Firewall Assistant User Guide

First Published: 2023-11-21

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

AI Assistant

Getting Started with 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

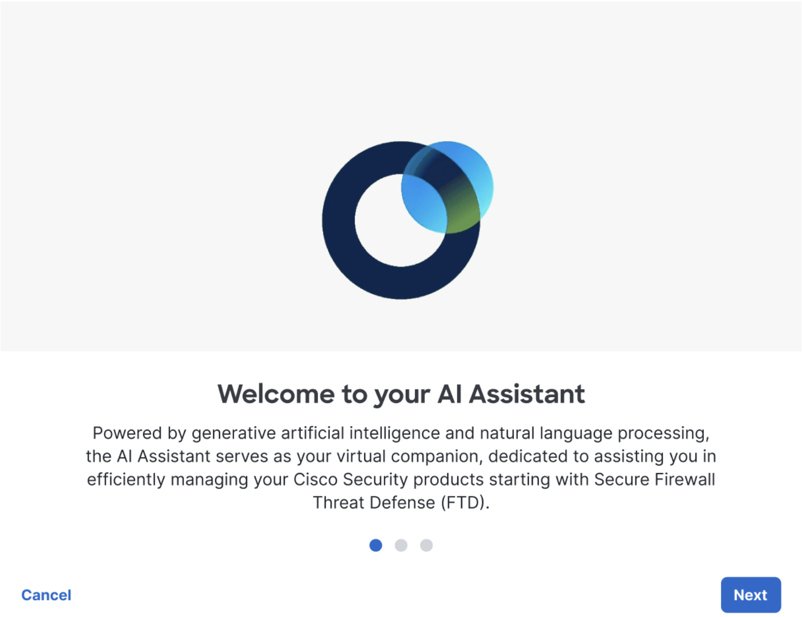
Administrators need to ensure they have met the following prerequisites to use the AI Assistant:

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

Upon successful login into your tenant, you will notice an AI Assistant button positioned in the top menu bar of the dashboard.

Onboarding First-Time User

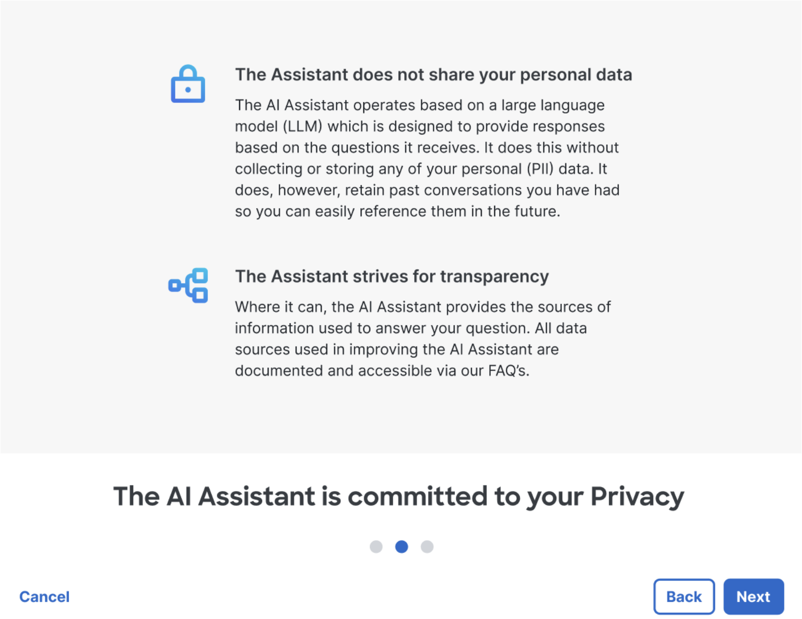
After clicking the AI Assistant button for the first time, you will be walked through an introduction to the AI Assistant, how Cisco protects the privacy of your data and finally a few tips on how to use the assistant to get the most out of it. The AI Assistant opens a carousel window of introductory and important information.



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 see how the AI Assistant works with your data. We recommend that you read through this to understand how the assistant is treating 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.

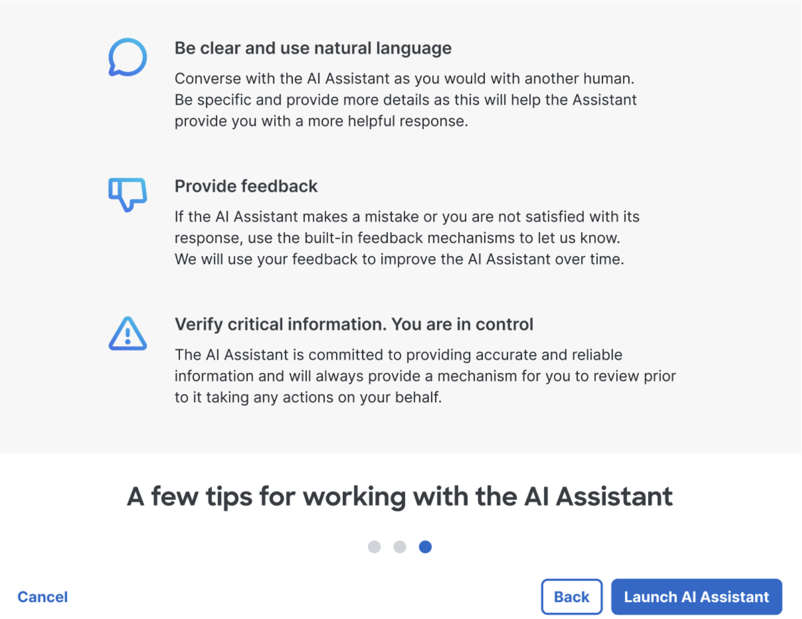
The Assistant strives for transparency

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

Click **Next** to see some helpful tips on how to get the most out of the AI Assistant.

At any point, if you click 'Cancel' the AI Assistant is not enabled for your use. Keep in mind that this and any other action you take with the AI Assistant is specific to your user account. Your actions do not enable or disable the assistant for other authorized administrators in your tenant.



Be clear and use natural language

Converse with the AI Assistant as you would with another human. Be specific and provide more details as this will help the Assistant provide you with a more helpful response.

Provide feedback

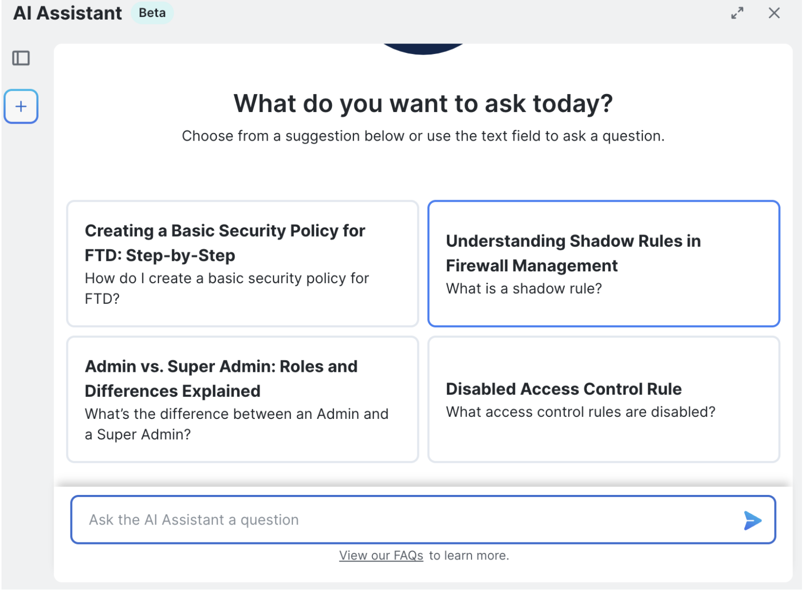
If the AI Assistant makes a mistake or you are not satisfied with its response, use the built-in feedback mechanisms to let us know. We will use your feedback to improve the AI Assistant over time.

Verify critical information. You are in control

The AI Assistant is committed to providing accurate and reliable information and will always provide a mechanism for you to review prior to it taking any actions on your behalf.

A few tips for working with the AI Assistant

Clicking Launch AI Assistant opens the 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.



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?

View our FAQs to learn more.

Cisco AI Assistant Components

The Cisco AI Assistant is thoughtfully engineered with user-friendly components that enable seamless interaction.

- **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 Chat -** Need a fresh start or have a new query? The AI Assistant provides the option to begin a new chat at any time. Click on the "+" icon on the left pane to initiate a new conversation.
- **Chat History -** The AI Assistant provides the option to access your chat history, you can see the list of your previous chats on the left pane. Select one of your previous chats to read through or continue the conversation.
- **Feedback -** Want to share your feedback? The Cisco AI Assistant has an option to provide feedback for its responses. you select 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.
- **Close -**Click on the close icon on the top right to close the AI Assistant.

Cisco AI Assistant Best Practices

We recommend the following best practices to provide you with the essential insights and guidelines for effectively communicating with the Cisco AI Assistant:

- Ask good questions - The Cisco AI Assistant is highly trained with a lot of data. In order to get a relevant response, we recommend that you provide important details to the assistant.

Note 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 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?

- The AI Assistant does not support uploading files or images.
- The AI Assistant currently provides support only in English language.

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 assists with the configuration of firewall rules, policies, and settings, ensuring that they align with best practices and security requirements.

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. Is the AI Assistant safe to use?

A. Yes, the AI Assistant is designed to be safe to use. We have implemented safety features and guidelines to ensure responsible and ethical usage.

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.

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 Assistant can 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.

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 Assistant understand your request better.
- **Use Proper Syntax:** While Cisco AI Assistant can 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.

Examples of Effective Prompts

Asking for distinct values:

What are the IP addresses and ports currently being blocked?

Without indicating the need for "both" or "all" attributes explicitly, the assistant might default to providing information on either IPs or ports, not both.

Can you provide me with the distinct IP addresses that are currently blocked by our firewall policies?

This is clear and uses the keyword "distinct" to specify the need for unique values, which aligns with the assistant's capabilities.

Requesting specific attributes by being explicit:

Tell me the firewall rules, who set them, and all the changes made last month.

This question is overloaded with requests and lacks clarity on whether all attributes are needed together, leading to potential confusion for the assistant.

I need both the names and descriptions of all active firewall rules. Please include both attributes in the output.

This question clearly states the requirement for multiple attributes by using "both," ensuring the assistant understands to include all requested information.

Asking for a list of rules along with actions:

What are the firewall rules for IP addresses X and Y, and how do I update them?

This question combines questions about rules and updating procedures, which can lead to incomplete or inaccurate responses due to lack of context or specificity.

Show me a list of all firewall rules along with their corresponding actions for the past week.

The question is specific about the need for a list of rules and their actions, making it a straightforward request for the assistant.

Breaking down multiple questions into smaller, follow-up questions:

Give me everything but only the names.

This query is contradictory and does not use the provided keywords in a manner that the assistant can effectively interpret.

Initial Question: What are the current firewall rules?

Follow-Up Question: Can you also provide the actions associated with these rules?

This approach helps maintain context and ensures each question is addressed accurately.

Access Control Policy:

Tell me everything about the policies on my account.

This question is too vague and lacks detail. The AI Assistant will be unable to determine which specific policy the user is requesting information about.

I want to understand my Edge ACP access control policy, can you tell me more about it?

This question informs the AI Assistant the user needs details for Edge ACP access policy. The AI Assistant will respond with all the relevant details.

Access Control Policy Rules:

Show me ports, protocols, and rule counts in Edge ACP policy, biggest to smallest.

This question lacks specificity, combining multiple complex requests without clear instructions, and assuming the AI has implicit knowledge of how to aggregate and present the data. This leads to potential misunderstandings and responses that may not meet user expectations.

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.

This question specifies the policy name and provides clear instructions to the AI Assistant to provide an accurate response.