



## **Cisco AI Assistant** 사용자 가이드

최종 변경: 2024년 12월 17일

### **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





# 1 장

## 개요

---





## 2 장

# Cisco AI Assistant 구성 요소

---

Cisco AI Assistant는 사용자 친화적 구성 요소로 설계되었습니다.

- 텍스트 입력 상자 -창 하단에는 입력을 하고 AI Assistant를 사용할 수 있는 텍스트 입력 상자가 있습니다.
- 새 스레드 - AI Assistant와 새 대화를 시작하려면 편집 아이콘을 클릭합니다.
- 채팅 기록 - 화면 왼쪽의 메뉴 트레이를 확장하면 채팅 기록을 확인할 수 있습니다.
- 피드백 - AI Assistant에는 응답에 대한 피드백을 제공하는 옵션이 있습니다. 좋아요를 클릭하여 감사를 표시하거나 싫어요를 클릭하여 어시스턴트가 더 잘할 수 있음을 알릴 수 있습니다.
- 확장 뷰 -오른쪽 상단의 확장 아이콘을 클릭하여 AI Assistant를 전체 화면 보기로 엽니다.
- 알림 - AI Assistant는 보안 환경 내의 중요한 작업, 업데이트 및 변경 사항에 대한 알림을 제공합니다.





# 3 장

## Cisco AI Assistant 모범 사례

AI Assistant와 효과적으로 통신하려면 다음과 같은 모범 사례를 권장합니다.

- 자세한 질문 하기 - AI Assistant는 정책/규칙 구성 및 설명서 데이터에 대해 교육을 받았습니다. 관련성 있는 응답을 받으려면 어시스턴트에 중요한 세부 정보를 제공하는 것이 좋습니다.



**팁** 샘플 질문 - 내 어카운트에는 몇 개의 암호 해독 정책이 활성화되어 있나요? 어디에서 정책에 액세스할 수 있나요? 정책에서 소스 및 대상이 활성화되어 있나요?

- 작업을 하위 작업으로 분할 - 여러 지침 집합이 필요한 작업의 경우 작업을 분할하고 이전 작업에 응답한 후 하위 작업을 입력하는 것이 유용할 수 있습니다.



**참고** AI Assistant는 정책 데이터베이스를 동기화하는 데 24시간이 걸립니다. 그 결과 정책 조회에 대한 응답에서 제공되는 데이터가 24시간 지연됩니다. 이는 다른 기능에 영향을 주지 않으며 사용자는 AI Assistant와 계속 상호 작용할 수 있습니다.



**팁** 위의 샘플 질문에서 - 질문을 더 작은 작업으로 분할하고 한 번에 하나씩 질문을 던집니다. 다음 질문으로 이동하기 전에 응답을 기다리십시오. 이 접근 방식은 정보 과부하를 방지하고 반복의 필요성을 줄이는 데 도움이 됩니다. -

- 내 어카운트에는 몇 개의 암호 해독 정책이 활성화되어 있나요?
- 어디에서 정책에 액세스할 수 있나요?
- 정책에서 소스 및 대상이 활성화되어 있나요?

- AI Assistant에 파일 또는 이미지를 업로드할 수 없습니다.
- AI Assistant는 현재 영어로만 지원됩니다.



---

참고 권장되는 모범 사례를 더욱 잘 이해하려면 [프롬프트 가이드](#)를 읽어보십시오.

---



# 4 장

## Cisco AI Assistant용 프롬프트 가이드

Cisco AI Assistant의 프롬프트 가이드는 AI Assistant와 더욱 효과적으로 상호 작용하여 쿼리 및 명령에 대한 정확하고 관련성 있으며 유용한 응답을 얻을 수 있도록 설계되었습니다. Cisco AI Assistant에서의 경험은 얼마나 효과적으로 커뮤니케이션하는지에 따라 크게 향상될 수 있습니다.

### 프롬프트 이해

프롬프트는 대화를 시작하거나 정보를 요청하기 위해 Cisco AI Assistant에 제공하는 질문 또는 텍스트 입력입니다. 기본적으로 이것은 AI Assistant에 제기하는 문제입니다. 프롬프트를 형식 지정하고 구성하는 방식은 AI Assistant에서 응답을 결정하는 데 중요한 역할을 합니다.

### 프롬프트의 주요 구성 요소:

- **명확성:** 요구하는 내용을 명확하고 구체적으로 작성합니다.
- **상황:** 필요한 배경 정보를 제공합니다.
- **목적:** 프롬프트를 사용하여 달성하고자 하는 것을 설명합니다.

### 효과적인 프롬프트의 예

일반 프롬프트	효과적인 프롬프트	그 차이는 무엇일까요?
현재 차단되고 있는 IP 주소 및 포트는 무엇입니까?	방화벽 정책에 의해 현재 차단된 개별 IP 주소를 알려줄 수 있습니까?	일반 프롬프트 - "both" 또는 "all" 속성의 필요성을 명시적으로 나타내지 않으면, 어시스턴트가 IP 또는 포트에 대한 기본 정보를 제공할 수 있을 뿐 둘 다 제공되지 않을 수도 있습니다.  유효 프롬프트 - 이 프롬프트는 명확하며 "distinct" 키워드를 사용하여 고유한 값의 필요성을 지정합니다. 이는 AI Assistant기능에 부합합니다.

일반 프롬프트	효과적인 프롬프트	그 차이는 무엇일까요?
방화벽 규칙과 해당 규칙을 설정한 사용자, 그리고 지난달에 적용된 모든 변경사항을 알려 주십시오.	모든 활성 방화벽 규칙의 이름과 설명이 모두 필요합니다. 출력에 두 속성을 모두 포함하십시오.	일반 프롬프트 - 요청이 과부하 상태이며 모든 속성이 함께 필요한지 여부에 대한 명확성이 부족하여 AI Assistant에 대한 잠재적 혼동을 야기합니다.  유효 프롬프트 - "both"를 사용하여 여러 속성에 대한 요구사항을 명확하게 제시하여 어시스턴트가 요청된 모든 정보를 포함해야 한다는 것을 이해할 수 있도록 합니다.
IP 주소 X 및 Y에 대한 방화벽 규칙은 무엇이며 어떻게 업데이트합니까?	지난 한 주 동안의 모든 방화벽 규칙 목록과 해당 동작을 보여 주십시오.	일반 프롬프트 - 규칙과 업데이트 절차에 대한 질문이 결합되어 있으며, 상황이나 특수성 부족으로 인해 응답이 불완전하거나 부정확할 수 있습니다.  유효 프롬프트 - 규칙 및 해당 작업 목록이 필요하다는 점에 대해 구체적이므로 AI Assistant에 대한 간단한 요청을 만듭니다.
이름만 제외한 모든 것을 알려 주십시오.	첫 번째 질문: 현재 방화벽 규칙은 무엇입니까?  후속 질문: 이러한 규칙과 관련된 작업도 제공할 수 있습니까?	일반 프롬프트 - 모호하며 AI Assistant에서 효과적으로 해석할 수 있는 방식으로 제공된 키워드를 사용하지 않습니다.  유효 프롬프트 - 이 접근 방식은 상황을 유지하는 데 도움이 되고 각 질문을 정확하게 해결합니다.
내 어카운트의 정책에 대한 모든 정보를 알려 주십시오.	내 Edge ACP 액세스 제어 정책을 이해하고 싶습니다. 자세히 설명해 줄 수 있습니까?	일반 프롬프트 - 너무 모호하며 세부 정보가 부족합니다. AI Assistant는 사용자가 정보를 요청 중인 특정 정책을 확인할 수 없습니다.  유효 프롬프트 - 사용자에게 Edge ACP 액세스 정책에 대한 세부 정보가 필요함을 AI Assistant에 알립니다. AI Assistant는 모든 관련 세부 정보로 응답합니다.

일반 프롬프트	효과적인 프롬프트	그 차이는 무엇일까요?
Edge ACP 정책의 포트, 프로토콜 및 규칙 수를 가장 큰 것 순으로 표시합니다.	Edge ACP 정책에서 어떤 포트 및 프로토콜이 규칙에 구성되어 있습니까? 이를 사용하는 규칙 수를 포함하고 가장 큰 것부터 가장 작은 것 순으로 정렬합니다.	일반 프롬프트 - 명확한 지침 없이 여러 복잡한 요청을 결합하며, 특수성이 부족하며, 데이터를 집계하고 표시하는 방법을 AI Assistant가 알고 있다고 가정합니다. 이는 사용자의 기대에 미치지 못할 수도 있는 응답과 잘못된 이해로 이어집니다.  유효 프롬프트 - 이 방식은 컨텍스트를 유지하는 데 도움이 되고 어시스턴트에게 명확한 지침을 제공합니다.

#### 유효 프롬프트 작성 지침

정확한 입력과 컨텍스트를 제공하면 AI Assistant로부터 관련성 있고 유용한 답변을 받을 수 있는 확률이 크게 높아집니다.

- 구체적이고 상황 정보를 제공: AI Assistant가 요청을 더 잘 이해하는 데 도움이 될 수 있는 관련 정보, 올바른 디바이스 이름, 정책 이름 등을 사용합니다.
- 적절한 구문 사용: AI Assistant는 구어체를 이해할 수 있지만 명확하고 문법적으로 올바른 문장은 응답 정확도를 높일 수 있습니다.
- 원하는 출력을 명확하게 하기: 응답 형식에 대한 기본 설정(예: 목록, 자세한 설명, 표)이 있는 경우 이를 언급합니다.
- 수정 및 피드백: 응답이 기대에 미치지 못하는 경우 다음 번에 피드백을 제공하거나 확인을 요청할 수 있습니다.
- 직접 명명 요청: "이름만 알려주세요" 구문을 사용하여 AI Assistant가 응답에서 이름만 제공하도록 지시합니다. 예를 들어 사용자가 추가 세부정보 없이 방화벽 규칙 또는 정책 이름을 알고자 하는 경우, '방화벽 규칙의 이름만 알려주세요' 구문을 사용하여 AI Assistant가 응답에서 이름만 제공하도록 지시할 수 있습니다.
- 고유 값: "unique" 키워드를 사용하여 AI Assistant에서 고유한 값을 요청할 수 있습니다.
- 규칙 및 작업: 규칙에 대한 정보를 요청할 때 사용자는 포괄적인 인사이트를 위해 응답에 포함할 속성을 지정할 수 있습니다. 예를 들어 사용자가 특정 영역에 액세스를 허용하는 방화벽 규칙에 대해 알고자 하는 경우, 작업(예: 허용 또는 거부) 및 관련 소스 영역과 같은 추가 속성을 지정할 수 있습니다. 사용자는 구체적인 지침을 제공함으로써 정확한 요구 사항에 맞게 응답을 조정하고 설정에 대한 심층적인 통찰력을 얻을 수 있습니다. 이 접근 방식을 통해 사용자는 AI Assistant에서 보다 관련성 있고 실행 가능한 정보를 얻을 수 있습니다.
- 순차적 질문: 여러 문의의 경우, 명확성과 컨텍스트를 높이기 위해 하나의 복잡한 질문으로 결합하는 대신 별도의 후속 질문을 제시합니다.

- **명시적 다중 속성 쿼리:** 여러 속성을 검색할 때 '둘 다' 또는 '다음 모두'를 명시해야 합니다. 그렇지 않으면 AI Assistant가 응답하기 위해 무작위로 속성을 선택할 수 있습니다. 예를 들어 방화벽 규칙에 대해 쿼리할 경우, 속성에는 규칙 이름, 설명, 작업(예: 허용 또는 거부), 소스 IP 주소, 대상 IP 주소, 포트, 프로토콜 등의 세부정보가 포함될 수 있습니다.

다중 속성 쿼리에서는 여러 속성에 대한 정보를 동시에 요청하는 것을 의미합니다. 예를 들어 사용자가 방화벽 규칙의 이름과 설명을 모두 알고 싶을 수도 있고, 네트워크 트래픽의 소스 IP 주소 및 대상 포트에 관심이 있을 수도 있습니다.



## 5 장

# 온라인 도움말 설명서

AI Assistant는 관리자에게 전체 기술 자료에 대한 완전한 액세스를 부여하므로 관리자는 어떤 쿼리도 요청하고 정확한 응답을 받을 수 있습니다. 따라서 프로세스가 간소화되어 시간과 노력이 절약됩니다. 또한 AI Assistant는 도움말 문서로 연결되는 관련 인용문 및 참조 링크를 제공하여 관리자가 원하는 결과를 쉽게 얻을 수 있도록 안내하여 사용자 경험을 개선합니다.

관리자는 AI Assistant의 채팅 인터페이스에 자신의 쿼리를 입력하기만 하면 됩니다. 어시스턴트는 추가 지침을 위한 도움말 문서의 인용 및 참조 링크와 함께 명확한 답변을 제공합니다.



팁 샘플 프롬프트:

- 새 방화벽 정책을 구성하는 단계는 무엇인가요?
- 규칙 최적화에 대한 문서는 어디에서 찾을 수 있나요?
- 방화벽 설정에서 만료된 규칙을 갱신하려면 어떻게 해야 하나요?

- 정책 인사이트, 12 페이지
- Policy Analyzer and Optimizer, 14 페이지
- 정책 규칙 생성 자동화, 17 페이지
- 지원 문의, 22 페이지
- 알람 센터, 25 페이지
- 정책 인사이트, 26 페이지
- Policy Analyzer and Optimizer, 28 페이지
- 정책 규칙 생성 자동화, 31 페이지
- 지원 문의, 36 페이지
- 알람 센터, 39 페이지

# 정책 인사이트

관리자는 질문을 통해 규칙 세부 사항, 상태 및 컴플라이언스 일치 여부를 비롯한 정책 구성에 대한 통찰력을 얻을 수 있습니다. AI Assistant는 정책을 스캔하고 분석하여 성능과 효율성을 향상시키기 위해 해결해야 하는 잠재적인 격차와 중복에 대한 세부 정보를 제공합니다.

## SUMMARY STEPS

1. 테넌트의 대시보드로 이동하여 오른쪽 상단에 있는 AI Assistant 아이콘을 클릭합니다.
2. 간단한 프롬프트(예: "모든 액세스 제어 규칙을 보여주세요")를 사용하여 기존 정책 규칙에 대해 문의합니다.
3. AI Assistant는 쿼리와 관련된 정책의 포괄적인 목록을 검색합니다.
4. 규칙 구성, 규칙 상태 및 주요 속성(예: 허용되는 트래픽, 차단된 포트 또는 IP 주소)을 포함하여 AI Assistant가 제공하는 세부사항을 검토합니다.

## DETAILED STEPS

프로시저

	명령 또는 동작	목적
단계 1	테넌트의 대시보드로 이동하여 오른쪽 상단에 있는 AI Assistant 아이콘을 클릭합니다.	
단계 2	간단한 프롬프트(예: "모든 액세스 제어 규칙을 보여주세요")를 사용하여 기존 정책 규칙에 대해 문의합니다.	
단계 3	AI Assistant는 쿼리와 관련된 정책의 포괄적인 목록을 검색합니다.	
단계 4	규칙 구성, 규칙 상태 및 주요 속성(예: 허용되는 트래픽, 차단된 포트 또는 IP 주소)을 포함하여 AI Assistant가 제공하는 세부사항을 검토합니다.	

예

### 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\_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.

**팁** 샘플 프롬프트

- `http://github.com`을 사용하는 규칙은 무엇인가요?
- 어떤 규칙에서 이 `IP 100.20.10.1`을 사용하나요?
- 어떤 정책이 `Webex` 애플리케이션 및 `Webex URL`을 차단하나요?
- 어떤 규칙이 인바운드 트래픽을 허용하나요?
- 조건이 만료된 규칙을 보여주세요.

## Policy Analyzer and Optimizer

AI Assistant는 방화벽 규칙 내의 격차와 불일치를 식별하여 관리자에게 이상 징후 또는 잠재적 문제에 대한 자세한 통찰력을 제공합니다. 이를 통해 관리자는 방화벽 정책의 전반적인 효율성을 최적화하고, 보안 취약점을 신속하게 해결하고 컴플라이언스를 보장할 수 있습니다. 규칙은 다음과 같을 수 있습니다.

- 병합 가능 규칙: 유사한 기준 또는 작업을 공유하기 때문에 결합하거나 통합할 수 있는 규칙입니다. 예를 들어 두 개 이상의 규칙이 동일한 소스, 대상 또는 프로토콜에 적용되지만 중복되거나 중첩되는 조건이 있는 경우 복잡성을 줄이고 전반적인 효율성을 개선하기 위해 규칙을 병합할 수 있습니다. 내 케이스의 상태는 어떻게 되나요?
- 만료된 규칙: 사전 정의된 만료일 또는 시간 제한이 경과하여 더 이상 활성 상태가 아닌 규칙입니다.
- 개체 중첩 - 규칙 필드에 있는 요소는 규칙의 동일한 필드에 있는 하나 이상의 요소의 하위 집합입니다. 예를 들어 `source` 필드는 `10.1.1.0/24`에 대한 네트워크 개체 및 호스트 `10.1.1.1`에 대한 또 다른 개체를 포함할 수 있습니다. `10.1.1.1`은 `10.1.1.0/24`가 적용되는 네트워크 내에 있으므로 `10.1.1.1`에 대한 개체는 중복되며 삭제할 수 있으므로 규칙을 간소화하고 디바이스 메모리를 절약할 수 있습니다.
- 중복 규칙: 두 개의 규칙이 동일한 유형의 트래픽에 동일한 작업을 적용하며, 기본 규칙을 제거해도 최종 결과는 변경되지 않습니다. 예를 들어 특정 네트워크에 대해 `FTP` 트래픽을 허용하는 규칙 다음에 동일한 네트워크에 대한 `IP` 트래픽을 허용하는 규칙이 있고 그 사이에 액세스 거부 규칙이 없는 경우, 첫 번째 규칙은 중복되므로 삭제할 수 있습니다.
- 숨겨진 규칙: 이는 중복 규칙의 반대입니다. 이 경우 한 규칙은 다른 규칙과 동일한 트래픽과 일치하므로 두 번째 규칙은 액세스 목록에서 나중에 제공되므로 트래픽에 적용되지 않습니다. 두 규칙에 대한 작업이 동일한 경우 새도잉 규칙을 삭제할 수 있습니다. 두 규칙이 트래픽에 대해 서로 다른 작업을 지정하는 경우 새도잉된 규칙을 이동하거나 두 규칙 중 하나를 편집하여 원하는 정책을 구현해야 할 수 있습니다. 예를 들어 기본 규칙은 `IP` 트래픽을 거부하고 새도잉된 규칙은 지정된 소스 또는 대상에 대한 `FTP` 트래픽을 허용할 수 있습니다.

1. **AI Assistant**는 방화벽 규칙을 지속적으로 모니터링하고 분석합니다. 어시스턴트에게 현재 정책을 분석하여 공백이나 비효율성이 있는지 확인하라는 메시지를 표시할 수 있습니다(예: "중복 구성에 대한 규칙 분석").
2. **AI Assistant**는 최적화할 수 있는 중복 또는 충돌 규칙에 플래그를 지정합니다. 방화벽 성능을 간소화하기 위한 규칙 병합 또는 업데이트에 대한 제안을 제공합니다.
3. **AI Assistant**는 분석을 기반으로 보안 강화를 위해 사용하지 않는 규칙 제거, 설정 조정, 액세스 제어 강화와 같은 최적화를 권장합니다.



---

**참고** **AI Assistant**가 정책 내에서 만료되는 규칙이나 성능 문제를 감지하면 자동으로 알림을 생성하여 관리자에게 적시에 조치를 취하도록 유도합니다.

---

**AI Assistant**

**You**  
Show me what policies can I optimize?

**AI Assistant**  
The policies that can be optimized include 'raj-acp', 'TEST1', 'child\_policy\_1', 'anna\_acp2', and 'nyc'. They have varying percentages of optimizable rules.

[View details](#)

Last data sync: about 5 hours ago

How this response was generated

**i** Your feedback helps us improve the AI Assistant.

👍 🗨️ 📄

Ask the AI Assistant a question

[View User Guide](#) to learn more.

**View Details**(세부 정보 보기)를 클릭하면 됩니다.



팁 샘플 프롬프트

- 방화벽 규칙의 불일치 사항을 식별합니다.
- 현재 방화벽 정책 구성의 차이를 보여주세요.
- 방화벽 설정에 중복되거나 충돌하는 규칙이 있나요?

### 비정상적인 정책 해결

관리자는 AI Assistant를 사용하여 정책 규칙의 차이를 효율적으로 해결할 수 있습니다. 도움을 받아 다음을 수행할 수 있습니다.

- 중복, 새도우 규칙, 만료된 모든 정책 규칙을 비활성화합니다.
- 중복, 새도우 규칙 및 만료된 모든 정책 규칙을 제거합니다.
- 중복되는 모든 정책 규칙을 병합합니다.



참고 이러한 작업을 수행해도 문제가 해결되지 않는 경우 [지원 티켓을 생성](#)하여 Cisco 지원팀에 문의할 수 있습니다.

## 정책 규칙 생성 자동화

AI Assistant는 Secure Firewall Threat Defense에서 관리하는 클라우드 제공 Firewall Management Center에 대한 정책 규칙 생성 프로세스를 간소화하고 광범위한 기술적 지식 또는 수동 구성의 필요성을 최소화합니다. 관리자는 [Cisco AI Assistant용 프롬프트 가이드](#)를 활용하여 강력한 보안 조치를 신속하게 설정하여 네트워크의 전반적인 효율성과 보안을 강화할 수 있습니다. 일단 생성된 이러한 규칙은 테넌트의 정책 섹션 아래에 나열됩니다.

### 예제 시나리오

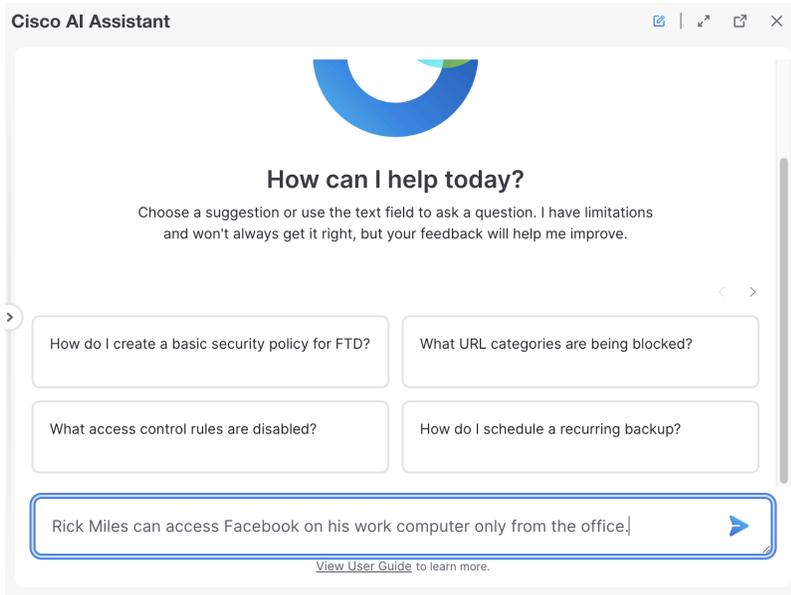
관리자가 다음 요청을 수신하는 시나리오를 가정해 보겠습니다.

*Rick Miles*는 사무실에 있는 업무용 컴퓨터에서만 *Facebook*에 액세스할 수 있습니다.

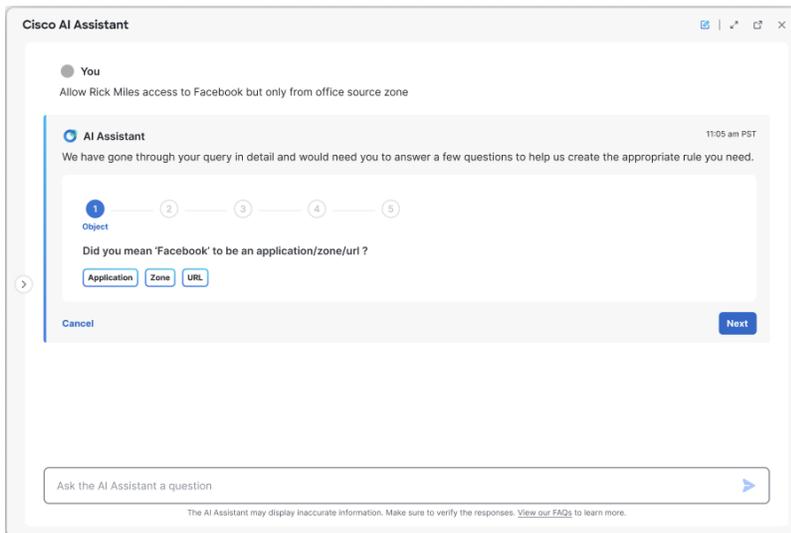
관리자는 규칙을 생성하기 위해 다음과 같은 프로세스를 따라야 합니다.

### 프로시저

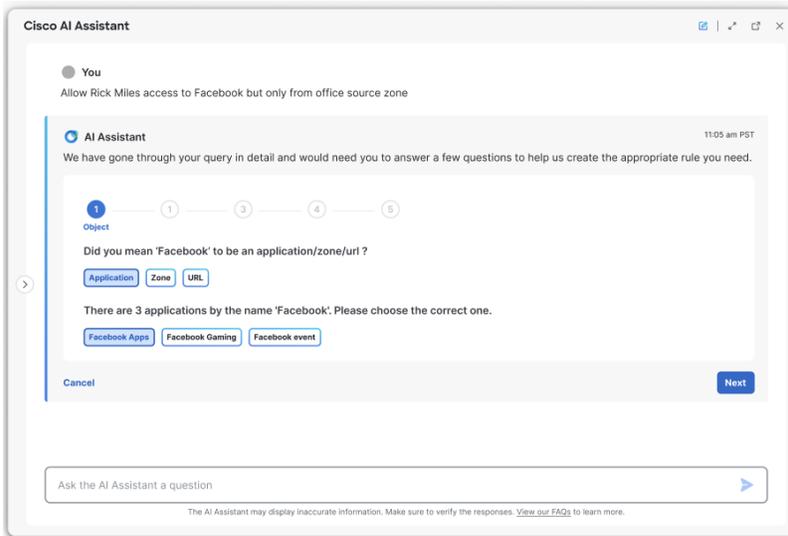
단계 1 관리자는 이 요청을 수용하기 위해 새 규칙을 생성해야 합니다. 관리자는 AI Assistant에 다음 요청을 제출합니다.



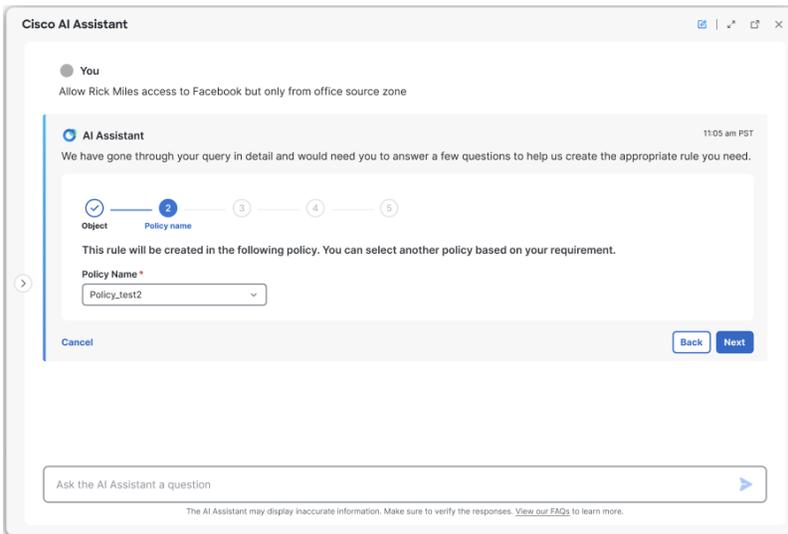
단계 2 AI Assistant는 관리자의 요구 사항을 더 잘 이해하기 위해 질문을 던지며, 규칙을 생성할 수 있는 여러 옵션을 안내합니다.



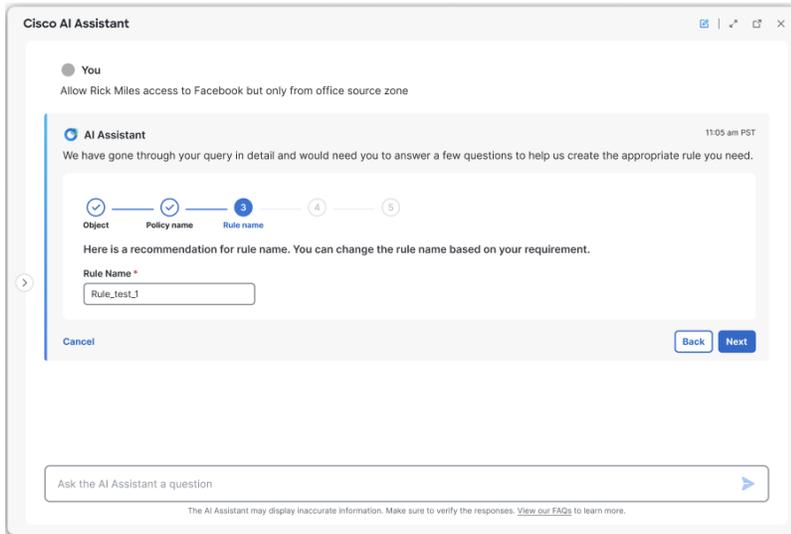
단계 3 AI Assistant는 Facebook에 대한 여러 결과를 찾고 관리자에게 Facebook을 애플리케이션, URL 또는 영역으로 참조하는지 확인하도록 요청합니다.



단계 4 AI Assistant는 규칙을 추가할 정책을 선택하라는 메시지를 관리자에게 표시합니다.

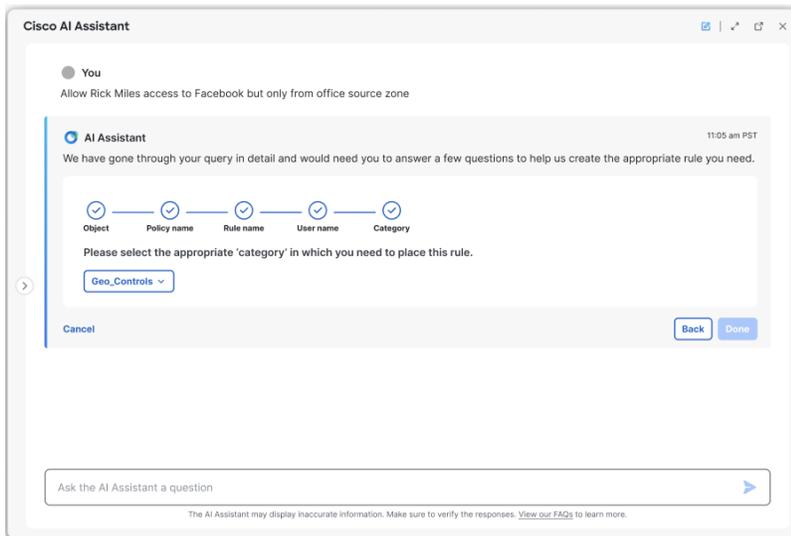


단계 5 AI Assistant는 "규칙 이름"을 제안하며, 필요한 경우 관리자가 수정할 수 있습니다.

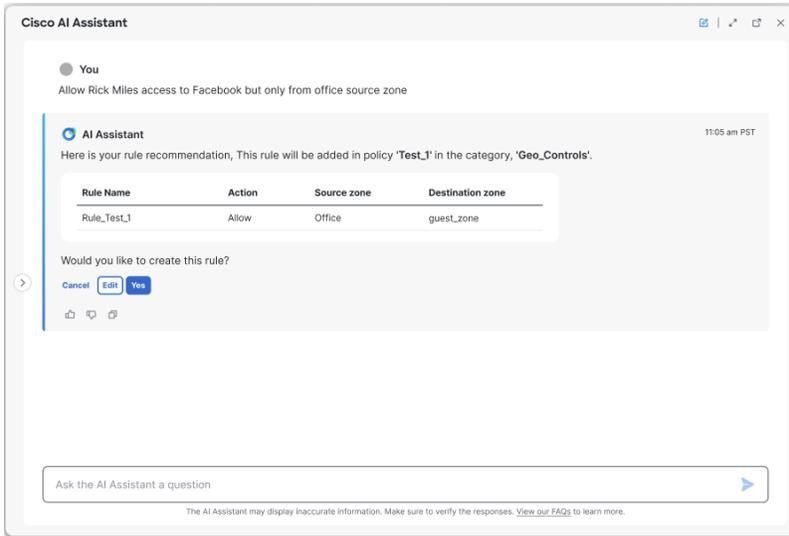


참고  
관리자가 정책에 이미 있는 "규칙 이름"을 선택하는 경우, 관리자에게 새 이름을 입력하라는 오류 메시지가 표시됩니다.

단계 6 AI Assistant는 관리자에게 규칙의 "사용자 이름"과 "범주"를 선택하라는 메시지를 표시합니다.



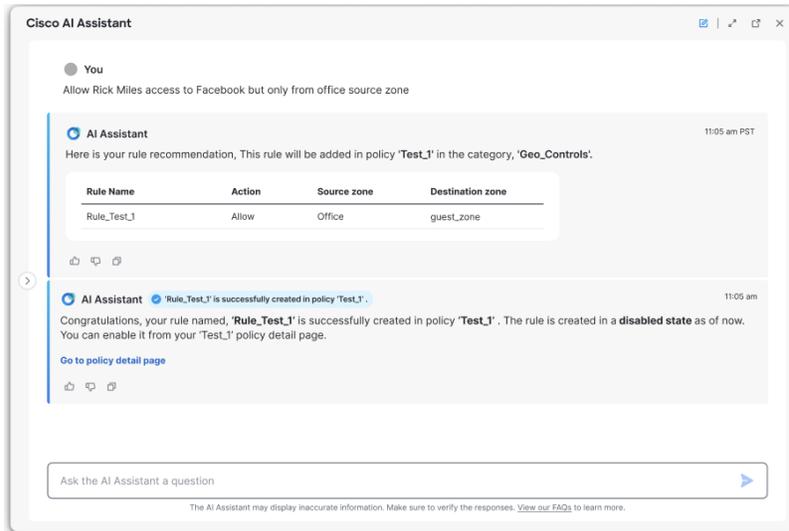
단계 7 AI Assistant는 규칙 생성에 대한 확인을 요청하고, 규칙에 대한 입력과 함께 관리자의 요청에 대한 요약을 제공합니다.



참고

관리자는 **Edit(편집)**를 클릭하여 규칙 정보를 편집하고 **Cancel(취소)**을 클릭하여 규칙 생성 프로세스를 취소할 수 있습니다.

**단계 8** 관리자가 규칙 생성에 대해 "Yes(예)"라고 확인한다고 가정하면, 규칙이 생성되고 관리자가 선택한 정책에 반영됩니다.



참고

정책 규칙을 생성할 수 없는 경우 [Cisco AI Assistant FAQ\(자주 묻는 질문\)](#), 41 페이지의 내용을 참조하십시오.

## 지원 문의

AI Assistant는 티켓 생성 및 관리 프로세스를 간소화하여 관리자가 지원 요청을 효율적이고 효과적으로 처리할 수 있도록 합니다. 이 통합을 통해 관리자는 해결되지 않은 문제가 발생하거나 AI의 권장 사항 이외의 추가 지원이 필요한 경우 AI Assistant를 통해 직접 지원 케이스를 생성할 수 있습니다.

주요 기능은 다음과 같습니다.

- 자동화된 티켓 생성: AI Assistant는 해결 방법으로 문제가 해결되지 않는 경우 지원 티켓 생성을 자동으로 제안합니다. 관리자는 간단한 프롬프트를 사용하여 수동으로 티켓을 만들 수도 있습니다.
- 티켓 관리: 관리자는 AI Assistant 내에서 티켓의 상태를 추적하고 "종료"에 대한 상태를 업데이트할 수 있습니다.

티켓 생성 및 관리를 AI Assistant에 통합함으로써 조직에서는 문제 해결에 소요되는 지연을 줄이고, 지원팀과 함께 지원 케이스를 생성하고, 문제 해결의 전반적인 효율성을 높일 수 있습니다.

---

CDO 및 클라우드 제공 Firewall Management Center를 사용 중인 고객만 AI Assistant를 통해 지원에 문의할 수 있습니다.

---

### 지원 사례 열기

AI Assistant는 대화의 컨텍스트에 따라 지원 티켓을 생성합니다. 이 지원 케이스는 **Support Case Manager**(지원 케이스 관리자)에서 생성되며 티켓 세부 정보가 사용자와 공유됩니다.

아래 단계에 따라 관리자는 AI Assistant를 통한 지원 티켓을 빠르고 원활하게 생성할 수 있습니다.

1. 테넌트의 대시보드로 이동하여 오른쪽 상단에 있는 AI Assistant 아이콘을 클릭합니다.
2. 텍스트 상자에 쿼리/문제를 입력하여 대화를 시작합니다.
3. AI Assistant는 제시된 문제를 기반으로 문제 해결 단계 또는 솔루션을 제안합니다.
4. AI Assistant의 권장 솔루션으로 문제가 해결되지 않거나 추가 도움이 필요한 경우 어시스턴트에서 **Open a Case**(케이스 열기) 프롬프트를 표시합니다.

"지원 케이스 생성"을 입력하여 지원 케이스 생성을 수동으로 요청할 수도 있습니다.

5. AI Assistant가 케이스를 생성하고 케이스 세부 정보를 제공합니다.




---

참고 참조용 케이스 번호가 포함된 확인 이메일이 전송됩니다.

---

## 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'll create a Technical Assistance 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 description 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.

**팁 샘플 프롬프트:**

- 방화벽의 문제를 보고해야 합니다.
- 지원 티켓을 여는 데 도움을 줄 수 있나요?
- 이 문제를 지원팀으로 에스컬레이션해 주세요.
- 이 제품에 대한 이의를 제기하려면 어떻게 해야 하나요?
- 방화벽의 오작동에 대해 문의해야 합니다.
- 이 제품 사용에 문제가 있어 케이스를 열어야 합니다.

**지원 케이스 관리**

관리자는 AI Assistant를 통해 지원 케이스를 신속하게 확인하고 업데이트할 수 있습니다. 지원 티켓의 상태는 다음과 같을 수 있습니다.

- **케이스 나열:** AI Assistant는 테넌트에 대해 열린 케이스 및 종료된 케이스를 모두 나열할 수 있습니다.
- **닫기:** 문제가 해결된 후 지원 케이스를 해결된 것으로 표시합니다.
- **검색:** 검토 또는 참조를 위해 기존 지원 케이스의 세부 사항에 액세스합니다.

**지원 케이스 목록**

관리자는 AI Assistant를 사용하여 테넌트 내에서 이전에 생성된 모든 지원 케이스의 포괄적인 목록에 쉽게 액세스할 수 있습니다. 어시스턴트에게 과거 케이스를 검색해달라고 요청하기만 하면, 관리자는 각 케이스의 케이스 번호, 상태, 설명 및 기타 필수 세부 정보를 볼 수 있습니다.

케이스를 검색하려면 다음을 수행합니다.

1. 텍스트 상자에서 AI Assistant로 이동하여 AI Assistant에 지원 케이스 목록을 검색하도록 요청합니다.
2. 또는 **Support Case Manager**(지원 케이스 관리자) 섹션에서 직접 케이스 목록을 검색할 수 있습니다.

**팁 샘플 프롬프트:**

- 지원 케이스 기록을 알고 싶습니다.
- 얼마나 많은 지원 케이스가 있나요?

**지원 케이스 상태**

관리자는 AI Assistant를 통해 지원 케이스의 상태를 확인할 수 있습니다.

1. 텍스트 상자에서 AI Assistant로 이동하여 AI Assistant에 지원 케이스의 상태를 검색하도록 요청합니다.
2. 또는 **Support Case Manager**(지원 케이스 관리자) 섹션에서 직접 티켓의 진행 상황을 추적할 수 있습니다.



팁 샘플 프롬프트:

- 지원 케이스 상태를 알고 싶습니다.
- 내 케이스의 상태는 어떤가요?

지원 케이스 종료

관리자는 AI Assistant를 통해 지원 케이스를 종료할 수 있습니다.

케이스를 종료하려면 다음을 수행합니다.

1. AI Assistant로 이동하고 텍스트 상자에서 AI Assistant에 케이스를 종료하도록 요청합니다.
2. 또는 지원 케이스 관리자 섹션에서 직접 티켓을 종료할 수도 있습니다.



팁 샘플 프롬프트:

- 케이스를 종료하고 싶습니다.
- 티켓을 종료하려면 어떻게 하나요?

## 알림 센터

Cisco AI Assistant의 알림 시스템은 보안 환경의 중요한 작업, 업데이트 및 변경 사항을 관리자에게 계속 알려줄 수 있도록 설계되었습니다. 사용자는 실시간 알림 및 예약된 알림을 활용하여 보안 사고를 사전에 관리하고 정책을 최적화 할 수 있습니다.

알림은 테넌트 대시보드의 오른쪽 상단에 있는 AI Assistant 아이콘을 통해 액세스합니다. 새 알림을 사용할 수 있으면 아이콘에 숫자 표시기가 나타나 읽지 않은 총 항목 수를 나타냅니다.

아이콘을 클릭하면 모든 알림의 포괄적인 목록을 볼 수 있는 알림 센터가 열립니다. 목록은 **Read**(읽음), **Unread**(읽지 않음) 등의 상태와 **Severity**(심각도)를 기준으로 쉽게 필터링할 수 있습니다. 따라서 중요한 작업의 우선 순위를 지정하고 최신 상태를 유지할 수 있습니다.

알림의 기본 상태는 읽지 않음입니다. 관리자는 알림을 읽음으로 표시하고 필요에 따라 알림을 삭제할 수 있습니다.

알림은 다음에 대해 트리거됩니다.

- 정책 분석기 및 최적화기: AI Assistant는 테넌트 내의 정책을 일상적으로 스캔하고 최적화를 위한 권장 사항을 제공합니다. 스캔 결과가 제공되면 어시스턴트가 시스템 생성 알림을 통해 사용자에게 알려 적시에 인식하고 조치를 취하도록 보장합니다.
- 정책 규칙 생성: 정책 규칙 생성을 시작하면 규칙은 초기에 기본적으로 "비활성화"로 설정되므로 수동으로 활성화해야 합니다. 규칙이 성공적으로 활성화되면 AI Assistant에서 알림을 보냅니다.

## 정책 인사이트

관리자는 질문을 통해 규칙 세부 사항, 상태 및 컴플라이언스 일치 여부를 비롯한 정책 구성에 대한 통찰력을 얻을 수 있습니다. AI Assistant는 정책을 스캔하고 분석하여 성능과 효율성을 향상시키기 위해 해결해야 하는 잠재적인 격차와 중복에 대한 세부 정보를 제공합니다.

### SUMMARY STEPS

1. 테넌트의 대시보드로 이동하여 오른쪽 상단에 있는 AI Assistant 아이콘을 클릭합니다.
2. 간단한 프롬프트(예: "모든 액세스 제어 규칙을 보여주세요")를 사용하여 기존 정책 규칙에 대해 문의합니다.
3. AI Assistant는 쿼리와 관련된 정책의 포괄적인 목록을 검색합니다.
4. 규칙 구성, 규칙 상태 및 주요 속성(예: 허용되는 트래픽, 차단된 포트 또는 IP 주소)을 포함하여 AI Assistant가 제공하는 세부사항을 검토합니다.

### DETAILED STEPS

#### 프로시저

	명령 또는 동작	목적
단계 1	테넌트의 대시보드로 이동하여 오른쪽 상단에 있는 AI Assistant 아이콘을 클릭합니다.	
단계 2	간단한 프롬프트(예: "모든 액세스 제어 규칙을 보여주세요")를 사용하여 기존 정책 규칙에 대해 문의합니다.	
단계 3	AI Assistant는 쿼리와 관련된 정책의 포괄적인 목록을 검색합니다.	
단계 4	규칙 구성, 규칙 상태 및 주요 속성(예: 허용되는 트래픽, 차단된 포트 또는 IP 주소)을 포함하여 AI Assistant가 제공하는 세부사항을 검토합니다.	

예

### 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\_access Control Policy, chuy\_test1, child\_policy\_1, anna\_acp2, TEST1, chuys\_test2, AA, raj-acp, and more.

[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.



#### 팁 샘플 프롬프트

- `http://github.com`을 사용하는 규칙은 무엇인가요?
- 어떤 규칙에서 이 `IP 100.20.10.1`을 사용하나요?
- 어떤 정책이 `Webex` 애플리케이션 및 `Webex URL`을 차단하나요?
- 어떤 규칙이 인바운드 트래픽을 허용하나요?
- 조건이 만료된 규칙을 보여주세요.

## Policy Analyzer and Optimizer

AI Assistant는 방화벽 규칙 내의 격차와 불일치를 식별하여 관리자에게 이상 징후 또는 잠재적 문제에 대한 자세한 통찰력을 제공합니다. 이를 통해 관리자는 방화벽 정책의 전반적인 효율성을 최적화하고, 보안 취약점을 신속하게 해결하고 컴플라이언스를 보장할 수 있습니다. 규칙은 다음과 같을 수 있습니다.

- 병합 가능 규칙: 유사한 기준 또는 작업을 공유하기 때문에 결합하거나 통합할 수 있는 규칙입니다. 예를 들어 두 개 이상의 규칙이 동일한 소스, 대상 또는 프로토콜에 적용되지만 중복되거나 중첩되는 조건이 있는 경우 복잡성을 줄이고 전반적인 효율성을 개선하기 위해 규칙을 병합할 수 있습니다. 내 케이스의 상태는 어떻게 되나요?
- 만료된 규칙: 사전 정의된 만료일 또는 시간 제한이 경과하여 더 이상 활성 상태가 아닌 규칙입니다.
- 개체 중첩 - 규칙 필드에 있는 요소는 규칙의 동일한 필드에 있는 하나 이상의 요소의 하위 집합입니다. 예를 들어 `source` 필드는 `10.1.1.0/24`에 대한 네트워크 개체 및 호스트 `10.1.1.1`에 대한 또 다른 개체를 포함할 수 있습니다. `10.1.1.1`은 `10.1.1.0/24`가 적용되는 네트워크 내에 있으므로 `10.1.1.1`에 대한 개체는 중복되며 삭제할 수 있으므로 규칙을 간소화하고 디바이스 메모리를 절약할 수 있습니다.
- 중복 규칙: 두 개의 규칙이 동일한 유형의 트래픽에 동일한 작업을 적용하며, 기본 규칙을 제거해도 최종 결과는 변경되지 않습니다. 예를 들어 특정 네트워크에 대해 `FTP` 트래픽을 허용하는 규칙 다음에 동일한 네트워크에 대한 `IP` 트래픽을 허용하는 규칙이 있고 그 사이에 액세스 거부 규칙이 없는 경우, 첫 번째 규칙은 중복되므로 삭제할 수 있습니다.
- 숨겨진 규칙: 이는 중복 규칙의 반대입니다. 이 경우 한 규칙은 다른 규칙과 동일한 트래픽과 일치하므로 두 번째 규칙은 액세스 목록에서 나중에 제공되므로 트래픽에 적용되지 않습니다. 두 규칙에 대한 작업이 동일한 경우 새도잉 규칙을 삭제할 수 있습니다. 두 규칙이 트래픽에 대해서도 다른 작업을 지정하는 경우 새도잉된 규칙을 이동하거나 두 규칙 중 하나를 편집하여 원하는 정책을 구현해야 할 수 있습니다. 예를 들어 기본 규칙은 `IP` 트래픽을 거부하고 새도잉된 규칙은 지정된 소스 또는 대상에 대한 `FTP` 트래픽을 허용할 수 있습니다.

1. **AI Assistant**는 방화벽 규칙을 지속적으로 모니터링하고 분석합니다. 어시스턴트에게 현재 정책을 분석하여 공백이나 비효율성이 있는지 확인하라는 메시지를 표시할 수 있습니다(예: "중복 구성에 대한 규칙 분석").
2. **AI Assistant**는 최적화할 수 있는 중복 또는 충돌 규칙에 플래그를 지정합니다. 방화벽 성능을 간소화하기 위한 규칙 병합 또는 업데이트에 대한 제안을 제공합니다.
3. **AI Assistant**는 분석을 기반으로 보안 강화를 위해 사용하지 않는 규칙 제거, 설정 조정, 액세스 제어 강화와 같은 최적화를 권장합니다.



---

**참고** **AI Assistant**가 정책 내에서 만료되는 규칙이나 성능 문제를 감지하면 자동으로 알림을 생성하여 관리자에게 적시에 조치를 취하도록 유도합니다.

---

**AI Assistant**

**You**  
Show me what policies can I optimize?

**AI Assistant**  
The policies that can be optimized include 'raj-acp', 'TEST1', 'child\_policy\_1', 'anna\_acp2', and 'nyc'. They have varying percentages of optimizable rules.

[View details](#)

Last data sync: about 5 hours ago

How this response was generated

**i** Your feedback helps us improve the AI Assistant.

Ask the AI Assistant a question

[View User Guide](#) to learn more.

**View Details**(세부 정보 보기)를 클릭하면 됩니다.



팁 샘플 프롬프트

- 방화벽 규칙의 불일치 사항을 식별합니다.
- 현재 방화벽 정책 구성의 차이를 보여주세요.
- 방화벽 설정에 중복되거나 충돌하는 규칙이 있나요?

### 비정상적인 정책 해결

관리자는 AI Assistant를 사용하여 정책 규칙의 차이를 효율적으로 해결할 수 있습니다. 도움을 받아 다음을 수행할 수 있습니다.

- 중복, 새도우 규칙, 만료된 모든 정책 규칙을 비활성화합니다.
- 중복, 새도우 규칙 및 만료된 모든 정책 규칙을 제거합니다.
- 중복되는 모든 정책 규칙을 병합합니다.



참고 이러한 작업을 수행해도 문제가 해결되지 않는 경우 [지원 티켓을 생성](#)하여 Cisco 지원팀에 문의할 수 있습니다.

## 정책 규칙 생성 자동화

AI Assistant는 Secure Firewall Threat Defense에서 관리하는 클라우드 제공 Firewall Management Center에 대한 정책 규칙 생성 프로세스를 간소화하고 광범위한 기술적 지식 또는 수동 구성의 필요성을 최소화합니다. 관리자는 [Cisco AI Assistant용 프롬프트 가이드](#)를 활용하여 강력한 보안 조치를 신속하게 설정하여 네트워크의 전반적인 효율성과 보안을 강화할 수 있습니다. 일단 생성된 이러한 규칙은 테넌트의 정책 섹션 아래에 나열됩니다.

### 예제 시나리오

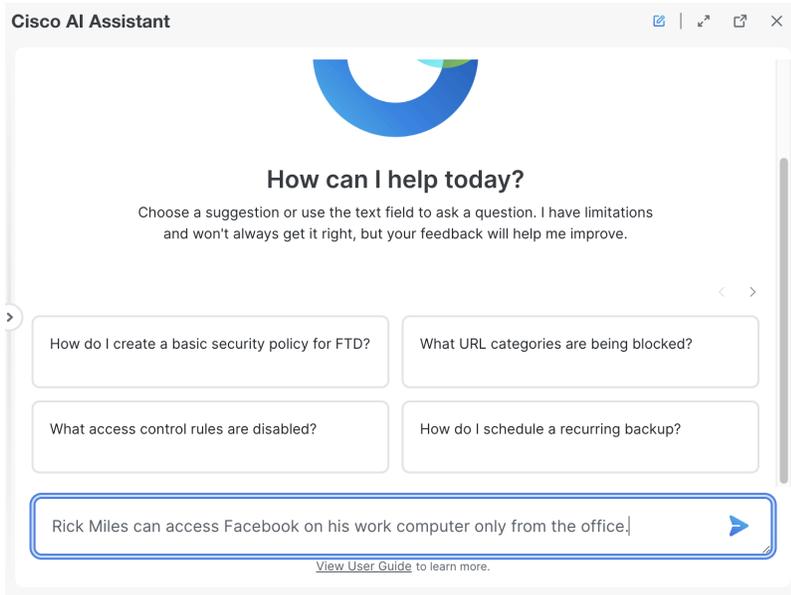
관리자가 다음 요청을 수신하는 시나리오를 가정해 보겠습니다.

*Rick Miles*는 사무실에 있는 업무용 컴퓨터에서만 *Facebook*에 액세스할 수 있습니다.

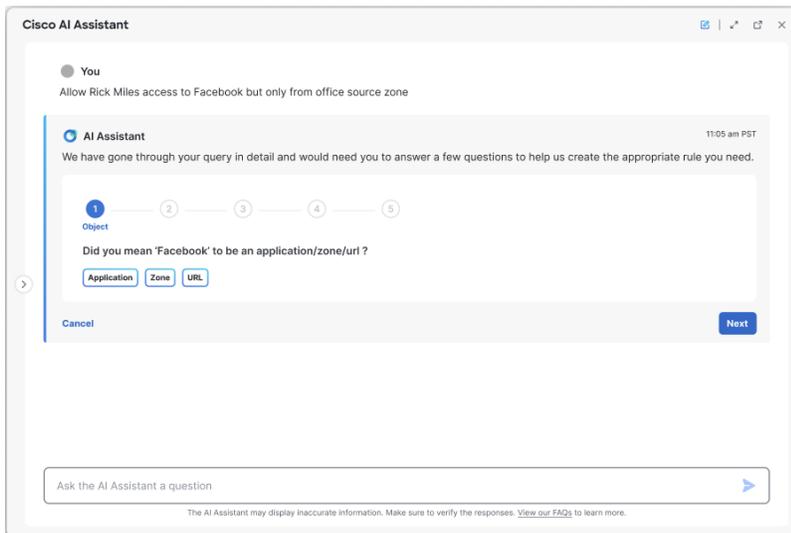
관리자는 규칙을 생성하기 위해 다음과 같은 프로세스를 따라야 합니다.

### 프로시저

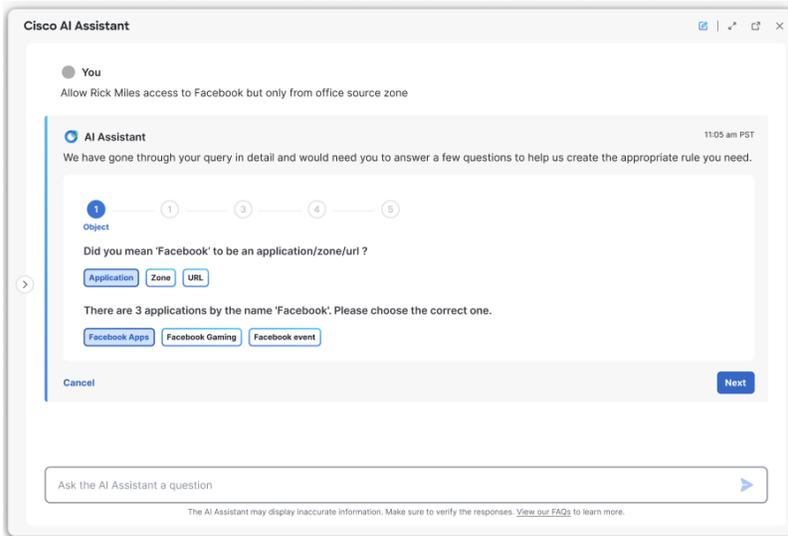
단계 1 관리자는 이 요청을 수용하기 위해 새 규칙을 생성해야 합니다. 관리자는 AI Assistant에 다음 요청을 제출합니다.



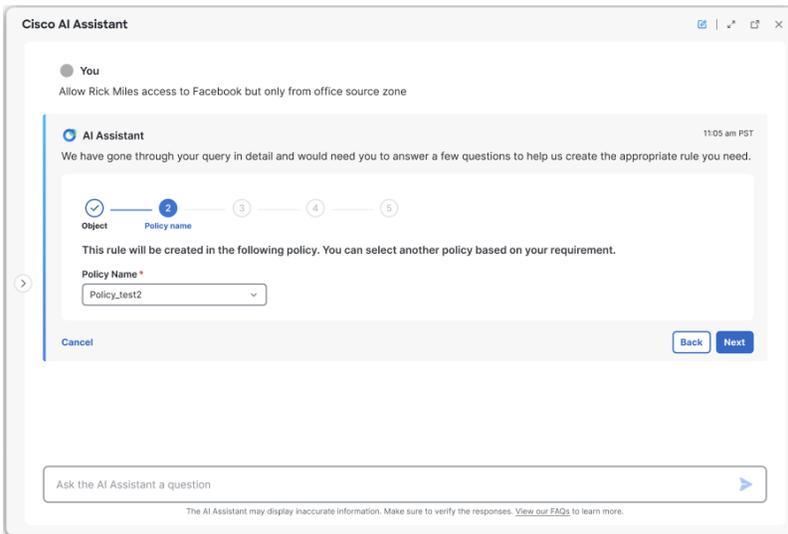
단계 2 AI Assistant는 관리자의 요구 사항을 더 잘 이해하기 위해 질문을 던지며, 규칙을 생성할 수 있는 여러 옵션을 안내합니다.



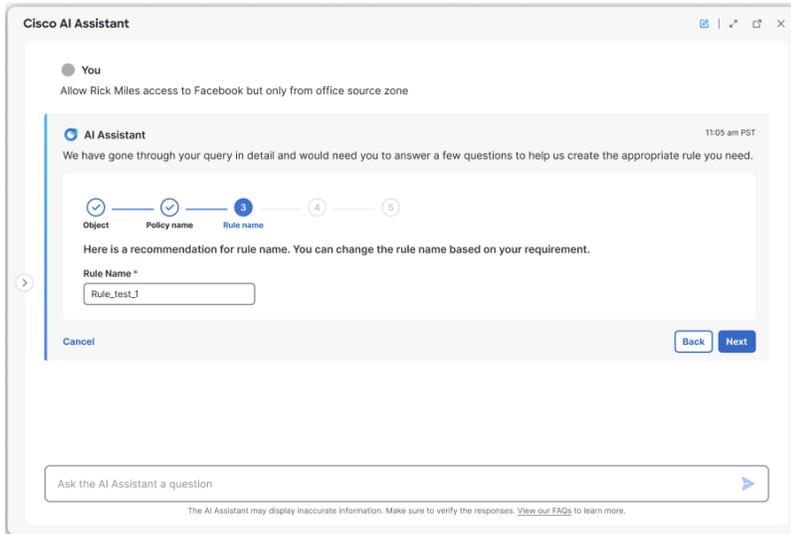
단계 3 AI Assistant는 Facebook에 대한 여러 결과를 찾고 관리자에게 Facebook을 애플리케이션, URL 또는 영역으로 참조하는지 확인하도록 요청합니다.



단계 4 AI Assistant는 규칙을 추가할 정책을 선택하라는 메시지를 관리자에게 표시합니다.

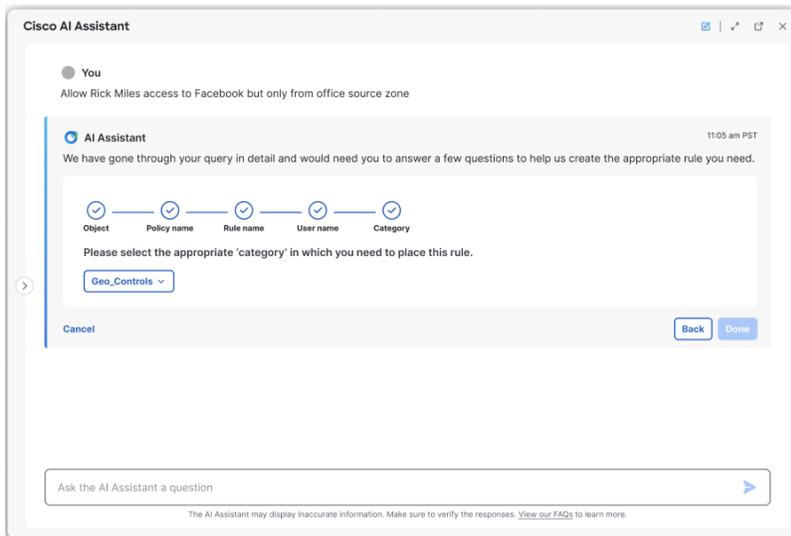


단계 5 AI Assistant는 "규칙 이름"을 제안하며, 필요한 경우 관리자가 수정할 수 있습니다.

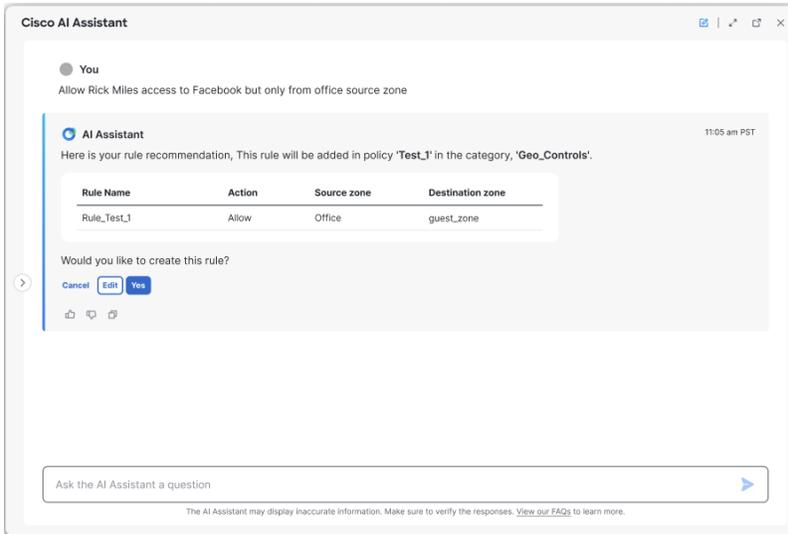


참고  
관리자가 정책에 이미 있는 "규칙 이름"을 선택하는 경우, 관리자에게 새 이름을 입력하라는 오류 메시지가 표시됩니다.

단계 6 AI Assistant는 관리자에게 규칙의 "사용자 이름"과 "범주"를 선택하라는 메시지를 표시합니다.



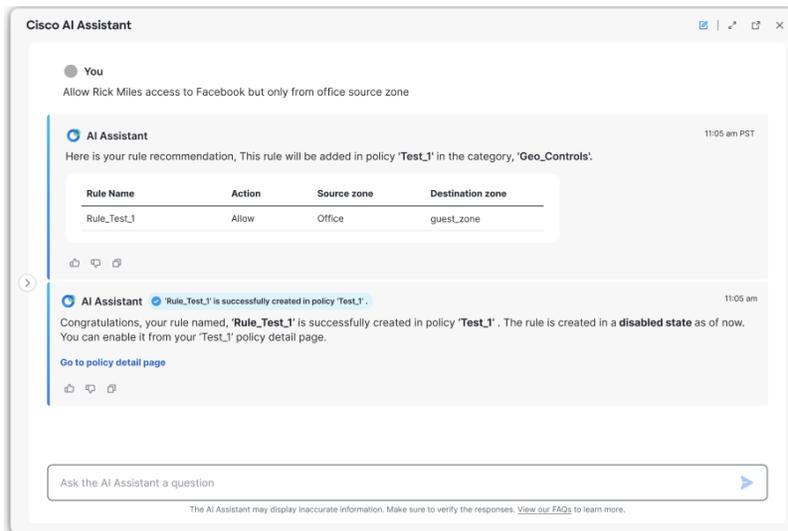
단계 7 AI Assistant는 규칙 생성에 대한 확인을 요청하고, 규칙에 대한 입력과 함께 관리자의 요청에 대한 요약을 제공합니다.



참고

관리자는 **Edit(편집)**를 클릭하여 규칙 정보를 편집하고 **Cancel(취소)**을 클릭하여 규칙 생성 프로세스를 취소할 수 있습니다.

**단계 8** 관리자가 규칙 생성에 대해 "Yes(예)"라고 확인한다고 가정하면, 규칙이 생성되고 관리자가 선택한 정책에 반영됩니다.



참고

정책 규칙을 생성할 수 없는 경우 [Cisco AI Assistant FAQ\(자주 묻는 질문\)](#), 41 페이지의 내용을 참조하십시오.

## 지원 문의

AI Assistant는 티켓 생성 및 관리 프로세스를 간소화하여 관리자가 지원 요청을 효율적이고 효과적으로 처리할 수 있도록 합니다. 이 통합을 통해 관리자는 해결되지 않은 문제가 발생하거나 AI의 권장 사항 이외의 추가 지원이 필요한 경우 AI Assistant를 통해 직접 지원 케이스를 생성할 수 있습니다.

주요 기능은 다음과 같습니다.

- 자동화된 티켓 생성: AI Assistant는 해결 방법으로 문제가 해결되지 않는 경우 지원 티켓 생성을 자동으로 제안합니다. 관리자는 간단한 프롬프트를 사용하여 수동으로 티켓을 만들 수도 있습니다.
- 티켓 관리: 관리자는 AI Assistant 내에서 티켓의 상태를 추적하고 "종료"에 대한 상태를 업데이트할 수 있습니다.

티켓 생성 및 관리를 AI Assistant에 통합함으로써 조직에서는 문제 해결에 소요되는 지연을 줄이고, 지원팀과 함께 지원 케이스를 생성하고, 문제 해결의 전반적인 효율성을 높일 수 있습니다.

---

CDO 및 클라우드 제공 Firewall Management Center를 사용 중인 고객만 AI Assistant를 통해 지원에 문의할 수 있습니다.

---

### 지원 사례 열기

AI Assistant는 대화의 컨텍스트에 따라 지원 티켓을 생성합니다. 이 지원 케이스는 **Support Case Manager**(지원 케이스 관리자)에서 생성되며 티켓 세부 정보가 사용자와 공유됩니다.

아래 단계에 따라 관리자는 AI Assistant를 통한 지원 티켓을 빠르고 원활하게 생성할 수 있습니다.

1. 테넌트의 대시보드로 이동하여 오른쪽 상단에 있는 AI Assistant 아이콘을 클릭합니다.
2. 텍스트 상자에 쿼리/문제를 입력하여 대화를 시작합니다.
3. AI Assistant는 제시된 문제를 기반으로 문제 해결 단계 또는 솔루션을 제안합니다.
4. AI Assistant의 권장 솔루션으로 문제가 해결되지 않거나 추가 도움이 필요한 경우 어시스턴트에서 **Open a Case**(케이스 열기) 프롬프트를 표시합니다.

"지원 케이스 생성"을 입력하여 지원 케이스 생성을 수동으로 요청할 수도 있습니다.

5. AI Assistant가 케이스를 생성하고 케이스 세부 정보를 제공합니다.




---

참고 참조용 케이스 번호가 포함된 확인 이메일이 전송됩니다.

---

## 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'll create a Technical Assistance 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 description 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.

**팁 샘플 프롬프트:**

- 방화벽의 문제를 보고해야 합니다.
- 지원 티켓을 여는 데 도움을 줄 수 있나요?
- 이 문제를 지원팀으로 에스컬레이션해 주세요.
- 이 제품에 대한 이의를 제기하려면 어떻게 해야 하나요?
- 방화벽의 오작동에 대해 문의해야 합니다.
- 이 제품 사용에 문제가 있어 케이스를 열어야 합니다.

**지원 케이스 관리**

관리자는 AI Assistant를 통해 지원 케이스를 신속하게 확인하고 업데이트할 수 있습니다. 지원 티켓의 상태는 다음과 같을 수 있습니다.

- **케이스 나열:** AI Assistant는 테넌트에 대해 열린 케이스 및 종료된 케이스를 모두 나열할 수 있습니다.
- **닫기:** 문제가 해결된 후 지원 케이스를 해결된 것으로 표시합니다.
- **검색:** 검토 또는 참조를 위해 기존 지원 케이스의 세부 사항에 액세스합니다.

**지원 케이스 목록**

관리자는 AI Assistant를 사용하여 테넌트 내에서 이전에 생성된 모든 지원 케이스의 포괄적인 목록에 쉽게 액세스할 수 있습니다. 어시스턴트에게 과거 케이스를 검색해달라고 요청하기만 하면, 관리자는 각 케이스의 케이스 번호, 상태, 설명 및 기타 필수 세부 정보를 볼 수 있습니다.

케이스를 검색하려면 다음을 수행합니다.

1. 텍스트 상자에서 AI Assistant로 이동하여 AI Assistant에 지원 케이스 목록을 검색하도록 요청합니다.
2. 또는 **Support Case Manager**(지원 케이스 관리자) 섹션에서 직접 케이스 목록을 검색할 수 있습니다.

**팁 샘플 프롬프트:**

- 지원 케이스 기록을 알고 싶습니다.
- 얼마나 많은 지원 케이스가 있나요?

**지원 케이스 상태**

관리자는 AI Assistant를 통해 지원 케이스의 상태를 확인할 수 있습니다.

1. 텍스트 상자에서 AI Assistant로 이동하여 AI Assistant에 지원 케이스의 상태를 검색하도록 요청합니다.
2. 또는 **Support Case Manager**(지원 케이스 관리자) 섹션에서 직접 티켓의 진행 상황을 추적할 수 있습니다.



팁 샘플 프롬프트:

- 지원 케이스 상태를 알고 싶습니다.
- 내 케이스의 상태는 어떤가요?

지원 케이스 종료

관리자는 AI Assistant를 통해 지원 케이스를 종료할 수 있습니다.

케이스를 종료하려면 다음을 수행합니다.

1. AI Assistant로 이동하고 텍스트 상자에서 AI Assistant에 케이스를 종료하도록 요청합니다.
2. 또는 지원 케이스 관리자 섹션에서 직접 티켓을 종료할 수도 있습니다.



팁 샘플 프롬프트:

- 케이스를 종료하고 싶습니다.
- 티켓을 종료하려면 어떻게 하나요?

## 알림 센터

Cisco AI Assistant의 알림 시스템은 보안 환경의 중요한 작업, 업데이트 및 변경 사항을 관리자에게 계속 알려줄 수 있도록 설계되었습니다. 사용자는 실시간 알림 및 예약된 알림을 활용하여 보안 사고를 사전에 관리하고 정책을 최적화 할 수 있습니다.

알림은 테넌트 대시보드의 오른쪽 상단에 있는 AI Assistant 아이콘을 통해 액세스합니다. 새 알림을 사용할 수 있으면 아이콘에 숫자 표시기가 나타나 읽지 않은 총 항목 수를 나타냅니다.

아이콘을 클릭하면 모든 알림의 포괄적인 목록을 볼 수 있는 알림 센터가 열립니다. 목록은 **Read**(읽음), **Unread**(읽지 않음) 등의 상태와 **Severity**(심각도)를 기준으로 쉽게 필터링할 수 있습니다. 따라서 중요한 작업의 우선 순위를 지정하고 최신 상태를 유지할 수 있습니다.

알림의 기본 상태는 읽지 않음입니다. 관리자는 알림을 읽음으로 표시하고 필요에 따라 알림을 삭제할 수 있습니다.

알림은 다음에 대해 트리거됩니다.

- 정책 분석기 및 최적화기: AI Assistant는 테넌트 내의 정책을 일상적으로 스캔하고 최적화를 위한 권장 사항을 제공합니다. 스캔 결과가 제공되면 어시스턴트가 시스템 생성 알림을 통해 사용자에게 알려 적시에 인식하고 조치를 취하도록 보장합니다.
- 정책 규칙 생성: 정책 규칙 생성을 시작하면 규칙은 초기에 기본적으로 "비활성화"로 설정되므로 수동으로 활성화해야 합니다. 규칙이 성공적으로 활성화되면 AI Assistant에서 알림을 보냅니다.



## 6 장

# Cisco AI Assistant FAQ(자주 묻는 질문)

- Q.** Cisco AI Assistant는 무엇입니까?
- A.** Cisco AI Assistant는 Secure Firewall Threat Defense 디바이스의 기존 구성과 Firepower Management Center 및 클라우드 제공 Firewall Management Center에서 해당 디바이스를 관리하는 방법에 대한 질문에 답변하는 애플리케이션입니다.
- Q.** AI Assistant가 무엇을 도와드릴까요?
- A.**
- AI Assistant는 Secure Firewall Threat Defense 디바이스를 구성하는 방법에 대한 질문에 답변합니다.
  - AI Assistant는 액세스 제어 및 기타 보안 정책을 구성하는 방법에 대한 질문에 대한 답변입니다.
  - AI Assistant는 구성을 간소화하여 빠르고 쉽게 정책 규칙을 구축할 수 있습니다.
  - AI Assistant는 방화벽 관련 문제 해결을 진단하고 해결하는 데 도움이 됩니다.
- Q.** AI Assistant에 어떻게 액세스합니까?
- A.** AI Assistant는 CDO Firewall Management Center 및 클라우드 제공 Firewall Management Center와 통합됩니다. AI Assistant에 액세스하려면 CDO 또는 클라우드 제공 Firewall Management Center 홈 페이지에서 AI Assistant 버튼()을 클릭합니다.
- Q.** 응답이 잘못된 경우 어떻게 해야 합니까?
- A.** 잘못된 정보를 보고하려면 Feedback(피드백) 옵션을 클릭하십시오.
- Q.** AI Assistant에 질문하려면 어떻게 합니까?
- A.** CDO 또는 클라우드 제공 Firewall Management Center 홈 페이지에서 AI Assistant 버튼()을 클릭하고 질문 텍스트 상자에 질문을 입력하십시오.
- Q.** 어떤 주제에 대해 질문할 수 있습니까?
- A.** 구성된 방화벽 디바이스, 정책, 설정에 대해 AI Assistant에게 질문할 수 있습니다. 방화벽을 구성하는 방법에 대해 질문하십시오.
- Q.** Cisco AI Assistant는 안전합니까?
- A.** 예. CDO 테넌트에 구현된 Cisco AI Assistant는 테넌트 및 클라우드 제공 Firewall Management Center에 대한 정보 및 보안 정책에만 액세스 할 수 있습니다(해당 기능을 구현한 경우). AI Assistant

는 다른 CDO 테넌트의 정책에 대해 "학습"할 수 없으므로, 다른 CDO 테넌트에 대한 질문에 답변하거나 정보를 통합할 수 없습니다.

**Q.** Cisco의 개인정보 보호정책은 무엇입니까?

**A.** 이는 Cisco Trust Center에 게시되는 [Cisco의 온라인 개인정보 보호정책](#)입니다.

**Q.** AI Assistant를 사용하여 규칙을 생성할 수 있습니까?

**A.** 예, AI Assistant를 사용하여 규칙을 생성할 수 있습니다. AI Assistant는 규칙 생성 프로세스를 안내하는 간단한 프롬프트가 포함된 사용자 친화적 인터페이스를 제공합니다. 정확성과 효율성을 보장하므로 워크플로우 내에서 정책 규칙을 원활하게 통합하고 관리할 수 있습니다.

**Q.** AI Assistant에서는 어떤 유형의 규칙을 지원합니까?

**A.** 현재 AI Assistant는 액세스 제어 정책 규칙을 지원합니다. 허용, 차단, BLOCK\_RESET 규칙을 생성할 수 있습니다. 관리자는 테넌트의 액세스 규칙 정책에 대한 구체적인 세부 정보를 요청할 수 있습니다.

**Q.** AI Assistant가 규칙을 생성할 수 없습니다. 이 문제를 어떻게 해결합니까?

**A.** AI Assistant에서 정책 규칙을 생성할 수 없습니다.

- 개체를 찾을 수 없음: AI Assistant는 테넌트 내에서 지정된 개체 이름을 찾을 수 없는 경우 관리자에게 개체 이름을 확인하고 다시 시도하라는 프롬프트가 표시됩니다. 어시스턴트에게 정확한 개체 이름을 포함하는 업데이트된 프롬프트를 제공하는 것이 좋습니다.
- 불안정한 요청: AI Assistant에서 규칙을 생성하려면 완전하고 정확한 정보가 필요합니다. 이해를 돕기 위해 아래 표를 참조하십시오.

사용자가 제공한 개체	필수 개체 (규칙 생성을 위한 더 나은 컨텍스트를 <b>AI Assistant</b> 에 제공하려면 사용자는 이러한 개체 중 하나 이상을 제공해야 합니다.)
<b>A.</b> <ul style="list-style-type: none"> <li>• 소스 영역</li> <li>• 소스 네트워크</li> <li>• 소스 동적 속성</li> </ul>	<ul style="list-style-type: none"> <li>• 대상 영역</li> <li>• 대상 네트워크</li> <li>• 대상 포트</li> <li>• 대상 동적 속성</li> <li>• 애플리케이션</li> <li>• URL</li> </ul>

사용자가 제공한 개체	필수 개체 (규칙 생성을 위한 더 나은 컨텍스트를 <b>AI Assistant</b> 에 제공하려면 사용자는 이러한 개체 중 하나 이상을 제공해야 합니다.)
사용자	<ul style="list-style-type: none"> <li>• 대상 영역</li> <li>• 대상 네트워크</li> <li>• 대상 포트</li> <li>• 대상 동적 속성</li> <li>• 애플리케이션</li> <li>• URL</li> </ul>
<ul style="list-style-type: none"> <li>• 대상 영역</li> <li>• 대상 네트워크</li> <li>• 대상 포트</li> <li>• 대상 동적 속성</li> </ul>	<ul style="list-style-type: none"> <li>• 소스 영역</li> <li>• 소스 네트워크</li> <li>• 소스 동적 속성</li> <li>• 사용자</li> <li>• 애플리케이션</li> <li>• URL</li> </ul>
<ul style="list-style-type: none"> <li>• 애플리케이션</li> <li>• URL</li> </ul>	<ul style="list-style-type: none"> <li>• 소스 영역</li> <li>• 소스 네트워크</li> <li>• 소스 동적 속성</li> <li>• 사용자</li> <li>• 대상 영역</li> <li>• 대상 네트워크</li> <li>• 대상 포트</li> <li>• 대상 동적 속성</li> </ul>

- Q.** Cisco AI Assistant for Firewall을 사용하려면 비용을 지불해야 합니까?
- A.** Cisco AI Assistant는 현재 고객 초기 평가를 무료로 제공하고 있습니다. 이 롤아웃 단계에서는 사용량이 무료입니다. 하지만 Cisco는 향후 이 제품을 GPL(일반 가격 목록)에 포함할 계획입니다.

GA 이후 Cisco는 고객이 계속 제품을 사용하려면 구독을 구매하도록 요구할 수 있는 권한을 갖고 있습니다.

- Q.** 위에 언급된 초기 고객 평가 기간 동안 특징 및 기능에 제한이 있습니까?
- A.** 아니요. 사용 가능한 기능 사용에 계획된 제한은 없습니다. 초기 가용성 기간 동안에는 제품의 모든 기능에 완전히 액세스할 수 있습니다. 그러나 Cisco는 사용 수준을 모니터링하고 단독 재량으로 이 평가 단계에서 특징을 추가 또는 제거할 뿐만 아니라 사용을 제한할 수 있습니다.
- Q.** 위에서 언급한 기간 이후에 제품에 대한 구독 및/또는 비용을 지불하지 않기로 선택하면 어떻게 됩니까?
- A.** 구독하지 않을 경우, 방화벽용 Cisco AI Assistant에 대한 액세스가 Cisco 정책에 따라 제한되거나 중단됩니다. 구독은 언제든지 다시 활성화할 수 있습니다.
- Q.** Cisco AI Assistant가 마지막으로 업데이트된 시간은 언제입니까?
- A.** AI Assistant는 설명서 변경 사항과 함께 매주 업데이트됩니다.

CDO에서 AI Assistant는 디바이스 및 테넌트에 적용한 정책 및 구성 변경으로 24시간마다 업데이트됩니다.

클라우드 제공 Firewall Management Center에서 AI Assistant가 디바이스 및 테넌트에 대해 수행한 정책 및 구성 변경 사항으로 24시간마다 업데이트됩니다. 또한 이 질문에 대한 답변에는 마지막 데이터 동기화가 발생한 시간도 포함되어 있습니다.

## 번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.