Cisco AI Assistant User Guide

Onboard with Cisco AI Assistant

Overview

Firewall administrators often encounter challenges in managing firewall policies and accessing related documentation. The AI Assistant with Security Cloud Control, cloud-delivered Firewall Management Center and on-prem Firewall Management Center streamlines these tasks, making it more efficient to manage firewall devices, policies, and reference documentation when needed.

Prerequisites

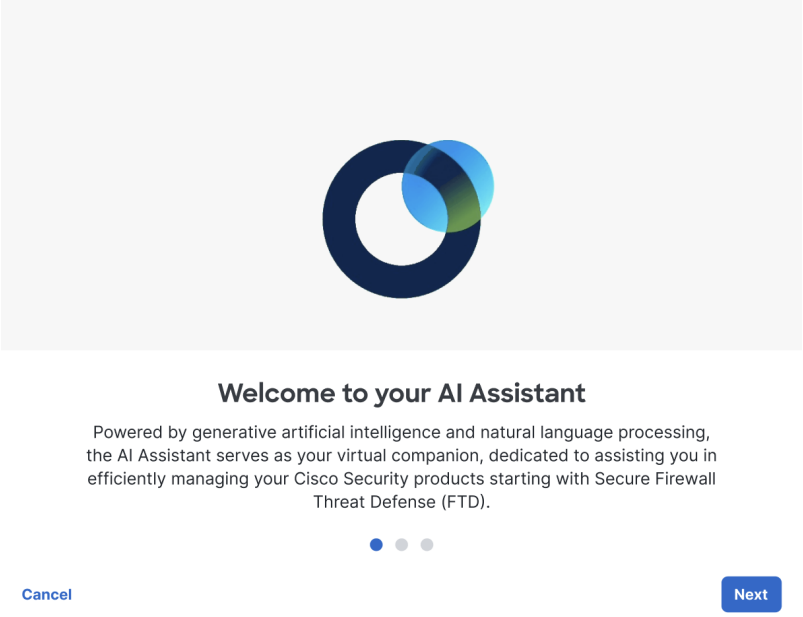
Administrators need to ensure they have met the following prerequisites to use the AI Assistant:

- User roles:
  - Security Cloud Control and cloud-delivered Firewall Management Center- Super Administrators or Administrators.
  - On-prem Firewall Management Center - Global Domain Admin.

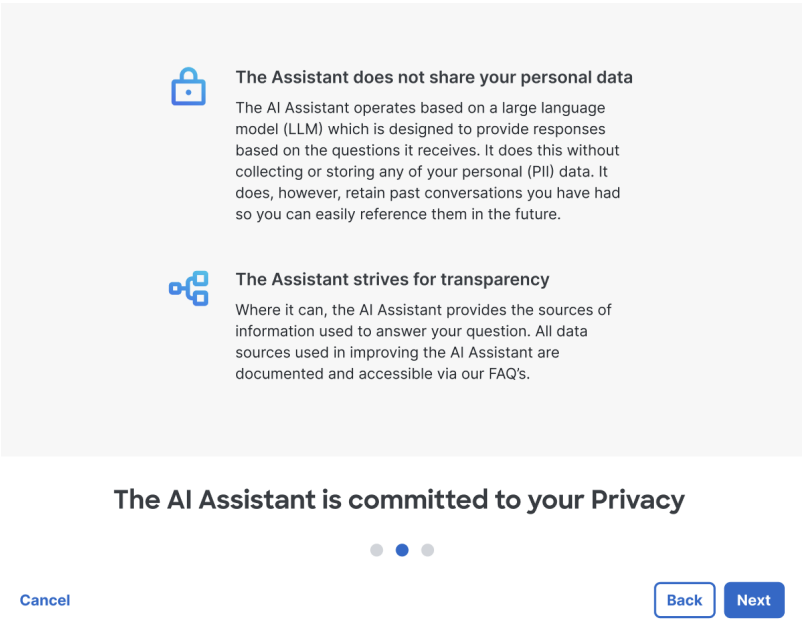
Upon successful login into your tenant, you will notice an AI Assistant widget positioned in the top menu bar of the dashboard ( ), click on the widget to launch the AI Assistant.

Onboarding First-Time User

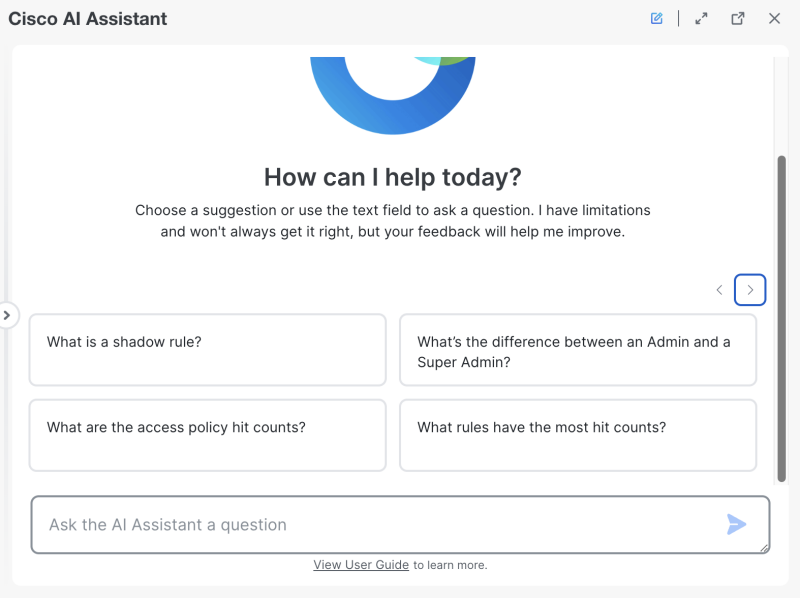
After opening the AI Assistant for the first time, a carousel window opens and you are introduced to the AI Assistant. You are presented with information on how the AI Assistant protects the privacy of your data, and a few tips on how to best use it.



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.



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

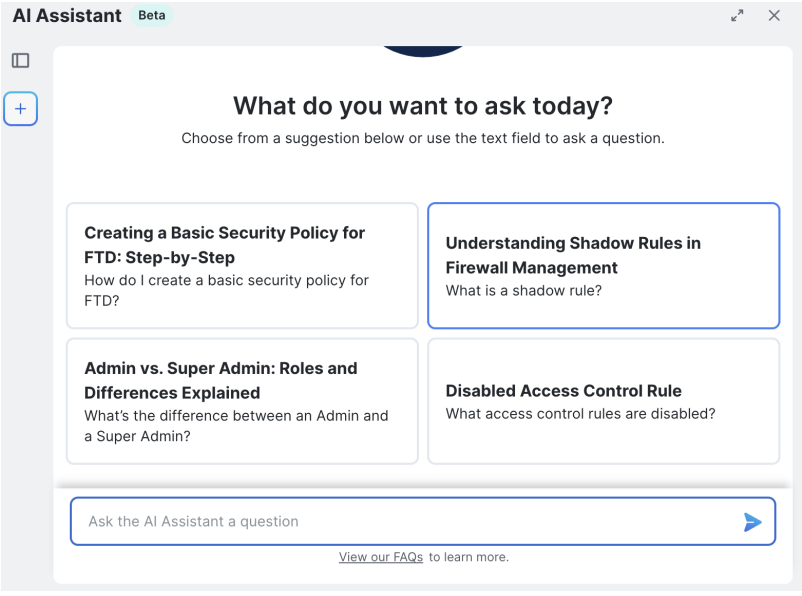


Note You will not be able to use the AI Assistant until you have navigated through all the screens in the carousel.

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

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

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.



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 Assistant toggle to disable it.

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.

Ask the Assistant: Sample prompts

- How to create an identity policy?
- How do I block social media sites in my access policy?
- What is the difference between block and block with reset actions in access control policy?
- What is the difference between trust and allow actions?
- How do I setup site to site vpn?
- What is a pre filter?
- Can you list all access control policies for my account?
- Can you tell me which policy on my account scans files for malware?
- Can you create a rule in Edge ACP Policy, Name: Block Youtube, Action: Block, Source network: Homebridge, Destination network: apde.amp.cisco.com, Application Youtube
- Show me optimizations for my policies including the Edge ACP policy.
- Are there any duplicate rules in my policies?

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.

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?*

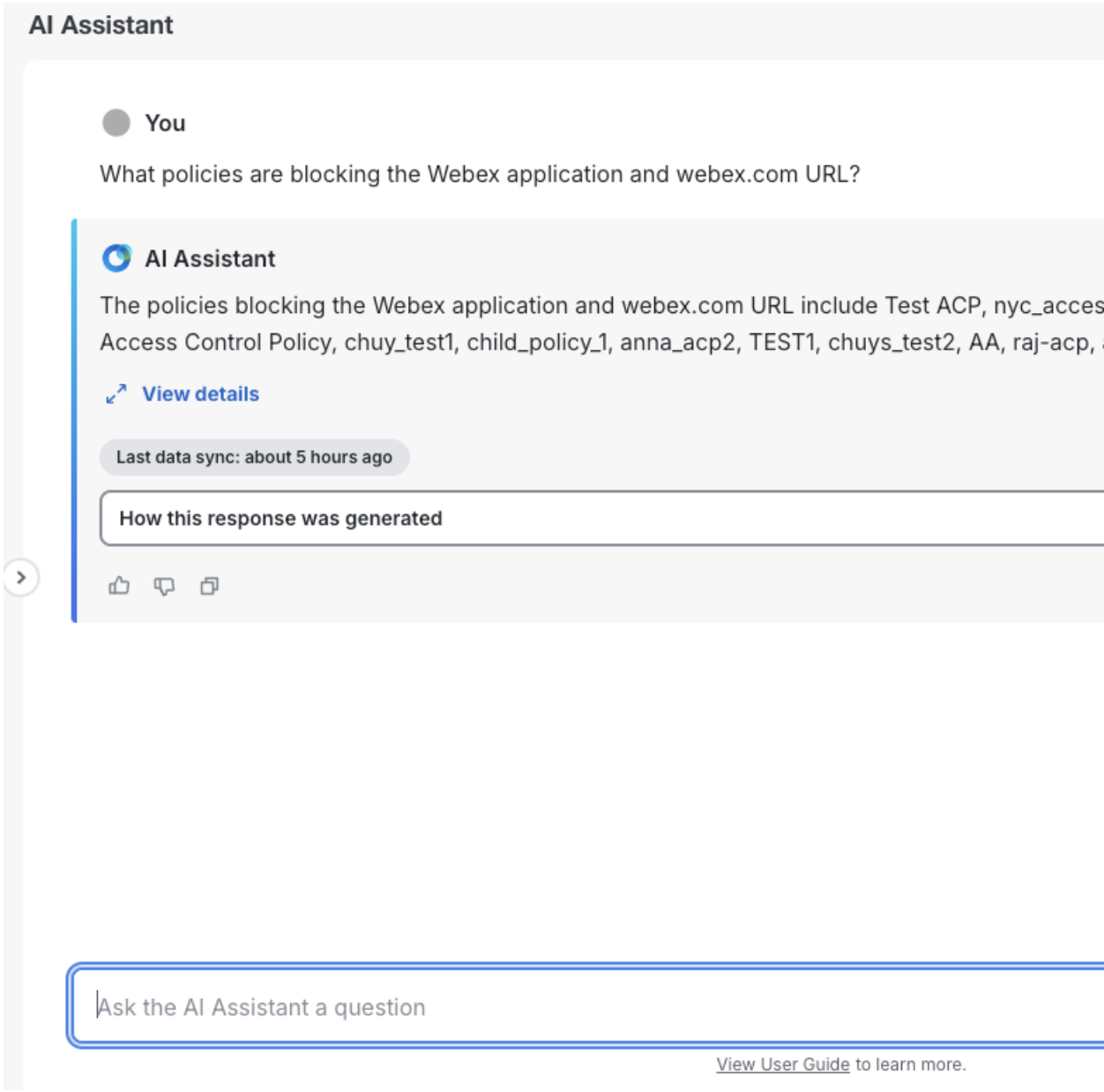
Policy Insights

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.

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., "*Show all access control rules*").	
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_acces
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*.

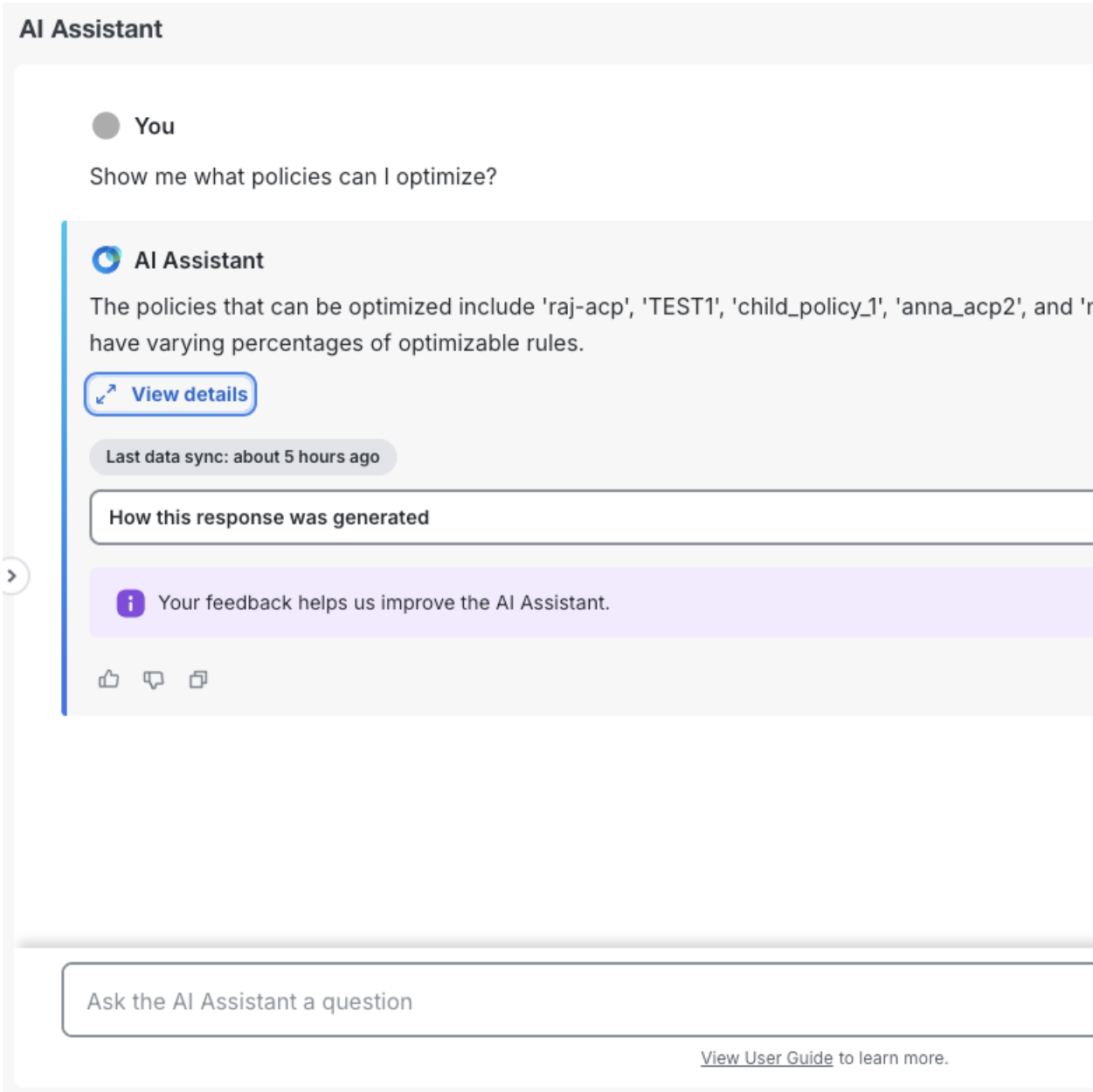
Policy Analyzer and Optimizer

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.



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

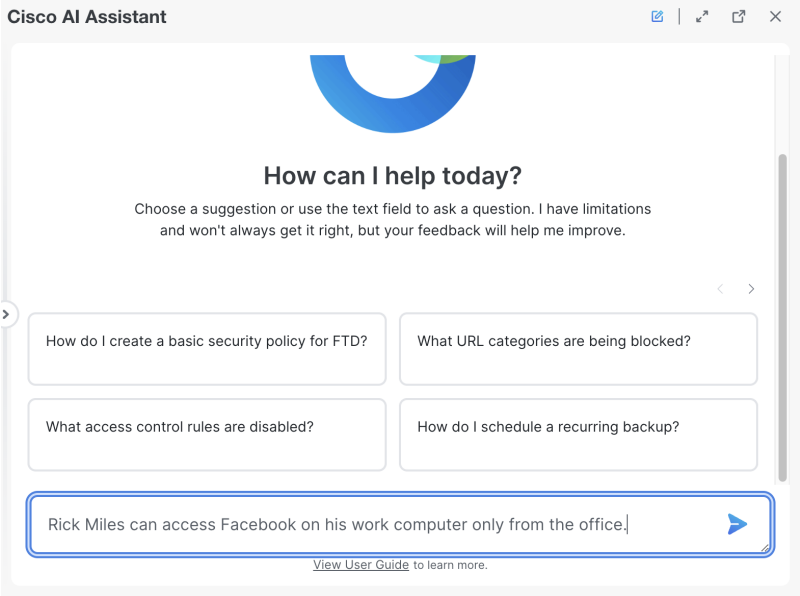
Consider a scenario where an administrator receives the following request:

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

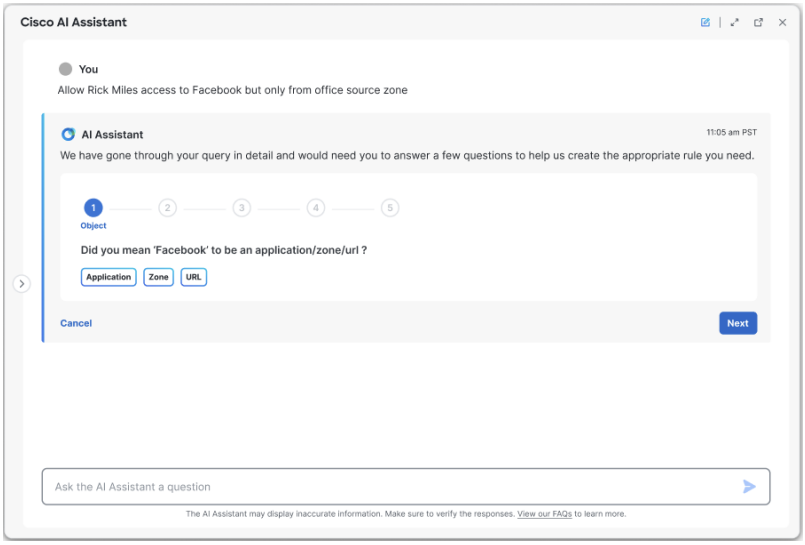
This would be the process the administrator would follow to create the rule:

Procedure

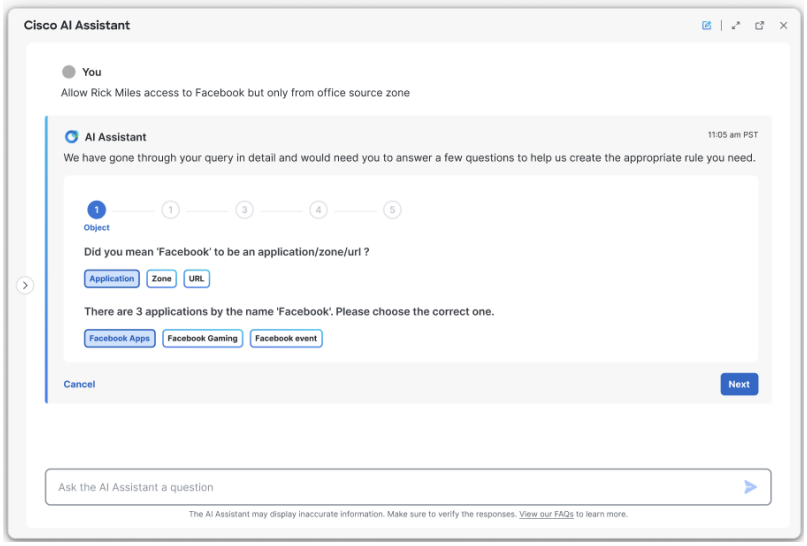
Step 1 The administrator needs to create a new rule to accommodate this request. They put this request to the AI Assistant:



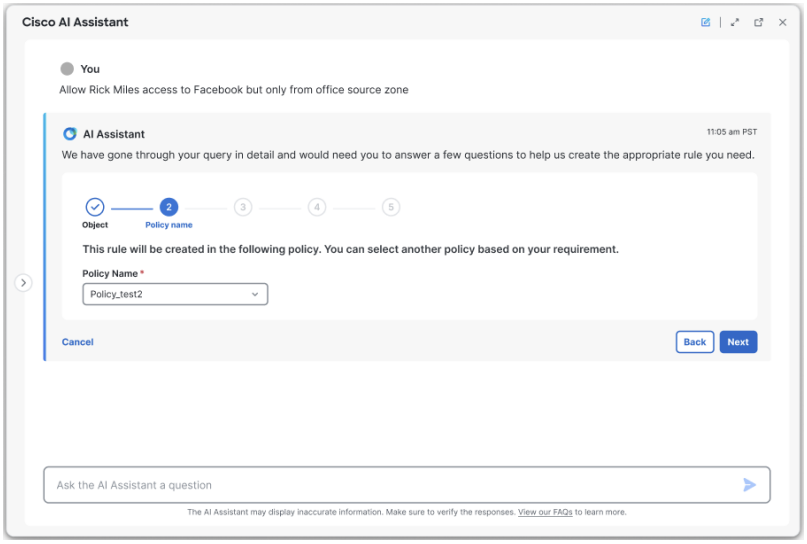
Step 2 The AI Assistant asks a question to better understand the administrator's requirement, and then guides them through a selection of options to create the rule:



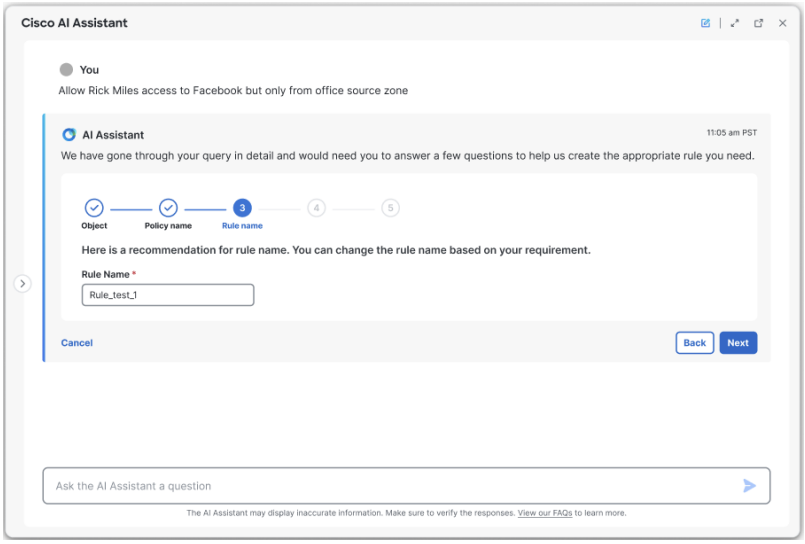
Step 3 The AI Assistant finds multiple results for Facebook, and asks the administrator to clarify if they are referring to Facebook as an application, URL or a Zone:



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

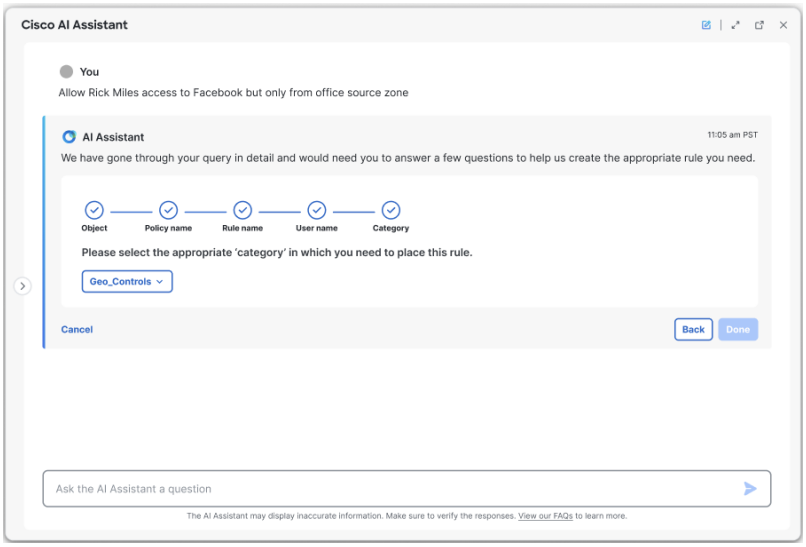


Step 5 The AI Assistant suggests a “Rule Name”, which the administrator can modify if needed:

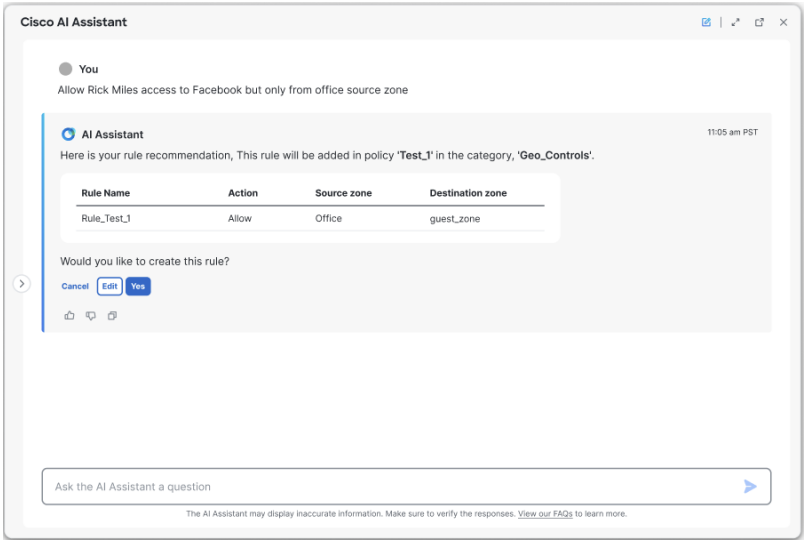


Note
If the administrator chooses a “Rule Name” that already exists in a policy, the assistant displays an error prompting the administrator to enter a new name.

Step 6 The AI Assistant prompts the administrator to select a “User name” and a “Category” for the rule:

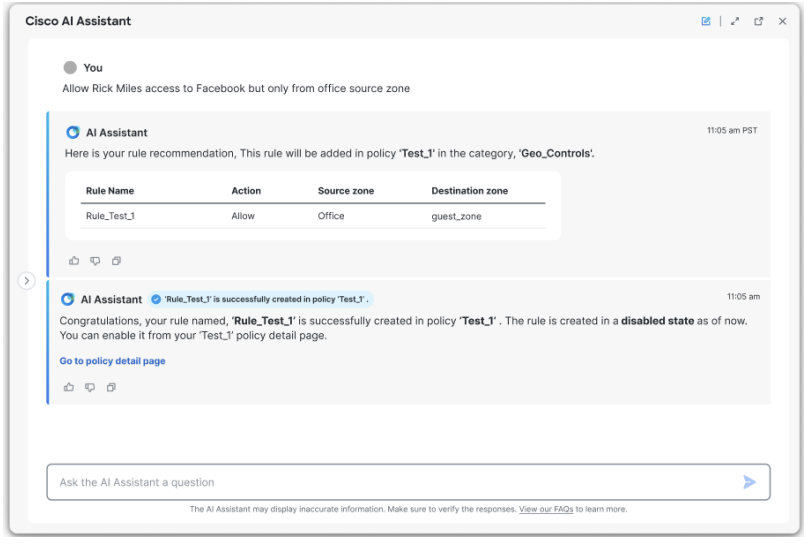


Step 7 The AI Assistant requests confirmation for rule creation and provides a summary of the administrator's request along with the inputs for the rule:



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), on page 21.

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 Security Cloud Control and Cloud-delivered Firewall Management Center can contact support through the AI Assistant.

Open Support Case

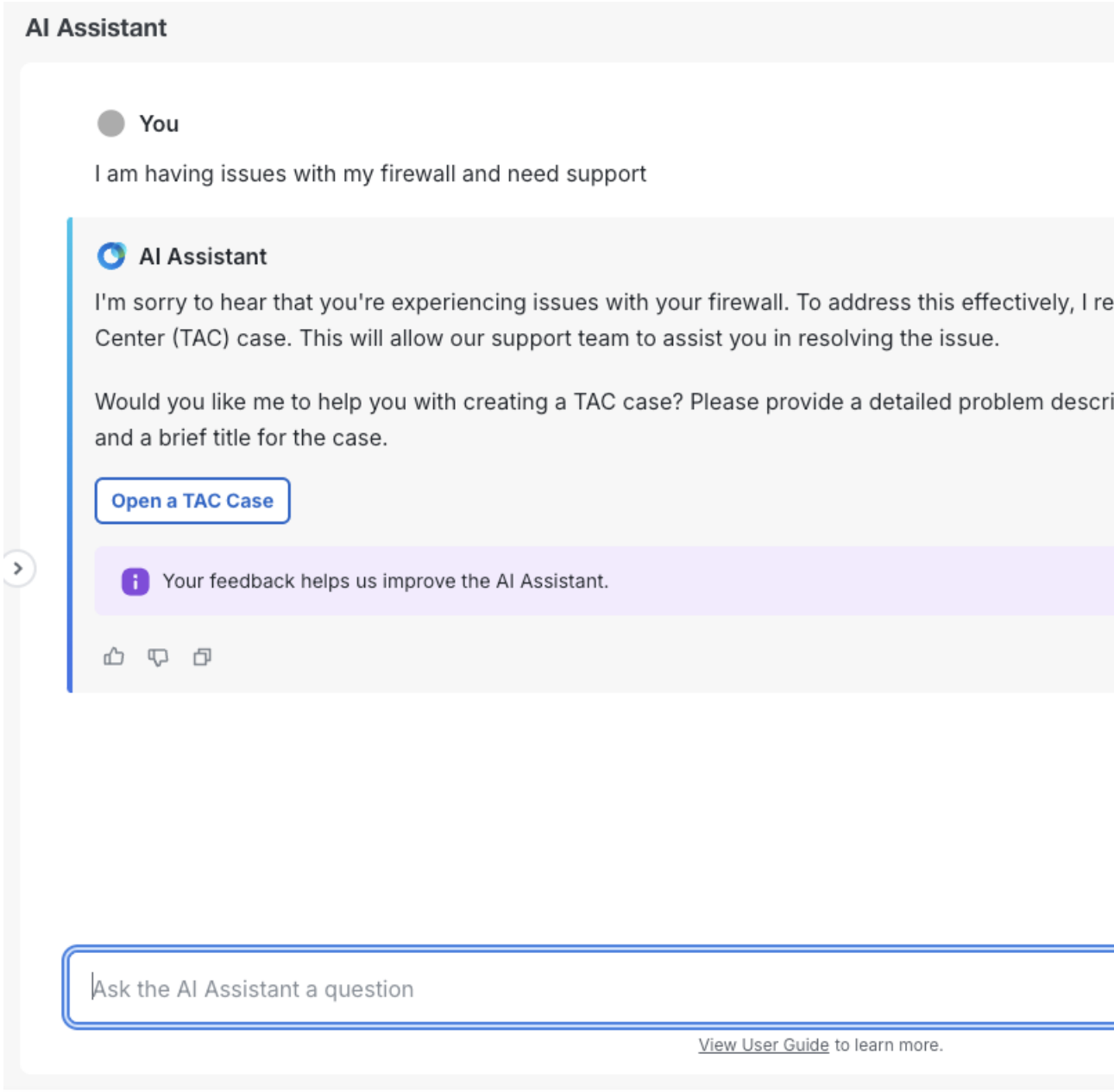
The AI Assistant creates a support ticket based on the context of the conversation. This support case is created in the **Support Case Manager** and the ticket details are shared with the user.

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 re
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 descri
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 thecase.
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.

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 Secure Firewall Management Center and 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.
- The AI Assistant answers questions about how to configure access control and other security policies.
- The AI Assistant simplifies the configuration for a quicker, easier policy rule building.
- The AI Assistant helps diagnose and troubleshoot firewall-related issues.

Q. How do you access the AI Assistant?

A. The AI Assistant is integrated with Security Cloud Control and Cloud-Delivered Firewall Management Center. To access the AI Assistant click the AI Assistant button () on the Security Cloud Control 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 Security Cloud Control 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. Is the Cisco AI Assistant Secure?

A. Yes. The Cisco AI Assistant implemented on your Security Cloud Control 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 Security Cloud Control tenants and so, can’t answer questions about other Security Cloud Control tenants or integrate information from them.

Q. What is Cisco's data privacy policy?

A.
- Access to customer data is strictly controlled based on role-based access control (RBAC) policies
- Only authorized personnel with specific privileges can access the data, and access is periodically reviewed.
- Audit logs track and record data access activities.

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

Q. Where is the data stored?

A. Data is stored within Cisco's Security Cloud infrastructure. Specific databases include Vector DB, Cockroach DB, and Databricks, all of which have industry-standard encryption at rest and in transit. Cisco AI solutions operate within private VPC environments to enhance security.

Q. How is our data being used?

A. Cisco does not use customer personally identifiable information (PII) to train AI models. Cisco AI solutions analyze usage data to improve product performance and threat detection. The Cisco Security Cloud utilizes data to provide threat intelligence and proactive security measures.

Q. What is Cisco doing with our data?

A. Cisco uses customer data within its security ecosystem to enhance threat intelligence and improve security posture. Cisco Talos threat research team analyzes data to identify and mitigate security threats. Customer logs and interactions help refine Cisco's AI assistant functionality.

Q. How is confidential information handled?

A. Data is classified according to Cisco’s organization-wide Data Classification taxonomy. Cisco follows country-specific data protection regulations and conducts periodic security, privacy, and supplier risk reviews. Data is encrypted at rest and in transit, ensuring protection against unauthorized access.

Q. Is our data being used to train Cisco’s AI models?

A. No, Cisco AI models are trained on public open-source and industry-standard data. Customer-specific data, including PII, is not used for AI training.

Q. If end-users input confidential data, will the AI Assistant stop it?

A. While the AI Assistant does not actively block confidential data input, Cisco employs security monitoring and controls to prevent unintended data exposure. Customers have control over AI features and can disable the AI Assistant if needed.

Q. What control do we have over our data?

A. Customers can configure AI functionality settings and request AI Assistant deactivation. Customers own their data and logs are managed as per Cisco’s data governance policies. Cisco follows a centralized Data Governance Framework to ensure proper data lifecycle management.

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 Assistant is 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.

Q. When was the last time the Cisco AI Assistant was updated?

A. The AI Assistant is updated weekly with documentation changes.

In Security Cloud Control, the AI Assistant is updated every 24 hours with the policy and configuration changes you made to your devices and tenant.

In cloud-delivered Firewall Management Center, the AI Assistant is also updated every 24 hours with the policy and configurations changes you made to your devices and tenant, and in addition, responses to those questions include when the last data sync occurred.