Key Concepts - Security and Administration in Copilot Studio

Copilot Studio adheres to a number of security and governance processes and controls, including geographic data storage, data loss prevention (DLP), multiple standards certification, regulatory compliance, environmental routing, and regional customization.

Copilot Studio adheres to a number of security and governance processes and controls, including geographic data storage, data loss prevention (DLP), multiple standards certification, regulatory compliance, environmental routing, and regional customization.

This article provides an overview of the security measures followed by Copilot Studio, a list of security and administrative controls and features, and examples and recommendations for safely implementing security in Copilot Studio for your agent creators and users.

Security and governance controls

Control	Core script
Runtime agent protection status	Creators can view the security status of agents from the Agents page.
Data policy control	Administrators can use data policies in the Power Platform admin center to manage the use and availability of Copilot Studio agent features and capabilities, including: 1. Authenticate the creator and the user. 2. Source of knowledge 3. Action, connector, and skill 4. HTTP request 5. Published on channels 6. AppInsights 7. Trigger
Audit logs in Microsoft Purview for administrators	Administrators have full access to view the manufacturer's audit logs in Microsoft Purview.
Audit logs in Microsoft Sentinel for administrators	Administrators can monitor and receive alerts about agent activity through Microsoft Sentinel.
Run the tools using the user's login credentials.	The agent creator can configure the tool to use the user's login credentials by default.

Control	Core script
Sensitivity labels for SharePoint data	Agent creators and users can view the highest sensitivity labels applied to sources used in agent responses and individual reference labels within the conversation.
Authenticate users using certificates.	Administrators and creators can configure agents to use manual Entra ID authentication with the certificate provider.
Manufacturer's security warning	Developers can view security alerts for their agent before publishing when the default security and administration configurations are modified.
Environment routing	Administrators can configure environment routing to provide users with a secure space to build agents.
Welcome message from the creator	Administrators can configure welcome messages to inform users about important privacy and regulatory compliance requirements.
Management using autonomous agents based on data policies.	Administrators can manage agent capabilities using triggers that utilize data policies, ensuring protection against data leaks and other risks.
CMK	Administrators can enable client-managed encryption keys (CMK) for their Copilot Studio environment.

Security development cycle

Copilot Studio follows the Security Development Lifecycle (SDL). The SDL is a set of rigorous processes that support security and compliance requirements.

Data processing and licensing agreements

The Copilot Studio service is governed by your commercial licensing agreements, including Microsoft's Product Terms and the Data Protection Appendix.

Adhere to standards and procedures.

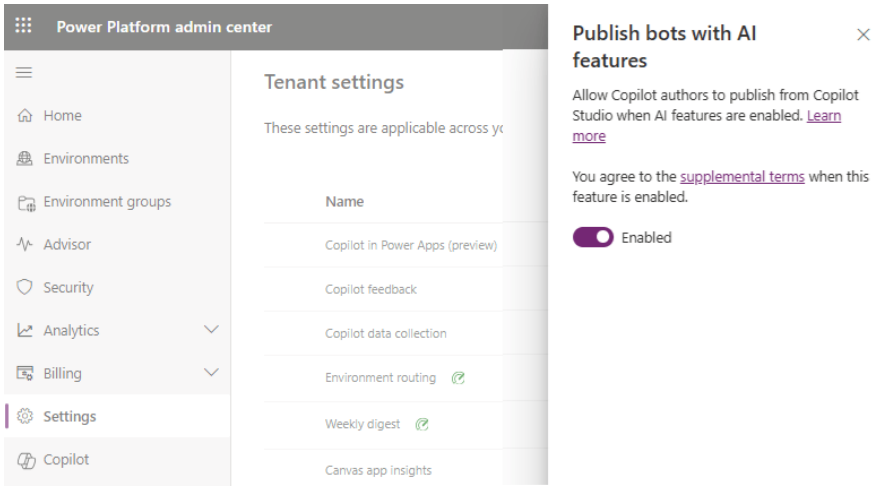
The Microsoft Trust Center is the primary resource for Power Platform compliance information.

Data loss prevention and management

Copilot Studio supports an extensive set of data loss prevention features to help you manage your data security, along with Power Platform data policies.

Additionally, to further manage and secure Copilot Studio using its Generative AI features within your organization, you can:

1. Disable agent publishing: Your administrators can use the Power Platform admin center to disable the ability to publish agents that use Generative AI features to your tenant.



1. Disable data transfer between geographic locations for Copilot Studio's Generative AI features outside the United States.
2. Use the Microsoft 365 admin center to manage actions and conversational agents and AI displayed in Microsoft 365 Copilot.

Finally, Copilot Studio supports secure access to customer data using Customer Lockbox.

Important note : The configured lockbox does not include data sent from Copilot Studio as part of the Agent 365 security audit log.