

QUICK WIN NO. 03 · COPILOT, AGENTS AND SHADOW AI

See every piece of AI in your Microsoft 365, and decide what stays.

Where to find, and control, Microsoft Copilot, the agents built on it and the AI tools staff use without approval. Work through the five steps once, then run the monthly routine. Each step ends in a row on your AI Register.

BEFORE YOU START Give whoever keeps the register the **AI Reader** role, and whoever changes settings the **AI Administrator** role, under **Roles** then **Role assignments** in the Microsoft 365 admin centre. Keep **Global Administrator** for step 5a only. Items marked **Frontier** are Microsoft previews and need the tenant opted in.

1. SEE EVERY AGENT	ANY PLAN	2. SET WHO CAN INSTALL AND SHARE	AGENTS, SETTINGS
01	In the admin centre, open Agents then Overview . Clear pending requests and agents without an owner.	01	Agent and plugin access: allow agents built by Microsoft and by your organisation. Keep external publishers off until each is reviewed.
02	Open All agents then Registry . Agents are Microsoft, external partner, published by your org, or shared by a member of staff.	02	User access: start with a named pilot group, then widen. The default is All users.
03	Filter Availability to All users , then Missing an owner . Assign an owner, or block the agent.	03	Sharing: limit to the people trained to build agents. The default is All users.
04	Register every agent available to everyone, and every external or shared agent that touches client data.	04	An external agent you allow works under its publisher's terms, so it needs its own DPA check and its own register row.

STEPS 3 AND 4 · COPILOT AND USAGE

Make Copilot the safe default, then see who is using it.

Copilot Chat signed in with a work account carries Microsoft enterprise data protection. Control the parts that send data beyond Microsoft.

3. CONFIGURE COPILOT	COPILOT, SETTINGS	4. SEE WHO IS USING IT	REPORTS, USAGE
01	Pin Copilot Chat in Teams and Outlook, so staff reach for the protected tool, not a consumer one.	01	Open Reports, Usage , then Microsoft Copilot .
02	AI providers for other large language models: off, or limited to a named group. Read the terms each provider shows first.	02	Copilot Chat shows use by staff without a paid licence; Copilot shows licensed use by app. Allow two to three days for data.
03	Web search: set the Allow web search in Copilot cloud policy on purpose. Left unset, it is on.	03	For an audit trail of individual interactions, use Audit in the Microsoft Purview portal.
04	Self-service purchase: set to Do not allow , so licences are bought centrally and appear in the register.	04	Move a use case from Proposed to Live on the register once the report shows it in use.

LICENCES

Steps 1 to 4 and 5a work on any Microsoft 365 business plan. Agent usage and risk figures need **Microsoft Agent 365**. The Shadow AI page needs Microsoft 365 E5 with Defender for Endpoint, and the Local agents page E3, both on Intune-managed Windows devices. Cloud discovery needs **Defender for Cloud Apps**, and prompt monitoring needs **Purview** data security licensing.

STEP 5 · SHADOW AI

Find the AI nobody approved, then bring it in or shut it out.

Start with 5a. It works on any plan and closes the route by which an unapproved app reaches your email and files. Then add whichever of 5b to 5e your licences allow.

5A. STOP APPS REACHING MAIL AND FILES ANY PLAN

- 01 In the Entra admin centre, open **Enterprise apps**, **Consent and permissions**, then **User consent settings**.
- 02 Choose **Do not allow user consent**, or allow it only for verified publishers and selected permissions.
- 03 In **Admin consent settings**, let users request approval and name the reviewers.
- 04 Existing grants stay. Review **All applications** and remove any AI app you will not approve.

5B TO 5E. IF YOUR LICENCES ALLOW

- 01 **Shadow AI** (Frontier): detects apps such as ChatGPT Desktop and Claude Desktop on managed devices, with users and devices.
- 02 **Local agents** (Frontier): lists AI developer tools found on managed devices. Outside your developers, it should be empty.
- 03 **Cloud discovery**: in the Defender portal, filter discovered apps to **Generative AI**, then sanction or unsanction each one.
- 04 **DSPM for AI**: in Purview, see sensitive data typed into AI sites, and warn or block it with endpoint DLP.

KEEPING IT CURRENT

Run this once a month and the register stays true.

Do these in order and update the AI Register as you go.

THE MONTHLY ROUTINE

- 01 **Agents, Overview:** clear pending requests and assign owners.
- 02 **Registry:** register any new agent available to more than its creator.
- 03 **Entra Admin consent requests** and **Enterprise apps:** approve or refuse, and remove anything granted outside the process.
- 04 **Shadow AI, Local agents** and **Cloud discovery**, where licensed: sanction and register, or unsanction, each new app.
- 05 **Reports, Usage:** move use cases to **Live**, or retire unused ones.
- 06 **AI Register:** check each tool's DPA and terms are current, and that every use needing a DPIA has one logged.

THREE THINGS WORTH KNOWING

- ◆ Do not block Copilot Chat with network or URL rules. Microsoft does not support it; use the settings in step 3 instead.
- ◆ An app marked **Not approved** still belongs on the register, with the date of the decision. That record is your evidence.
- ◆ Everything here comes from Microsoft Learn as at October 2026. Frontier features change often, so recheck them each quarter.