

AI Assistant auf FMC-Geräten konfigurieren und Fehlerbehebung dafür durchführen

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[AI-Assistent konfigurieren](#)

[Best Practices für die Verwendung des AI Assistant](#)

[Erstellung von Richtlinien automatisieren](#)

[Fehlerbehebung](#)

[Verbindungs- und Zugriffsprobleme](#)

[Automatisierte Ticketerstellung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie den AI Assistant auf Cisco Secure Firewall Management Center (FMC)-Geräten konfigurieren und Fehler bei diesen beheben.

Voraussetzungen

Ein gültiges Abonnement für die unterstützten Cisco Security-Produkte:

- Security Cloud Control (SCC)
- Firewall Management Center (FMC) vor Ort (v7.6 oder spätere Version)
- Das FMC benötigt ausgehenden Internetzugriff, um Cisco Cloud-Services zu erreichen.
- AI Assistant ist nur für FMC-Benutzer mit der Administratorrolle verfügbar.
- Wenn FMC im Hochverfügbarkeitsmodus ausgeführt wird, ist der AI Assistant auf dem Standby-Gerät nicht verfügbar.
- Das Firewall Management Center muss in die Cisco Security Cloud integriert sein.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Firewall Management Center
- Cisco Secure Firewall Threat Defense (FTD)

Verwendete Komponenten

Integration von Firewall Management Center in Cisco Security Cloud (Version 7.6)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

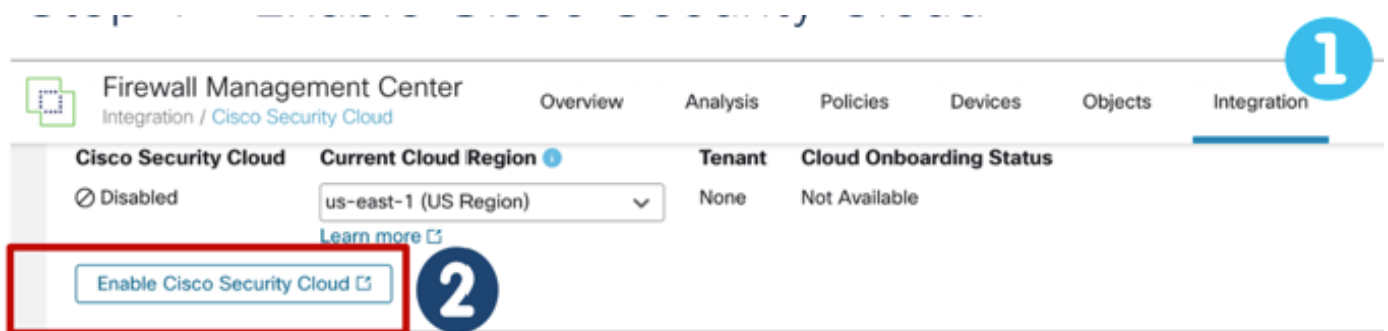
Hintergrundinformationen

Cisco AI Assistant innerhalb von FMC optimiert das Management der Netzwerksicherheit durch die Nutzung erweiterter KI zur Vereinfachung komplexer Aufgaben. Durch proaktive Einblicke, kontextbezogene Anleitungen und eine beschleunigte Fehlerbehebung unterstützt es Teams bei der Optimierung von Sicherheitsrichtlinien und der Reduzierung des betrieblichen Aufwands.

Mit diesem Tool können Administratoren schneller datengestützte Entscheidungen treffen und so den allgemeinen Sicherheitsstatus der Infrastruktur erheblich verbessern. Der auf Effizienz ausgelegte Cisco AI Assistant verändert das Management von Firewalls und bietet zuverlässigen Schutz vor neuen Bedrohungen. Gleichzeitig sorgt er für klare Transparenz und Kontrolle in Ihrer gesamten digitalen Umgebung.


AI-Assistent konfigurieren

Schritt 1: Sie müssen das Firewall Management Center in die Cisco Security Cloud integrieren. Sie können das FMC integrieren, indem Sie zu Integration > Cisco Security Cloud > Cisco Security Cloud aktivieren navigieren.



Schritt 2: Aktivieren Sie das Kontrollkästchen Enable Cisco AI Assistant for Security, und speichern Sie die Änderungen.

Cisco AI Assistant for Security

Powered by generative artificial intelligence and natural language processing, Cisco AI Assistant for Security is your virtual companion, assisting you in efficiently managing the Secure Firewall Threat Defense devices in your network. The AI Assistant helps you understand and create firewall policy rules and configurations, and generates custom guides to walk you through common administration tasks. [Learn more](#) 

Enable Cisco AI Assistant for Security

Schritt 3: Nach der Aktivierung wird ein neues Symbol in der Menüleiste des AI Assistant angezeigt.



Anmerkung: Der AI-Assistent benötigt für die Synchronisierung mit der Richtliniendatenbank 24 Stunden. Daher können Antworten auf politikbezogene Anfragen Daten widerspiegeln, die bis zu einem Tag alt sind. Dieser Synchronisierungsvorgang wirkt sich nicht auf andere Funktionen aus, und Sie können den AI Assistant ohne Unterbrechung weiterhin verwenden.

Schritt 4: Klicken Sie auf das Widget, um den KI-Assistenten zu starten. Beim ersten Zugriff auf den AI Assistant wird ein einleitendes Karussell angezeigt. In diesem Leitfaden wird erläutert, wie das System den Schutz Ihrer Daten gewährleistet. Darüber hinaus enthält er hilfreiche Tipps zur Optimierung der Umgebung.



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).



Cancel

Next

Klicken Sie im Einführungsdiagramm auf Weiter, um zu überprüfen, wie der AI Assistant Ihre Informationen verarbeitet.



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

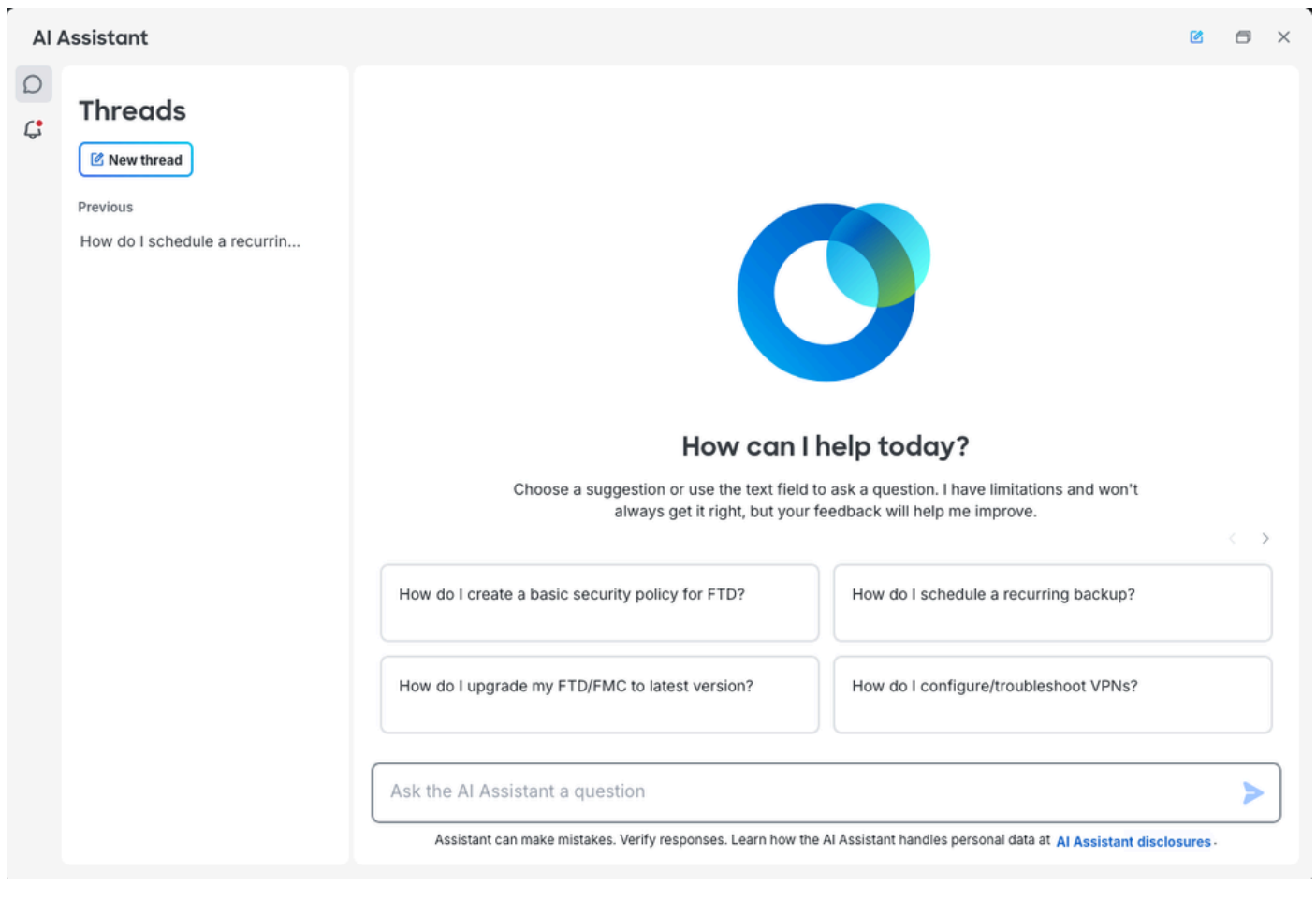


Cancel

Back

Next

Schritt 5: Klicken Sie auf AI Assistant starten, um den AI Assistant in einem Dialogfenster zu öffnen.



Anmerkung: Feedback: Der KI-Assistent hat die Möglichkeit, Feedback für seine Antworten abzugeben. Klicken Sie auf Daumen hoch, um die Wertschätzung anzuzeigen, oder auf Daumen runter, um dem Assistenten mitzuteilen, dass es besser gehen kann.

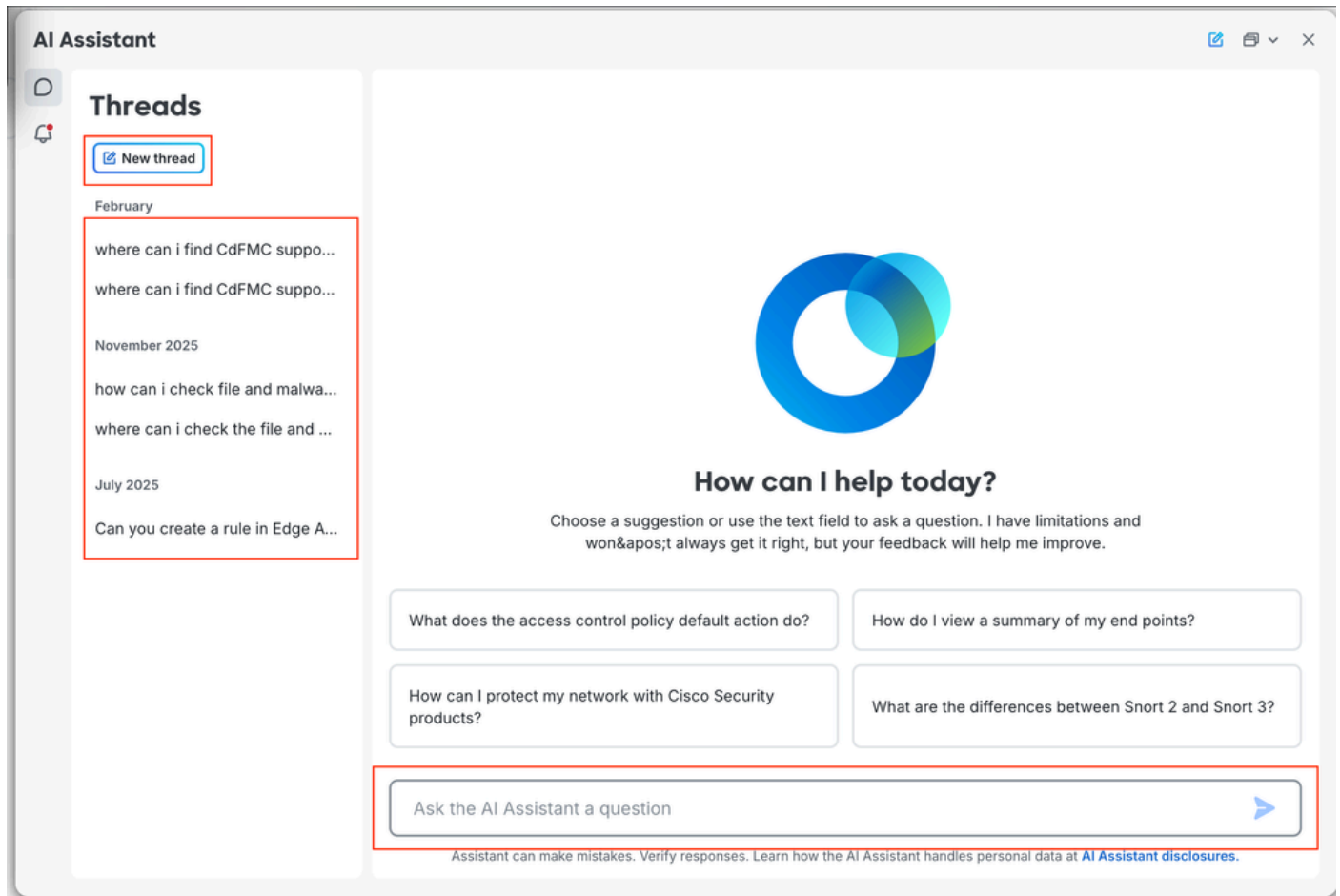
Best Practices für die Verwendung des AI Assistant

Der KI-Assistent ist ein leistungsstarkes Tool zur Optimierung des Richtlinienmanagements, Beschleunigung der Fehlerbehebung und Optimierung des allgemeinen Sicherheitsstatus. Berücksichtigen Sie die Best Practices, um sicherzustellen, dass Sie die genauesten und aussagekräftigsten Erkenntnisse erhalten:

- Seien Sie präzise: Vermeiden Sie zu umfangreiche Abfragen. Geben Sie spezifische Details zu den Objekten, Regeln oder Vorfällen an, die Sie derzeit untersuchen.
- Kontext bereitstellen: Geben Sie bei der Behebung von Verbindungsproblemen relevante Umgebungsdetails an, z. B. die betroffenen Geräte, Zonen oder Schnittstellen.
- Iterat für Tiefe: Wenn Ihre erste Antwort nicht vollständig auf Ihre Anforderungen eingeht, können Sie weitere Fragen verwenden, um die KI-Ausgabe zu optimieren.

Sobald Sie eine Anfrage einreichen, generiert der AI Assistant eine Antwort, die häufig Links zu relevanten Dokumentationen für weitere Lesungen enthält. Um eine neue Konversation zu starten, klicken Sie einfach auf die Schaltfläche Neuer Thread oder geben Sie Ihre nächste Frage in das Textfeld am unteren Bildschirmrand ein. Sie können den Verlauf Ihrer Interaktion jederzeit

überprüfen, indem Sie im Navigationsmenü links auf den Abschnitt Threads klicken.



Erstellung von Richtlinien automatisieren

Das Bild zeigt, wie der KI-Assistent die Richtlinienkonfiguration optimieren kann. Durch einfaches Angeben der gewünschten Parameter wie Richtlinienname, Quellnetzwerk und Anwendungsbenutzer wird die KI veranlasst, eine strukturierte Zusammenfassung der vorgeschlagenen Regel zu erstellen. Diese Schnittstelle bietet einen Administrator-Validierungsschritt, bei dem das System die Konfiguration in einer übersichtlichen Tabelle zur Überprüfung anzeigt. Schließlich bestätigt die KI die Aktion und sendet eine Statusbenachrichtigung, in der der Benutzer darüber informiert wird, dass die Regel im deaktivierten Zustand erstellt wurde. So wird sichergestellt, dass der Administrator die vollständige Kontrolle über die endgültige Bereitstellung der Richtlinie behält.

You

Can you create a rule in Default Access Control Policy, Name: Allow Youtube, Action: Allow, Source network: Test, Destination network: any, Application Youtube

AI Assistant Confirmation

07/18/2025

Here is your rule recommendation. This rule will be added in policy **Default Access Control Policy**.

Source Networks	Action	Policy Name	Rule Name	Applications	Destination Networks	Section
IPv4-Benchmark-Tests	ALLOW	Default Access Control Policy	Allow Youtube	YouTube	any-ipv4	DEFAULT

Congratulations, your rule named **Allow Youtube** is successfully created in policy **Default Access Control Policy**. The rule is created in a **disabled state** as of now. You can enable it from your policy detail page.

Fehlerbehebung

Wenn beim Zugriff auf oder bei der Verwendung des AI Assistant Probleme auftreten, gehen Sie wie folgt vor:

Verbindungs- und Zugriffsprobleme

- Überprüfung der Cloud-Verbindungen: Der AI Assistant benötigt eine stabile Verbindung zu den Cloud-Services von Cisco. Navigieren Sie zu Integration > Cisco Security Cloud, und stellen Sie sicher, dass der Status auf Enabled (Aktiviert) gesetzt ist und dass Port 8989 offen ist und nicht von Ihrer Firewall blockiert wird. Überprüfen Sie, ob die Cisco Security Cloud-Region/-Tenant korrekt ist.
- Proxy-Konfiguration: Wenn in Ihrer Umgebung ein Proxyserver verwendet wird, stellen Sie sicher, dass das FMC korrekt konfiguriert ist, um den Datenverkehr durch den Proxyserver zu leiten.
- Symbol fehlt: Wenn das Symbol für den KI-Assistenten nicht angezeigt wird, stellen Sie sicher, dass das FMC erfolgreich in SSC integriert wurde und der Port 8989 geöffnet ist und nicht von Ihrer Firewall blockiert wird.
- "Etwas ist schief gelaufen" Fehler: Dies deutet in der Regel auf ein Verbindungsproblem zwischen FMC und SSC hin. Vergewissern Sie sich, dass der Onboarding-Prozess erfolgreich abgeschlossen wurde und Port 8989 geöffnet ist und nicht von Ihrer Firewall blockiert wird.
- Veraltete Informationen: Die Synchronisierung mit der aktuellen Richtliniendatenbank kann bis zu 24 Stunden dauern. Wenn Sie vor Kurzem wichtige Konfigurationsänderungen vorgenommen haben, warten Sie diese Synchronisierungsperiode ab, bevor Sie erwarten, dass der Assistent diese Updates berücksichtigt.
- Fehler in SCC (HA-Umgebungen): Wenn Ihr FMC Teil eines HA-Paars ist, kann ein Failover von Standby zu Active die Cloud-Verbindung unterbrechen. In diesem Szenario müssen Sie die Cloud-Integration auf dem neu aktiven Gerät deaktivieren und erneut aktivieren, um die Funktionalität wiederherzustellen.

Sammeln Sie zur weiteren Fehlerbehebung Browser-Konsolenprotokolle, um mögliche Fehler zu identifizieren:

So greifen Sie auf die Entwicklertools zu:

- Chrom, Rand: Drücken Sie F12 oder Strg+Umschalt+I (Befehlstaste+Wahltaste+I unter MacOS).
- Firefox: Drücken Sie F12 oder Strg+Umschalt+K (Befehlstaste+Wahltaste+K unter MacOS).

Aktualisieren Sie die Seite, sobald die Konsole geöffnet ist. Alle Fehler werden in rotem Text angezeigt. Klicken Sie mit der rechten Maustaste auf den Konsolenbereich, um das Protokoll als Datei zu speichern, wenn Sie es zur weiteren Untersuchung freigeben möchten.

Automatisierte Ticketerstellung

Der AI Assistant optimiert den Support-Prozess, indem er ein Ticket empfiehlt, wenn die automatisierten Lösungen nicht ausreichen. Administratoren können zudem jederzeit eine manuelle Support-Anfrage einleiten.

Sobald ein Ticket im Support Case Manager erstellt wurde, stellt Ihnen der Assistent alle relevanten Details für die Nachverfolgung und das Ticketmanagement zur Verfügung.

Gehen Sie folgendermaßen vor, um Ihre Support-Anfragen schnell und effizient zu verwalten:

- Start: Öffnen Sie den KI-Assistenten, indem Sie auf das Symbol in der rechten oberen Ecke Ihres Dashboards klicken.
- Abfrage: Geben Sie Ihre technische Frage oder Ihr Problem in das Chat-Feld ein, um die Sitzung zu beginnen.
- Analyse: Überprüfen Sie die Schritte oder Lösungen zur Fehlerbehebung, die vom Assistenten bereitgestellt werden.
- Eskalieren: Wenn das Problem mit den automatisierten Vorschlägen nicht behoben werden kann, öffnen Sie ein Ticket beim TAC.
- Manueller Trigger: Sie können eine Supportanfrage jederzeit manuell starten, indem Sie die folgende Eingabeaufforderung eingeben: Ticket beim TAC erstellen

You

open a case with TAC

AI

AI Assistant

11:49 am

I can certainly help you open a TAC case. Could you please provide the following information?

1. A detailed description of the problem you are facing.
2. A brief title for the TAC case.
3. The device name, serial number, or IP address that the case is related to.

👍 🗨️ 📄

Zugehörige Informationen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.