

# FMCデバイスでのAI Assistantの設定およびトラブルシューティング

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[バックグラウンド情報](#)

[AI Assistantの設定](#)

[AI Assistantの使用に関するベストプラクティス](#)

[ポリシールール作成の自動化](#)

[トラブルシューティング](#)

[接続とアクセスの問題](#)

[自動チケット作成](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、Cisco Secure Firewall Management Center(FMC)デバイスでAI Assistantを設定およびトラブルシューティングする方法について説明します。

## 前提条件

サポートされているシスコセキュリティ製品の有効なサブスクリプション：

- セキュリティクラウド制御(SCC)
- オンプレミスのファイアウォール管理センター(FMC) ( v7.6以降 )
- FMCでは、シスコクラウドサービスに到達するためにアウトバウンドインターネットアクセスが必要です
- AI Assistantは、管理者ロールを持つFMCユーザだけが使用できます
- ハイアベイラビリティモードでFMCを実行している場合、スタンバイユニットではAI Assistantを使用できません
- Firewall Management CenterをCisco Security Cloudと統合する必要がある

## 要件

次の項目に関する知識があることが推奨されます。

- Cisco Secureファイアウォール管理センター
- Cisco Secure Firewall Threat Defense(FTD)

## 使用するコンポーネント

バージョン7.6でCisco Security Cloudと統合されたFirewall Management Center。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

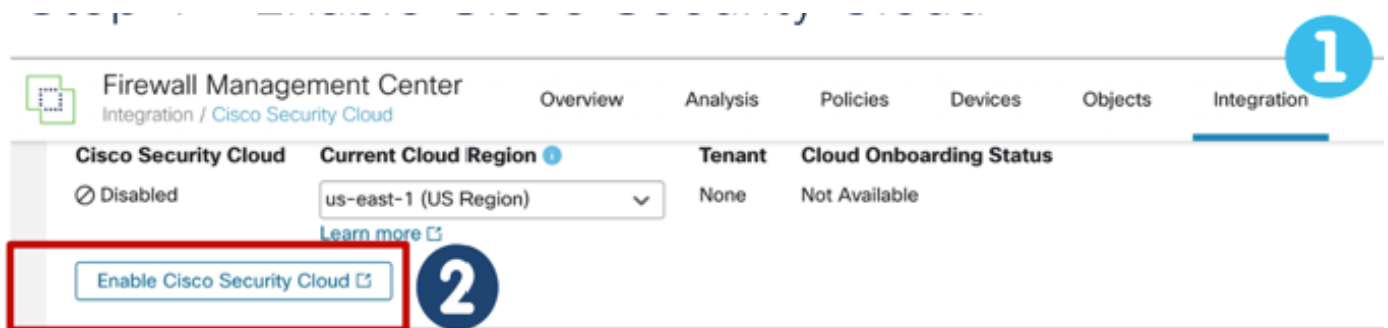
## バックグラウンド情報

FMC内のCisco AI Assistantは、高度なAIを活用して複雑なタスクを簡素化することで、ネットワークセキュリティ管理を合理化します。予防的な洞察、コンテキストに基づくガイダンス、迅速なトラブルシューティングを提供することで、チームはセキュリティポリシーを最適化し、運用オーバーヘッドを削減できます。

このツールにより、管理者はデータに基づく意思決定を迅速に行うことができるようになり、インフラストラクチャの全体的なセキュリティ体制が大幅に強化されます。効率性を重視して設計されたCisco AI Assistantは、ファイアウォールの管理方法を変革し、変化する脅威に対する堅牢な保護を確保すると同時に、デジタル環境全体で明確な可視性と制御を維持します。


## AI Assistantの設定

ステップ 1 : Firewall Management CenterとCisco Security Cloudを統合する必要があります。FMCを統合するには、Integration > Cisco Security Cloud > Enable Cisco Security Cloudの順に選択します。



ステップ 2 Enable Cisco AI Assistant for Securityボックスにチェックマークを入れて、変更を保存します。

## 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

ステップ 3 有効にすると、AI Assistantのメニューバーに新しいアイコンが表示されます。



注:AI Assistantをポリシーデータベースと同期させるには24時間かかります。その結果、ポリシー関連の問い合わせに対する回答には、最長で1日前のデータが反映されます。この同期プロセスは他の機能には影響を与えません。中断することなくAI Assistantを引き続き使用できます。

ステップ 4 ウィジェットをクリックしてAI Assistantを起動します。AI Assistantに初めてアクセスすると、最初のカルーセルが表示されます。このガイドでは、システムがデータプライバシーを維持する方法について説明し、エクスペリエンスを最適化するためのヒントを提供します。



### Welcome to your AI Assistant

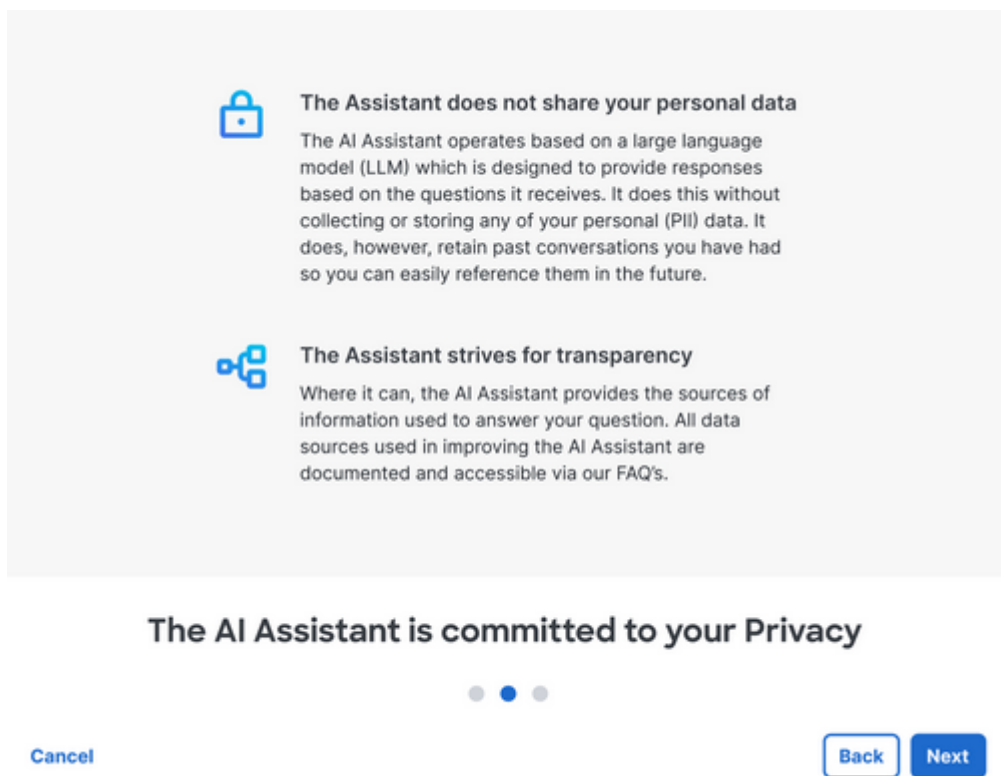
Powered by generative artificial intelligence and natural language processing, the AI Assistant serves as your virtual companion, dedicated to assisting you in efficiently managing your Cisco Security products starting with Secure Firewall Threat Defense (FTD).



Cancel

Next

最初のカルーセルでNextをクリックして、AI Assistantによる情報の処理方法を確認します。



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.

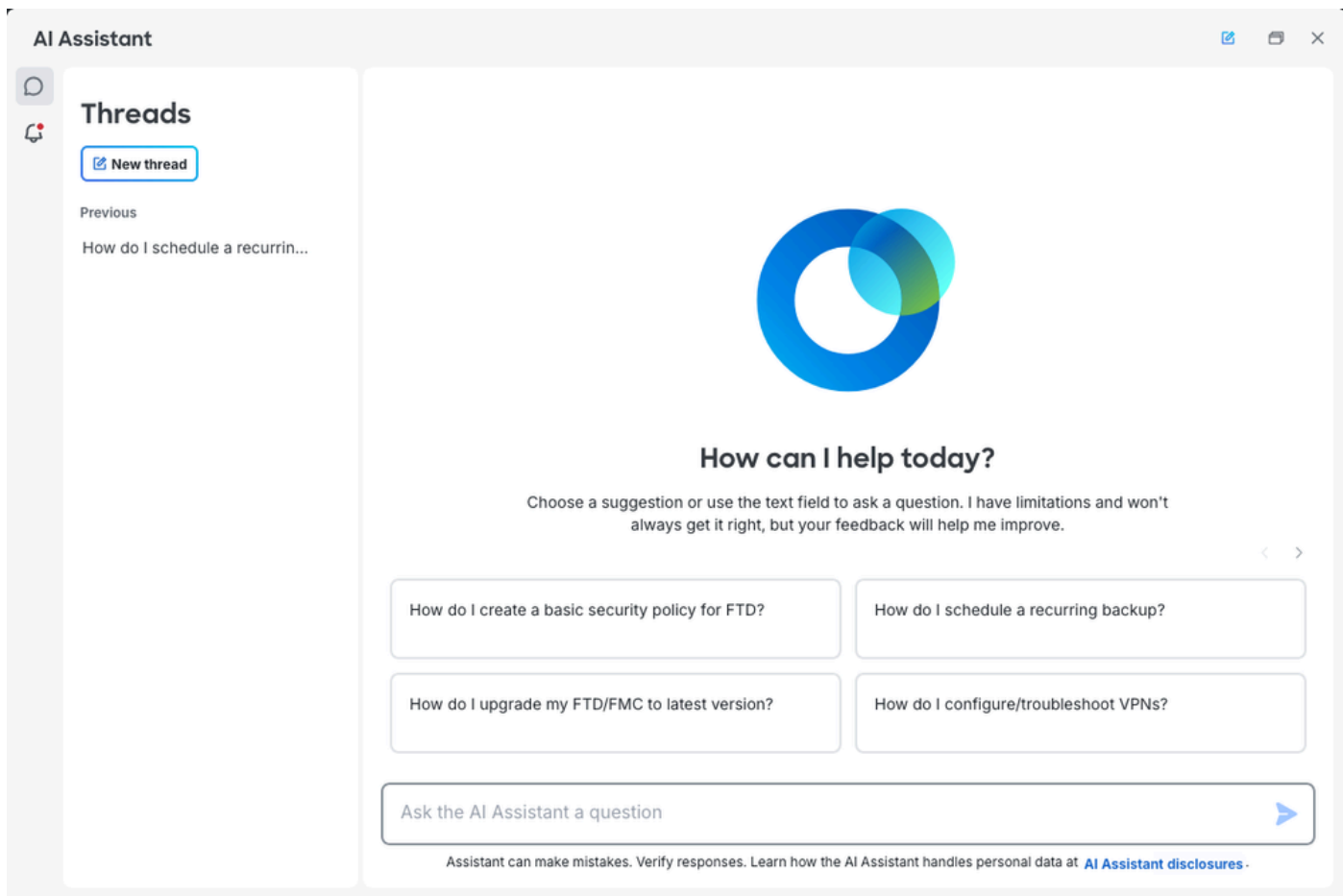
The Assistant strives for transparency

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

ステップ 5 Launch AI Assistantをクリックして、ダイアログボックスウィンドウでAI Assistantを開きます。



AI Assistant

Threads

New thread

Previous

How do I schedule a recurrin...

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?

How do I schedule a recurring backup?

How do I upgrade my FTD/FMC to latest version?

How do I configure/troubleshoot VPNs?

Ask the AI Assistant a question

Assistant can make mistakes. Verify responses. Learn how the AI Assistant handles personal data at [AI Assistant disclosures](#).



注：フィードバック：AI Assistantには、応答に関するフィードバックを提供するオプションがあります。感謝の気持ちを表すには親指を上げるを、改善できることをアシスタントに知らせるには親指を下げるをクリックします。

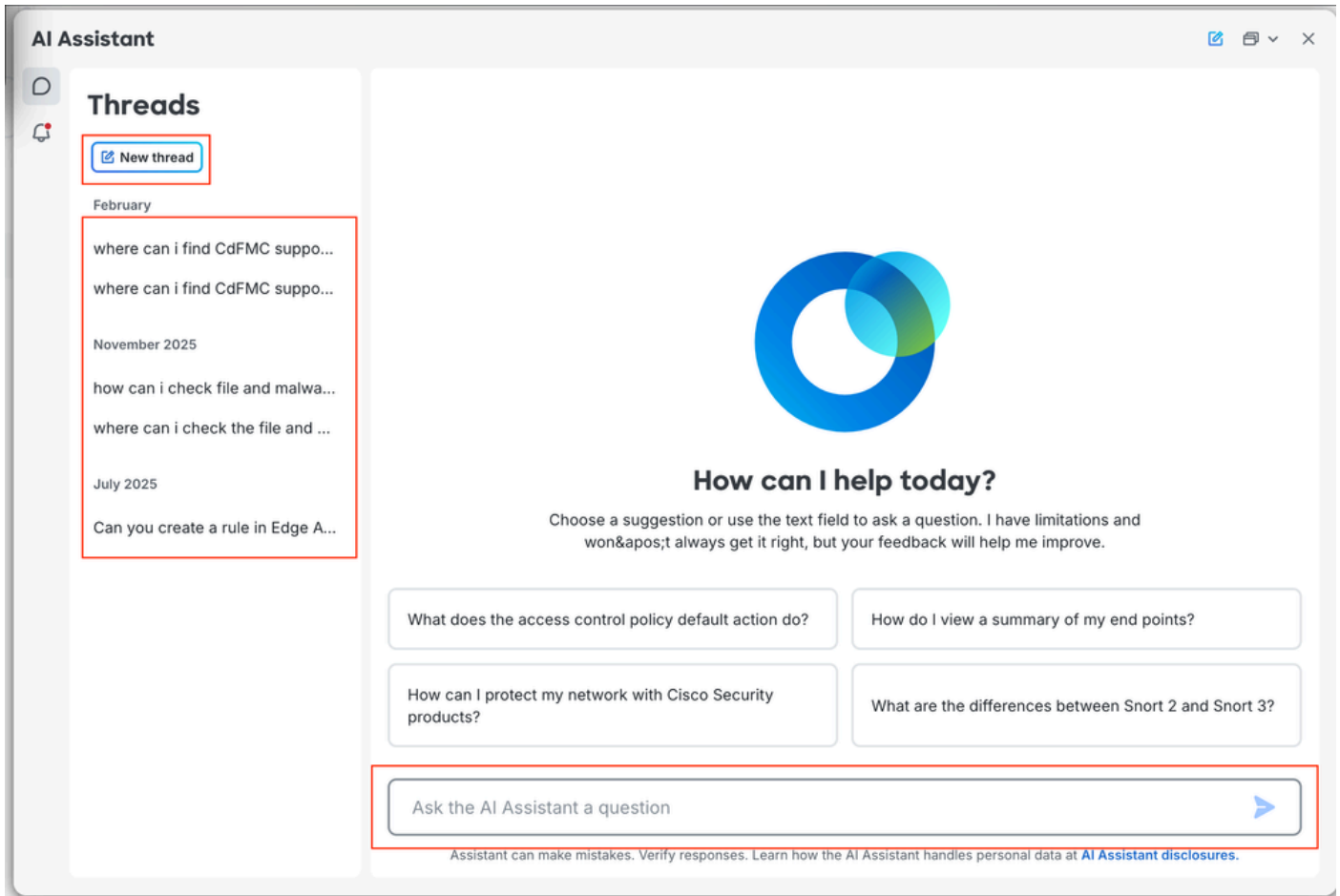
---

#### AI Assistantの使用に関するベストプラクティス

AI Assistantは、ポリシー管理を合理化し、トラブルシューティングを加速し、全体的なセキュリティポスチャを最適化するように設計された強力なツールです。最も正確で実用的な洞察を得るために、ベストプラクティスを検討してください。

- 正確に：過度に広い範囲のクエリを避けます。現在調査中のオブジェクト、ルール、またはインシデントに関する具体的な詳細を提供します。
- コンテキストの提供：接続の問題のトラブルシューティングを行う際には、関係する特定のデバイス、ゾーン、またはインターフェイスなどの関連する環境の詳細を含めます。
- 深さについて繰り返し説明する：最初の応答がニーズに完全に対応していない場合は、さらに質問を使用してAI出力を調整します。

クエリを送信すると、AI Assistantが応答を生成します。多くの場合、関連するドキュメントへのリンクを含めて、さらに詳しく読むことができます。新しい会話を始めるには、New Threadボタンをクリックするか、画面下部のテキストボックスに次の質問を入力します。左側のナビゲーションメニューのThreadsセクションをクリックすると、対話履歴をいつでも確認できます。



## ポリシールール作成の自動化

この画像は、ポリシー設定を合理化するAI Assistantの機能を示しています。ポリシー名、ソースネットワーク、およびアプリケーションユーザとして目的のパラメータを入力するだけで、AIは提案されたルールの構造化された要約を生成します。このインターフェイスでは、管理者による検証ステップが提供されます。システムでは、設定が確認用にクリアテーブルで表示されます。最後に、AIはアクションを確認し、ルールが無効状態で作成されたことをユーザーに通知するステータス通知を提供し、管理者がポリシーの最終的な展開に対する完全な制御を維持できるようにします。

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.**

## トラブルシューティング

AI Assistantへのアクセスまたは使用中に問題が発生した場合は、次の診断手順を実行してください。

### 接続とアクセスの問題

- クラウド接続の検証：AI Assistantは、シスコクラウドサービスへの安定した接続に依存します。Integration > Cisco Security Cloudの順に移動し、ステータスがEnabledに設定されていること、ポート8989が開いていてファイアウォールでブロックされていないことを確認し、Cisco Security Cloudのリージョンとテナントが正しいことを確認します。
- プロキシ設定：環境でプロキシサーバを使用している場合は、トラフィックをプロキシサーバ経由でルーティングするようにFMCが正しく設定されていることを確認します。
- 不足しているアイコン：AIアシスタントアイコンが表示されない場合は、FMCがSSCに正常にオンボーディングされ、ポート8989が開いていて、ファイアウォールによってブロックされていないことを確認します。
- 「Something went wrong」エラー：通常、これはFMCとSSC間の接続の問題を示しています。オンボーディングプロセスが正常に完了し、ポート8989が開いていて、ファイアウォールによってブロックされていないことを確認します。
- 古い情報：AI Assistantは、現在のポリシーデータベースと同期するのに最大24時間かかることがあります。最近、重要な設定変更を行った場合は、この同期期間を考慮してから、これらの更新がアシスタントに反映されるようにしてください。
- SCCでのエラー（HA環境）：FMCがHAペアの一部である場合、スタンバイからアクティブへのフェールオーバーによってクラウド接続が中断される可能性があります。このシナリオでは、機能を復元するために、新しくアクティブになったデバイスでクラウド統合を無効にしてから再度有効にする必要があります。

さらに詳細なトラブルシューティングを行うには、ブラウザコンソールログを収集して、潜在的なエラーを特定します。

開発者ツールにアクセスするには、次の手順に従います。

- Chrome、Edge: F12またはCtrl+Shift+I ( macOSの場合はCmd+Option+I ) を押します。
- Firefox:F12またはCtrl+Shift+K ( macOSではCmd+Option+K ) を押します。

コンソールが開いたら、ページを更新します。エラーは赤いテキストで表示されます。詳細な調査のためにログを共有する必要がある場合は、コンソール領域を右クリックしてログをファイルとして保存します。

### 自動チケット作成

AI Assistantは、自動ソリューションが不十分な場合にチケットを推奨することでサポートプロセスを合理化し、管理者はいつでも手動のサポート要求を開始できます。

Support Case Managerでケースを作成すると、追跡とケース管理に関連するすべての詳細情報がアシスタントから提供されます。

次の手順を実行して、サポート要求を迅速かつ効率的に管理します。

- 起動：ダッシュボードの右上隅にあるアイコンをクリックして、AI Assistantを開きます。
- クエリー：チャットボックスに技術的な質問を入力するか、問題を入力して、セッションを開始します。
- 分析：アシスタントが提供するトラブルシューティングの手順またはソリューションを確認します。
- エスカレーション：自動提案で問題が解決しない場合は、プロンプトを使用してTACでケースをオープンします。
- 手動トリガー：プロンプト「Open a Case with TAC」を入力することで、いつでも手動でサポートリクエストを開始できます。

● You

open a case with TAC

🗨️ 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.

👍 🗨️ 📄

## 関連情報

[Cisco AI Assistantのプロンプトガイド](#)

---

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。