



Cisco AI Assistant Skills

- [Online Help Documentation](#), on page 1
- [Policy Insights](#), on page 1
- [Policy Analyzer and Optimizer](#), on page 4
- [Automate Policy Rule Creation](#), on page 6
- [Contact Support](#), on page 10
- [Notifications Center](#), on page 14

Online Help Documentation

The AI Assistant grants administrators full access to the entire knowledge base, allowing them to ask any query and receive precise, accurate responses. This streamlines the process, saving both time and effort. Additionally, the AI Assistant enhances the user experience by offering relevant citations and reference links to help documents, guiding administrators toward the intended outcome with ease.

Administrators can simply type their query into the AI Assistant's chat interface. The Assistant will respond with a clear answer, along with citations and reference links to help documents for additional guidance.



Tip **Sample prompts:**

- *What are the steps to configure a new firewall policy?*
 - *Where can I find documentation on rule optimization?*
 - *How do I renew an expired rule in my firewall settings?*
-

Policy Insights

Administrators can ask questions to gain insights into policy configurations, including rule details, status, and compliance alignment. AI Assistant scans and analyses policies to provide details of potential gaps and overlaps that need to be resolved resulting in better performance and efficiency.

SUMMARY STEPS

1. Navigate to your tenant's dashboard and click on the AI Assistant icon located in the right top corner.

2. Use a simple prompt to inquire about existing policy rules (e.g., "*Show all access control rules*").
3. The AI Assistant retrieves a comprehensive list of policies relevant to your query.
4. Review the details provided by the AI Assistant, including rule configurations, rule status, and key attributes such as allowed traffic, blocked ports, or IP addresses.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	Navigate to your tenant's dashboard and click on the AI Assistant icon located in the right top corner.	
Step 2	Use a simple prompt to inquire about existing policy rules (e.g., " <i>Show all access control rules</i> ").	
Step 3	The AI Assistant retrieves a comprehensive list of policies relevant to your query.	
Step 4	Review the details provided by the AI Assistant, including rule configurations, rule status, and key attributes such as allowed traffic, blocked ports, or IP addresses.	

Example

AI Assistant

You

What policies are blocking the Webex application and webex.com URL?

AI Assistant

The policies blocking the Webex application and webex.com URL include Test ACP, nyc_access Control Policy, chuy_test1, child_policy_1, anna_acp2, TEST1, chuys_test2, AA, raj-acp,

[View details](#)

Last data sync: about 5 hours ago

How this response was generated



Ask the AI Assistant a question

[View User Guide](#) to learn more.



Tip Sample Prompts

- *What rules are using http://github.com ?*
 - *What rules are using this IP 100.20.10.1?*
 - *What policies are blocking the Webex application and webex.com URL?*
 - *Which rules allow inbound traffic?*
 - *Show rules with expired conditions.*
-

Policy Analyzer and Optimizer

The AI Assistant identifies gaps and inconsistencies within firewall rules, providing administrators with detailed insights into anomalies or potential issues. This allows administrators to quickly address security vulnerabilities, ensure compliance, and optimize the overall effectiveness of their firewall policies. The rules can be:

- **Mergable Rule:** Rules that can be combined or consolidated because they share similar criteria or actions. For example, if two or more rules apply to the same source, destination, or protocol, but have redundant or overlapping conditions, they can be merged to reduce complexity and improve the overall efficiency.
 - **Expired Rule:** Rules that are no longer active because they have passed a predefined expiration date or time limit.
 - **Object Overlap:** An element in a field of a rule is a subset of one or more elements in the same field of the rule. *For example, the source field might include a network object for 10.1.1.0/24, and another object for the host 10.1.1.1. Because 10.1.1.1 is within the network covered by 10.1.1.0/24, the object for 10.1.1.1 is redundant and can be deleted, simplifying the rule and saving device memory.*
 - **Duplicate/Redundant Rule:** Two rules apply the same action to the same type of traffic and removing the base rule would not change the ultimate result. *For example, if a rule permitting FTP traffic for a particular network were followed by a rule allowing IP traffic for that same network, and there were no rules in between denying access, then the first rule is redundant, and you can delete it.*
 - **Shadowed Rule:** This is the reverse of a redundant rule. In this case, one rule will match the same traffic as another rule such that the second rule will never be applied to any traffic because it comes later in the access list. If the action for both rules is the same, you can delete the shadowed rule. If the two rules specify different actions for traffic, you might need to move the shadowed rule or edit one of the two rules to implement your desired policy. *For example, the base rule might deny IP traffic, and the shadowed rule might permit FTP traffic, for a given source or destination.*
1. The AI Assistant continuously monitors and analyzes your firewall rules. You can prompt the Assistant to analyze current policies for gaps or inefficiencies (e.g., "Analyze rules for redundant configurations").
 2. The AI Assistant flags any redundant, duplicate, or conflicting rules that could be optimized. It provides suggestions on merging or updating rules to streamline firewall performance.
 3. Based on the analysis, the **AI Assistant** recommends optimizations, such as removing obsolete rules, adjusting configurations, or tightening access control for better security.



Note If the **AI Assistant** detects expiring rules or performance issues within a policy, it automatically generates alerts to prompt timely actions from the administrator.

AI Assistant

● You

Show me what policies can I optimize?

🗨️ AI Assistant

The policies that can be optimized include 'raj-acp', 'TEST1', 'child_policy_1', 'anna_acp2', and 'r' have varying percentages of optimizable rules.

[↗️ View details](#)

Last data sync: about 5 hours ago

How this response was generated

i Your feedback helps us improve the AI Assistant.



Ask the AI Assistant a question

[View User Guide](#) to learn more.

You can click on **View Details**.



Tip Sample Prompts

- Identify any inconsistencies in my firewall rules.
 - Show me gaps in current firewall policy configurations.
 - Are there any redundant or conflicting rules in my firewall setup?
-

Resolve Policy Abnormalities

Administrators can address policy rule gaps efficiently using the AI Assistant. With its help, they are able to:

- Disable all the policy rules that are redundant, shadow rules, and expired.
- Remove all the policy rules that are redundant, shadow rules, and expired.
- Merge all the policy rules that are redundant.



Note In case performing any of these actions does not resolve the issue, you can [create a support ticket](#) to contact Cisco Support Team.

Automate Policy Rule Creation

The AI Assistant simplifies policy rule creation process for the Secure Firewall Threat Defense managed by cloud-delivered Firewall Management Center and minimizes the need for extensive technical knowledge or manual configuration. By leveraging [simple prompts](#), administrators can quickly establish robust security measures, enhancing the overall efficiency and security of their network. These rules once created are listed under the policies section in your tenant.

Example Scenario

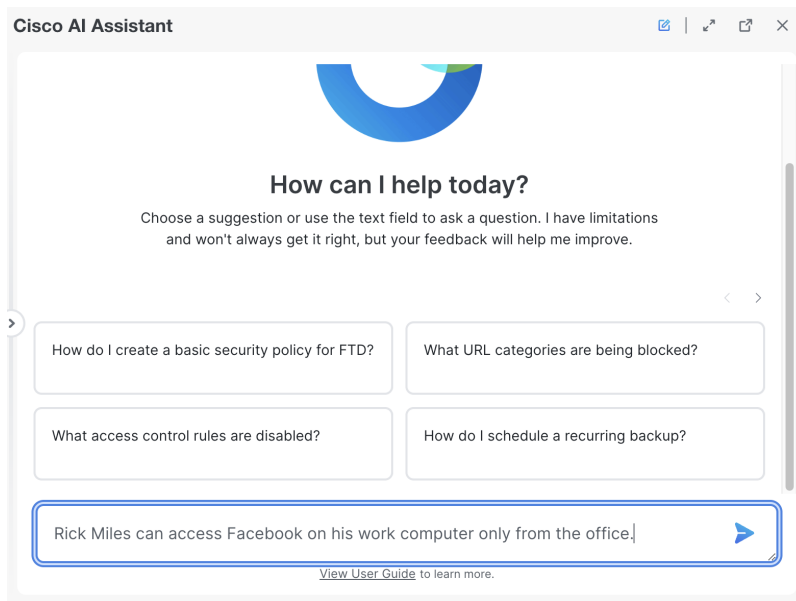
Consider a scenario where an administrator receives the following request:

Rick Miles can access Facebook on his work computer only from the office.

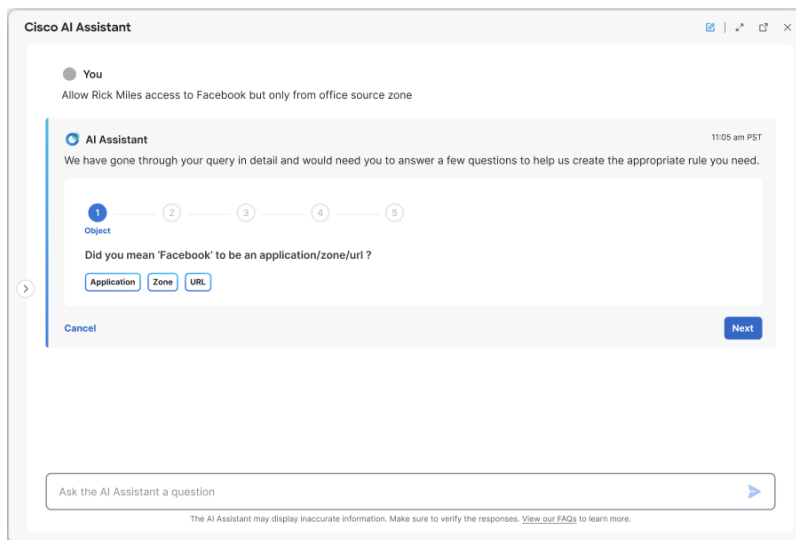
This would be the process the administrator would follow to create the rule:

Procedure

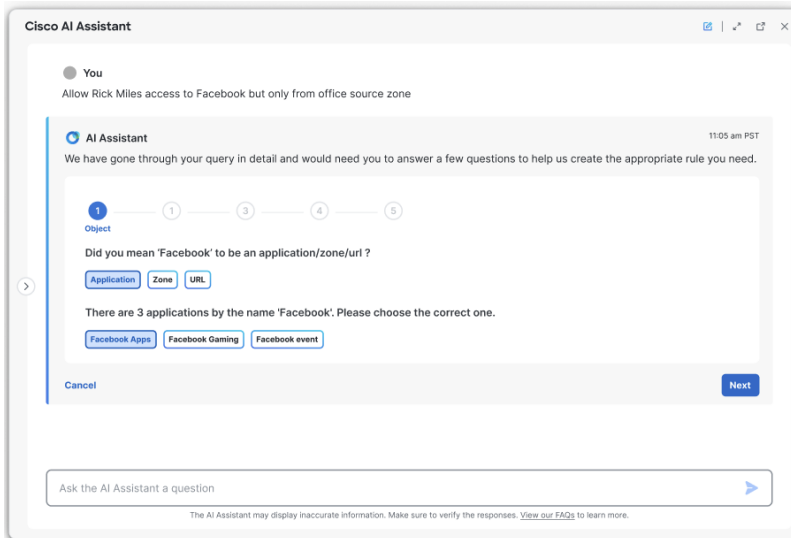
Step 1 The administrator needs to create a new rule to accommodate this request. They put this request to the AI Assistant:



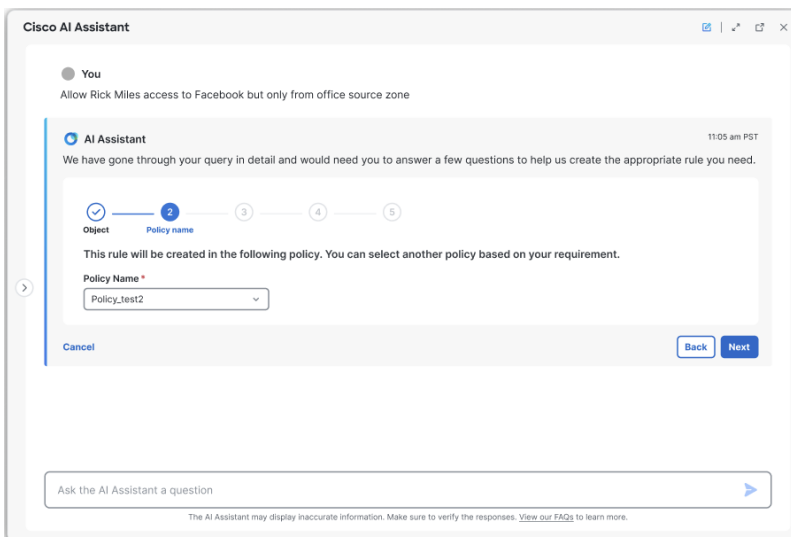
Step 2 The AI Assistant asks a question to better understand the administrator's requirement, and then guides them through a selection of options to create the rule:



Step 3 The AI Assistant finds multiple results for Facebook, and asks the administrator to clarify if they are referring to Facebook as an application, URL or a Zone:



Step 4 The AI Assistant prompts the administrator to select the policy to which the rule will be added:



Step 5 The AI Assistant suggests a "Rule Name", which the administrator can modify if needed:

The screenshot shows a chat window titled "Cisco AI Assistant". At the top, it says "You" and "Allow Rick Miles access to Facebook but only from office source zone". Below that, the AI Assistant message says: "We have gone through your query in detail and would need you to answer a few questions to help us create the appropriate rule you need." A progress bar shows five steps: 1. Object, 2. Policy name, 3. Rule name (current), 4. User name, and 5. Category. The text says: "Here is a recommendation for rule name. You can change the rule name based on your requirement." Below this is a text input field labeled "Rule Name *" containing the text "Rule_test_1". There are "Cancel", "Back", and "Next" buttons. At the bottom, there is a text input field for asking questions and a small disclaimer: "The AI Assistant may display inaccurate information. Make sure to verify the responses. View our FAQs to learn more."

Note

If the administrator chooses a "Rule Name" that already exists in a policy, the assistant displays an error prompting the administrator to enter a new name.

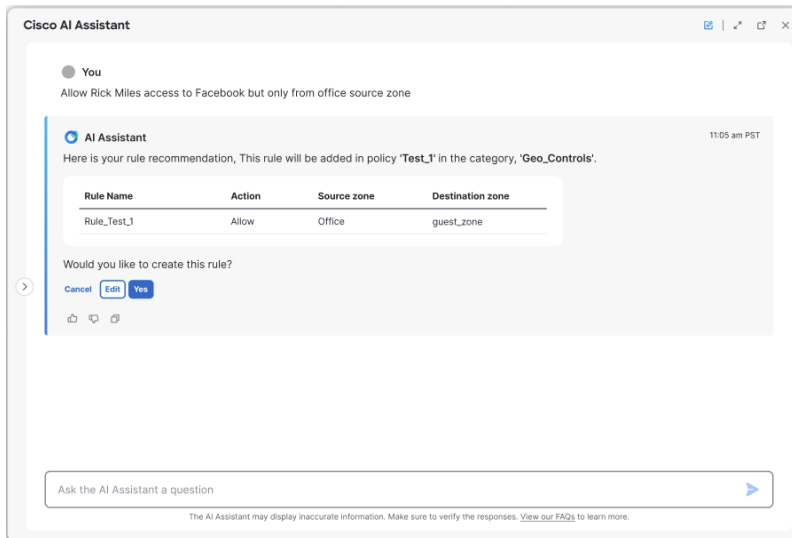
Step 6

The AI Assistant prompts the administrator to select a "User name" and a "Category" for the rule:

The screenshot shows the same chat window as in Step 5. The progress bar now shows all five steps completed: 1. Object, 2. Policy name, 3. Rule name, 4. User name, and 5. Category. The text says: "Please select the appropriate 'category' in which you need to place this rule." Below this is a dropdown menu with "Geo_Controls" selected. There are "Cancel", "Back", and "Done" buttons. At the bottom, there is a text input field for asking questions and the same disclaimer as in Step 5.

Step 7

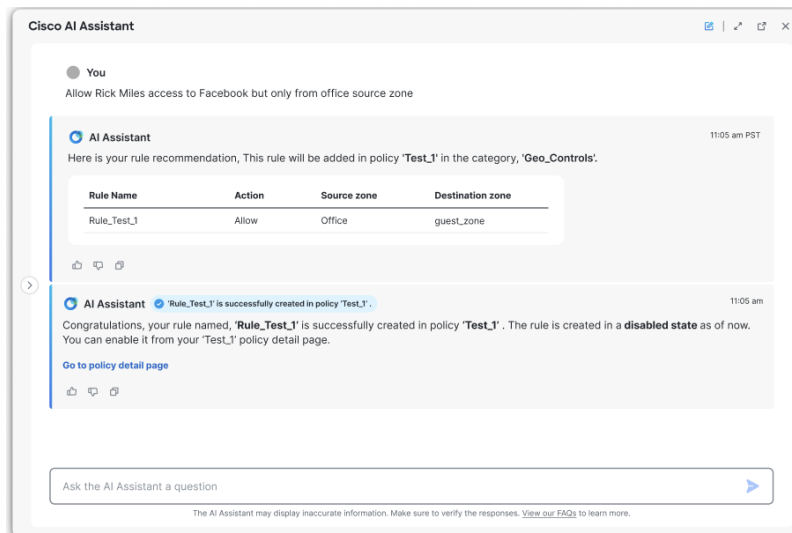
The AI Assistant requests confirmation for rule creation and provides a summary of the administrator's request along with the inputs for the rule:

**Note**

The administrator can edit the rule information by clicking **Edit** and cancel the process of rule creation by clicking **Cancel**.

Step 8

Assuming that the administrator confirms "Yes" for rule creation, the rule is created and will be reflected in the policy the administrator chose:

**Note**

If you are unable to create a policy rule, refer to [Cisco AI Assistant Frequently Asked Questions \(FAQ\)](#).

Contact Support

The AI Assistant streamlines the process of ticket creation and management, enabling administrators to handle support requests efficiently and effectively. With this integration, administrators can generate support cases

directly through the AI Assistant when they encounter unresolved issues or require additional assistance beyond the AI's recommendations.

Key capabilities include:

- **Automated Ticket Creation:** The AI Assistant automatically suggests creating a support ticket if its solutions don't resolve the issue. Administrators can also manually create tickets with a simple prompt.
- **Manage Tickets:** Administrators can track and update the status of their tickets to "Close" within the AI Assistant.

By incorporating ticket creation and management into the AI Assistant, organizations can reduce delays in troubleshooting, help create a support case with support teams, and enhance the overall efficiency of issue resolution.

Only customers using CDO and Cloud-delivered Firewall Management Center can contact support through the AI Assistant.

Open Support Case

The AI Assistant creates a support ticket based on the context of the conversation. This support case is created in the **Support Case Manager** and the ticket details are shared with the user.

By following the steps below, administrators can quickly and seamlessly create a support ticket through the AI Assistant.

1. Navigate to your tenant's dashboard and click on the AI Assistant icon located in the right top corner.
2. Initiate a conversation by typing your query/issue in the text box.
3. The AI Assistant will suggest troubleshooting steps or solutions based on the issue presented.
4. If the AI Assistant's recommended solutions do not resolve the issue or if further help is needed, the Assistant will prompt you to **Open a Case**.

You can also manually request the creation of a support case by typing "create a support case".

5. The AI Assistant will generate the case and provide you with a case details.




Note A confirmation email will be sent, including a case number for reference.

AI Assistant

 You

I am having issues with my firewall and need support

 AI Assistant

I'm sorry to hear that you're experiencing issues with your firewall. To address this effectively, I recommend opening a Technical Assistance Center (TAC) case. This will allow our support team to assist you in resolving the issue.

Would you like me to help you with creating a TAC case? Please provide a detailed problem description and a brief title for the case.

[Open a TAC Case](#)

 Your feedback helps us improve the AI Assistant.



Ask the AI Assistant a question

[View User Guide](#) to learn more.



Tip Sample Prompts:

- *I need to report an issue with my firewall.*
 - *Can you help me open a support ticket?*
 - *Please escalate this problem to your support team.*
 - *How do I file a complaint about this product?*
 - *I need to speak to someone about a malfunctioning firewall.*
 - *This product is giving me trouble, I need to open a case.*
-

Manage Support Case

Administrators can quickly view and update a support case through the AI Assistant. The status of a support ticket can be:

- **List cases:** The AI Assistant can list all the open and closed cases for the tenant.
- **Close:** Mark the support case as resolved once the issue has been addressed.
- **Retrieve:** Access the details of an existing support case for review or reference.

Support Case List

Administrators can easily access a comprehensive list of all previously created support cases within their tenant using the AI Assistant. By simply asking the assistant to retrieve past cases, they can view case numbers, statuses, descriptions, and other essential details for each case.

To retrieve cases:

1. Navigate to the AI Assistant, in the text box, ask the AI Assistant to **retrieve the list of support cases**.
2. Alternatively, you can retrieve the list of cases directly in the **Support Case Manager** section.



Tip Sample prompts:

- *I want to know my support case history.*
 - *How many support cases we have?*
-

Support Case Status

Administrators can check the status of their support case via the AI Assistant.

1. Navigate to the AI Assistant, in the text box, ask the AI Assistant to **retrieve the status of support cases**.
2. Alternatively, you can track the progress of the ticket directly in the **Support Case Manager** section.



Tip Sample prompts:

- *I want to know my support case status.*
 - *What is the status of my case?*
-

Support Case Close

Administrators can close their support cases via the AI Assistant.

To close a case:

1. Navigate to the AI Assistant, in the text box, ask the AI Assistant to close the case.
2. Alternatively, you can close the ticket directly in the **Support Case Manager** section.



Tip Sample prompts:

- *I want to close my case.*
 - *How do I close my ticket?*
-

Notifications Center

The Cisco AI Assistant's alert and notification system is designed to keep administrators informed of critical actions, updates, and changes within their security environment. By leveraging real-time alerts and scheduled notifications, users can manage security incidents and optimize policies proactively.

The alerts and notifications are accessed via the AI Assistant icon located in the top-right corner of your tenant dashboard. When new alerts or notifications are available, a number indicator will appear on the icon, displaying the total count of unread items.

Clicking the icon opens the **Notification Center**, where you can view a comprehensive list of all alerts and notifications. The list can be easily filtered by status, including **Read**, **Unread**, and by **Severity**, allowing you to prioritize critical actions and stay informed.

The default status of the notifications are unread. The administrators can mark the notifications as read and delete the notifications as required.

The notifications are triggered for:

- **Policy analyzer and optimizer:** The AI Assistant routinely scans policies within your tenant and provides recommendations for optimization. Once the scan results are available, the Assistant will notify the user through a system-generated notification, ensuring timely awareness and action.
- **Policy rule creation:** Upon initiating policy rule creation, the rule is initially set to "disabled" by default, requiring you to manually enable it. The AI Assistant will then notify you once the rule is successfully enabled.