Cisco AI Assistant User Guide

First Published: 2024-05-30

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CHAPTER 1

Getting Started with Cisco AI Assistant

Getting Started with Cisco AI Assistant

Overview

Firewall administrators often encounter challenges in managing firewall policies and accessing related documentation. The AI Assistant with Cisco Defense Orchestrator (CDO) and cloud-delivered Firewall Management Center streamlines these tasks, making it more efficient to manage firewall devices, policies, and reference documentation when needed.

Prerequisites

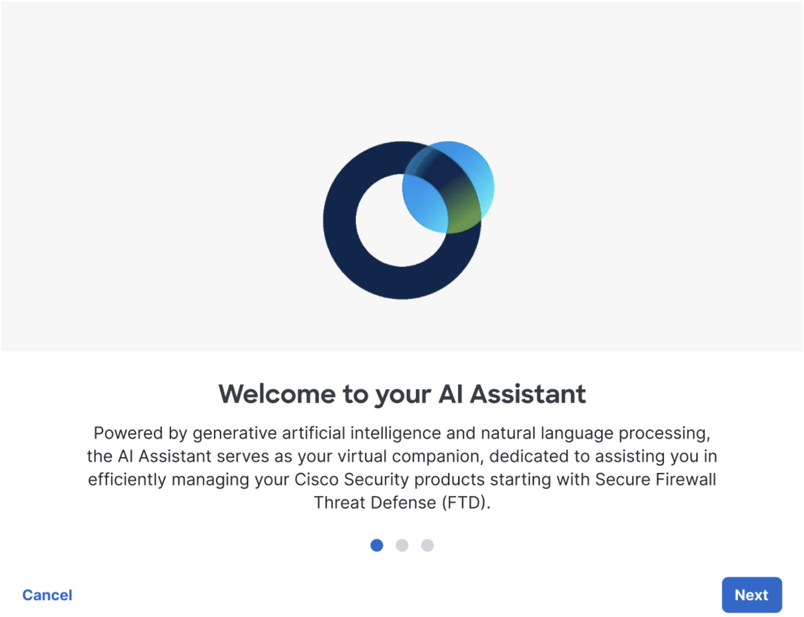
Administrators need to ensure they have met the following prerequisites to use the AI Assistant:

- User roles:
  - CDO and cloud-delivered Firewall Management Center- Super Administrators or Administrators.
  - On-Prem FMC - Global Domain Admin.

Upon successful login into your tenant, you will notice an AI Assistantwidget positioned in the top menu bar of the dashboard (●), click on the widget to launch the AI Assistant.

Onboarding First-Time User

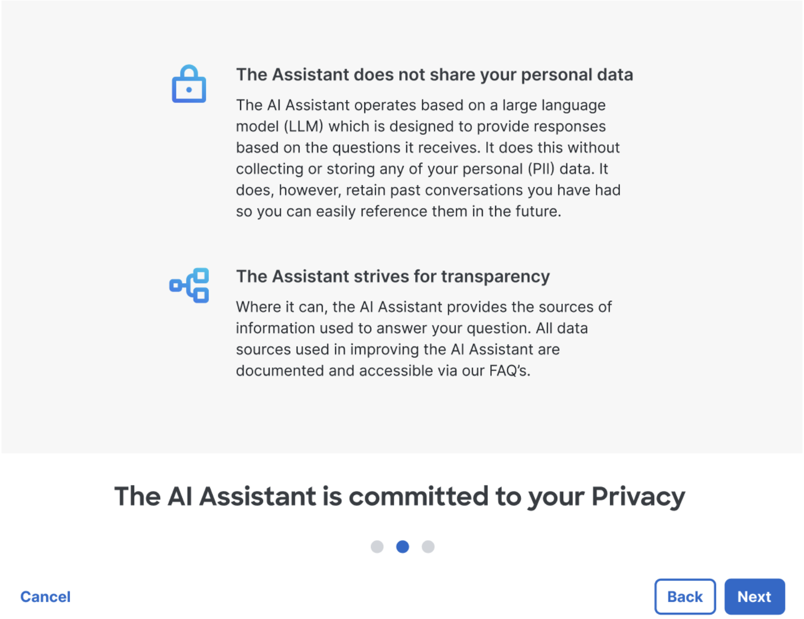
After opening the AI Assistant for the first time, a carousel window opens and you are introduced to the AI Assistant. You are presented with information on how the AI Assistant protects the privacy of your data, and a few tips on how to best use it.



Welcome to your AI Assistant

Powered by generative artificial intelligence and natural language processing, the AI Assistant serves as your virtual companion, dedicated to assisting you in efficiently managing your Cisco Security products starting with Secure Firewall Threat Defense (FTD).

In the carousel window, Click **Next** to the learn how the AI Assistant works with your data. We recommend that you read through this to understand how the AI Assistant treats your data and strives for transparency.



The Assistant does not share your personal data

The AI Assistant operates based on a large language model (LLM) which is designed to provide responses based on the questions it receives. It does this without collecting or storing any of your personal (PII) data. It does, however, retain past conversations you have had so you can easily reference them in the future.

The Assistant strives for transparency

Where it can, the AI Assistant provides the sources of information used to answer your question. All data sources used in improving the AI Assistant are documented and accessible via our FAQ's.

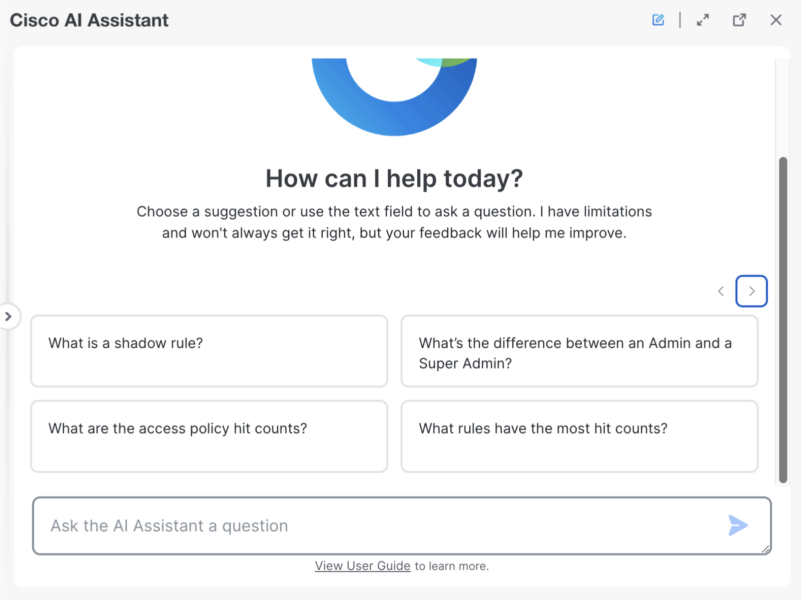
The AI Assistant is committed to your Privacy

At any point, if you click **Cancel** the AI Assistant carousel closes.

Note You will not be able to use the AI Assistant until you have navigated through all the screens in the carousel.

This and any other action you take with the AI Assistantis specific to your user account.

Your actions do not affect other authorized administrators of your tenant.


Cisco AI Assistant

How can I help today?

Choose a suggestion or use the text field to ask a question. I have limitations and won't always get it right, but your feedback will help me improve.

What is a shadow rule?

What's the difference between an Admin and a Super Admin?

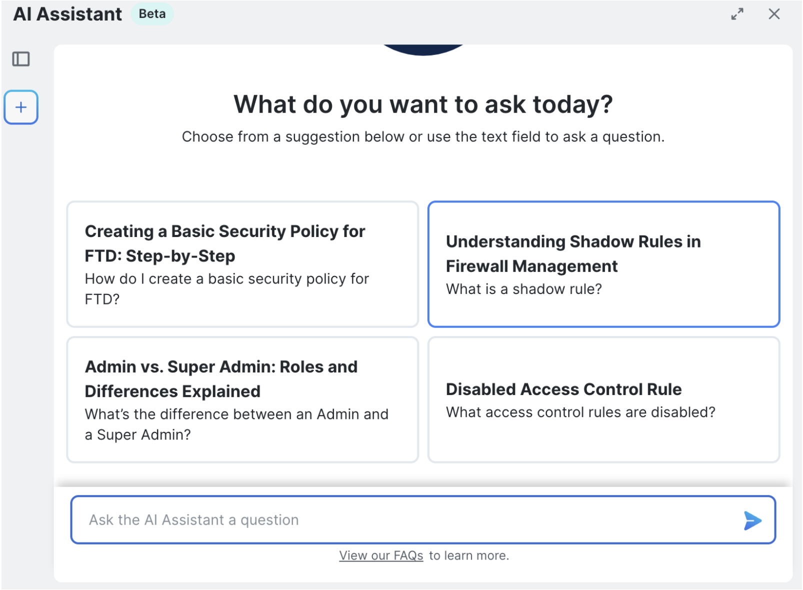
What are the access policy hit counts?

What rules have the most hit counts?

Ask the AI Assistant a question

View User Guide to learn more.

Clicking **Launch AI Assistant** opens the AI Assistant in a floating conversation window; You can select a response from one of our suggestion tiles or type in a question in the text box.


AI Assistant Beta

What do you want to ask today?

Choose from a suggestion below or use the text field to ask a question.

Creating a Basic Security Policy for FTD: Step-by-Step
How do I create a basic security policy for FTD?

Understanding Shadow Rules in Firewall Management
What is a shadow rule?

Admin vs. Super Admin: Roles and Differences Explained
What's the difference between an Admin and a Super Admin?

Disabled Access Control Rule
What access control rules are disabled?

Ask the AI Assistant a question

View our FAQs to learn more.

Note The AI Assistant comes pre-enabled on every tenant. If you prefer to disable the AI Assistant navigate go to the **Settings** page and switch off the AI Assistanttoggle to disable it.

Cisco AI Assistant Components

The Cisco AI Assistant is engineered with user-friendly components.

- **Text Input Box -**At the bottom of the window, you have a text input box that allows you to type and engage with the AI Assistant.
- **New Thread -** Click the "+" icon to start a new conversation with the AI Assistant
- **Chat History -** Expand the menu tray on the left side of the screen to see your chat history.
- **Feedback -** The AI Assistant has an option to provide feedback for its responses. Click thumbs up to show appreciation or thumbs down to let the assistant know that it can do better.
- **Expand View -**Click on the expand icon on the top right to open the AI Assistant in full screen view.

Cisco AI Assistant Best Practices

We recommend the following best practices to effectively communicate with the AI Assistant:

- Ask detailed questions - The AI Assistant is trained with policy/rule configuration and documentation data.. In order to receive a relevant response, we recommend that you provide the assistant with important details.

Tip Sample question- How many decryption policies are enabled on my account? Where can I access the policies? Do the policies have source and destination enabled?

- Divide the tasks into sub-tasks - For tasks that required multiple sets of instructions it can be beneficial to divide the tasks and input the sub-tasks after the previous task is answered.

Note The AI Assistant takes 24-hours to sync policy database, this results in a 24hr delay of the data provided in responses for policy inquiry. This does not impact any other features and users can continue to interact with the AI Assistant.

Tip In the sample question above - We suggest breaking down the question into smaller tasks and asking them one at a time, waiting for a response before moving on to the next question. This approach helps prevent information overload and reduces the need for repetition. -

- How many decryption policies are enabled on my account?
- Where can I access the policies?
- Do the policies have source and destination enabled?

- You cannot upload files or images to the AI Assistant.
- The AI Assistant currently provides support only in English language.

Note Please read through the Prompt Guide to gain a better understanding of the recommended best practices.

CHAPTER 2

Prompt Guide for Cisco AI Assistant

Prompt Guide for Cisco AI Assistant

The Cisco AI Assistant’s Prompt Guide is designed to help you interact more effectively with our AI Assistant, ensuring you get accurate, relevant, and helpful responses to your queries and commands. Your experience with Cisco AI Assistantcan be greatly enhanced by how effectively you communicate with it.

Understanding a Prompt

A prompt is a question or any text input that you provide to the Cisco AI Assistant to initiate a conversation or request information. Essentially, it's the question you pose to the AI Assistant. The way you format and construct your prompt plays a crucial role in determining the response from the AI Assistant.

Key Components of a prompt:

- **Clarity**: Be clear and specific about what you're asking for.
- **Context**: Provide necessary background information.
- **Purpose**: State what you want to achieve with your prompt.

Examples of Effective Prompts

General Prompt	Effective Prompt	What’s the difference?
What are the IP addresses and ports currently being blocked?	Can you provide me with the distinct IP addresses that are currently blocked by our firewall policies?	**General prompt** - Without indicating the need for "both" or "all" attributes explicitly, the assistant might provide default information on either IPs or ports, not both. **Effective prompt** - This prompt is clear and uses the keyword "distinct" to specify the need for unique values, which aligns with the AI Assistantcapabilities.

General Prompt	Effective Prompt	What's the difference?
Tell me the firewall rules, who set them, and all the changes made last month.	I need both the names and descriptions of all active firewall rules. Please include both attributes in the output.	**General prompt** - This is overloaded with requests and lacks clarity on whether all attributes are needed together, leading to potential confusion for the AI Assistant. **Effective prompt** - This clearly states the requirement for multiple attributes by using "both," ensuring the assistant understands to include all requested information.
What are the firewall rules for IP addresses X and Y, and how do I update them?	Show me a list of all firewall rules along with their corresponding actions for the past week.	**General prompt** - This combines questions about rules and updating procedures, which can lead to incomplete or inaccurate responses due to lack of context or specificity. **Effective prompt** - The is specific about the need for a list of rules and their actions, making it a straightforward request for the AI Assistant.
Give me everything but only the names.	Initial Question: What are the current firewall rules? Follow-Up Question: Can you also provide the actions associated with these rules?	**General prompt** - This is ambiguous and does not use the provided keywords in a manner that the AI Assistant can effectively interpret. **Effective prompt** - This approach helps maintain context and ensures each question is addressed accurately.
Tell me everything about the policies on my account.	I want to understand my Edge ACP access control policy, can you tell me more about it?	**General prompt** - This is too vague and lacks detail. The AI Assistant is unable to determine which specific policy the user is requesting information about. **Effective prompt** - This informs the AI Assistant the user needs details for Edge ACP access policy. The AI Assistant will respond with all the relevant details.

General Prompt	Effective Prompt	What's the difference?
Show me ports, protocols, and rule counts in Edge ACP policy, biggest to smallest.	In Edge ACP policy, what ports and protocols are configured in the rules? Include the counts of the number of rules using it and sort largest to smallest.	**General prompt** - This lacks specificity, combining multiple complex requests without clear instructions, and assuming the AI Assistant has implicit knowledge of how to aggregate and present the data. This leads to potential misunderstandings and responses that may not meet user expectations. **Effective prompt** - This approach helps maintain context and provides the assistant with clear instructions.

Guidelines for Crafting Effective Prompts

By providing precise input and context, you significantly increase the chances of receiving a targeted, relevant, and useful answer from the AI Assistant

- **Be Specific and provide context:** Draft your with relevant information, use the correct device names, policy names, etc. that could help the AI Assistantunderstand your request better.
- **Use Proper Syntax:** While AI Assistantcan understand colloquial language, clear and grammatically correct sentences can improve response accuracy.
- **Clarify the Desired Output:** If you have a preference for the response format (e.g., a list, a detailed explanation, tables), mention it.
- **Correction and Feedback:** If the response doesn't meet your expectations, you can provide feedback or ask for clarification within your next .
- **Direct Naming Requests:** Use the phrase "give me only the names" to instruct the AI Assistant to provide solely names in its response. For example, if a user wants to know the names of firewall rules or policy names without additional details, they can use the phrase 'give me only the names of firewall rules' to instruct the AI Assistant to provide solely the names in its response.
- **Unique Values:**Employ the keyword "unique" to request unique values from the AI Assistant.
- **Rules and Actions:** When requesting information about rules, users can specify which attributes they want to include in the response for comprehensive insights. For example, if a user wants to know about firewall rules allowing access to a specific zone, they can specify additional attributes such as the action (e.g., allow or deny) and any relevant source zones. By providing specific instructions, users can tailor the response to their exact requirements and gain deeper insights into the configuration. This approach allows users to obtain more relevant and actionable information from the AI Assistant.
- **Sequential Questioning:** For multiple inquiries, pose them as separate, follow-up questions to enhance clarity and context, rather than combining them into a single complex .
- **Explicit Multi-Attribute Queries:**Clearly state "Both" or "all of the following" when seeking multiple attributes; otherwise, the AI Assistant might select an attribute at random to respond to. For example, when querying about firewall rules, attributes could include details such as the rule name, description, action (e.g., allow or deny), source IP addresses, destination IP addresses, ports, protocols, etc.

In the context of multi-attribute queries, it means requesting information about multiple characteristics or properties simultaneously. For instance, a user might want to know both the names and descriptions of firewall rules, or they might be interested in the source IP addresses and destination ports of network traffic.

CHAPTER 3

Cisco AI Assistant Skills

Create Policy Rules

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 Prompt Guide for Cisco AI Assistant, 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.

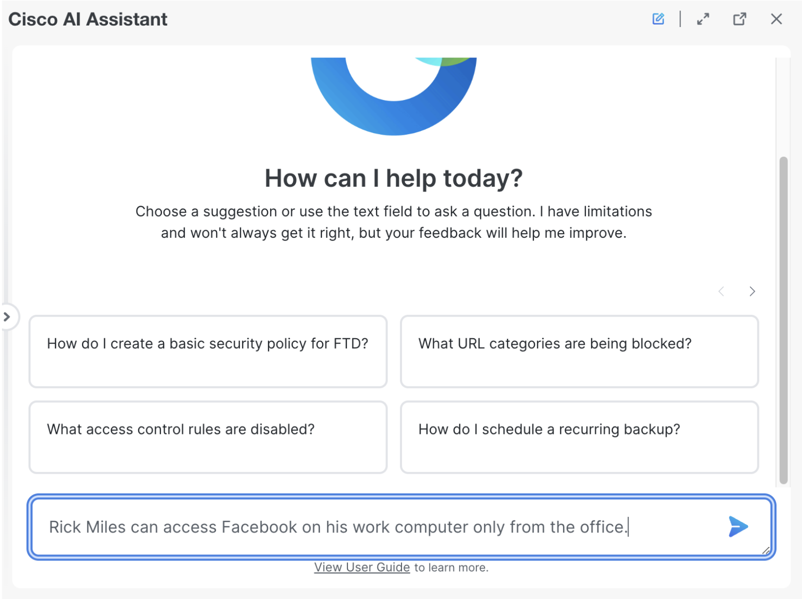
Example Scenario

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:

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



Cisco AI Assistant

How can I help today?

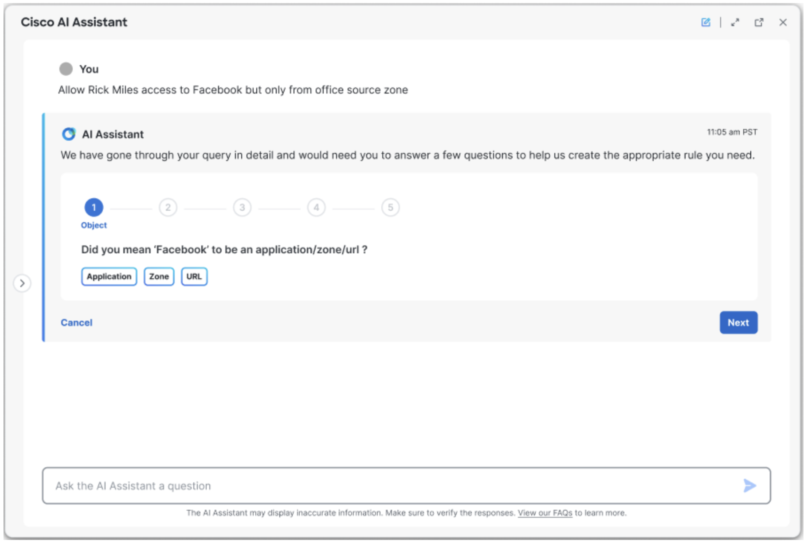
Choose a suggestion or use the text field to ask a question. I have limitations and won't always get it right, but your feedback will help me improve.

How do I create a basic security policy for FTD?
What URL categories are being blocked?
What access control rules are disabled?
How do I schedule a recurring backup?

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

View User Guide to learn more.

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:



Cisco AI Assistant

You

Allow Rick Miles access to Facebook but only from office source zone

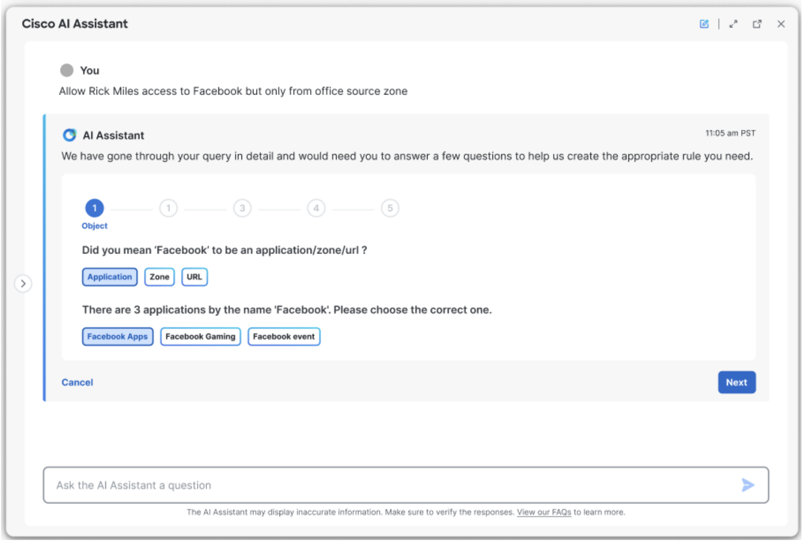
AI Assistant 11:05 am PST

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.

Did you mean 'Facebook' to be an application/zone/url ?

The AI Assistant may display inaccurate information. Make sure to verify the responses. View our FAQs to learn more.

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:



Cisco AI Assistant

You
Allow Rick Miles access to Facebook but only from office source zone

AI Assistant 11:05 am PST
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.

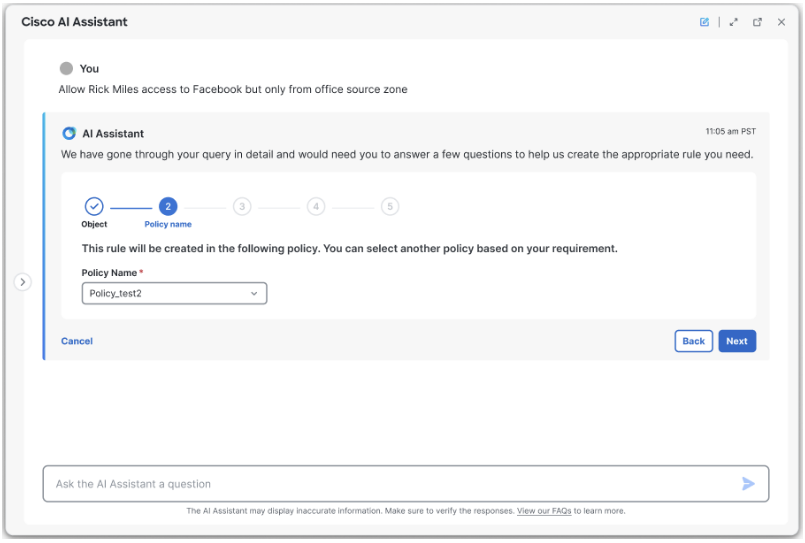
Did you mean 'Facebook' to be an application/zone/url ?

There are 3 applications by the name 'Facebook'. Please choose the correct one.

Ask the AI Assistant a question

The AI Assistant may display inaccurate information. Make sure to verify the responses. View our FAQs to learn more.

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



Cisco AI Assistant

You
Allow Rick Miles access to Facebook but only from office source zone

AI Assistant 11:05 am PST
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.

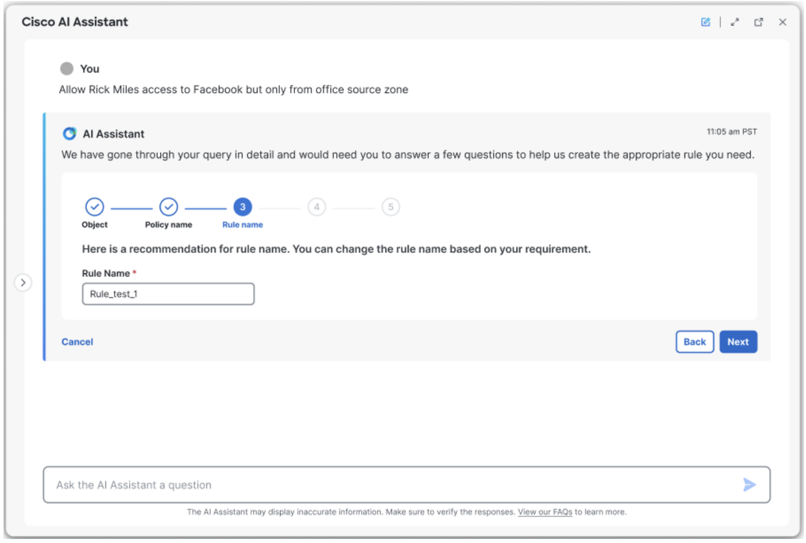
This rule will be created in the following policy. You can select another policy based on your requirement.

Policy Name * Policy_test2

Ask the AI Assistant a question

The AI Assistant may display inaccurate information. Make sure to verify the responses. View our FAQs to learn more.

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



Cisco AI Assistant

You

Allow Rick Miles access to Facebook but only from office source zone

AI Assistant 11:05 am PST

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.

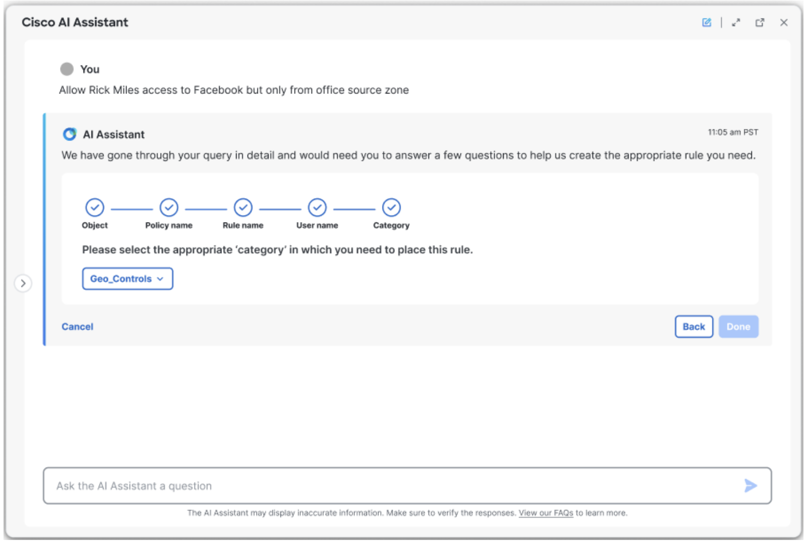
Here is a recommendation for rule name. You can change the rule name based on your requirement.

Rule Name *: Rule_test_1

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:



Cisco AI Assistant

You

Allow Rick Miles access to Facebook but only from office source zone

AI Assistant 11:05 am PST

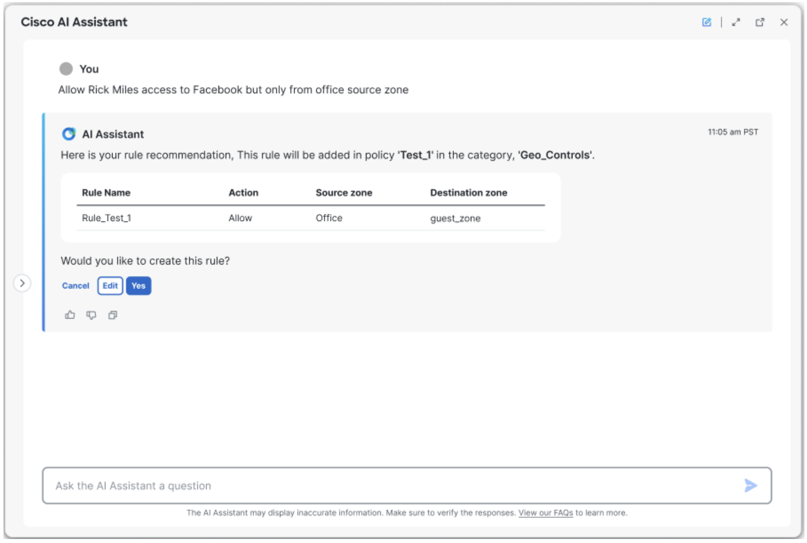
We have gone through your query in detail and would need you to answer a few questions to help us create the appropriate rule you need.

Please select the appropriate 'category' in which you need to place this rule.

Geo_Controls

The AI Assistant may display inaccurate information. Make sure to verify the responses. View our FAQs to learn more.

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:



Cisco AI Assistant

You

Allow Rick Miles access to Facebook but only from office source zone

AI Assistant 11:05 am PST

Here is your rule recommendation, This rule will be added in policy '**Test_1**' in the category, '**Geo_Controls**'.

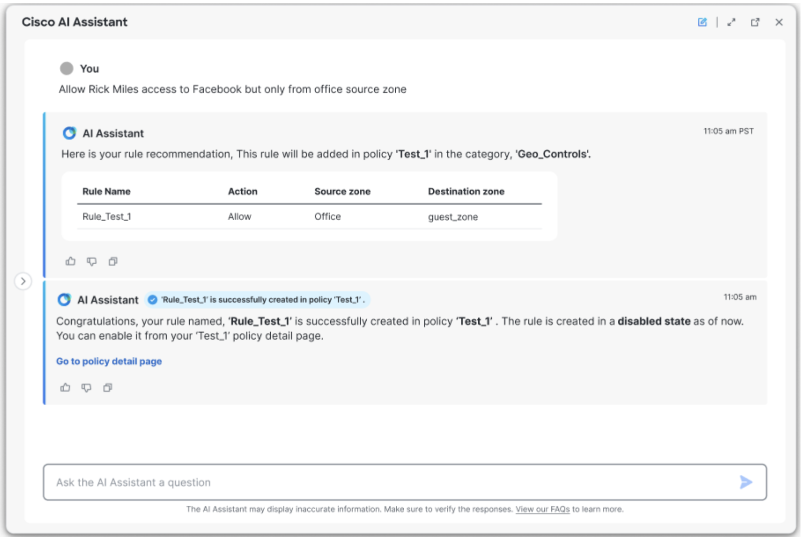
Rule Name	Action	Source zone	Destination zone
Rule_Test_1	Allow	Office	guest_zone

Would you like to create this rule?

The AI Assistant may display inaccurate information. Make sure to verify the responses. View our FAQs to learn more.

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:



Cisco AI Assistant

You

Allow Rick Miles access to Facebook but only from office source zone

AI Assistant 11:05 am PST

Here is your rule recommendation, This rule will be added in policy '**Test_1**' in the category, '**Geo_Controls**'.

Rule Name	Action	Source zone	Destination zone
Rule_Test_1	Allow	Office	guest_zone

AI Assistant 'Rule_Test_1' is successfully created in policy 'Test_1'. 11:05 am

Congratulations, your rule named, '**Rule_Test_1**' is successfully created in policy '**Test_1**' . The rule is created in a **disabled state** as of now. You can enable it from your 'Test_1' policy detail page.

Go to policy detail page

The AI Assistant may display inaccurate information. Make sure to verify the responses. View our FAQs to learn more.

Note If you are unable to create a policy rule, refer to Cisco AI Assistant Frequently Asked Questions (FAQ), on page 17.

CHAPTER 4

Cisco AI Assistant FAQ

Cisco AI Assistant Frequently Asked Questions (FAQ)

Q. What is the Cisco AI Assistant?

A. The Cisco AI Assistant is an application that answers questions about existing configurations on your Secure Firewall Threat Defense device and how to manage those devices in the cloud-delivered Firewall Management Center.

Q. What can the AI Assistant help you with?

A.

- The AI Assistant answers questions about how to configure your Secure Firewall Threat Defense devices and about how your access control and other security policies are configured.
- The AI Assistant helps diagnose and troubleshoot firewall-related issues by analyzing logs and configuration data.

- The AI Assistant simplifies the configuration for a quicker, easier rule building.

Q. How do you access the AI Assistant?

A. The AI Assistant is integrated with Cisco Defense Orchestrator and cloud-delivered Firewall Management Center. To access the AI Assistant click the AI Assistant button ( ) on the CDO or cloud-delivered Firewall Management Center home page.

Q. What do I do if a response is wrong?

A. Click the feedback option to report incorrect information.

Q. How do I ask the AI Assistant a question?

A. Click the AI Assistant button ( ) on Cisco Defense Orchestrator or cloud-delivered Firewall Management Center home page and type your question text box.

Q. What subjects can I ask about?

A. You can ask the AI Assistant about your configured firewall devices, policies, and settings; and ask questions about how to configure your firewall.

Q. What subjects can I ask about?

A. You can ask the AI Assistant about your configured firewall devices, policies, and settings; and ask questions about how to configure your firewall.

Q. Is the Cisco AI Assistant Secure?

A. Yes. The Cisco AI Assistant implemented on your CDO tenant only has access to the information and security policies on your tenant and your cloud-delivered Firewall Management Center, if you have implemented that feature. The AI Assistant cannot “learn” about policies on other CDO tenants and so, can’t answer questions about other CDO tenants or integrate information from them.

Q. What is Cisco's data privacy policy?

A. This is Cisco's Online Privacy Statement in the Cisco's Trust Center.

Q. Can I use the AI Assistant to create rules?

A. Yes, you can use the AI Assistant to create rules. The AI Assistant provides a user-friendly interface with simple prompts that guide you through the rule creation process. It ensures accuracy and efficiency, allowing you to seamlessly integrate and manage policy rules within your workflow.

Q. What types of rules are supported by the AI Assistant?

A. Currently, the AI Assistant supports the Access Control Policy Rules. You can create rule to `Allow`, `block` , `BLOCK_RESET`. Administrators can request specific details about Access Rule policies for their tenant.

Q. The AI Assistant is unable to create a rule, how do I fix this?

A. The AI Assistantis unable to create a policy rule:

- **Object not found:** If the AI Assistant cannot find the specified object name within the tenant, it will prompt the admin to verify the object name and try again. We recommend providing the assistant with an updated prompt that includes the correct object name.

- **Incomplete Request**: The AI Assistant requires complete and accurate information to create a rule. For a better understanding, please refer to the table below:

Object provided by the user	**Required Object** (***The user must provide at least one of these objects to give the AI Assistantbetter context for rule creation.***)
A. • Source Zone • Source Network • Source Dynamic Attribute	• Destination Zone • Destination Network • Destination Port • Destination Dynamic Attribute • Application • URL
User	• Destination Zone • Destination Network • Destination Port • Destination Dynamic Attribute • Application • URL
• Destination Zone • Destination Network • Destination Port • Destination Dynamic Attribute	• Source Zone • Source Network • Source Dynamic Attribute • User • Application • URL

Object provided by the user	**Required Object** (***The user must provide at least one of these objects to give the AI Assistantbetter context for rule creation.***)
• Application • URL	• Source Zone • Source Network • Source Dynamic Attribute • User • Destination Zone • Destination Network • Destination Port • Destination Dynamic Attribute

Q. Do I need to pay to use the Cisco AI Assistant for Firewall?

A. The Cisco AI Assistant is currently available for early customer evaluation at no cost. During this rollout phase, usage is free of charge. However, Cisco plans to include the product in the General Price List (GPL) in the future. After general availability, Cisco reserves the right to require customers to purchase a subscription to continue using the product.

Q. Are there any limitations on features and functionality during the above -mentioned initial customer evaluation period?

A. No, there are no planned limitations on the usage of available functionality. During the early availability period, you will have full access to all features and functionalities of the product. However, Cisco will monitor usage levels and may, at its sole discretion, restrict or limit usage, as well as add or remove features and functionalities during this evaluation phase.

Q. What happens if I choose not to subscribe and/or do not pay for the product after the above-mentioned period?

A. If you choose not to subscribe, your access to the Cisco AI Assistant for Firewall will be limited or discontinued in accordance with our policy. You will have the option to reactivate your subscription at any time.