

Manage access to SharePoint agents

SharePoint agents, powered by AI, help users quickly find information and insights on SharePoint sites, pages, and document libraries. SharePoint agents access your organization's data the same way [Copilot in other Microsoft 365 apps](#) does, responding to users based on their access permissions to the data. As a SharePoint admin, you can manage users' access to an agent in multiple ways by managing:

- Who can access the agents
- What information the user can access through the agent
- Where agents are available

Manage who can access the agents

Use file permissions on the agent file

As SharePoint agents are represented as [.agent files](#), permissions on the *.agent* file govern who can access or edit the agent. Only users who are able to create or access files on a SharePoint site can create or access agents.

Note

For users who can access and use a SharePoint agent, the agent's responses depend on permissions for each user to the agent's data sources. For instance, if a user has access to the agent but not to the site or document library it references, the agent's responses for this user won't include content from those restricted sources.

Control user access through licensing

Currently, users with a [Microsoft 365 Copilot license](#) can use the agents. You can use the [Microsoft 365 Copilot setup guide](#) in the Microsoft 365 admin center to assign the required licenses to users. For more information, see [Assign licenses to users in the Microsoft 365 admin center](#) and [Microsoft 365 Copilot requirements](#).

Admins can choose to edit the service plans under the Copilot license to specifically allow or block users from using Copilot experiences on SharePoint. Under the [license details page for Microsoft 365 Copilot](#) on the Microsoft 365 admin center, admins can turn '*Microsoft 365 Copilot for SharePoint*' on or off on a per-user basis. For example, a user could be allowed to use Microsoft 365 Copilot on Teams but not use any agents on SharePoint alone. This will also disable Copilots on OneDrive and the SharePoint page authoring Copilot for that user.

Note

From January 6, 2025, to June 30, 2025, enterprise tenants with 50 or more Microsoft 365 Copilot licenses will receive 10,000 free SharePoint agents queries for unlicensed users every month as a trial. Users with a role of SharePoint administrator or higher can [check the trial promotion status](#) and [set trial promotion](#) using PowerShell cmdlets. See the terms of trial usage [here](#).

Manage what information a user can access through the agents

With built-in SharePoint features

SharePoint agents use SharePoint sites, pages, and document libraries as knowledge sources to respond to the user. You can control a user's access to the information when they use an agent by controlling their access to the site. SharePoint provides many tools to control access to a site:

- Control access to a site that is associated with a [Microsoft 365 group](#) by [setting the site as private](#) (team sites only) and controlling group membership.
- Control access to a site that isn't associated with a group using [site permissions](#).
- Control access with access governance policies available in the SharePoint admin center and PowerShell.

Learn more about using SharePoint's built-in features to control access [here](#).

With SharePoint Advanced Management

Currently, to restrict access to a site by Microsoft 365 Copilot, the SharePoint Admin can set up a [restricted access control policy](#). As a result, all access to the site is restricted to only the group of users specified in the policy. Accordingly, the content from this site is visible in Microsoft 365 Copilot only for this restricted group of users. You can restrict access to individual sites or OneDrive. Learn more about more features to prevent oversharing, control access, and enhance your content governance with SharePoint Advanced Management [here](#).

With Microsoft Purview Data Loss Prevention (DLP)

You can prevent selected files from being used by agents by using sensitivity labels along with [Microsoft Purview Data Loss Prevention \(DLP\)](#). You [do this](#) by creating a DLP custom policy with the **Content contains > Sensitivity labels** condition to exclude items from being processed. Identified items are available in the citations of the response, but the content of the item isn't used in the response. We don't yet support adding a sensitivity label directly to the [.agent file](#). If you want to govern your *.agent* file with DLP, instead of using the sensitivity labels as the condition, you can use conditions based on the *.agent* extension. We'll support the ability of adding a sensitivity label directly to a *.agent* file in the future.

Manage where agents are available in SharePoint

Site owner controls

Agents created in SharePoint aren't automatically listed or published anywhere. Users can manually navigate to *.agent* files to use them just like how they would discover or use Word or Excel files. Site owners can choose to designate specific agents from their sites as 'approved' ones. These agents would be guaranteed to show up on the picker for that particular site, and users can differentiate them from the ones that are recommended to them. Learn more [here](#).

Turn off agents on sites with restricted content discovery

You as a SharePoint Admin can turn off all agent-related features on individual sites with the [restricted content discovery](#). Once a site is flagged with restricted content discovery, users can't see the Copilot icon on the upper right of the site. Therefore, they don't have access to use the ready-made agent, create new agents, or add content from that site to any other agents. The restricted content discovery policy leaves site access unchanged but prevents the site's content from being surfaced in Microsoft 365 Copilot or organization-wide search for all users.

More resources