Microsoft Security Copilot Plugin Guide – ServiceNow

Plugin overview

ServiceNow is an enterprise app ecosystem designed to connect and automate business processes, delivered as a SaaS application. Many security operation centers (SOCs) use ServiceNow as part of their incident management flow, and often extend the core functionality with customizations, integrations, and security-specific modules.

The Security Copilot plugin for ServiceNow enables connectivity between a Security Copilot session and a ServiceNow incident queue. Users can import a ServiceNow incident into Security Copilot, easily correlate with data from Microsoft security products such as Defender for Endpoint, enrich with external threat intelligence, and persist the results of their investigation in ServiceNow. These capabilities, combined with the narrative prompt and generative AI powered by Azure OpenAI, speed incident resolution, help up-skill team members, and provide more comprehensive views into any security incident.

Connect to ServiceNow

Prerequisites

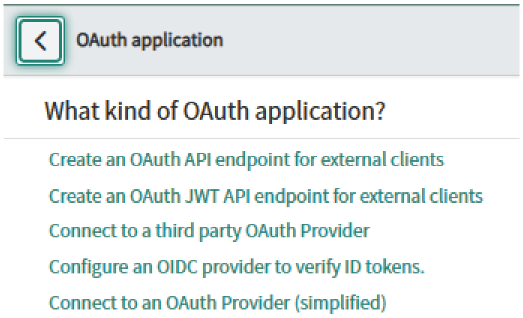
1. ServiceNow IT Service Management (ITSM) standard edition (at a minimum)
2. Access to your ServiceNow SaaS instance, with permissions to create new users
3. Access to Security Copilot, with permissions to activate new connections
4. Available ServiceNow API quota

ServiceNow setup

There are two connectivity methods to ServiceNow, choose the one that suits your needs.

1. HTTP Basic auth
    a. Access your ServiceNow instance and locate the option to create a new user
    b. Create a user within ServiceNow with the following roles (aka permissions):
        i. Itil
        ii. rest_api_explorer
    c. Optionally limit the API user's access to only read incidents (see below)
    d. Note the credentials and the ServiceNow instance URL
2. OAuth authorization_code auth
    a. Access your ServiceNow instance and create a new Application Registry object by following these steps:
    b. Navigate to System OAuth -> Application Registry, click New

c. Select “Create an OAuth API endpoint for external clients”



OAuth application

What kind of OAuth application?

- Create an OAuth API endpoint for external clients
- Create an OAuth JWT API endpoint for external clients
- Connect to a third party OAuth Provider
- Configure an OIDC provider to verify ID tokens.
- Connect to an OAuth Provider (simplified)

d. Enter a name that identifies Security Copilot.

e. Enter a redirect URI corresponding to the Security Copilot instance you are using (example: https://securitycopilot.microsoft.com/auth/v1/callback. The domain name can be substituted to point to other instances. Multiple URIs can be comma-separated)

f. Assign an auth scope corresponding to your access control needs.

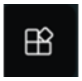
g. Save the Application Registry object.

h. From the newly created object, note the client ID, client secret, and the ServiceNow instance URL.

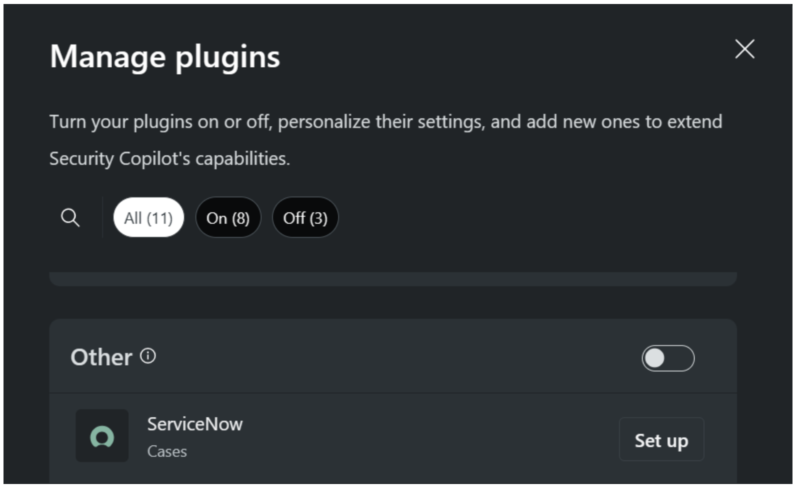
i. This OAuth setup should only be done once per ServiceNow instance. The resulting OAuth Application Registry object can be used multiple times by different users.

Security Copilot connection

1. Access Security Copilot at https://securitycopilot.microsoft.com/ and ensure you are authenticated.
2. Click the plugins icon in the lower left corner of the screen.



3. Scroll down to the “Other” section to locate ServiceNow and click “Set up”.



Manage plugins

Turn your plugins on or off, personalize their settings, and add new ones to extend Security Copilot's capabilities.

4. Select a preferred authorization method and fill in the fields to connect to your ServiceNow instance.
   a. HTTP Basic instructions
      i. Enter the username and password corresponding to the dedicated ServiceNow account you created earlier.
   b. OAuth authorization_code instructions

i. Enter auth parameters corresponding to the Application Registry object you created earlier.

ii. The instance URL, client ID, and client secret correspond to values of the same name in the Application Registry object. To determine what to enter for each value, refer to the following table:

Setting name	Description	Example
Instance	Set to the ServiceNow instance URL	https://ven01958.service-now.com/
ClientId	Set to client ID in ServiceNow Application Registry object	5bcebf3ecb26bd945a7bb126b7bcc34b
ClientSecret	Set to client secret in ServiceNow Application Registry object	Q2?`pW7_
AuthorizationEndpoint	Set to https://<service-now-instance-domain>/oauth_auth.do.	https://ven01958.service-now.com/oauth_auth.do
TokenEndpoint	Set to https://<service-now-instance-domain>/oauth_token.do.	https://ven01958.service-now.com/oauth_token.do
Scopes	Set to the scopes defined in the ServiceNow Application Registry object. Comma-separate multiple scopes.	useraccount
AuthorizationContentType	Should be left unchanged from default application/x-www-form-urlencoded	application/x-www-form-urlencoded

iii. Note: Each individual Security Copilot user must enter these values to perform OAuth setup for themselves. This is a known issue, and there is a workaround available. Please reach out to us to configure your tenant once with these OAuth values and allow individual users to skip this setup step.

5. Click "Save" or "Connect" to complete the setup.
   NOTE: Currently, the system does not validate your credentials when you save your settings. If they are not correct, you will see an error later when Security Copilot attempts to invoke the ServiceNow plugin.
6. Close the plugins window.

Getting started

Tips for effective prompting

Security Copilot operates primarily with natural language prompts. When you are ready to load an incident into your Security Copilot session or search for related ServiceNow incidents, you will submit a prompt that will guide Security Copilot to select the ServiceNow skillset and invoke the proper skill.

When you word your prompt, **ensure you mention ServiceNow as the preferred source of your incident**; Security Copilot can connect to several systems that each provide incidents, and it benefits from guidance on which source you prefer.

Example prompts for incident queries

"Load ServiceNow incident INC12345"

"What ServiceNow incidents refer to IP address 10.0.0.1?"

> "Show me recent high severity ServiceNow incidents" *followed by*
> "Show details on the third incident" *and then, if IP addresses are listed:*
> "What is the MDTI reputation score for those IP addresses?"

Appending comments to ServiceNow incidents

If enabled with appropriate permissions, the ServiceNow connector can append comments to ServiceNow incidents. The comment text can be provided by the user, or sourced from Security Copilot features, such as session sharing links or pinned prompt investigation summaries. Example prompts include:

> "Write a link to this Copilot investigation to ServiceNow incident INC12345"
>
> *After loading an incident:* "Write the following text to that ServiceNow incident: Investigated with Security Copilot and deployed new detection logic."
>
> *After pinning a few prompts:* "Write a summary of this investigation to ServiceNow incident INC12345" *or if the session is already loaded* "Summarize this investigation and write it as a comment on the ServiceNow incident."

Note the current version of the plugin appends comments to the ServiceNow incident. Future versions may provide the option of writing to the work notes instead.

Plugin capabilities reference

Normally, Security Copilot will select and invoke the appropriate capability based on your prompt, but it is also possible to directly invoke specific capabilities by typing "/" in the prompt bar and providing the necessary inputs.

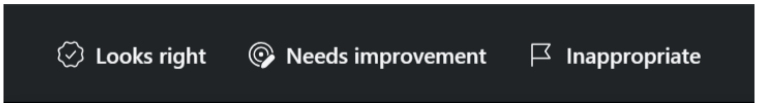
In either case, it can be helpful to know which capabilities are available and how they are designed to operate.

Capability	**Behavior**
GetServiceNowIncident	*Retrieves ServiceNow incident based on the incident details.* **Required input:** ServiceNow incident number [INC___] or SysID **Behaviors:** a. Incidents with greater detail may be truncated to fit within prompt space and the Security Copilot UX. b. Work notes and comments are limited to the last 5 notes. c. Work notes with extensive content may be summarized or truncated. d. Security Copilot will select just one incident to display even if the prompt could return multiple incidents. Avoid prompts such as "Summarize those incidents".
SearchServiceNowIncidents	*Finds ServiceNow incidents based on a keyword search, optionally filtered by state and priority.* **Required inputs:** Search term(s) **Optional inputs:** a. *State* – "New", "In Progress", "On Hold", "Resolved", "Closed" or "Canceled" (default is "In Progress") b. *SortBy* – "Ascending" or "Descending" (default is descending) c. *Priority* – "Critical", "High", "Moderate", "Low", "Planning" d. *IncidentCount* – Equal to or less than (default is 10) **Behaviors:**

	a. Incidents with greater detail may be truncated to fit within prompt space and the Security Copilot UX. b. Uses the ServiceNow text search feature that searches incident titles, many fields, work notes and comments. c. The Security Copilot UX and the underlying GPT models are not optimized to handle large volumes of results. Use specific searches when possible and consider filtering to specific priorities for best outcomes.
AppendCommentToServiceNowIncident	*Appends a comment to a specific ServiceNow incident*. **Required inputs:** Text of the comment to write, or a prompt that triggers writing a sharing link or investigation summary. **Behaviors:** a. Consider wrapping your comment text in "quotes" when using an open prompt to clearly define what portion of your prompt you want written to the comment. b. Currently the plugin only writes to comments; future versions may provide the option to write to work notes instead. c. Security Copilot has the ability to write the session sharing link to the comment if you prompt it to do so. d. You can also prompt Security Copilot to write the current investigation summary to the comment. Ensure you have an investigation summary populated by first pinning a few prompts and reviewing the incident summary that appears in the right side panel.
GetServiceNowIncidentWorkNotes	*Retrieves work notes from a specific ServiceNow incident*. **Required inputs:** An incident number or sys_id corresponding to the incident.
GetServiceNowIncidentComments	*Retrieves comments from a specific ServiceNow incident*. **Required inputs:** An incident number or sys_id corresponding to the incident.

Providing Feedback

Your feedback on Security Copilot generally, and the ServiceNow plugin specifically, is vital to guide current and planned development on the product. The optimal way to provide this feedback is directly in the product, using the feedback buttons at the bottom of each completed prompt:



We recommend "Looks right" when the result matches expectations, "Needs improvement" when it does not, and "Inappropriate" when the result is harmful in some way.

Whenever possible, and especially when the result is “Needs improvement”, please write a few words explaining what we can do to improve the outcome. This also applies when you expected Security Copilot to invoke the ServiceNow plugin, but another plugin was selected instead.