access from devices that aren't connected to the network.
- Idle session sign-out
Automatically sign out users from inactive sessions.
- Network location
Allow access only from specific IP addresses.
- Apps that don't use modern authentication
Block access from Office 2010 and other applications.
- Site-level access restriction **PRO**
Allow SharePoint Administrators and site administrators to restrict access to content.
- OneDrive access restriction
Restrict access to OneDrive content by security groups.

Active sites
Use this page to sort and manage active sites. [Learn more about managing sites.](#)

DEMO
Private group
Email View site Delete

General Activity Membership **Settings**

Email

- Let people outside the organization email this team
- Send copies of team emails and events to team members' inboxes
- Don't show team email address in Outlook

Privacy

- Private
- Public

External file sharing

New and existing guests

[More sharing settings](#)

Restrict content from Microsoft 365 Copilot **PRO**

- On
- Off

Custom scripts

Blocked Edit

Sensitivity label

None

Restricted site access **PRO**

Not set Edit

Version history limit

Same as Organization-level (Manual)

Save

Copilot Settings: SharePoint – User Access Report

The image shows a screenshot of the SharePoint Admin Center interface. The main content area is titled "Site permissions for users" under the "Data access governance" section. It includes a description: "Identify all sites a user can access and determine whether they can access the entire site or specific sections, granted directly to the user or indirectly through groups as of the report date." Below this is a "Create a report" dialog box. The dialog box has the following fields and options:

- Added users:** 2 [Edit](#)
- Scope:** SharePoint, OneDrive
- Report name:** OneDrive User Access Report

At the bottom of the dialog box are two buttons: "Create and run" and "Cancel".

The background interface shows the "Data access governance" sidebar with various options like "Active containers", "Policies", "Sharing", "Access control", "Site lifecycle management", "Settings", "Content services", "Term store", "Content type gallery", "Migration", "Reports", "Agent insights", "App insights", "Change history", "Data access governance", "OneDrive accounts", "Site policy comparison", "Advanced", "More features", "Advanced management", and "Customize navigation".

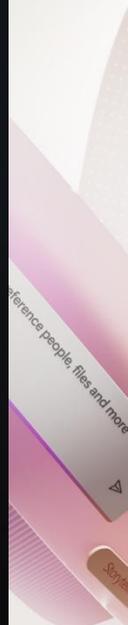
Copilot Settings: SharePoint – Site Permissions

The screenshot displays the SharePoint Admin Center interface. On the left is a navigation pane with categories like Active containers, Policies, Sharing, Access control, Site lifecycle management, Settings, Content services, Term store, Content type gallery, Migration, Reports, Agent insights, App insights, Change history, Data access governance (selected), OneDrive accounts, Site policy comparison, Advanced, More features, and Advanced management (PRO). The main content area is split into two panels. The left panel, titled 'Data access governance', includes a 'Reports' section with 'All review requests' and a 'Get started' card. The right panel, titled 'Site permissions across your organization', shows a 'SharePoint report' and a 'OneDrive report', both with 'Generating report' status and a 'View report' button. The top right of the interface includes 'Copilot', 'Light mode', and a user profile icon.

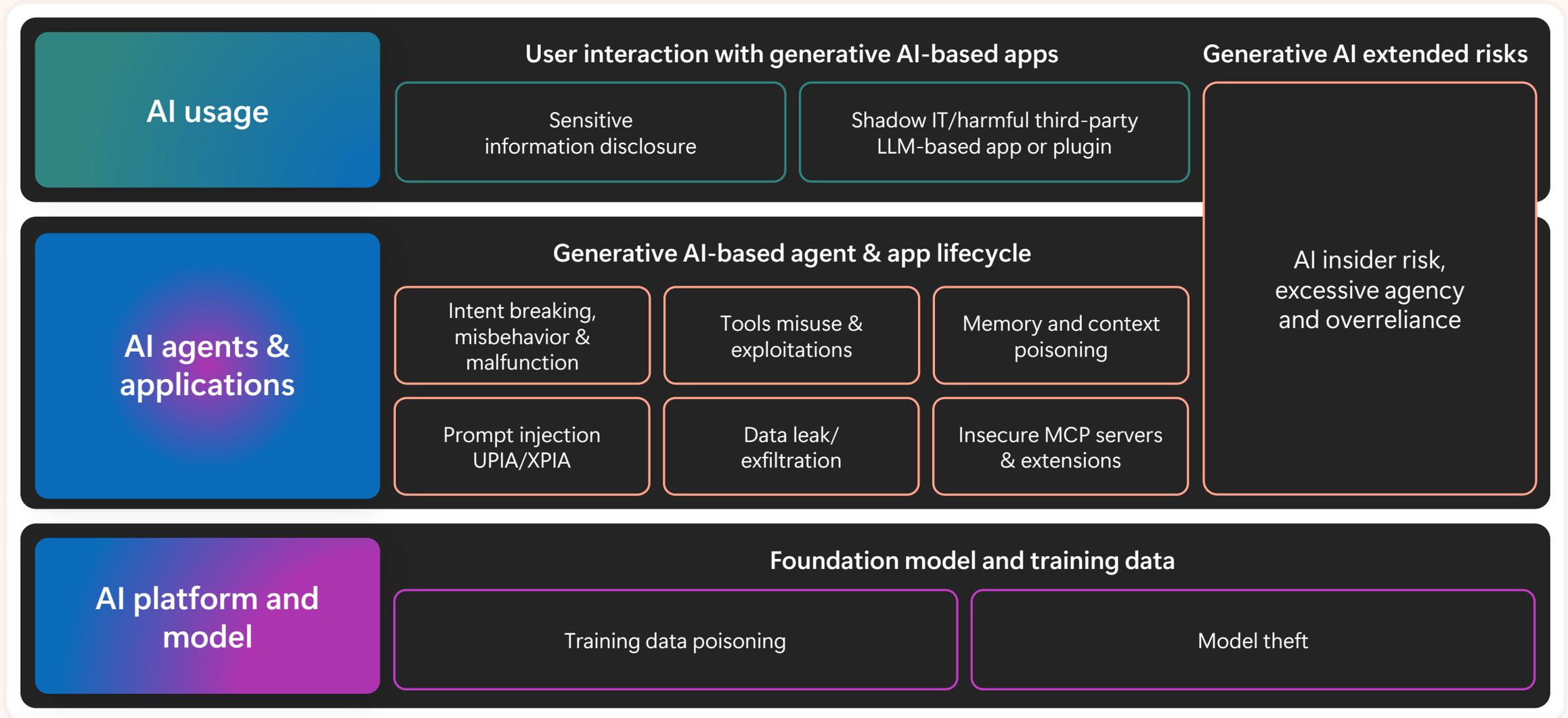
Reports to help identify overshared sites and provide recommended actions to mitigate risks.



Security Best Practices

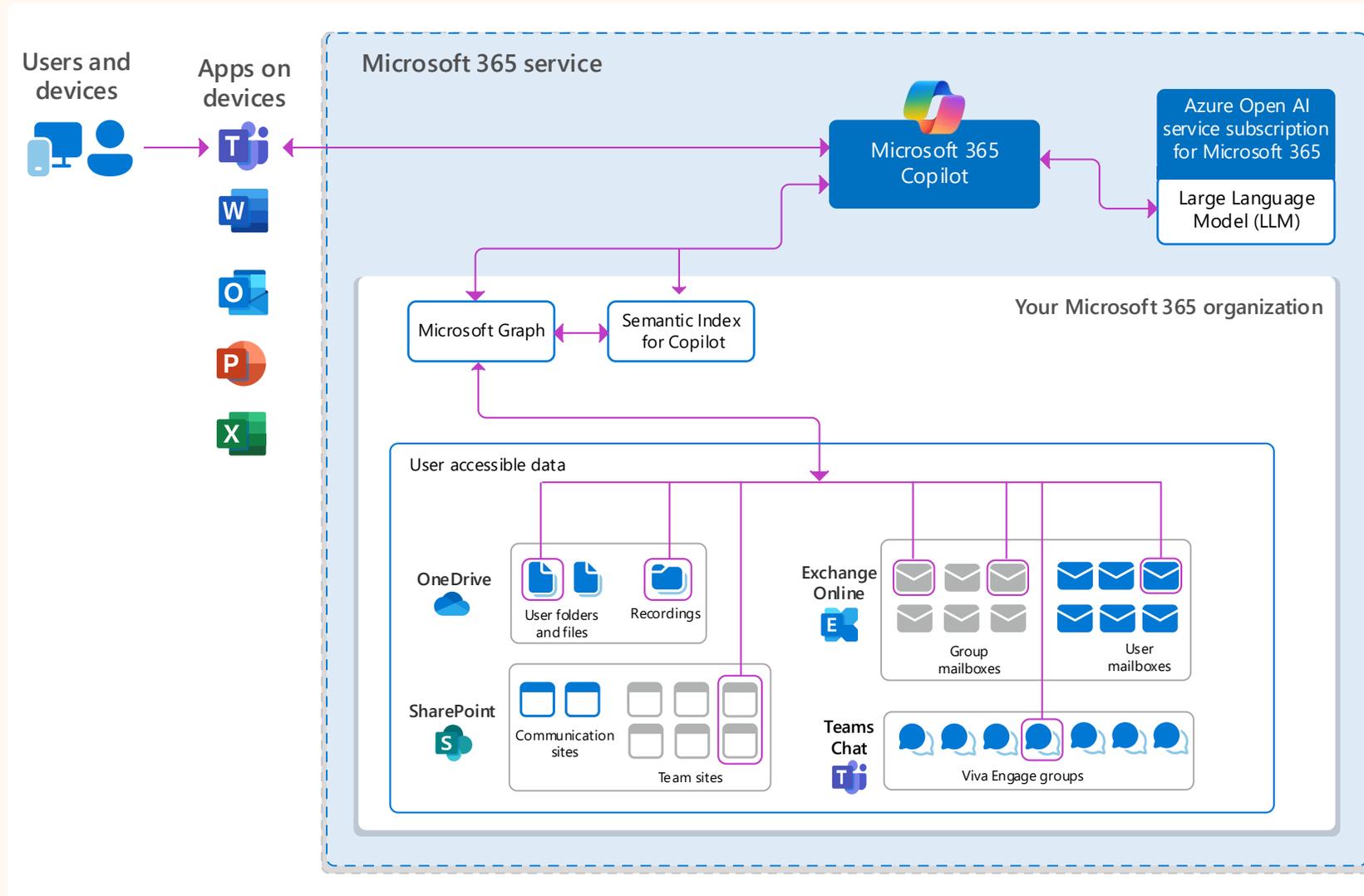


Evolving threat map with the rise of (agentic) AI



Zero Trust with Microsoft 365 Copilot

- Data protection
- Identity and access
- App protection
- Device management and protection
- Threat protection
- Secure collaboration with Teams
- User permissions to data



[How do I apply Zero Trust principles to Microsoft 365 Copilot?](#)

Microsoft Purview

https://purview.microsoft.com/fabrikam/en-us/

Microsoft Purview Preview

Home

DSPM for AI

Overview

Recommendations

Reports

Data assessments Preview

Policies

Activity explorer

Data assessments

Assessment for the week of November 1, 2024

Assessment info

Description
Default assessment

Total items: 22842 Users included: 100

Sources included: 105

[View assessment details](#)

Total items

22.8K

Scanned for sensitive info types (Green) Not scanned (Red)

Sensitivity labels on data

Labeled: [Progress bar]

Not labeled: [Progress bar]

No sensitive info types detected (Green) Sensitive info types detected (Yellow) Data (Red)

Sources

Data source ID ↓	Source type	Total items	Total items accessed	Times users accessed items ⓘ	Unique users accessing items
/sites/ObsidianMerger/	SharePoint	47000	4432	8076	700
/sites/Contoso	SharePoint	65784	873	938	456
/sites/Jasper	SharePoint	76845	653	783	243

Obsidian Merger

Overview **Protect** Monitor

Limit Microsoft 365 Copilot access to this site

Choose how you would like Copilot to access data in this SharePoint site.

Restrict access by label
Microsoft Purview Data Loss Prevention

Restrict all items
SharePoint Restricted Content Discovery

Labels found in this site

Sensitivity labels: **8**
[View all labels](#)

Labels referenced by Copilot: **5**
[View labels referenced](#)

Use a Microsoft Purview Data Loss Prevention policy to limit access to any files in your organization with sensitivity labels. [Learn more about this policy](#)

Steps at a glance

1. Go the Data Loss Prevention in Microsoft Purview portal.
2. Create new policy. Select "Policies" to create a new policy
3. Choose a custom policy. Select Custom policy in the Custom category
4. Customize your policy. Name your policy, and then select "Microsoft 365 Copilot" in the location.
5. Create an new advanced DLP rule.
6. Add labels you want to excluded. In the fields for the new rule, Select "Content contains sensitivity labels" and add the labels
7. Select an action. Choose "Exclude Copilot from processing"
8. Save the rule and the policy.

Other labeling policies

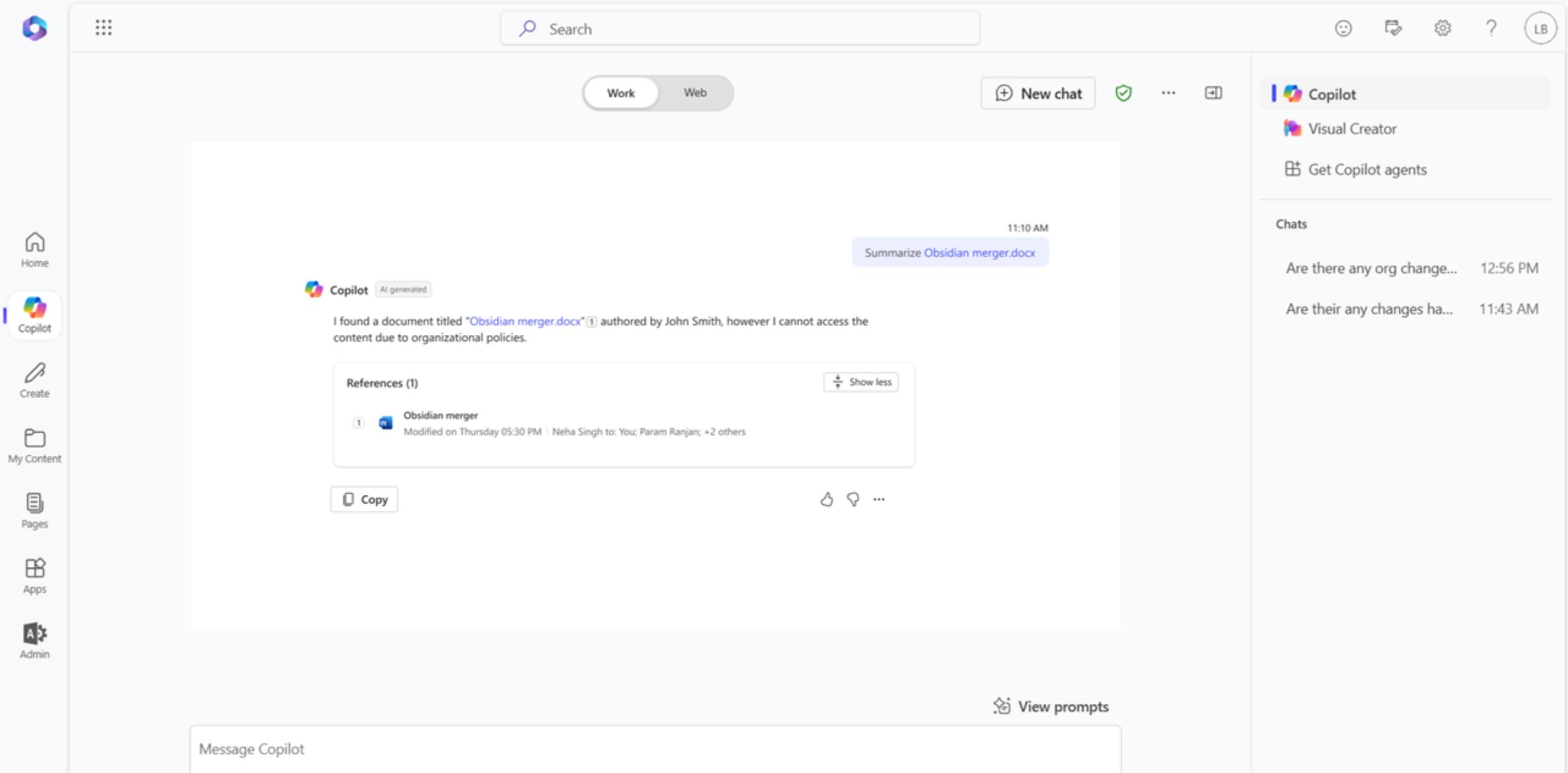
Default sensitivity label for SharePoint document library

When a default sensitivity label gets created, the label will only apply to new items added to the site. Select a sensitivity label within the SharePoint site.

Oversharing assessments help identify overshared sites and content and provide recommended actions to mitigate risks.

/sites/Marketing	SharePoint	87593	3759	8190	74
------------------	------------	-------	------	------	----

Label all new items by default using sensitivity labels. Labels can have no protection or protection defined by the admin.

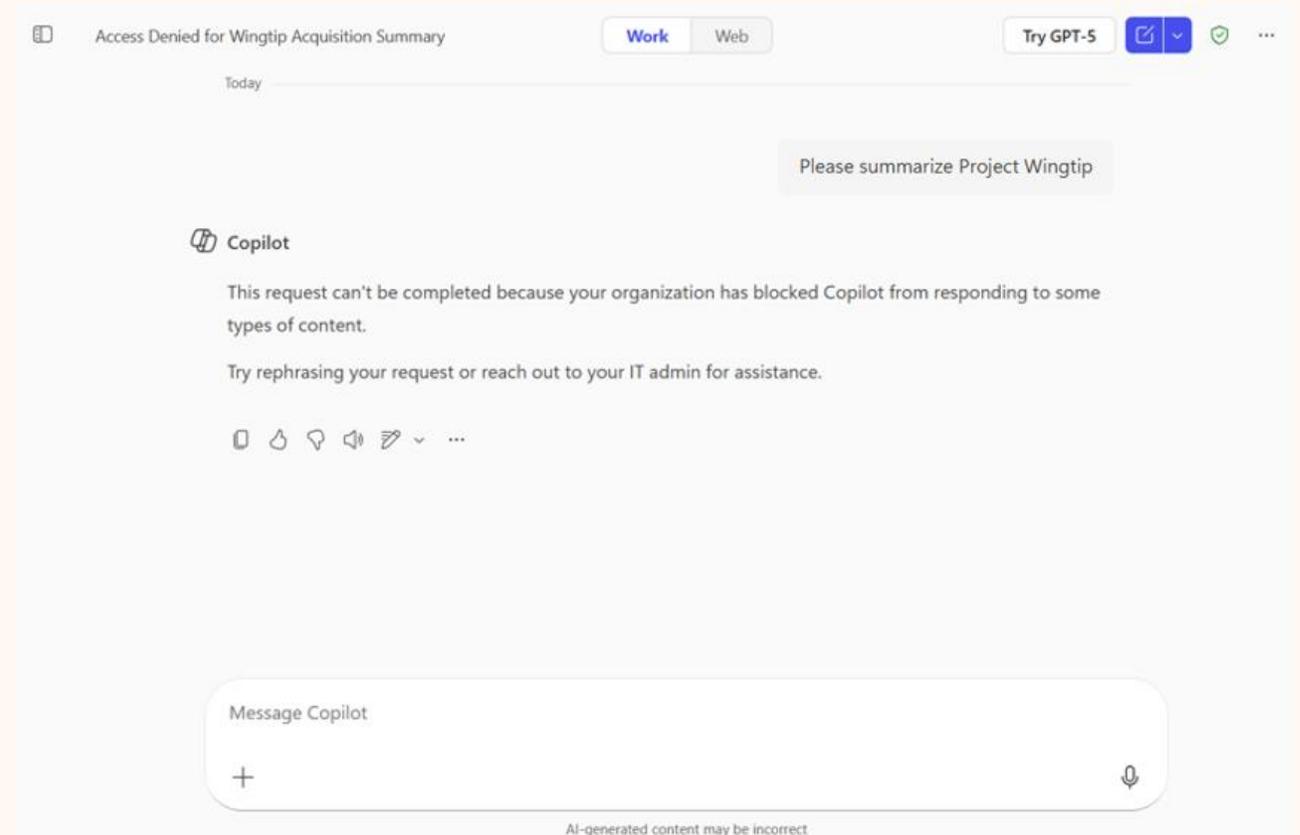


Purview DLP for Microsoft 365 Copilot policy can prevent Copilot from using sensitive data to generate responses.

Microsoft Purview DLP to safeguard prompts

Reduce data leakage and oversharing risks with real-time protection for sensitive data in prompts

- Prevents Copilot from responding to prompts, connecting to internal data sources, and performing web searches, if the prompt contains sensitive data
- Extends to Copilot Chat, M365 Copilot, and agents built in Copilot Studio that are published to Microsoft 365 Channel.



Project Wingtip is on the organization's sensitive information block list

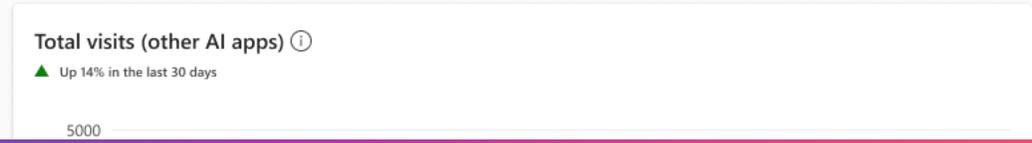
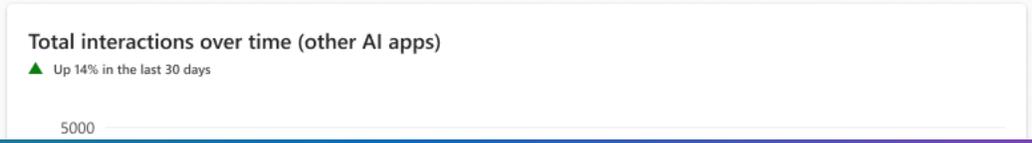
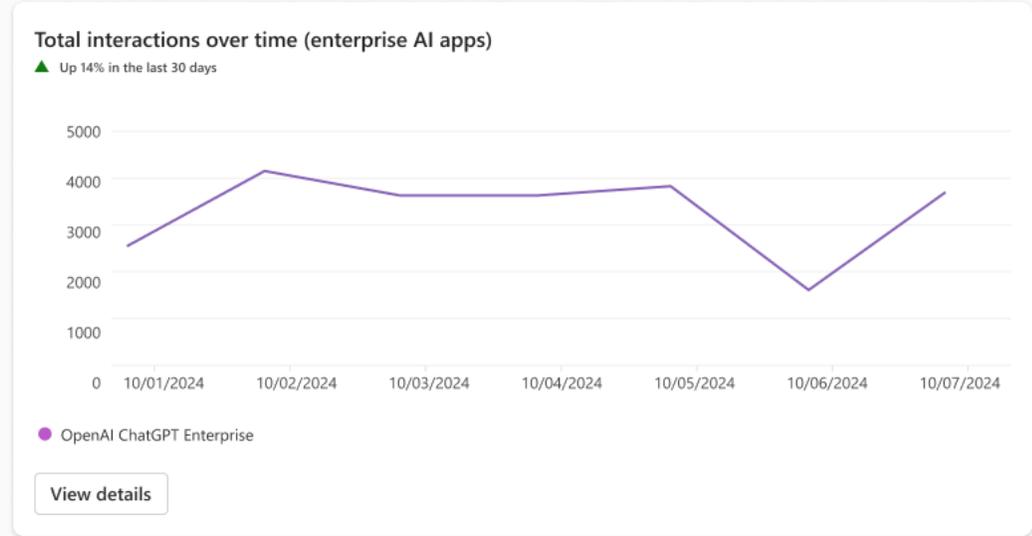
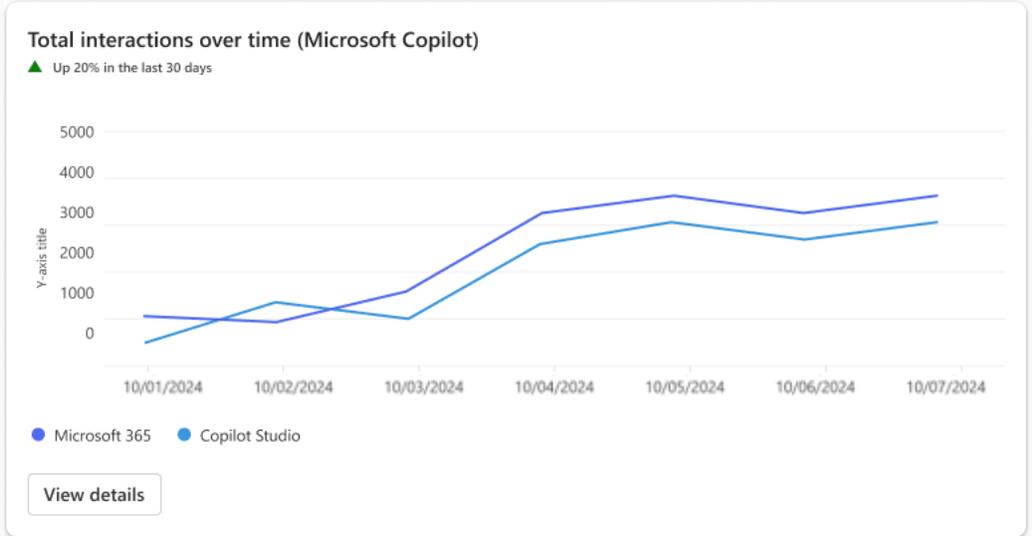
Rollout start to Public Preview Nov 2025

← Overview

Reports

- Microsoft Copilot experiences
- Enterprise AI apps
- Other AI apps

Activity



Copilot and Purview

Capability or solution in Microsoft Purview	Supported for AI interactions
DSPM for AI (classic) and DSPM (preview)	✓
Auditing	✓
Data classification	✓
Sensitivity labels	✓
Encryption without sensitivity labels	✓
Data loss prevention	✓
Insider Risk Management	✓
Communication compliance	✓
eDiscovery	✓
Data Lifecycle Management	✓
Compliance Manager	✓

<https://learn.microsoft.com/en-us/purview/ai-m365-copilot>



Copilot Data Privacy and Security



ChatGPT vs Microsoft 365 Copilot Chat



ChatGPT (Pro)



ChatGPT (Business)



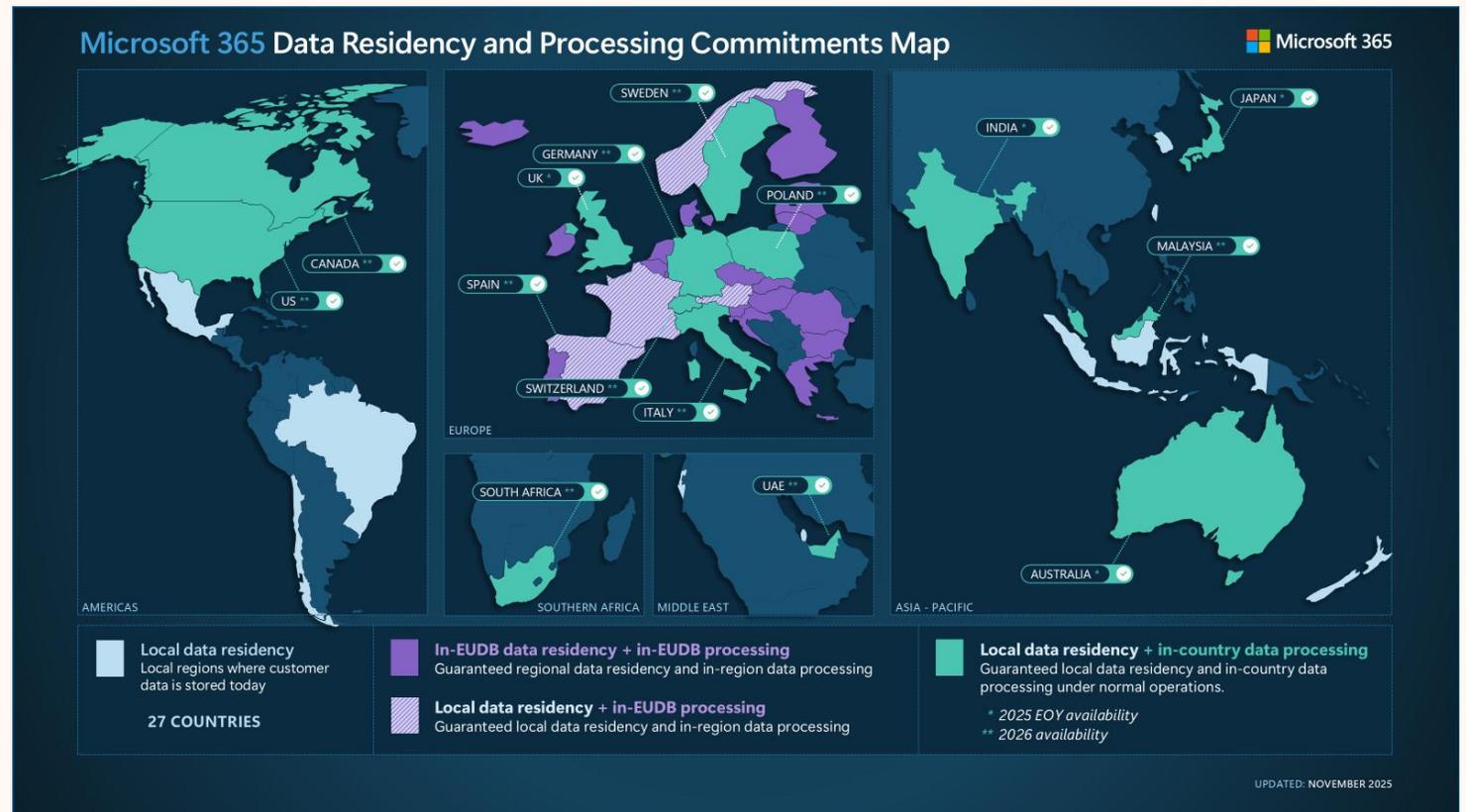
Copilot (Chat & Paid)

Use of data for model training	Data is used unless the user explicitly opts out	Not used. Data may be used for operations, security, and detection	Not used. Data may be used for Microsoft 365 telemetry
Who operates the service	OpenAI	OpenAI	Microsoft
Where the service is operated	Global OpenAI infrastructure. Region not configurable	Global OpenAI infrastructure, no guarantee of a specific region	Azure datacenters in the region of your M365 tenant, within service boundaries
Data residency	Not available. Data may be stored globally	Not available for Business. Data residency only for ChatGPT Ent / Edu	Yes. Governed by Microsoft 365 tenant settings / Preferred Data Location
Security and compliance	Shared multi-tenant OpenAI service	Multi-tenant OpenAI service with data encryption and basic administration	Uses the same identity, encryption, DLP, audit, and compliance controls as M365
Administration and retention	Managed by the end user. Retention governed by OpenAI consumer policies	Managed by workspace admin and users. Retention by OpenAI for Business	Managed by M365 tenant admin. Retention by existing M365 policies

Local Processing for prompts and responses

In-country data handling for secure, compliant Microsoft 365 Copilot experiences

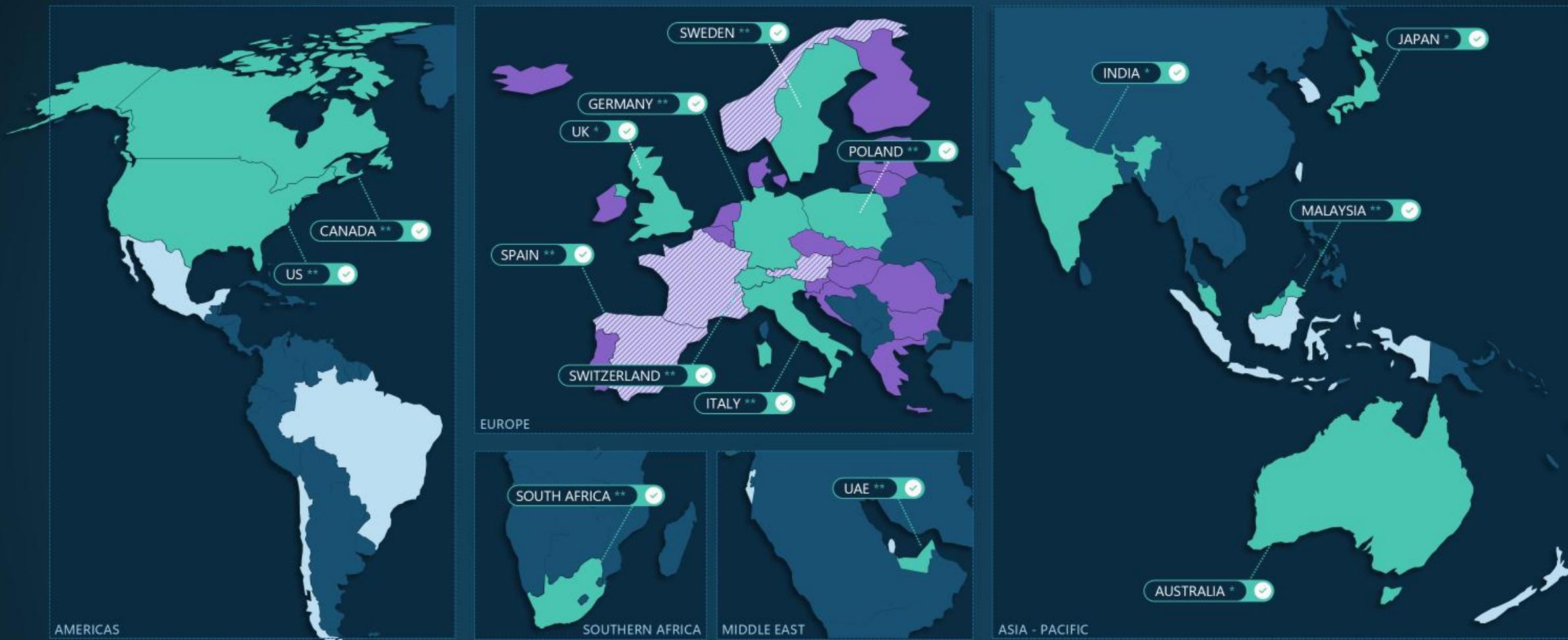
- Process Microsoft 365 Copilot interactions in-country to keep data local and safeguard privacy and integrity.
- Enables compliance for regulated industries by keeping data local and meeting legal requirements.
- Available by end of 2025 customers in Australia, UK, Japan, and India and an additional 11 countries¹ throughout 2026.



Rollout start Dec 2025

1. UAE, Canada, Germany, Italy, Malaysia, Poland, South Africa, Spain, Sweden, Switzerland, US

Microsoft 365 Data Residency and Processing Commitments Map



 Local data residency Local regions where customer data is stored today 27 COUNTRIES	 In-EUDB data residency + in-EUDB processing Guaranteed regional data residency and in-region data processing	 Local data residency + in-country data processing Guaranteed local data residency and in-country data processing under normal operations. * 2025 EOY availability ** 2026 availability
 Local data residency + in-EUDB processing Guaranteed local data residency and in-region data processing		

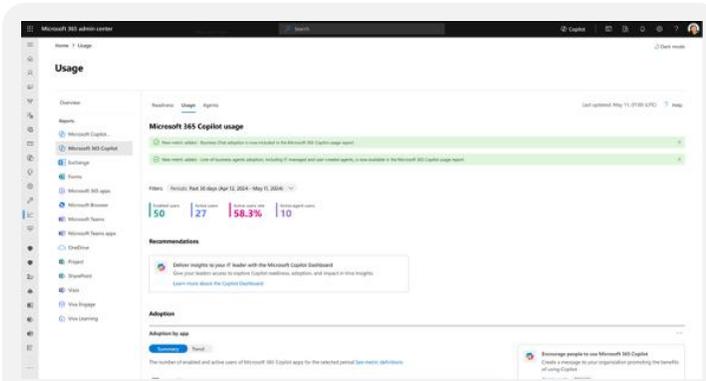


Reporting & Monitoring



Copilot and Agent Analytics

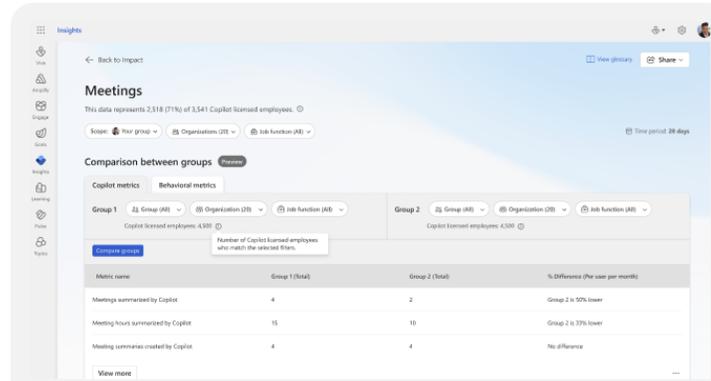
Measure the impact of Copilot and agents on your business



Admin Center

Usage & Adoption

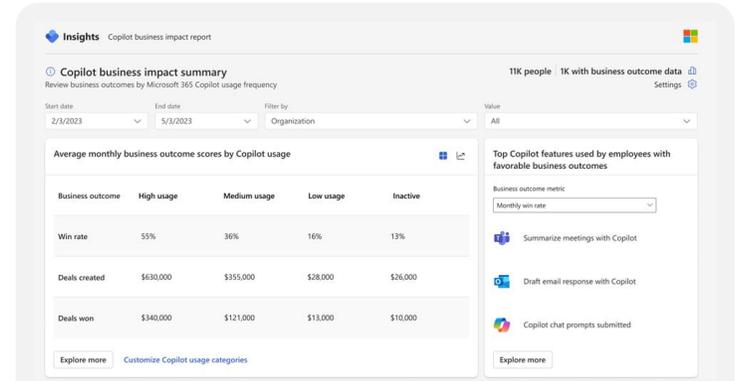
See Copilot and Agents usage and adoption trends



Copilot and Agent Dashboards

Impact & Productivity

Explore how AI transforms the way your teams work.



Advanced Reporting (Insights)

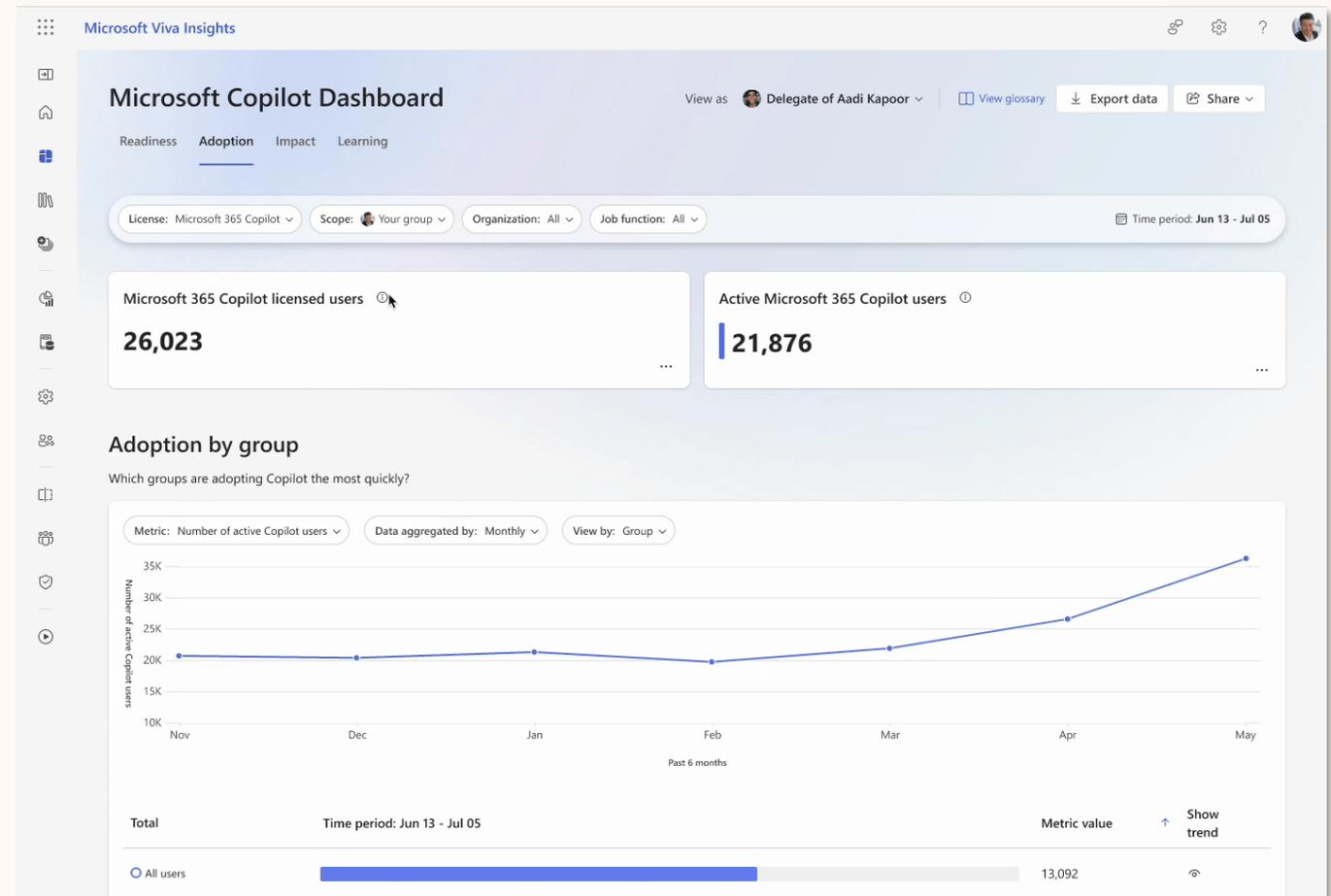
Business value & ROI

Measure the value of Copilot and Agents on your business processes

Copilot Chat reports

Analyze Microsoft 365 Copilot Chat adoption in the Copilot Dashboard

- **View** total users, adoption trends by group, usage intensity, and retention.
- **Understand** how different groups use Copilot Chat across the Microsoft 365 apps.
- **Spot trends and identify top groups** to accelerate adoption by filtering on usage with organizational attributes.



Rollout start to general availability Nov 2025
for customers with 50+ M365 Copilot licenses

Teams Admin Center

Delegate and scale Microsoft Teams administration tasks with dedicated agents

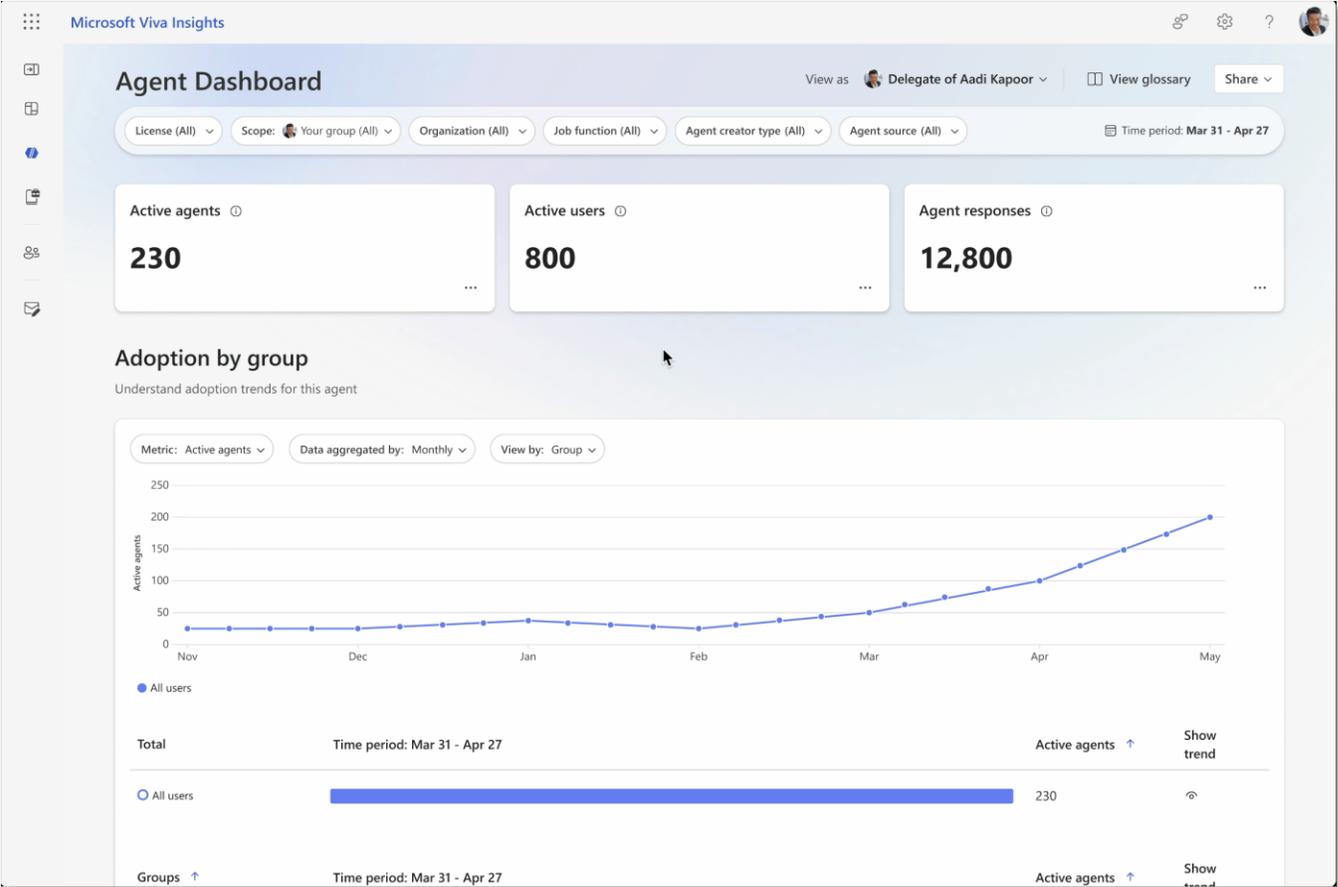
- **Delegate tasks** like meeting monitoring and scale your expertise.
- **Stay in control** while the agents accomplish the tasks autonomously and securely.
- **Focus on what matters most** with intelligent prioritization and remediate issues **proactively**.



Agent Dashboard

Measure the adoption and impact of agents across your organization

- View **performance metrics for all agents**, including your custom-built agents, Microsoft agents, and third-party agents.
- **Understand agent adoption trends** across teams, functions, and more.
- **Identify** your most popular agents and **dive deeper** into how **specific agents are used**.



Rollout start to Public Preview Jan 2026 Rollout start to worldwide Feb 2026

Audit logs for Copilot and AI applications

- Copilot User interaction and admin activities are part of Audit Standard
- Non-Microsoft AI applications are billed pay-as-you-go

[Audit logs for Copilot and AI applications](#)

[Auditing solutions in Microsoft Purview](#)

The screenshot displays the Microsoft Purview Audit logs search interface. The search filters are as follows:

- Search:** Audit retention policies
- Searches completed:** 2
- Active searches:** 0
- Active unfiltered searches:** 0
- Date and time range (UTC) Start:** Jan 09 2026 00:00
- Date and time range (UTC) End:** Jan 10 2026 00:00
- Keyword Search:** Enter the keyword to search for
- Admin Units:** Choose which Admin Units to search for
- Activities - friendly names:** Choose which activities to search for
- Activities - operation names:** Enter operation values, separated by commas
- Record Types:** Select the record types to search for. The dropdown menu is open, showing the following options:
 - copilot
 - CopilotInteraction
 - CreateCopilotPlugin
 - CreateCopilotPromptBook
 - CreateCopilotWorkspace
 - DeleteCopilotPlugin
 - DeleteCopilotPromptBook
- Users:** Add the users whose audit logs you want to search
- ObjectID (File, folder, or site):** Enter all or a part of the name of a file, website, or folder
- Workloads:** Enter the workloads to search for

The search results table shows the following entry:

Search name	Creation ti...	Search performed by
<input type="checkbox"/> Dec 28 - Jan 10 CopilotInteraction.Microsoft365CopilotScheduledPrompt.OutlookCopilotAutomation	Completed 100% 2m, 59s 1406	Jan 10, 2026 1:08 ... ondrej@vysek.net

Microsoft Purview

Home

Solutions

Agents

Learn

Usage center (preview)

Settings

Audit

DSPM (preview)

Compliance Manager

DSPM for AI (classic)

Audit

Search

Policies

Pay-as-you-go usage

Related solutions

eDiscovery

Data Security Investigations

Home

Solutions

Agents

Learn

Usage center (preview)

Settings

Audit

DSPM (preview)

Compliance Manager

DSPM for AI (classic)

Audit

Search

Policies

Pay-as-you-go usage

Related solutions

eDiscovery

Data Security Investigations

Audit > Audit search

Search Query Information: Sun, 28 Dec 2025 00:00:00 GMT to Sat, 10 Jan 2026 00:00:00 GMT
 Microsoft365CopilotScheduledPrompt, OutlookCopilotAutomation, , {S

Total Result Count: 1406 items

Export

Date (UTC) ↓	IP Address ↓	User ↓	Record Type ↓	
Jan 9, 2026 10:19 PM	2a00:1268:2a:1000:d9b3:8b...	ondrej@vysek.net	CopilotInteracti...	
Jan 9, 2026 9:39 PM	2a00:1268:2a:1000:d9b3:8b...	ondrej@vysek.net	CopilotInteracti...	
Jan 9, 2026 9:14 PM	::ffff:10.0.29.11	ondrej@vysek.net	CopilotInteracti...	
Jan 9, 2026 4:12 PM	20.86.93.35	ondrej@vysek.net	CopilotInteracti...	
Jan 9, 2026 3:03 PM	20.86.93.35	ondrej@vysek.net	CopilotInteracti...	
Jan 9, 2026 7:03 AM	2a00:1268:2a:1000:d9b3:8b...	ondrej@vysek.net	CopilotInteracti...	
Jan 9, 2026 5:52 AM	20.86.93.35	ondrej@vysek.net	CopilotInteracti...	
Jan 9, 2026 5:42 AM	20.86.93.35	ondrej@vysek.net	CopilotInteracti...	
Jan 9, 2026 5:03 AM	20.86.93.35	ondrej@vysek.net	CopilotInteracti...	
Jan 9, 2026 4:09 AM	20.86.93.35	ondrej@vysek.net	CopilotInteracti...	
Jan 8, 2026 8:45 PM	20.86.93.35	ondrej@vysek.net	CopilotInteracti...	
Jan 8, 2026 8:12 PM	::ffff:10.0.29.11	ondrej@vysek.net	CopilotInteracti...	
Jan 8, 2026 8:08 PM	::ffff:10.0.29.9	ondrej@vysek.net	CopilotInteracti...	
Jan 8, 2026 7:24 PM	2a00:1268:2a:1000:d9b3:8b...	ondrej@vysek.net	CopilotInteracti...	
Jan 8, 2026 8:08 PM	::ffff:10.0.29.9	ondrej@vysek.net	CopilotInteraction	Interacted with C...
Jan 8, 2026 7:24 PM	2a00:1268:2a:1000:d9b3:8b...	ondrej@vysek.net	CopilotInteraction	Interacted with C...

Details

UserType
0

Version
1

Workload
Copilot

ClientIP
20.86.93.35

UserId
ondrej@vysek.net

ClientRegion
prd

CopilotEventData

```
{
  "AccessedResources": [],
  "AppHost": "Autonomous",
  "MessageIds": [],
  "Messages": [
    {
      "Id": "1767975133001",
      "isPrompt": true
    },
    {
      "Id": "1767975133002",
      "isPrompt": false
    }
  ],
  "ThreadId": "19:aM0ufAb1lhhim28gUDtTxTR3uw_v1AoU2YaDIGING1@t"
}
```

CopilotLogVersion
1.0.0.0

Close

Audit

The screenshot displays the Microsoft Purview interface. The top navigation bar includes the Microsoft Purview logo, a search bar, and the Copilot icon. The left sidebar contains a navigation menu with categories like Home, Solutions, Agents, Learn, Usage center, and Related solutions. The main content area is titled 'Cases > Content Search > Review sets > Demo Review Set'. It features a table of cases with columns for Subject/Title, Status, Tag Stat..., and Date. The table shows 53 rows, with row 50 selected. A Copilot chat window is open on the right, displaying a conversation about creating a QR code for a specific URL.

Microsoft Purview Search

Copilot

Cases > Content Search > Review sets > Demo Review Set

Search Hold Review set Export

Process manager

1 of 290 selected

	#	Subject/Title	Status	Tag Stat...	Date (U
<input type="checkbox"/>	42.2	Microsoft Copilot.h...	Ready	No Tag	Dec 6, 2
<input type="checkbox"/>	> 43	analyze attached fil...	Ready	No Tag	Jan 7, 2
<input type="checkbox"/>	> 44	in the TestDocume...	Ready	No Tag	Sep 12,
<input type="checkbox"/>	> 45	["visualizer":"plotly"...	Ready	No Tag	Dec 6, 2
<input type="checkbox"/>	> 46	Adoption Data.xlsx ...	Ready	No Tag	Dec 6, 2
<input type="checkbox"/>	> 47	Recommended Ch...	Ready	No Tag	Jan 3, 2
<input type="checkbox"/>	> 48	Směrnice o použív...	Ready	No Tag	Sep 4, 2
<input type="checkbox"/>	> 49	Python Script for In...	Ready	No Tag	Jan 3, 2
<input checked="" type="checkbox"/>	50	using python creat...	Ready	No Tag	Dec 4, 2
<input type="checkbox"/>	50.1	Microsoft Copilot.h...	Ready	No Tag	Jan 7, 2
<input type="checkbox"/>	50.2	Microsoft Copilot.h...	Ready	No Tag	Jan 7, 2
<input type="checkbox"/>	50.3	Microsoft Copilot.h...	Ready	No Tag	Jan 7, 2
<input type="checkbox"/>	50.4	Microsoft Copilot.h...	Ready	No Tag	Jan 7, 2

using python create a QR code for https://softwareone.com

Source Plain text Annotate Metadata

Show pinned metadata

Copilot Chat <copilotchat@vysek.net> 12/4/2025 1:45 PM

using python create a QR code for https://softwareone.com and execute it

Message deleted: 12/4/2025 1:45 PM

Microsoft Copilot 12/4/2025 1:45 PM

Analysis

```
python import qrcode # Data to encode in the QR code data = "https://softwareone.com" # Create QR code instance qr = qrcode.QRCode( version=1, error_correction=qrcode.constants.ERROR_CORRECT_H, box_size=10, border=4, ) # Add data to the QR code qr.add_data(data) qr.make(fit=True) # Generate the QR code image img = qr.make_image(fill_color="black", back_color="white") # Save the QR code image img.save("softwareone_qrcode.png") # Print success message
```

Tag Group by families (5) Group by conversations (5)

Viewing: Page 1 of 2 | 1-50 of 53 Rows

Items per page 50

Jan 4, 2026 11:48 AM 28:b929e817-efe8-f011-8406-7c1...

Copilot Reporting: Basics

The screenshot displays the Microsoft 365 admin center interface, specifically the Copilot Usage reporting page. The page is titled "Usage" and shows the following data for the period of Dec 8, 2025 - Jan 6, 2026:

- Enabled users: 2
- Active users: 1
- Active users rate: 50.0%
- Active agent users: 1
- Total prompts submitted: 75
- Average prompts submitted per user: 75

The dashboard also includes a "Recommendations" section with a card titled "Deliver insights to your IT leader with the Microsoft Copilot Dashboard" and an "Adoption" section with a bar chart showing adoption by app. The bar chart shows 2 enabled users and 1 active user across various Microsoft 365 apps.

Adoption by app

App	Enabled Users	Active Users
Microsoft 365 Copilot	2	1
Microsoft Teams	0	0
Microsoft Outlook	0	0
Microsoft Word	0	0
Microsoft Excel	0	0
Microsoft PowerPoint	0	0
Microsoft OneDrive	0	0
Microsoft SharePoint	0	0
Microsoft Visio	0	0

Advanced Copilot analysis with Viva Insights

Viva Insights customers can use **analyst workbench** capabilities to dive deeper with custom reports, including incorporating data from other relevant sources.

For a limited time only, Copilot for Microsoft 365 customers will be eligible for a promotional offer that will provide access to all of [Viva Insights](#), including Copilot Dashboard, as well as access to advanced insights and manager and leader insights.

Copilot Dashboard features and capabilities		License requirement		
		Microsoft or Office 365	Copilot for Microsoft or Office 365*	Viva Insights**
Readiness	Tenant level visibility into Copilot eligibility, licensing, and activation status.	●	●	●
	Microsoft 365 app usage and supporting research to help assess potential impact.	●	●	●
Adoption	Visibility into adoption trends, such how many people are using Copilot, in which apps, and in what ways.		●	●
	Apply scopes and filters to adoption trend reports for deeper organizational views.		●	●
	Tailorable advanced capabilities to create custom reports for additional visibility into adoption trends.			●
Impact	Understand the impact of using key Copilot features on key metrics and workplace behaviors.		●	●
	Apply scopes and filters to compare Copilot usage and key workplace metrics between groups of Copilot users and between Copilot users and non-Copilot users.		●	●
	Tailorable advanced capabilities to create custom reports for additional visibility into Copilot impact and return on investment.			●
Sentiment	Tenant level visibility into employee feedback about the value and benefits of Copilot.		●	●
	Visibility into how Copilot user sentiment differs across teams (heatmap).			●
Learning	Research and best practices to help throughout the AI journey.	●	●	●
Egress	Ability to export Copilot data via Microsoft 365 Reporting Graph APIs.		●	●
	Ability to export Copilot data via Viva Insights Analyst Workbench.			●

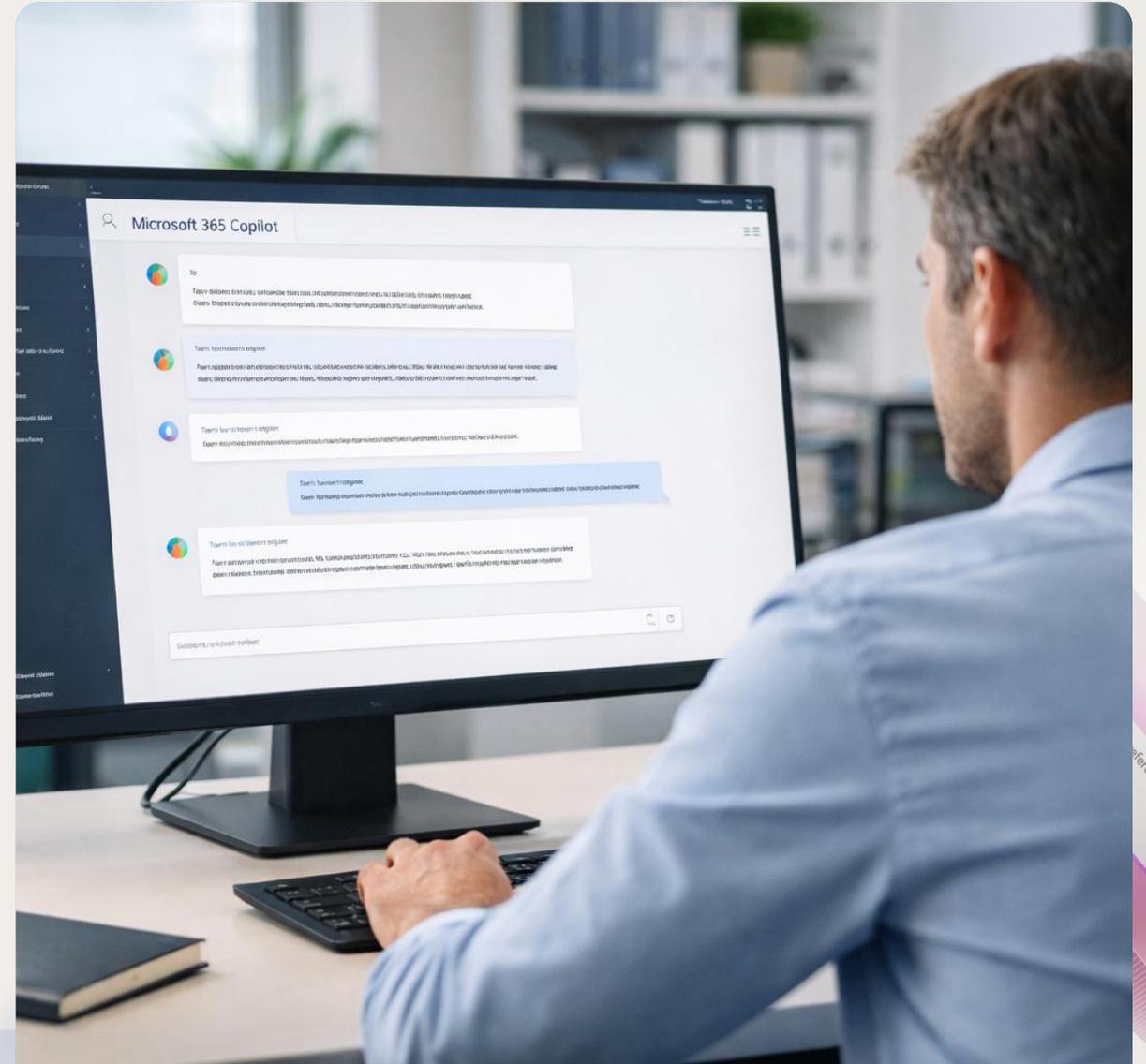
* Copilot Dashboard will be included in the Copilot for M365 SKU/service plan (Starting FY25 Q1)

** [Viva Insights](#), [Workplace Analytics and Employee Feedback](#), or [Viva Suite](#) SKUs



Microsoft 365 Copilot for admin center

[Copilot in Microsoft 365 Admin Centers](#)



Copilot for admins in Microsoft 365 admin centers

The image displays the Microsoft 365 Admin center interface. On the left, the navigation sidebar includes options like 'New chat', 'Search', 'Library', 'Create', 'Frontier', and 'Agents'. The 'Microsoft 365 Admin' option is highlighted with a red arrow. The main content area shows a 'Message Copilot' chat window and several informational cards, including 'Recap priority info' and 'Discover agent capabilities'. On the right, a detailed view of the Copilot interface is shown, featuring a 'Good evening, Ondrej Vysek' greeting and a 'Simplified view' toggle. A red arrow points to the 'Copilot' icon in the top right corner of this interface. Below the greeting, there are sections for 'For organizations like yours' and 'Your organization'. The 'Your organization' section includes a table of users and their licenses.

Name	Username for sign-in	Licenses
CC Copilot Chat		Microsoft Copilot EEA (no Teams)
JV Jenda Vysek		Unlicensed
MC M365 Copilot		M365 Copilot Sp ES EEA (no Team

Copilot for admins – Sample prompts (read only)

Recap

- Recap relevant info from across the admin center

Get Help

- How do I view Copilot usage across my organization?
- How do I restore a deleted user?
- How do I set up multifactor authentication?

Service Health

- Show me the health of Teams?
- Are there any service issues right now?

Licensing Information

- Show me users without a Copilot license?
- How many Copilot licenses are available?
- What available licenses I have - format table

Search

- Show me users in Australia with an assigned Teams license?
- Identify all groups in my organization with an owner.
- Show me all the users who are not using Copilot in the last 30 days.

Teams

- Search and return a list of all policies where the meeting recording is turned Off.
- Analyze the call quality of for their meeting with Meeting ID. Were there any quality issues?
- List the most common quality issues in meetings for the last 30 days.

SharePoint

- Find sites with external sharing on



M365 Copilot Agents



AI agents are **software systems** that use AI to pursue goals and complete tasks on behalf of users.

The Set-and-Forget approach is not the right one; AI agents need to be monitored and maintained.



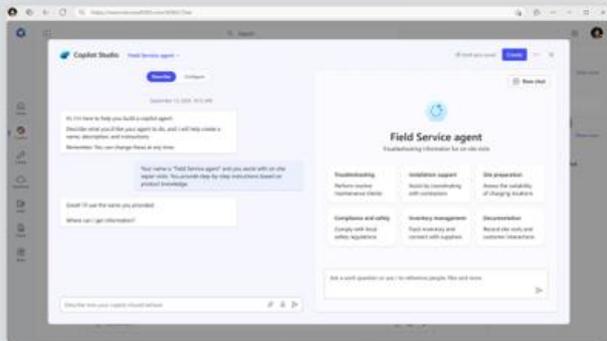
A range of tools for agent creation

No code



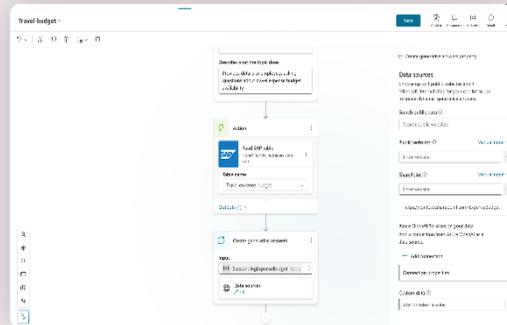
Pro code

For end users



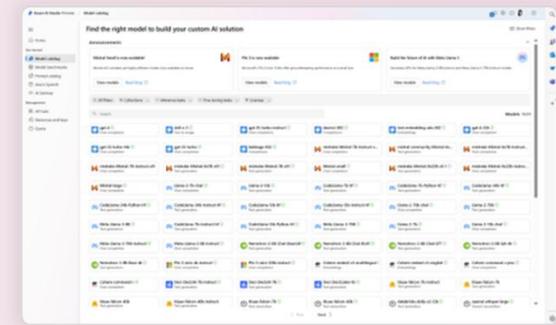
Copilot Studio
Lite

For makers



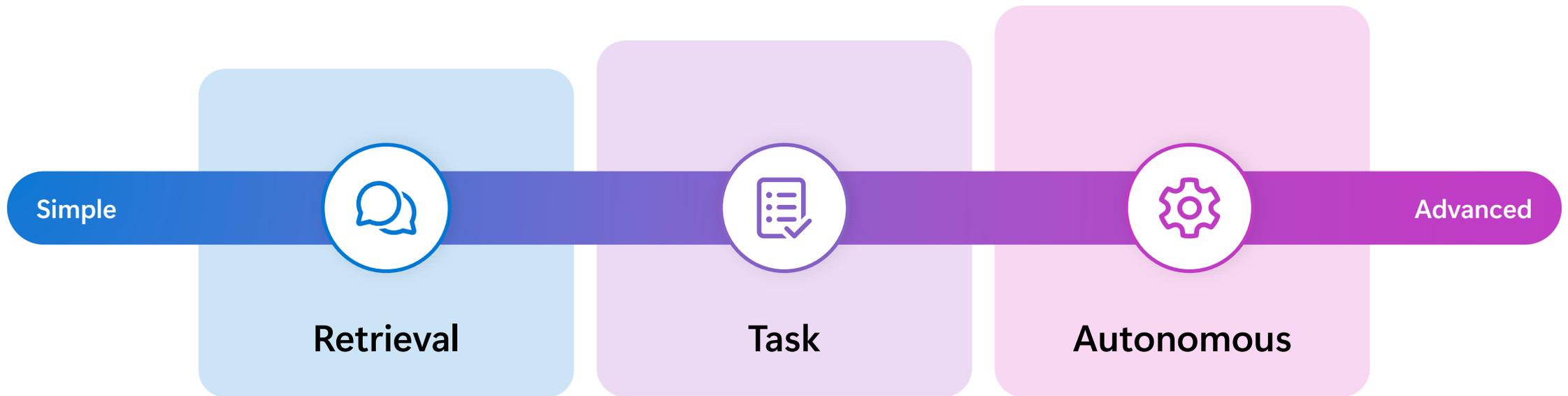
Copilot Studio
Full

For developers



VS Code, Copilot Studio,
Azure AI Foundry

View agent starters and scenarios based the level of agent complexity. Ranging from Simple → Advanced.



← Agents vary complexity and capabilities depending on your need →

Simple agents can be made in the Copilot Studio lite version in Copilot Chat + M365 Copilot

Advanced agents need to be made in the Copilot Studio full version



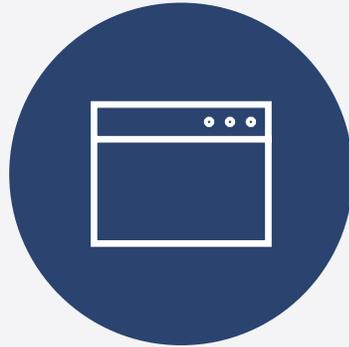
Microsoft Agent 365

The control plane for agents

Agents are a new type of identity



User



App

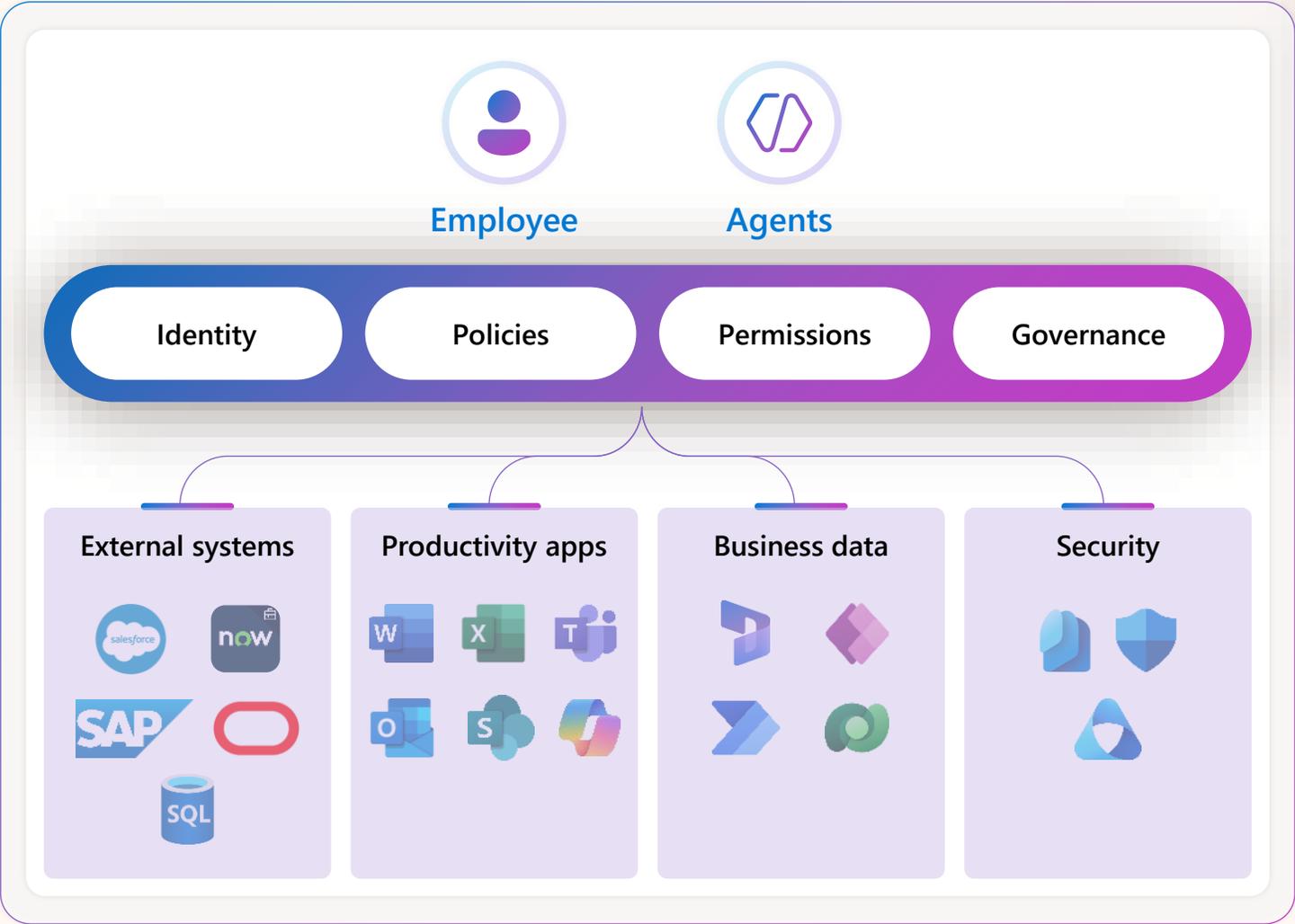


Device



Agent

Microsoft 365 for employees, Agent 365 for agents



Unlock agent productivity –
Extend the tools you already use
to secure & enable people



Every agent gets

- An identity
- Access to productivity tools, systems and data



IT gets

- Total observability and visibility
- Control, security and governance

Microsoft Agent 365

The same Microsoft's management, security, and productivity solutions are tailor-made for your agents.



Microsoft Defender

Extend comprehensive security posture and advanced threat protection to agents.



Microsoft Entra

Protect agent identities, and secure their access to any app or resource, from anywhere.



Microsoft Purview

Manage, protect and govern data that agents use and create across your entire organization.



Work IQ

Enable agents to use your organization's unique data and context to seamlessly join workflows and effectively complete tasks.



Microsoft 365

Enable agents to access and work in Word, Outlook, Excel and other productivity apps.



Microsoft Power Apps

Enable agent workflows with access to Power Apps and power Automate.



Microsoft Power BI

Enable agents to create analytics and Power BI dashboards to support collaboration.



Microsoft 365 Admin Center

Centralized hub to manage users, apps, and settings securely across your Microsoft 365 environment.

- Home
- Copilot
- Agents
 - Overview
 - All agents
 - Tools
 - Settings
- Users
- Devices
- Teams & groups
- Marketplace
- Billing
- Setup
- Customize navigation
- Show all



Agent 365 overview

Last updated: Nov 14, 2025 (Last 30 days)

Track agent usage across your org over the last 30 days and take steps to improve impact. Adjust settings, manage access, and help teams unlock more value while staying aligned with governance goals.

Agent inventory [Explore all agents](#)

26,350 ↑ 28% this week

Total agents in your org

Active users

58,293 ↑ 12% this week

Unique users interacting with agents

Time saved with agents

45,208 ↑ 6% this week

Hours saved by using agents

Agent analytics

Agent publishers

Created by your organization

Shared by creator	14.6k
Used only by creator	4k
Published by your org	6.8k

Created by external partners

Microsoft	154
Workday	136
Other	710

Agent platforms

Copilot Studio (lite)	11k
Copilot Studio (full)	10.4k
Microsoft Foundry	3.7k
Workday	114
ServiceNow	6
Windows 365	5
Manus	1

Active users over time

Trending agents by active users

Claims Processing Agent	10,992
Contract intelligence	8,146
Researcher	7,392
Incident resolution	6,100
Manus	583

Top actions for you

Pending requests for agents

3 +2 this week

Open requests to add specific agents

Staffing Genie Agent	Nov 17, 2025
----------------------	--------------

Agent risks

6 +3 this week

Agents with security risks

Comms agent	2 risks
-------------	---------

Ownerless agents

8 -4 this week

Agents without a creator or business owner

DataBridge	Nov 16, 2025
------------	--------------

Agents with exceptions

100 +10 this week

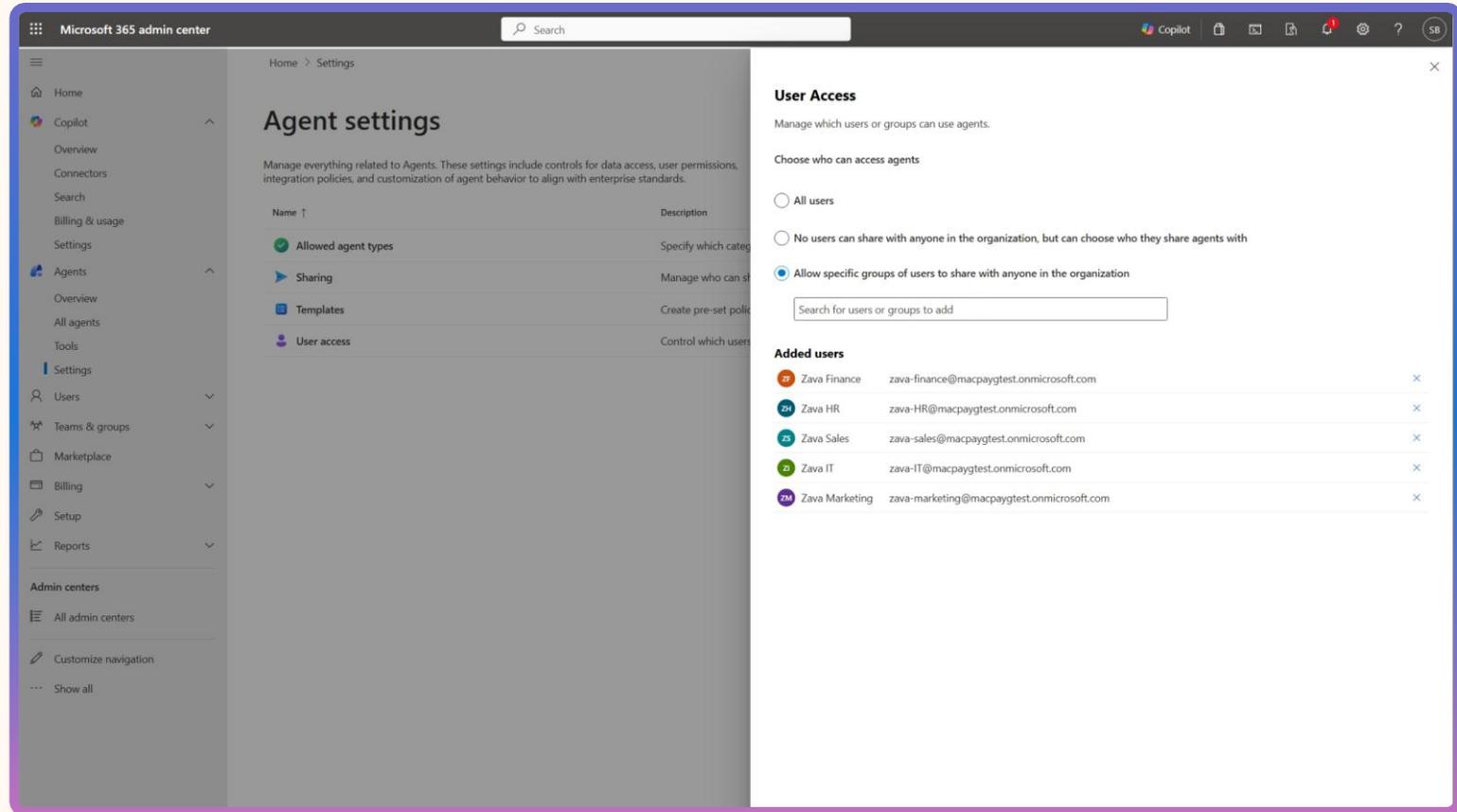
Agents needing your input to complete tasks

Insights Hub	65%
--------------	-----

Access control settings

Agent 365

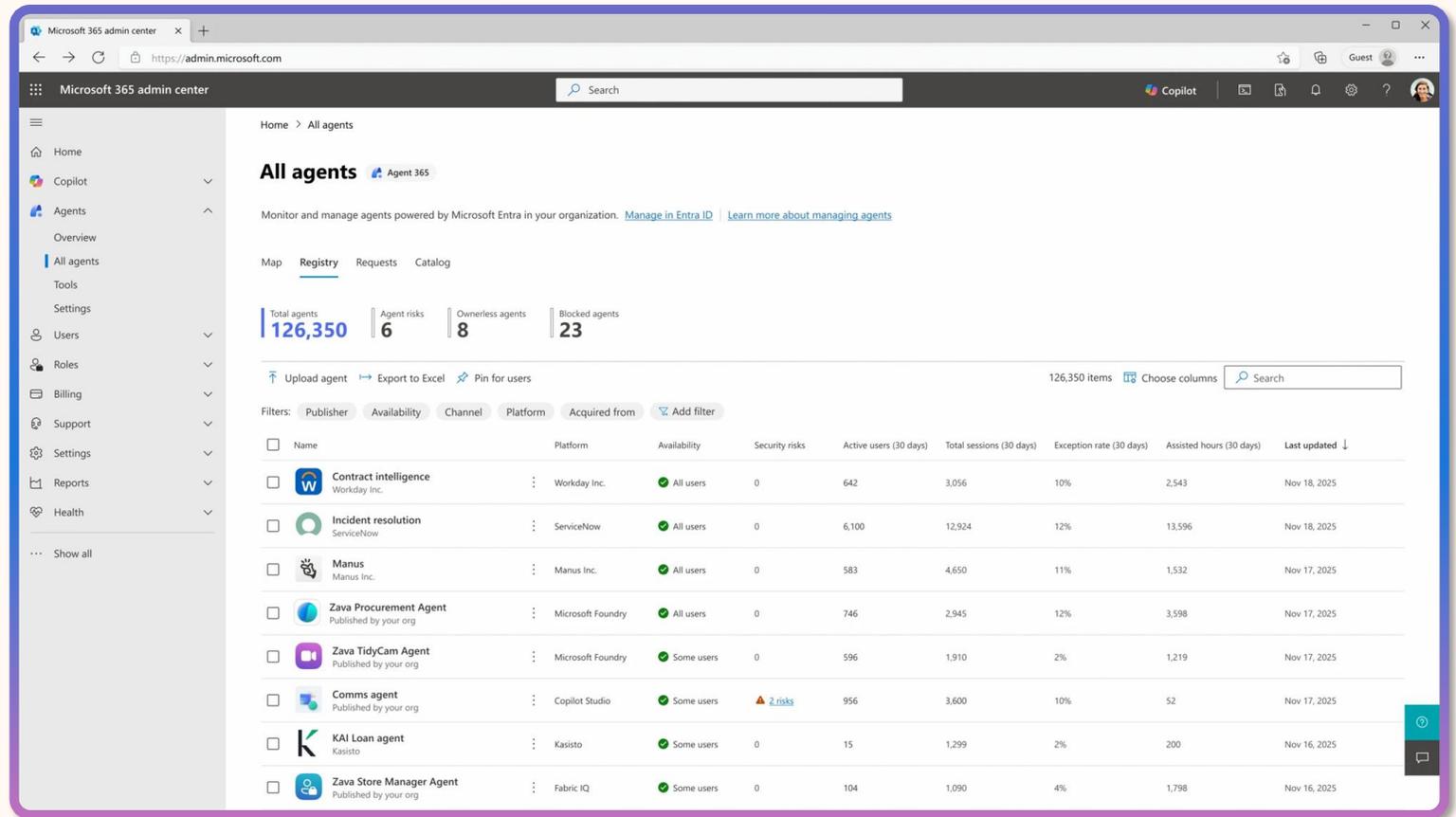
- Set guardrails for who creates, onboards, and manages agents.
- Choose how broad agents can be shared.
- Manage agents and limit their access only to the resources they need.



Single agent registry

Agent 365

- Start with a single registry for all agents.
- Quarantine unsanctioned agents to block discovery and connections.
- Use the Agent Store for easy agent discovery in Microsoft 365 Copilot and Teams.



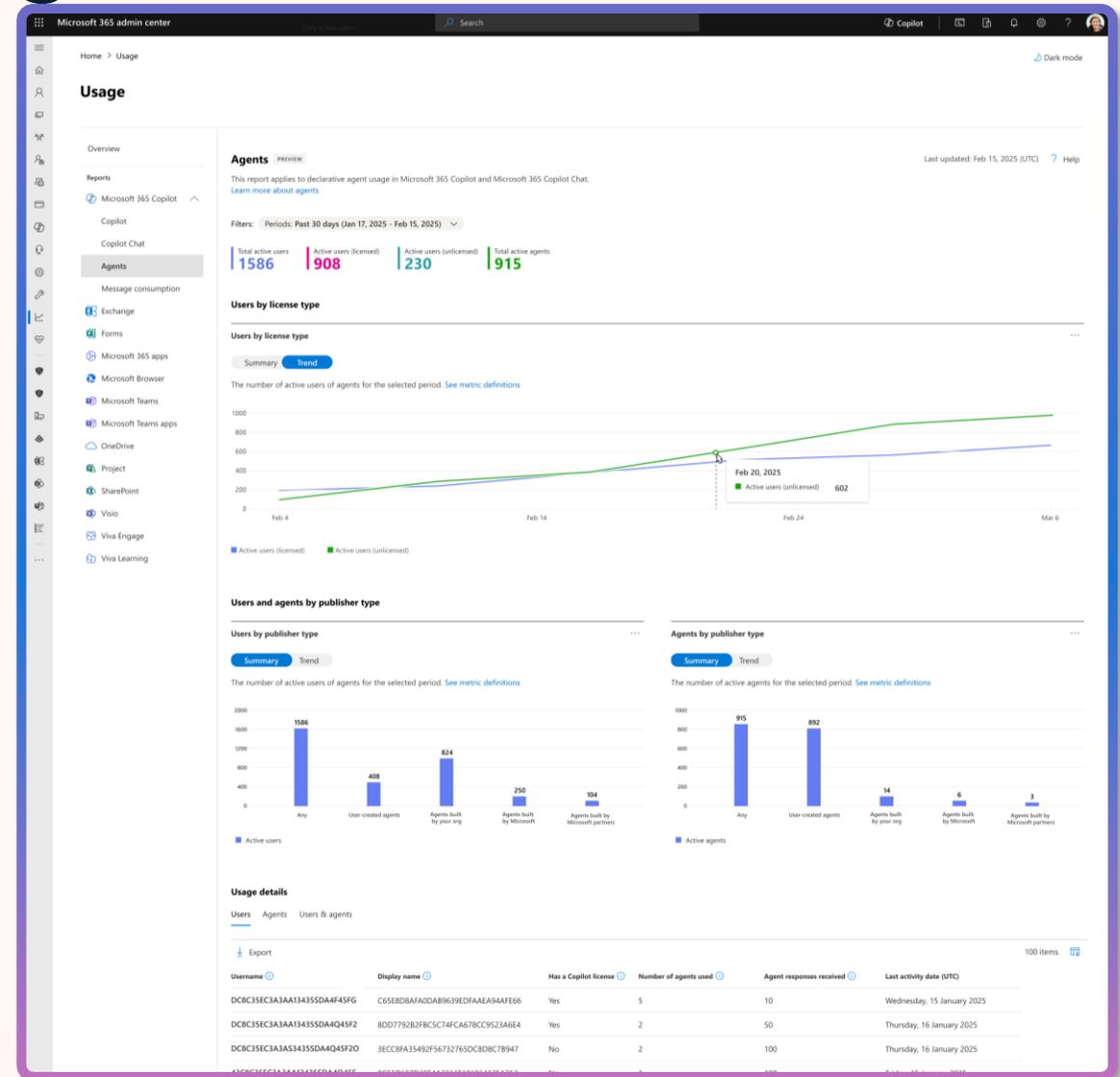
Agent observability & usage

Agent 365

Admins can gain insights to guide agent management and adoption strategy.

Sample metrics:

- Total active users & agents
- Active users and agents by publisher type
- Line-level consumption details per user, agent, billing policy, and user-agent pair
- High-consumption alerts to prevent over-spending



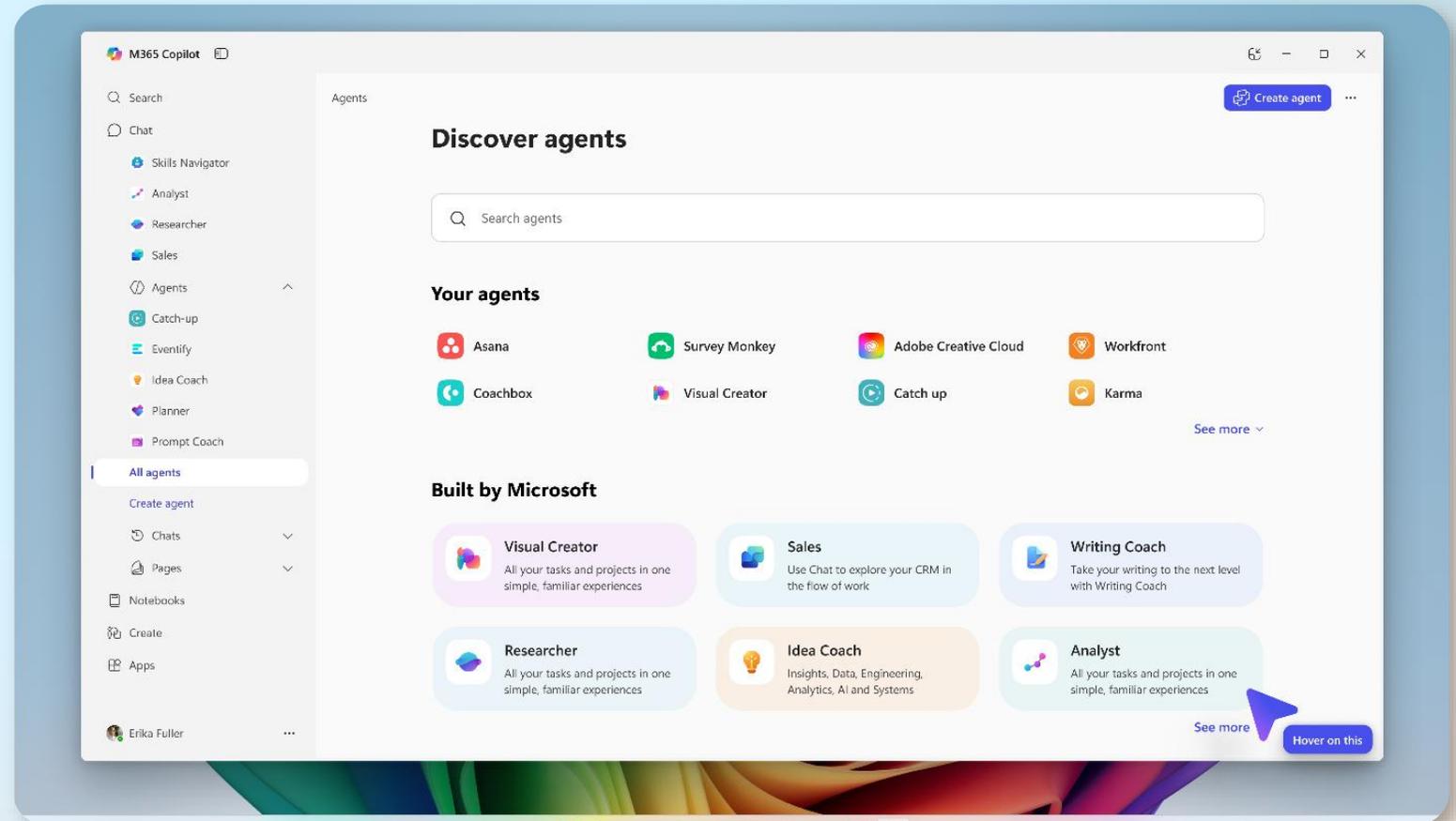
Agent Store

Agent Store is an agent marketplace featuring agents from **Microsoft, partners and customer organizations**. You can also share agents with colleagues via Copilot Chat or other Microsoft 365 Copilot endpoints to boost collaboration.

All agents, whether developed by Microsoft or partners, undergo **strict validation processes to meet enterprise standards for functionality, security, and compliance**.

IT admins have full visibility and control over how agents are deployed in their organization.

Consider which 3rd party agents will be available to users



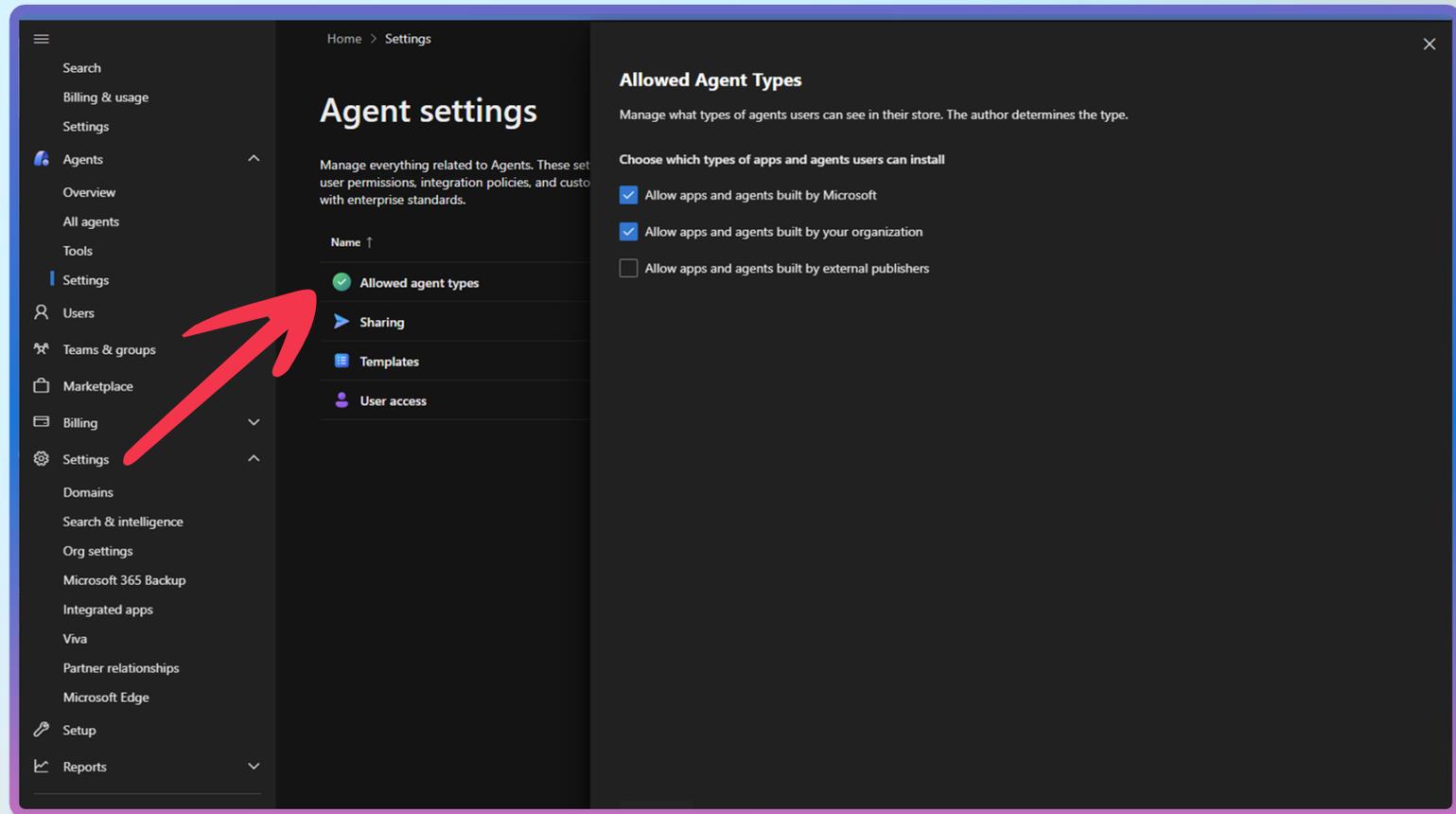
Agent Store

Agent Store is an agent marketplace featuring agents from **Microsoft, partners and customer organizations**. You can also share agents with colleagues via Copilot Chat or other Microsoft 365 Copilot endpoints to boost collaboration.

All agents, whether developed by Microsoft or partners, undergo **strict validation processes to meet enterprise standards for functionality, security, and compliance**.

IT admins have full visibility and control over how agents are deployed in their organization.

Consider which 3rd party agents will be available to users



Because you chose Microsoft authentication, only the Teams + Microsoft 365 and SharePoint channel is available. To use other channels, change your authentication settings.

Review the following before publishing:

Published agent status

Published by Ondřej Vyšek 1/5/2026, 10:33 AM

Share a preview

Demo website

Microsoft channels

Teams and Microsoft 365 Copilot

SharePoint

Other channels

Web app

Native app

Facebook

WhatsApp

Slack

Telegram

Twilio

Line

GroupMe

Direct Line Speech

Email

Customer engagement hub

Connect to a customer engagement app to enable your agent to hand off a chat session to a live agent or other agent.

Dynamics 365 Customer Service

Telephony

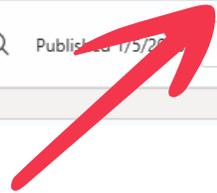
Genesys

LivePerson

Salesforce

ServiceNow

Custom engagement hub



Because you chose Microsoft authentication, only the Teams + Microsoft 365 and SharePoint channel is available. To use other channels, [change your authentication](#)

Draft agent status

Review the following before publishing:

- Your agent is shared with all users in the organization
Allowing anyone in an organization to chat with your agent allows them to access content added to your agent. [Learn more](#)
- Preview model selected
Preview models might not have gone through our full testing process yet. They can have variation in performance, latency, quality of responses and mess and availability. This model should not be used for production purposes and [preview terms apply](#).

Published agent status

Published by Ondrej Vysek 1/5/2026, 10:33 AM

Share a preview

- Demo website

Microsoft channels

- Teams and Microsoft 365 Copilot
- SharePoint

Other channels

- Web app
- Native app
- Facebook
- WhatsApp
- Twilio
- Line
- GroupMe
- Direct Line Speech

Customer engagement hub
Connect to a customer engagement app to enable your agent to hand off a chat session to a live agent or other agent.

Teams and Microsoft 365 Copilot

Microsoft 365 is your cloud-powered productivity solution and includes Outlook, Word, Excel, PowerPoint, and OneDrive. [Learn more](#)

When you publish your agent to Microsoft 365, we'll publish it to Teams too. You'll get all of your agent's advantages in Teams: meeting summaries and transcripts, pointers to open issues or unresolved questions, and more effective collaboration.

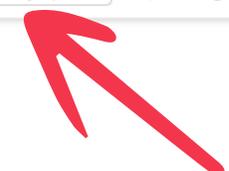
Turn on Microsoft 365

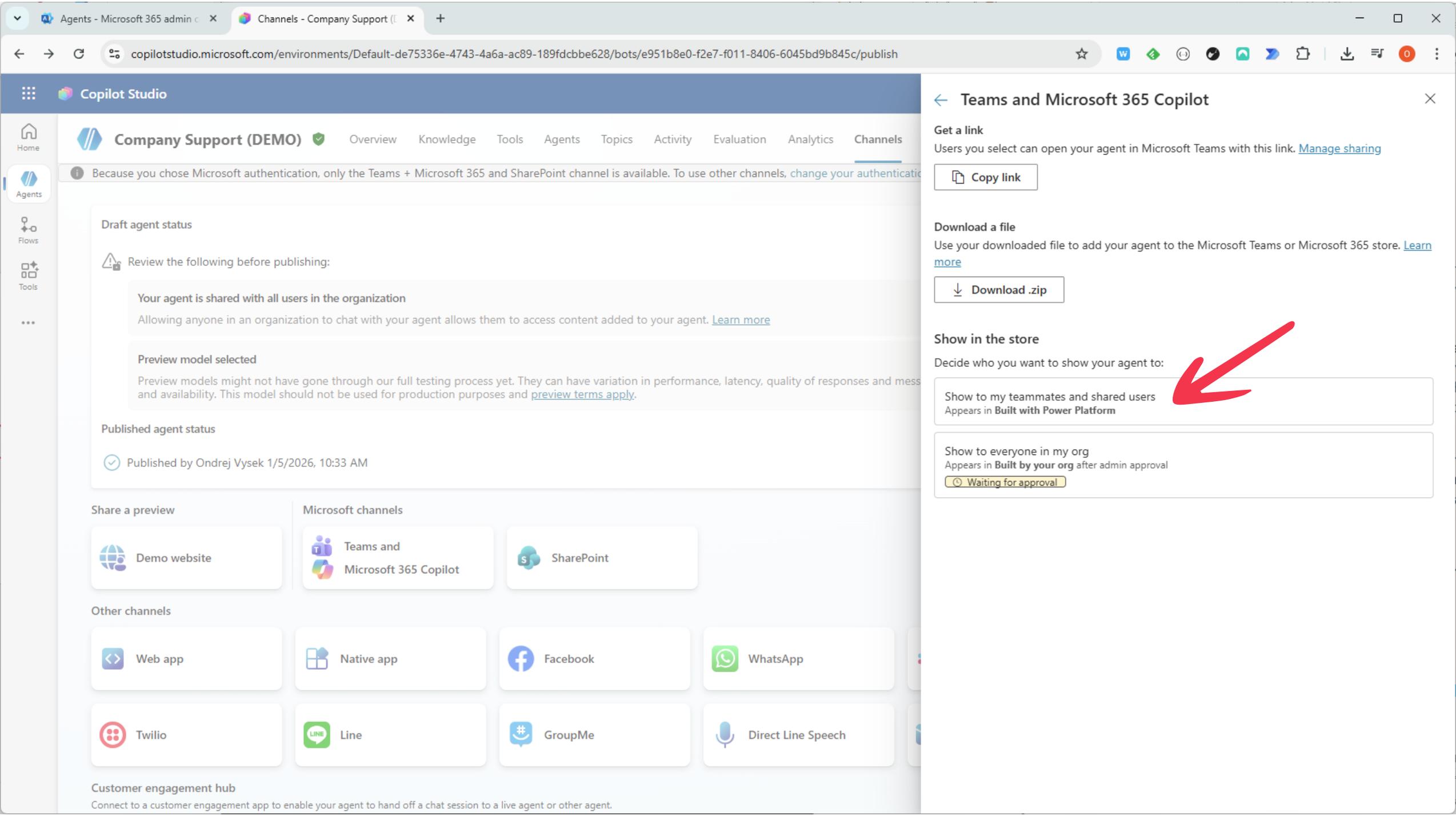
Make agent available in Microsoft 365 Copilot

Agent preview

 **Company Support (DEMO)** [Edit details](#)
This is Company onboarding and support agent

[Availability options](#)  See agent in Microsoft 365  See agent in Teams





Teams and Microsoft 365 Copilot

Get a link

Users you select can open your agent in Microsoft Teams with this link. [Manage sharing](#)

Copy link

Download a file

Use your downloaded file to add your agent to the Microsoft Teams or Microsoft 365 store. [Learn more](#)

Download .zip

Show in the store

Decide who you want to show your agent to:

Show to my teammates and shared users
Appears in **Built with Power Platform**

Show to everyone in my org
Appears in **Built by your org** after admin approval

Waiting for approval

Company Support (DEMO)

Because you chose Microsoft authentication, only the following users can access your agent:

Draft agent status

Review the following before publishing:

Your agent is shared with all users in the organization. Allowing anyone in an organization to chat with your agent allows them to access content added to your agent.

Preview model selected

Preview models might not have gone through our full testing process yet. They can have variation in performance, latency, quality of responses and message consumption. You may also experience slowdowns or timeouts due to limited capacity and availability. This model should not be used for production purposes and [preview terms apply](#).

Published agent status

Published by Ondrej Vysek 1/5/2026, 10:33 AM

Share a preview

Demo website

Other channels

Web app

Twilio

Share "Company Support (DEMO)"

Review the following before publishing: 2 items

- Your agent is shared with all users in the organization**
Allowing anyone in an organization to chat with your agent allows them to access content added to your agent. [Learn more](#)
- Preview model selected**
Preview models might not have gone through our full testing process yet. They can have variation in performance, latency, quality of responses and message consumption. You may also experience slowdowns or timeouts due to limited capacity and availability. This model should not be used for production purposes and [preview terms apply](#).
- This agent is configured for Microsoft Teams and Microsoft 365 Copilot. Make sure your users are in security groups that can access the agent in Teams.** [Learn more](#)

New Users
You can add multiple users

User permissions

Add or select a user to set their permissions

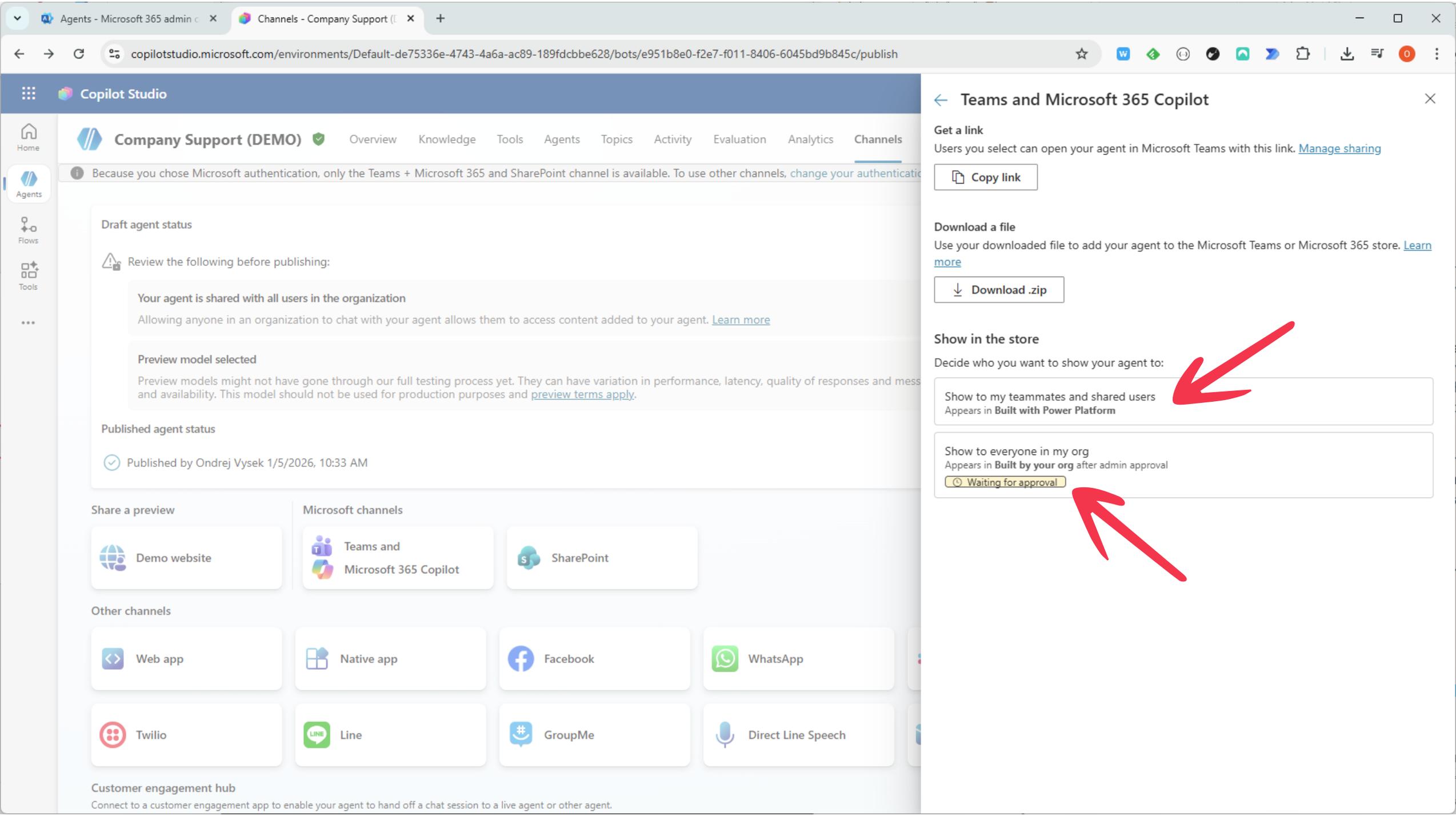
Existing users (1)

Sort by name

- OV Ondrej Vysek
Owner

My organization

Cancel
Update



Because you chose Microsoft authentication, only the Teams + Microsoft 365 and SharePoint channel is available. To use other channels, change your authentication

Draft agent status

Review the following before publishing:

Your agent is shared with all users in the organization

Allowing anyone in an organization to chat with your agent allows them to access content added to your agent. [Learn more](#)

Preview model selected

Preview models might not have gone through our full testing process yet. They can have variation in performance, latency, quality of responses and mess and availability. This model should not be used for production purposes and [preview terms apply](#).

Published agent status

Published by Ondrej Vysek 1/5/2026, 10:33 AM

Share a preview

Demo website

Microsoft channels

Teams and Microsoft 365 Copilot

SharePoint

Other channels

Web app

Native app

Facebook

WhatsApp

Twilio

Line

GroupMe

Direct Line Speech

Customer engagement hub

Connect to a customer engagement app to enable your agent to hand off a chat session to a live agent or other agent.

Teams and Microsoft 365 Copilot

Get a link

Users you select can open your agent in Microsoft Teams with this link. [Manage sharing](#)

Copy link

Download a file

Use your downloaded file to add your agent to the Microsoft Teams or Microsoft 365 store. [Learn more](#)

Download .zip

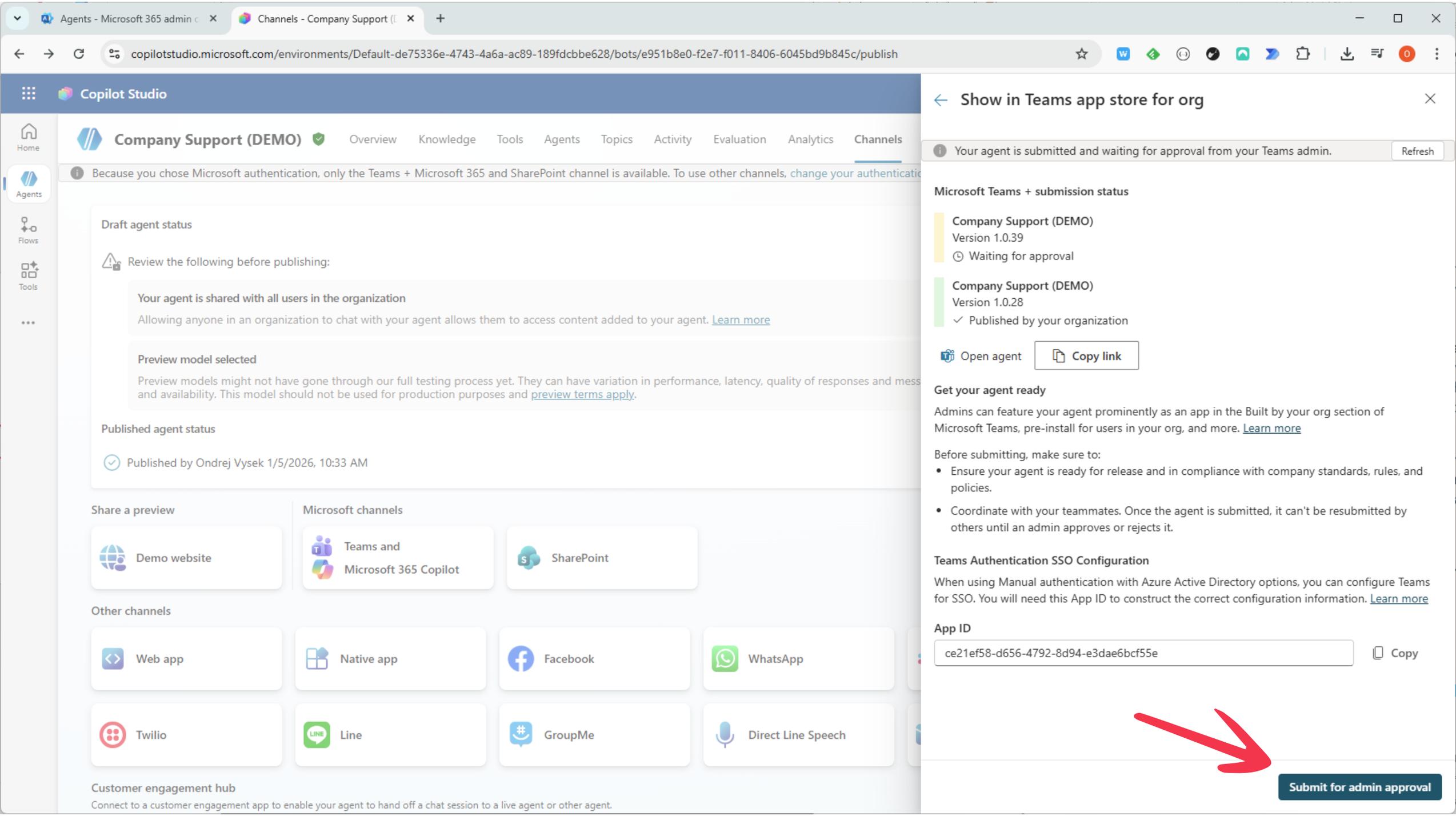
Show in the store

Decide who you want to show your agent to:

Show to my teammates and shared users
Appears in **Built with Power Platform**

Show to everyone in my org
Appears in **Built by your org** after admin approval

Waiting for approval



Because you chose Microsoft authentication, only the Teams + Microsoft 365 and SharePoint channel is available. To use other channels, change your authentication

Draft agent status

Review the following before publishing:

Your agent is shared with all users in the organization. Allowing anyone in an organization to chat with your agent allows them to access content added to your agent. Learn more

Preview model selected. Preview models might not have gone through our full testing process yet. They can have variation in performance, latency, quality of responses and mess and availability. This model should not be used for production purposes and preview terms apply.

Published agent status

Published by Ondrej Vysek 1/5/2026, 10:33 AM

Share a preview

Demo website

Microsoft channels

Teams and Microsoft 365 Copilot

SharePoint

Other channels

Web app

Native app

Facebook

WhatsApp

Twilio

Line

GroupMe

Direct Line Speech

Customer engagement hub

Connect to a customer engagement app to enable your agent to hand off a chat session to a live agent or other agent.

Show in Teams app store for org

Your agent is submitted and waiting for approval from your Teams admin. Refresh

Microsoft Teams + submission status

Company Support (DEMO) Version 1.0.39 Waiting for approval

Company Support (DEMO) Version 1.0.28 Published by your organization

Open agent Copy link

Get your agent ready

Admins can feature your agent prominently as an app in the Built by your org section of Microsoft Teams, pre-install for users in your org, and more. Learn more

Before submitting, make sure to:

- Ensure your agent is ready for release and in compliance with company standards, rules, and policies.
Coordinate with your teammates. Once the agent is submitted, it can't be resubmitted by others until an admin approves or rejects it.

Teams Authentication SSO Configuration

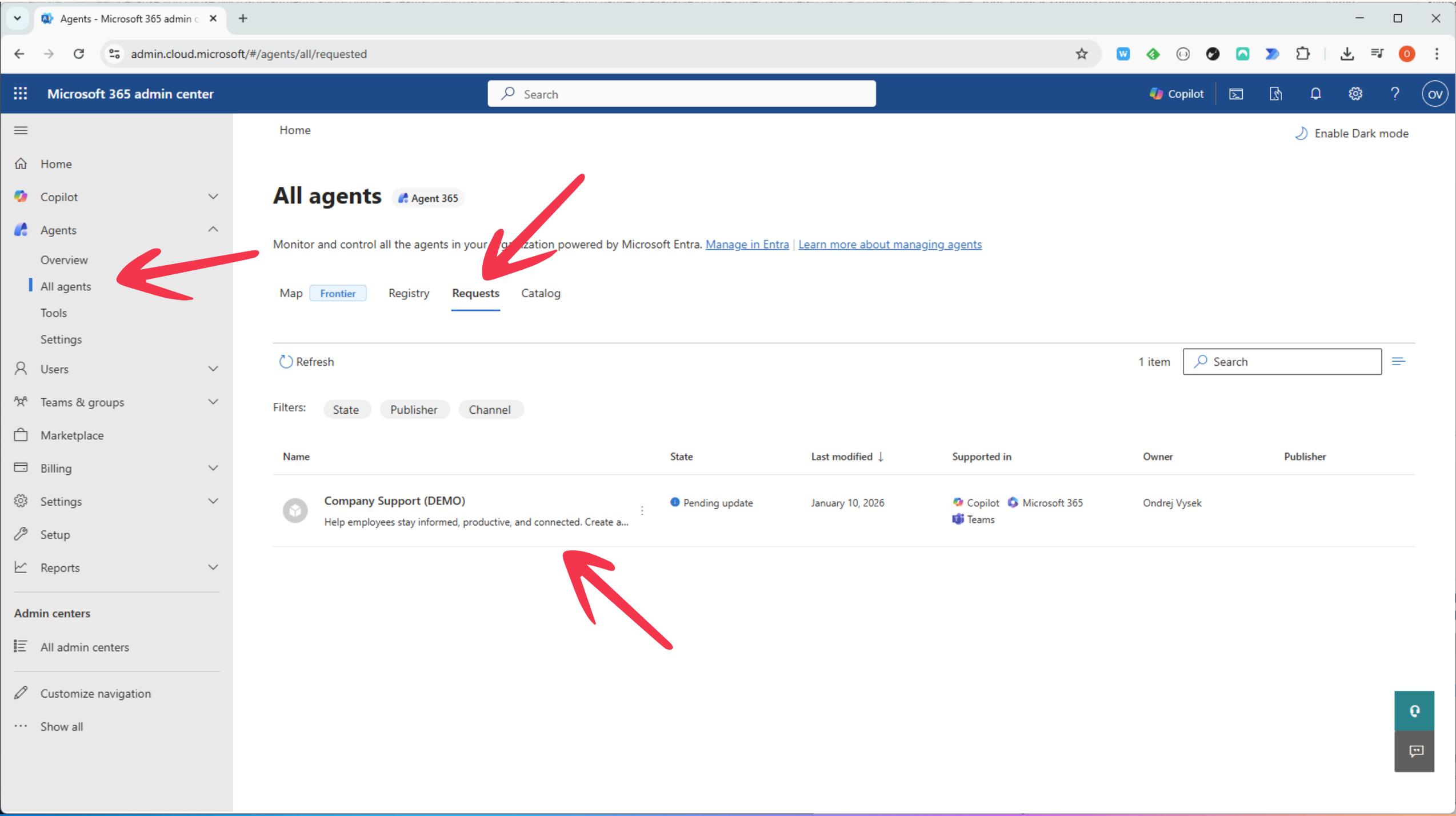
When using Manual authentication with Azure Active Directory options, you can configure Teams for SSO. You will need this App ID to construct the correct configuration information. Learn more

App ID

ce21ef58-d656-4792-8d94-e3dae6bcf55e Copy



Submit for admin approval



Home

Enable Dark mode

All agents Agent 365

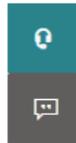
Monitor and control all the agents in your organization powered by Microsoft Entra. [Manage in Entra](#) | [Learn more about managing agents](#)

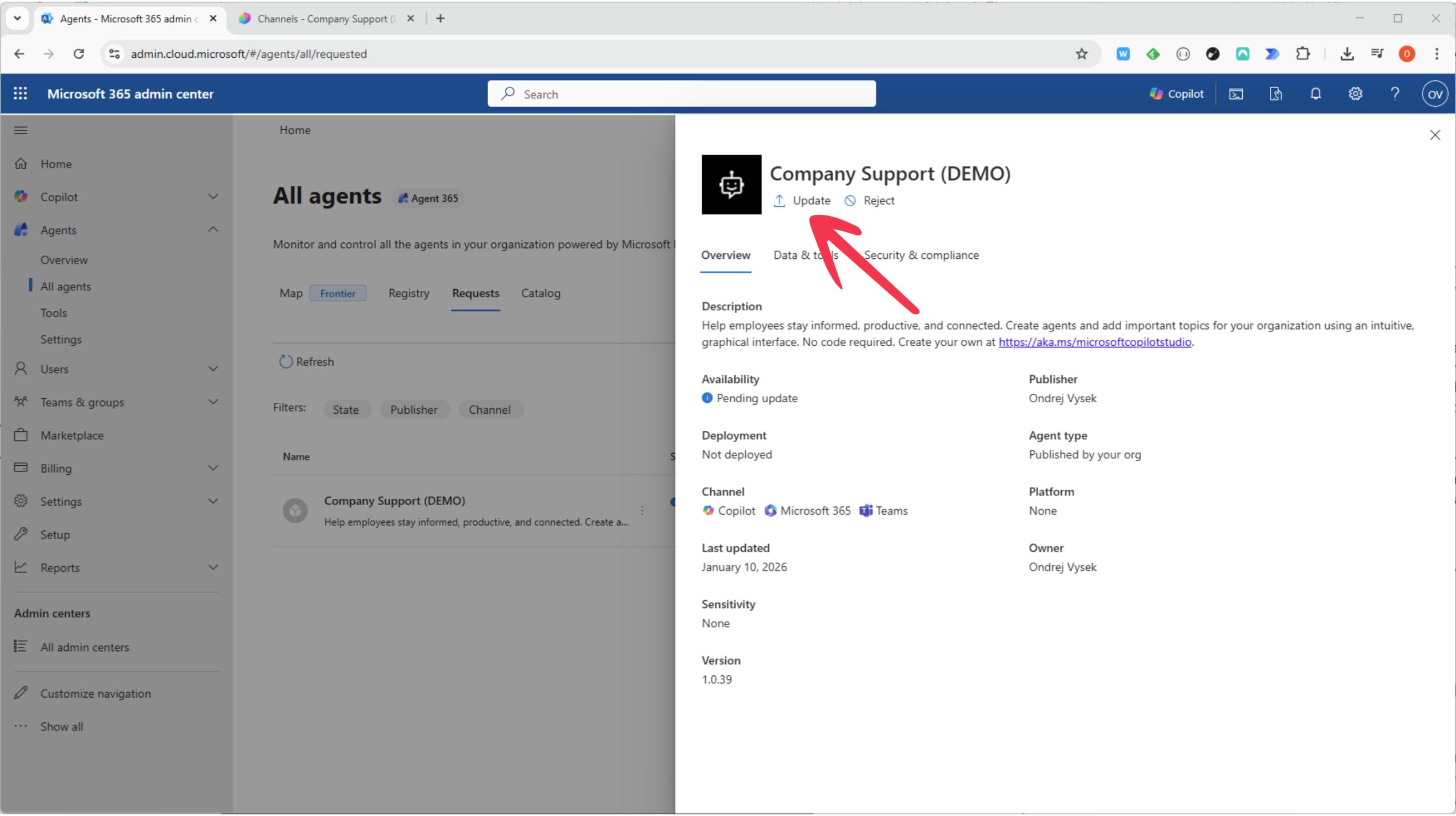
Map **Frontier** Registry Requests Catalog

Refresh 1 item

Filters: **State** Publisher Channel

Name	State	Last modified ↓	Supported in	Owner	Publisher
 Company Support (DEMO) Help employees stay informed, productive, and connected. Create a...	 Pending update	January 10, 2026	 Copilot  Microsoft 365  Teams	Ondrej Vysek	





Home

All agents Agent 365

Monitor and control all the agents in your organization powered by Microsoft

Map **Frontier** Registry **Requests** Catalog

Refresh

Filters: State Publisher Channel

Name

Name
 Company Support (DEMO) Help employees stay informed, productive, and connected. Create a...



Company Support (DEMO)

[Update](#) [Reject](#)

Overview Data & tools Security & compliance

Description

Help employees stay informed, productive, and connected. Create agents and add important topics for your organization using an intuitive, graphical interface. No code required. Create your own at <https://aka.ms/microsoftcopilotstudio>.

Availability

1 Pending update

Publisher

Ondrej Vysek

Deployment

Not deployed

Agent type

Published by your org

Channel

 Copilot  Microsoft 365  Teams

Platform

None

Last updated

January 10, 2026

Owner

Ondrej Vysek

Sensitivity

None

Version

1.0.39

Create agent

See more

- New chat
- Search
- Library
- Create
- Frontier
- Agents
 - Researcher
 - Analyst
 - App Builder (Frontier)
 - AMAZING: Quiz Tutor
 - Onboarding Buddy
 - New agent
 - All agents**
- Notebooks
 - Demo Notebook
 - All notebooks
- Chats
 - Creating an Onboarding Buddy fr...
 - ...
- Apps
 - Ondřej Výšek

Built by Microsoft

- Workflows (Frontier)**
Build agent flows with natural language, no code needed.
- SharePoint page agent**
Transform conversation results into SharePoint pages.
- People (Frontier)**
Build connections, prepare for meetings, and find people in you...
- Learning (Frontier)**
Upskill in AI and other areas with personalized learning...
- Workforce Insights (Fro...**
Real-time insights into your organization's people, structure,...
- Surveys**
Surveys agent automates survey creation, distribution, and analysis.
- Skills (Frontier)**
Find experts, areas to upskill, and more
- Researcher**
With Researcher, now every employee has access to expertis...
- Analyst**
Perform complex data analysis over files in a variety of formats

See more

Built by your org

- Company Support (DEMO)**
Home Development
This is Company onboarding and support agent



Microsoft Entra Agent ID

Secure access for AI agents

Register and manage
agents

- Agent ID
- Registry

Govern agent identities
and lifecycle

- Lifecycle management
- Sponsors and managers
- Access governance

Protect agent access to
resources

- Conditional access
- Identity Protection
- Traffic filtering

How Microsoft Entra manages agent identity and access

Get a directory of your AI agents

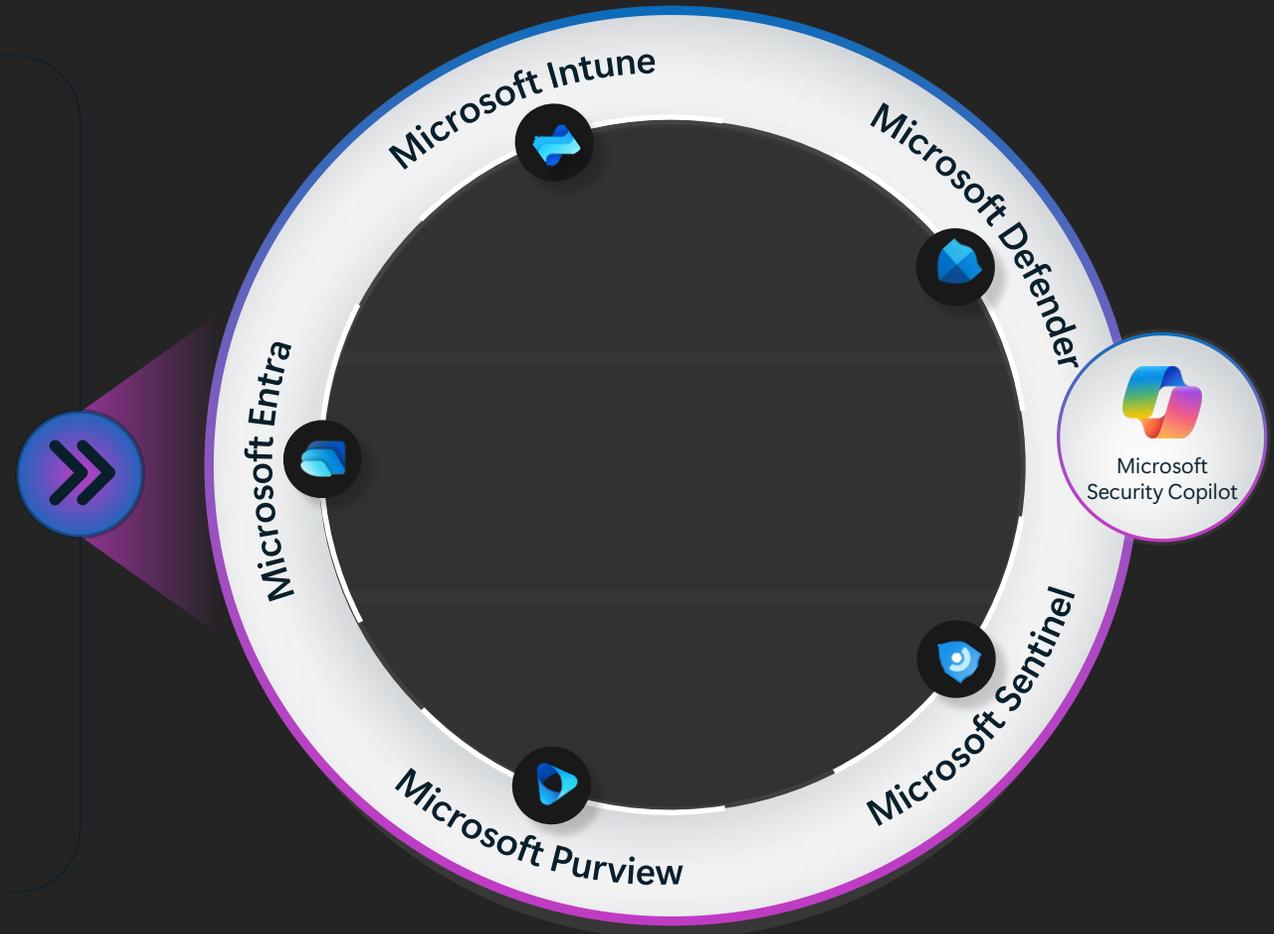
Natively integrated with Copilot Studio and Microsoft Foundry

Control agent access to resources

Adaptive access and permissions management

Protect and govern agent identities

Prevent agent compromise and manage lifecycle



- Home
- Entra agents
- Favorites
- Entra ID
 - Overview
 - Users
 - Groups
 - Devices
 - Agent ID
 - Enterprise applications
 - App registrations
 - Roles & admins
 - Identity Protection
 - Conditional Access
 - Authentication
 - External Identities
 - Custom security attributes
 - Certificate authorities
 - Cross-tenant synchronization
 - Microsoft Entra Connect
 - Domains
 - Custom branding
 - Mobility
 - Monitoring & health
 - Identity governance

Home > **Agent ID | Overview**
Entra ID

- Overview
- All agent identities
- Agent registry
- Agent collections
- Activity
 - Audit logs
 - Sign-in logs

Search for agent identities by name or object ID

Got feedback?

Agents in your tenant
6,053 ↑ 31% Last 7 days

Gain full visibility into agent identities in your tenant, and secure them by default with policies and lifecycle controls. [Learn more](#)

[View all agent identities](#)

Recently created
Created in last 30 days
74 ↑ 17% [View](#)

Unmanaged
No owners or sponsors
29 ↓ 24% [View](#)

Active
Enabled for access
5,016 [View](#)

No identities
Agents without identities
141 [View](#)

Types of agents
Breakdown of different types of agents in the tenant

Agent identities (Non-users)	4,011 View	Agent identities (Users)	892 View
Agents with service principals	1,009 View	Agents with no identities	141 View

Agent blueprints
Blueprints are parent templates that power agent identities in your tenant.

Agent blueprints ⓘ
342 ↑ 28%

[View all](#)

Recently created blueprints

SA Sales Agent blueprint	13 agent identities
Finance agent	124 agent identities
OP Orion Pulse	69 agent identities

Agent collections overview
Automatically or manually-created groups of agents in your tenant.

Global 1210 agents

Custom 122 agents

Quarantined 0 agents

[View all](#)

- Home
- Entra agents
- Favorites
- Entra ID
 - Overview
 - Users
 - Groups
 - Devices
 - Agent ID
 - Enterprise applications
 - App registrations
 - Roles & admins
 - Identity Protection
 - Conditional Access
 - Authentication
 - External Identities
 - Custom security attributes
 - Certificate authorities
 - Cross-tenant synchronization
 - Microsoft Entra Connect
 - Domains
 - Custom branding
 - Mobility
 - Monitoring & health
 - Identity governance

Home > Agent ID > Agent registry >

Agent ID | Agent registry

Entra ID

- Overview
 - All agent identities
 - Agent registry
 - Agent collections
- Activity**
- Audit logs
 - Sign-in logs

Refresh Columns

Search by name or object ID Add filter

Showing 6,053 items

Name	Registry ID	Platform	Has Agent ID	Source ID
Image Recognition Agent	jpgig5qtp-hr5o-iq9s-me2r-le4t2n4p...	PixelNova AI	No	default_055beb02-87cc-48e1-b4ab-7...
Inventory Management Agent	58b744c1-e3b9-4205-8016-dbc9194...	Adatum	No	ab9c6ad5-9da3-4610-bd2f-7db8de2c... View more
Procurement & logistics	microsoftCopilotStudio_055beb02-87...	Copilot Studio	Yes	default_bd1aeecb-6e88-41aa-90ab-e3...
Content Generation Agent	10314218-d641-48aa-aa2c-e9e2ea6a...	BrightMind Systems	No	default_b0e53276-403b-49dd-9720-c...
HR Actions	microsoftAzureFoundry_088beb02-8...	Microsoft Foundry	Yes	783beb02-87cc-48e1-b4ab-784889ed... View more
Deal advisor	microsoftCopilotStudio_055beb02-87...	Copilot Studio	Yes	default_982beb02-87cc-48e1-b4ab-78...
Conditional Access Optimization Agent	becef3a5-8a8b-4b6b-87b5-bace1fb5...	Security Copilot	Yes	376f8eee-0fc8-4345-9f82-6e3bcea65... View more
Manus	0a52a0fb-5b3b-4ebc-b231-5cc98f7b...	Manus AI	Yes	95deb0cd-6d3d-441d-9ace-5b1c5be3...
HR self-servicve	microsoftCopilotStudio_055beb02-87...	Copilot Studio	Yes	default_675ref02-87cc-48e1-b4ab-784... View more
Finance optimizer	microsoftCopilotStudio_055beb02-87...	Copilot Studio	Yes	default_426117dc-2180-4057-9939-ae... View more
Zava Assist	microsoftAzureFoundry_088beb02-8...	Microsoft Foundry	Yes	2900dfd4-b521-480b-8125-79293609...
Sales Forecasting Agent	84e24f35-b1f9-4e39-b700-bbae2cc6...	FutureCast Labs	No	default_055beb02-87cc-48e1-b4ab-7...
Genspark Super	41d8d132-7546-4b9c-8589-f2a5d16...	Genspark	Yes	d6f078d6-feeb-4dd3-933d-e87573bc... View more
Test HR 123	microsoftCopilotStudio_055beb02-87...	Copilot Studio	Yes	default_055beb02-87cc-48e1-b4ab-78... View more
Customer Assist	e97c3dc4-17c0-4236-a0e1-3451cc86...	Kasisto	Yes	7a065927-bbc7-4aa2-b4ae-429d8582...
Stock monitor	microsoftCopilotStudio_055beb02-87...	Copilot Studio	Yes	default_055beb02-87cc-48e1-b4ab-78...

- Home
- Entra agents
- Favorites
- Entra ID
 - Overview
 - Users
 - Groups
 - Devices
 - Agent ID
 - Enterprise applications
 - App registrations
 - Roles & admins
 - Identity Protection
 - Conditional Access
 - Authentication
 - External Identities
 - Custom security attributes
 - Certificate authorities
 - Cross-tenant synchronization
 - Microsoft Entra Connect
 - Domains
 - Custom branding
 - Mobility
 - Monitoring & health
 - Identity governance

Home > Agent ID >

Agent ID | All agent identities

Entra ID

- Overview
- All agent identities
- Agent registry
- Agent collections

Activity

- Audit logs
- Sign-in logs

Disable Download Refresh Columns View agent blueprints

Search by name or object ID Status: All Add filter

Showing 5,912 items

<input type="checkbox"/>	Name	Status	Created on	Object ID
<input type="checkbox"/>	HR Self-Service Agent	Active	10/14/2025	a5ab672c-af21-484e-8dc8-93104c7ee003
<input type="checkbox"/>	Zava Assist	Active	10/13/2025	ee83c249-c54d-4888-b27b-103dd9a842de
<input type="checkbox"/>	Procurement & logistics	Active	10/13/2025	15139328-96c2-4058-b936-eb2ff4698556
<input type="checkbox"/>	Finance optimizer	Active	10/13/2025	c5988f7c-0533-4ce1-9f69-d344217e806a1
<input type="checkbox"/>	Conditional Access Optimization Agent	Active	10/10/2025	1f7531a6-2568-4ea7-b2a3-8cf80223e5bb
<input type="checkbox"/>	Stock monitor	Active	10/10/2025	2964b7a6-20d7-4dfe-9be5-b13e0a2ac832...
<input type="checkbox"/>	HR Actions Agent	Active	10/10/2025	d41234e9-9988-47da-9724-d51cdb99fd9d...
<input type="checkbox"/>	Manus Agent	Active	10/10/2025	cb889b16-54bf-4db1-a5de-07629904252f...
<input type="checkbox"/>	Deal advisor	Active	10/10/2025	8a061d40-75b7-4cd6-b1de-872d989ec8e8...
<input type="checkbox"/>	Genspark Super	Active	10/10/2025	d3813e44-21f5-4a9e-bd26-e932e1fa62b4...
<input type="checkbox"/>	Customer Assist	Active	10/09/2025	acedf255-393d-4796-9a8c-e7625bd36440...
<input type="checkbox"/>	NowAssist	Active	10/09/2025	6770647e-1ce6-464a-ae31-3dc4308fbce4...
<input type="checkbox"/>	Glean	Active	10/09/2025	b4fc7b68-d937-4d4d-9fd9-56e3912d2eb4...
<input type="checkbox"/>	Test HR 123	Active	09/19/2025	f1611e33-2b9b-4c8f-bdf0-79831faec0294
<input type="checkbox"/>	Genie Space	Disabled	09/19/2025	bcc40574-8e66-46d6-bb9f-81b4353829e4
<input type="checkbox"/>	Stock monitor	Disabled	09/19/2025	7ecae9f7-5613-4697-bb47-8c263449dcfe...

- Home
- Entra agents
- Favorites
- Entra ID
 - Overview
 - Users
 - Groups
 - Devices
 - Agent ID
 - Enterprise applications
 - App registrations
 - Roles & admins
 - Identity Protection
 - Conditional Access
 - Authentication
 - External Identities
 - Custom security attributes
 - Certificate authorities
 - Cross-tenant synchronization
 - Microsoft Entra Connect
 - Domains
 - Custom branding
 - Mobility
 - Monitoring & health
 - Identity governance

Home > Agent ID | all agent identities >

HR-Self-Service Agent | Overview

- Overview
- Custom security attributes
- Access
 - Owners and sponsors
 - Agent identity's access
- Activity
 - Audit logs
 - Sign-in logs

Disable | Got feedback?



HR-Self-Service Agent

Agent identity

Answers HR policy questions, initiates HR cases when needed.

Status	: Active
Sponsors	: Lawrence Gilbertson
Owners	: -
Blueprint ID	: cb889b16-54bf-4db1-a5de-07629904255 🔗
Object ID	: a5ab672c-af21-484e-8dc8-93104c7ee003 🔗
Agent blueprint	: HR Self-Service Agent Blueprint
Created on	: 10/14/2025

Agent identity's access

View

View the permissions, roles and resources that this agent has access to

Permissions	Entra roles
4	0

Policies & ID Governance

Useful links to policies and ID Governance features for this agent identity

CA policies [View](#)

Access packages [View](#)

- Home
- Agents
- Favorites
- Entra ID
 - Overview
 - Users
 - Groups
 - Devices
 - Agent identities
 - Enterprise apps
 - App registrations
 - Roles & admins
 - Delegated admin partners
 - Domain services
 - Conditional Access
 - Multifactor authentication
 - Identity Secure Score
 - Authentication methods
 - Password reset
 - Custom security attributes
 - Certificate authorities
 - External Identities
 - Cross-tenant synchronization
 - Entra Connect

Home >

Policies

[+ New policy](#)
[+ New policy from template](#)
[↑ Upload policy file](#)
[What if](#)
[Refresh](#)
[Preview features](#)
[Got feedback?](#)

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. [Learn more](#)



Conditional Access Optimization Agent

Policies created ⓘ Policy suggestions ⓘ

6

[Manage agent](#)



Microsoft-managed policies

Policies created ⓘ

4



User created policies

Policies created ⓘ

74

Add filter
Actors: Agents (Preview) ×
Reset filters

4 out of 84 policies found

Policy name	Created by	State	Alert	Creation date	Modified date
Allow HR approved agents to access resources	USER	On		11/6/2025, 11:55:57 AM	11/7/2025, 5:56:28 PM
EB - Test Risky Agent Block	USER	Report-only		10/16/2025, 7:39:11 PM	10/16/2025, 7:42:08 PM
High Risk Agents Template	USER	Off		10/23/2025, 3:38:44 PM	11/7/2025, 5:56:57 PM
Review all high risk agents from accessing all resources	CONDITIONAL ACCESS OPTIMIZATION AGENT	Report-only		10/27/2025, 3:48:50 PM	11/7/2025, 5:57:20 PM

Defend against emerging AI threats + vulnerabilities

Discover and prevent risks

Defender - AI Security Posture Management
Azure AI Foundry - Red Teaming

Defend and block AI threats

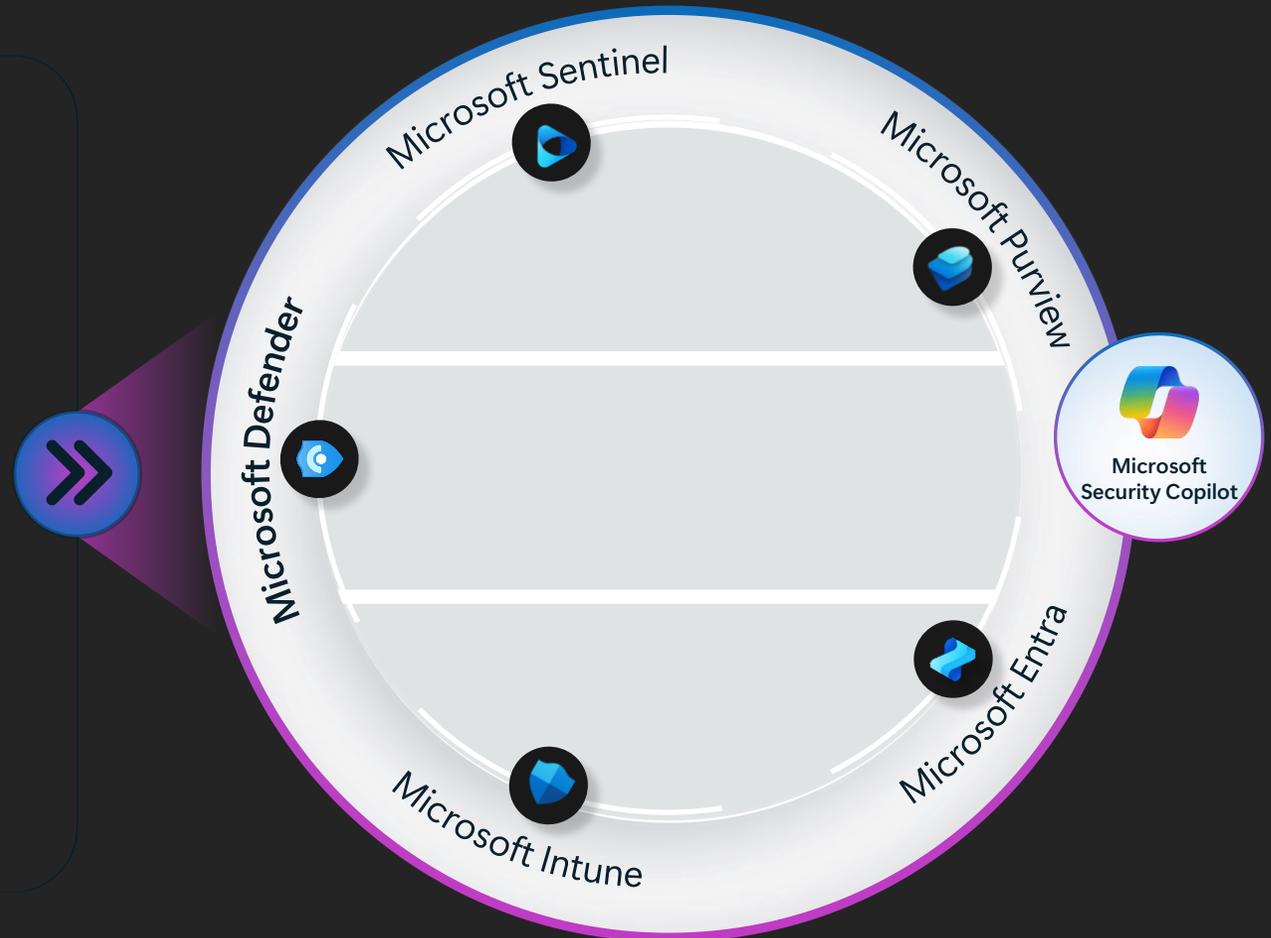
Defender for Cloud, Defender XDR
Azure AI Foundry - Content Safety Prompt Shields

Gain complete attack visibility

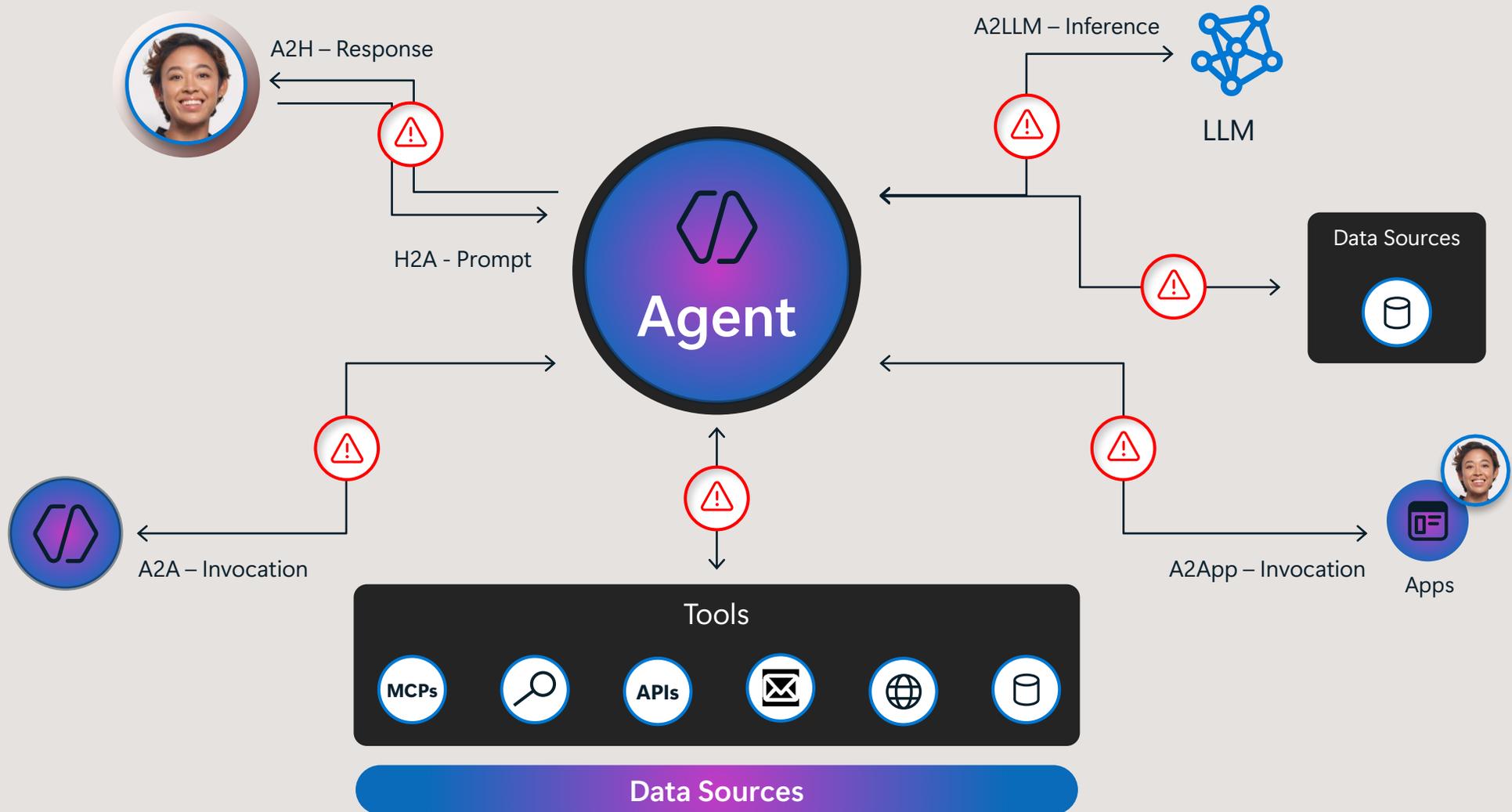
Defender for Cloud

Enforce identity guardrails

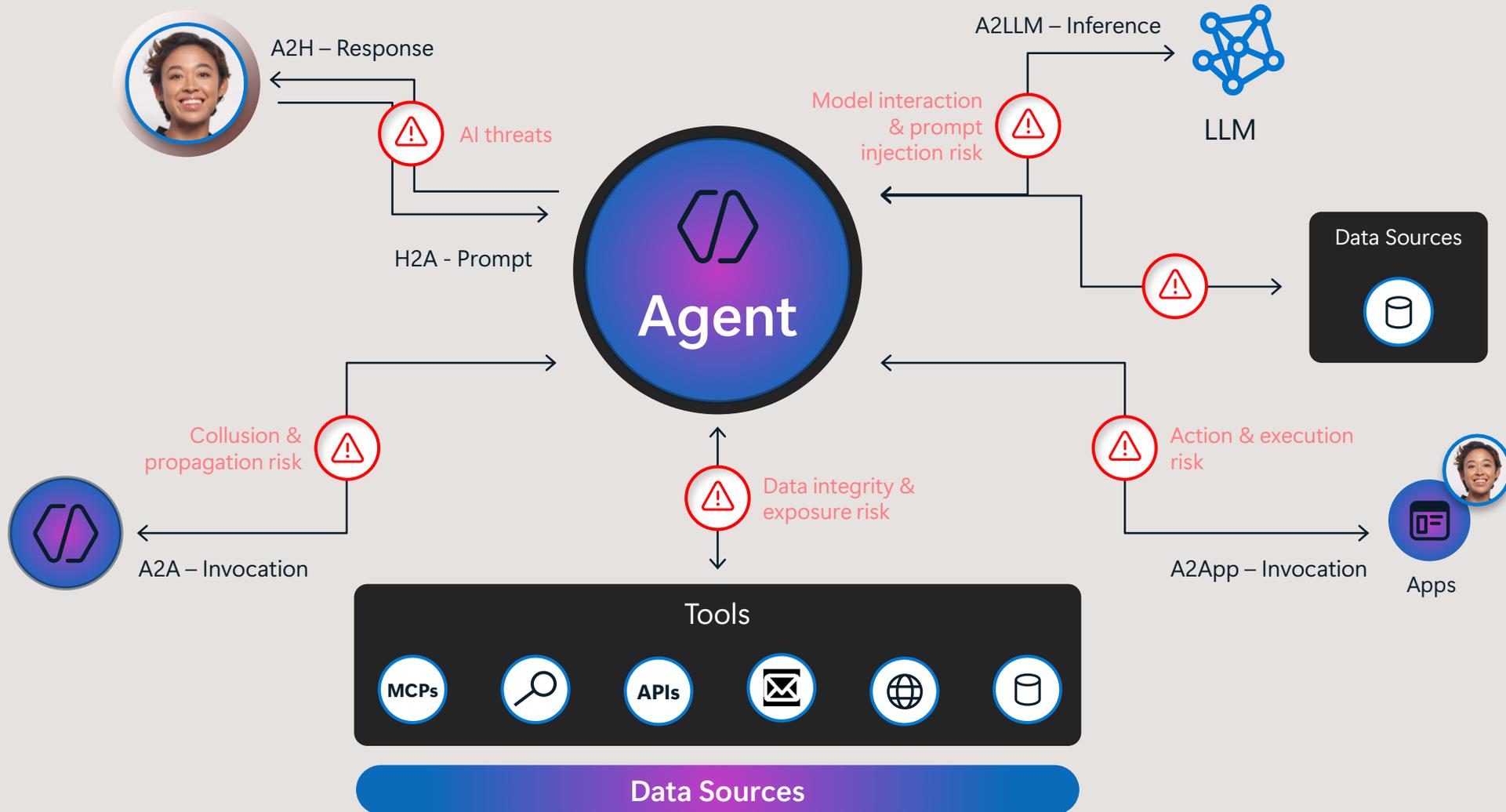
Microsoft Entra - risk-based conditional access



Agents need same protection as users and more



Agents need same protection as users and more



- Home
- Exposure management
- Investigation & response
- Threat intelligence
- Assets
- Devices
- Identities
- Applications
- Cloud infrastructure
- AI Agents
- Microsoft Sentinel
- Identities
- Endpoints
- Email & collaboration
- Cloud apps
- Cloud infrastructure
- Security Copilot
- Agents
- Security Store
- Cases

AI Agents

All (551) **Azure AI Foundry (142)** Copilot Studio (409)

Security Posture for Agents

This feature is currently in preview and included with your Microsoft Defender CSPM license at no extra cost. Licensing requirements might change when the feature you'll be notified should you wish to re-enable it under the new license.

Last 7 days



Refresh Export

Filter set:

Account: Any Project: Any Model: Any Deployment: Any Agent Name: Any Add filter

Agent name	Status	ID	Creation time	Deployment	Account
[Redacted]	Published	asst_D5FvPArWjVOj4G0msuDjR4Kx	Oct 16, 2025, 1...	gpt-4.1	d4ai-foundry
Agent780	Published	asst_e1ITVCx9xPCAYCWdcjenMlcr	Nov 3, 2025, 7:...	gpt-4.1	foundry145
Agent217	Published	asst_ZAbVJB0S6YysloSRARwEUIDr	Nov 3, 2025, 7:...	gpt-4.1	foundry145
Agent629	Published	asst_crFtoC50JXG83e1H1FTLO075	Oct 30, 2025, 8...	gpt-4.1	foundry145
Agent487	Published	asst_IdE1svKmaGephqFUa21ErkAK	Oct 19, 2025, 5...	gpt-4.1	foundry145
coordinator					

Contoso Assist

Covered Published Platform: Azure AI Foundry

Open agent page Go hunt View on map

Agent info

ID: asst_D5FvPArWjVOj4G0msuDjR4Kx

Name: coordinatorAgent Creation time: Oct 16, 2025, 1:26 PM

Account: d4ai-foundry Project: D4AI-Foundry/Dev-project

Deployment: gpt-4.1 Model: gpt-4.1 version 2025-04-14

Attack paths: 18

Risk factors: Grounded With Sensitive Data

Recommendations

2 Recommendations

Critical: 0 High: 0 Medium: 0 Low: 2

- Home
- Exposure management
- Investigation & response
- Incidents & alerts
- Incidents
- Alerts
- Hunting
- Actions & submissions
- Partner catalog
- Threat intelligence
- Assets
- Microsoft Sentinel
- Identities
- Endpoints
- Email & collaboration
- Cloud apps
- Cloud infrastructure
- Security Copilot
- Agents
- Security Store

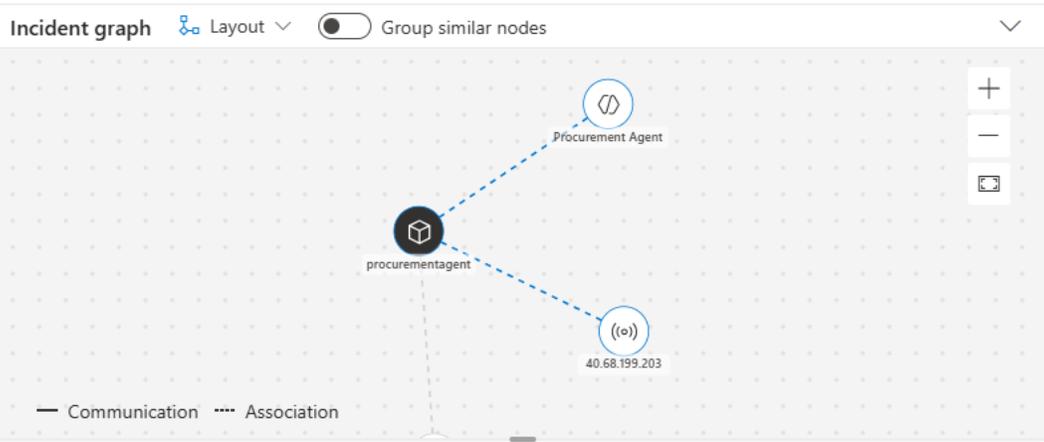
Incidents > Attack on Procurement Agent

Attack on Contoso Assist Agent

High Active Unassigned Agents CriticalAsset

Attack story Alerts (3) Activities Assets (2) Investigations (0) Evidence and Response (3) Summary Similar incidents (1)

- ### Alerts
- Nov 6, 2025 4:02 AM New **A user phishing attempt was detected on an AI agent (Preview)**
procurementagent
 - Nov 6, 2025 10:03 AM New **A Jailbreak attempt was blocked on an AI agent (Preview)**
procurementagent
 - Nov 9, 2025 2:19 PM New **DLP policy (Exfiltration to external recipient blocked) matched for email with subject (Procurement details for Orion)**
Abbi Atkins



- A user phishing attempt was detected on an...
- A Jailbreak attempt was blocked on an AI a...

What happened

There was 1 blocked attempt of a Jailbreak attack on AI agent Procurement Agent on an Azure AI Foundry project procurementagent. A Jailbreak attack is also known as User Prompt Injection Attack (UPIA). It occurs when a malicious user manipulates the system prompt, and its purpose is to bypass a generative AI's large language model's safeguards in order to exploit sensitive data stores or to interact with privileged functions. Learn more at <https://aka.ms/RAI/jailbreak>. The attempts on your AI Agent were using direct prompt injection techniques and were detected by Azure Responsible AI Content Filtering. To get detailed information on the prompt injection attempts, refer to the 'Supporting evidence events' section in the Azure Portal.

This alert is triggered by MDC detection
[View alert page in MDC](#)

- ### Activities
- Activity details
 - Related activities

Copilot Manage incident Tasks

A Jailbreak attempt was blocked on an AI agent (Preview)

Medium Unknown New

Open alert page Manage alert

Details Recommendations

INSIGHT

Quickly classify this alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert

Alert state

Classification	Assigned to
Not Set	Unassigned
Set Classification	

Alert details

Alert ID	Category
dc4cd5e5ae-2bab-	Privilege escalation



Wrap-up

And btw, there is a lot more, e.g.,
Power Platform, Viva Analytics,
MCP servers,...



1. Copilot is more than just AI chat - It's a comprehensive ecosystem that spans productivity, security, governance, and automation.
2. Copilot Agents are the future of scalable IT - With Agent 365 and Copilot Studio, but admins have control.
3. Security and compliance are built-in, not bolted on - Tools like Microsoft Purview, Entra, and Defender ensure Copilot usage aligns with Zero Trust.
4. Oversharing is the #1 risk - Use DSPM for AI and oversharing assessments to identify and mitigate data exposure.
5. Insights drive adoption and ROI - The Copilot Dashboard and Viva Insights help measure usage, impact, and business value.



Q & A



Ondrej Vysek

Unlocking Infinite Possibilities Through
Technology | SoftwareOne | Microsoft MVP



Team meeting.doc



files and more

SoftwareOne



Microsoft Copilot for Admins:

<https://admin.cloud.microsoft/>

software **one**



Ondrej Vysek

Unlocking Infinite Possibilities Through
Technology | SoftwareOne | Microsoft MVP

