Frequently Asked Questions about Copilot Studio Security

These frequently asked questions (FAQs) focus on security issues to help you find answers, thereby accelerating the adoption and use of Copilot Studio in your organization.

1. Copilot Studio **creates a single-tenant Microsoft Entra ID application registration when creating a new agent. Existing agents continue to use the multi-tenant Microsoft Entra ID application registration. Does this multi-tenant Microsoft Entra ID application registration for existing agents pose any security risks?**

No, registering for the Microsoft Entra ID multitenant application does not pose any security risks.

Copilot Studio creates a custom application registration for each agent to identify and enable secure communication with the channels and skills that agent can use. This application registration does not access or disclose any client data, resources, or agent information. Copilot Studio stores and manages application registrations securely and in compliance with regulations.

This application registration is used to authenticate and secure calls from Copilot Studio to Azure Bot Service resources. Copilot Studio creates and manages registrations for customer applications. This functionality has been available in the Bot Framework and Azure Bot Service since 2016.

1. All newly created agents are registered with the Microsoft Entra ID single-tenant application. We are exploring the possibility of migrating existing agents to Microsoft Entra ID single-tenant application registration in the future.

2. Microsoft Power Platform has a rich ecosystem of connectors based on Microsoft Entra ID, allowing authorized Microsoft Entra ID users to build compelling applications and flows, establishing connections to available business data through these data repositories. User isolation makes it easier for administrators to ensure that these connectors can be used securely and safely within the user's scope, while minimizing the risk of data leaks outside the user's scope. Does Copilot Studio support user isolation?

No, Copilot Studio does not support user isolation.

The default configuration in Power Platform with user isolation turned off allows for seamless connection establishment between tenants if a user from tenant A establishes a connection with tenant B providing the appropriate Microsoft Entra ID credentials.

If administrators want to allow only a specific group of users to establish connections to or from their account, they can enable account isolation.

3. Copilot Studio creates service accounts and certificates in the client's Microsoft Entra ID tenant each time a custom agent is created. What is the purpose of service accounts and certificates, and how are they managed?

To allow custom agents to communicate with your data sources and services, Copilot Studio creates an application within your Microsoft Entra ID account, along with a linked service account.

A service account is an identity that represents an application and allows that application to access resources within your account. For security and compliance reasons, Copilot Studio uses linked identities.

4. Can you disable the creation of Microsoft Copilot Studio agents in your organization?

You cannot disable agent creation. The guideline is to use data policies to disable anyone from chatting with that agent.

5. You are the responsible AI manager or compliance leader in your organization. Where can you find information about agent security and privacy related to the data used by the agent, the data used by the platform models within the agent, data protection measures, and content moderation before Copilot generates a response?

Microsoft operates on trust. They are committed to security, privacy, and compliance in everything they do, and their approach to AI is no exception.

6. What auditing capabilities does Copilot Studio offer by default? How do you request other capabilities if needed?

You are an IT administrator in a Fortune 1000 organization. You want to manage custom agents built by users within your organization. To truly democratize Copilot Studio within your organization, you need granular auditing capabilities. For example, consider the following questions:

1. Who built the custom agent?
2. Are there any co-owners?
3. Are there any public endpoints for generated answers?
4. Who configured or modified an agent?

As an administrator, you can use Copilot Studio's default auditing capabilities to secure and manage your environment. Log in to the Microsoft Purview portal and use filters to define specific events and activities to be audited.

If you're looking for more events or auditing schools, please submit your product ideas.

7. How can you control the Generative AI capabilities in Copilot Studio?

You are a Power Platform administrator in your organization. As part of your role, you need to selectively grant users access to Generative AI capabilities in Copilot Studio across multiple environments.

Copilot Studio provides granular administrative controls and tenant levels for custom agents within your organization. Use the Power Platform admin center to:

1. Allow or disallow publishing custom agents at the tenant level.
2. Control whether custom agents can use public URLs as knowledge sources at the environment level.
3. This allows for the movement of data between geographic locations for environmental-level Generative AI features.

If you're looking for more granular control over managing custom agents, please submit your product idea.

8. How do you enforce access to knowledge resources across your environments?

As a Power Platform environment administrator in your organization, you need to control which knowledge sources are available to users when they build custom agents. For example, you might want users in your default environment to only upload files or use specific websites as knowledge sources when building custom agents.

Copilot Studio provides granular control over enabling or disabling specific knowledge sources using data policies in the Power Platform admin center. You can configure data policies to control the use of SharePoint, public websites, or documents as knowledge sources. You can then apply these policies at the environment or tenant level.

9. Does Copilot Studio offer data encryption during storage?

Your conversations may contain sensitive information, and you want to protect that information by encrypting it using a client-managed key (CMK).

Copilot Studio allows you to enable CMK. When CMK is enabled for the Copilot Studio environment, all Copilot Studio data will be encrypted using the client's key. Clients can change the key or disable CMK as needed.

10. How does Copilot Studio ensure that responses from confidential websites are not visible to people who are not authorized to view that information?

You can configure custom agents to access multiple internal websites, some of which contain confidential information that only certain authenticated users can access.

Copilot Studio is secure by default. The system tailors its responses based on who is speaking to it and their permissions. Copilot Studio supports security labels to prevent excessive information sharing. It also supports endpoint filtering to prevent data loss for SharePoint knowledge sources.