

MICROSOFT 365 COPILOT SERVICENOW CONNECTORS NOW APPLY SERVICENOW ROLE PERMISSIONS

OPERATIONAL SIGNAL

DOMAIN: CTRL — Control | CONFIDENCE LEVEL: HIGH

INSTITUTIONAL DIMENSIONS: Authority | Attribution | Visibility | Escalation | Continuity

Signal ID	Platform	Source	Audience	Signal Date
SIG-CTRL-002	Microsoft 365 Copilot	Link	Security Digital Workplace Admin	11 Aug 2026

CAPABILITY SHIFT

Microsoft 365 Copilot ServiceNow Knowledge and Catalog connectors now include assigned ServiceNow roles when checking access to knowledge articles and catalog items. Microsoft says earlier connector permissions were determined only by user criteria; the connectors now also evaluate roles such as admin, knowledge manager and knowledge admin.

ORGANISATIONAL CONSEQUENCE

The retrieval boundary can therefore change without changing the connector itself. A user's ServiceNow role assignments now help determine which connected content Copilot can return, so role design and maintenance in ServiceNow have a more direct effect on what users can access through the connectors.

WHAT TO WATCH

- Copilot connector results changing when ServiceNow role assignments are added or removed
- Knowledge articles or catalog items available in ServiceNow but unavailable through the connector because role requirements differ
- Unexpected access when ServiceNow roles no longer match intended responsibilities

WHY THIS MATTERS NOW

Microsoft documented the change on 11 August 2026. Organisations using these connectors now have an additional permission input when investigating missing or unexpected Copilot retrieval results.

WHAT TO REVIEW

- Which ServiceNow knowledge articles and catalog items are exposed through these Copilot connectors, and which roles govern access to them
- Whether those ServiceNow roles still reflect the intended access boundary for Copilot-connected content
- Who owns changes to those roles, including custom or non-standard roles

GOVERNANCE CONTEXT

Authority and visibility now depend partly on role configuration in the source system, not only connector-level user criteria. Permission reviews should therefore include the ServiceNow roles that shape connector access.

Scope Boundary: This artefact translates observed platform capability changes into operational considerations. It does not constitute policy, legal advice, or enforcement guidance.