FTD의 Syslog를 사용하여 Splunk에서 맞춤형 대시보드 및 경고 생성

목차

소개

이 문서에서는 Splunk에 syslog를 전송하도록 FTD를 구성하고 이러한 로그를 사용하여 사용자 지정 대시보드 및 알림을 구축하기 위한 단계별 연습을 설명합니다.

사전 요구 사항

요구 사항

이 컨피그레이션 가이드를 진행하기 전에 다음 항목에 대해 알고 있는 것이 좋습니다.

- Syslog
- Splunk의 SPL(Search Processing Language)에 대한 기본 지식

또한 이 문서에서는 서버에 Splunk Enterprise 인스턴스가 이미 설치되어 있고 웹 인터페이스에 액세스할 수 있다고 가정합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 버전 7.2.4에서 실행되는 Cisco FTD(Firepower Threat Defense)
- 버전 7.2.4에서 실행되는 Cisco FMC(Firepower Management Center)
- Windows 시스템에서 실행 중인 Splunk Enterprise 인스턴스(버전 9.4.3)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.

배경 정보

Cisco FTD 디바이스는 침입 이벤트, 액세스 제어 정책, 연결 이벤트 등에 대한 자세한 syslog를 생성합니다. 이러한 로그를 Splunk와 통합하면 네트워크 보안 운영을 위한 강력한 분석 및 실시간 알림이 가능합니다.

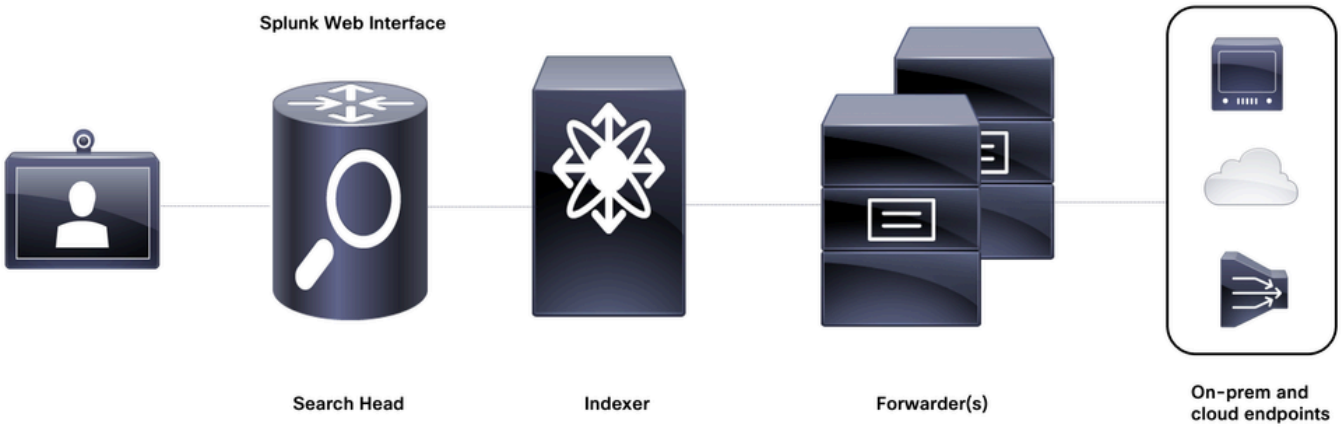
Splunk는 시스템에서 생성된 데이터를 수집, 인덱싱, 검색 및 시각화하기 위해 설계된 실시간 데이터 분석 플랫폼입니다. Splunk는 다음과 같은 기능을 통해 SIEM(Security Information and Event Management) 툴로서 사이버 보안 환경에서 특히 효과적입니다.

- 규모에 맞게 로그 데이터 수집
- SPL로 복합 검색 수행
- 대시보드 및 경고 생성
- 보안 오케스트레이션 및 사고 대응 시스템과 통합

Splunk는 비정형 또는 반정형 머신 데이터를 유용하고 실행 가능하도록 만들기 위해 정형 파이프라인을 통해 데이터를 처리합니다. 이 파이프라인의 주요 단계를 종종 IPIS라고 하며 이는 다음을 의미합니다.

- 입력
- 구문 분석
- 색인 지정
- 검색

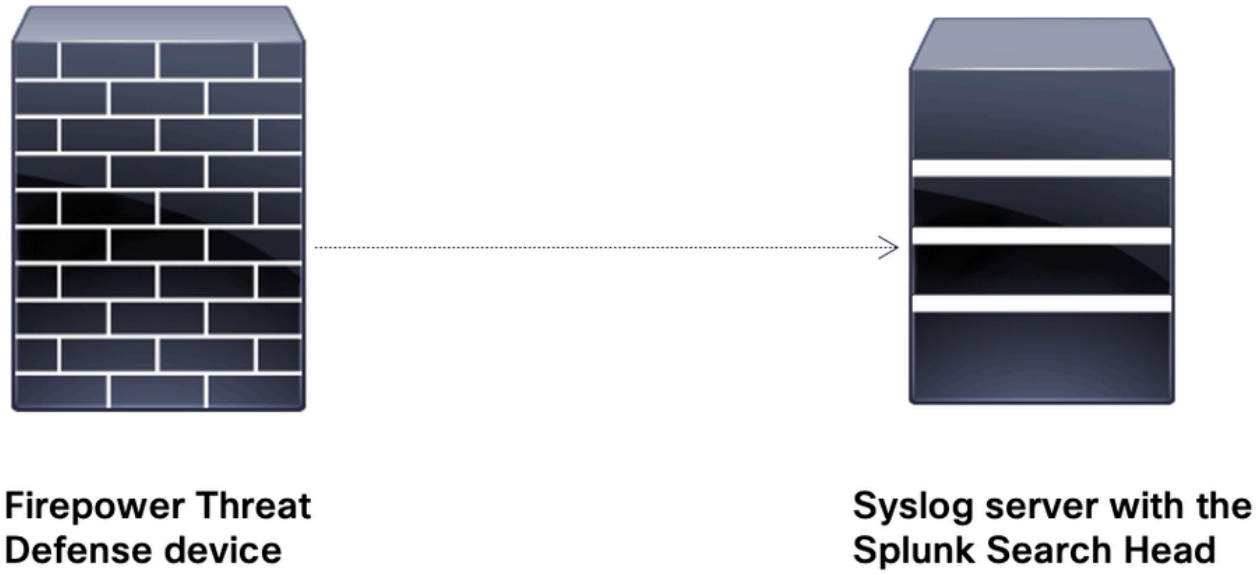
이 다이어그램에는 IPIS 파이프라인을 구현하는 데 사용되는 기본 아키텍처의 주요 구성 요소가 나와 있습니다.



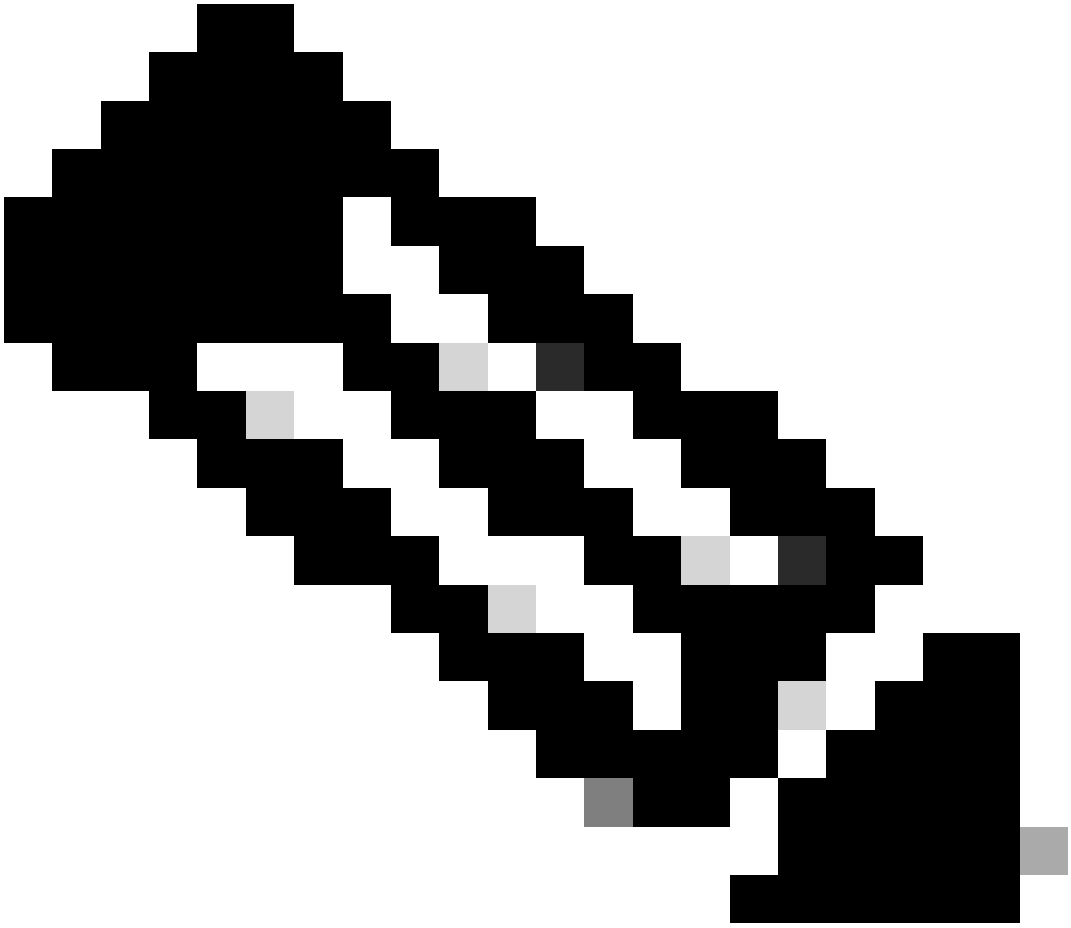
Splunk 기반 아키텍처

구성

네트워크 다이어그램



네트워크 다이어그램

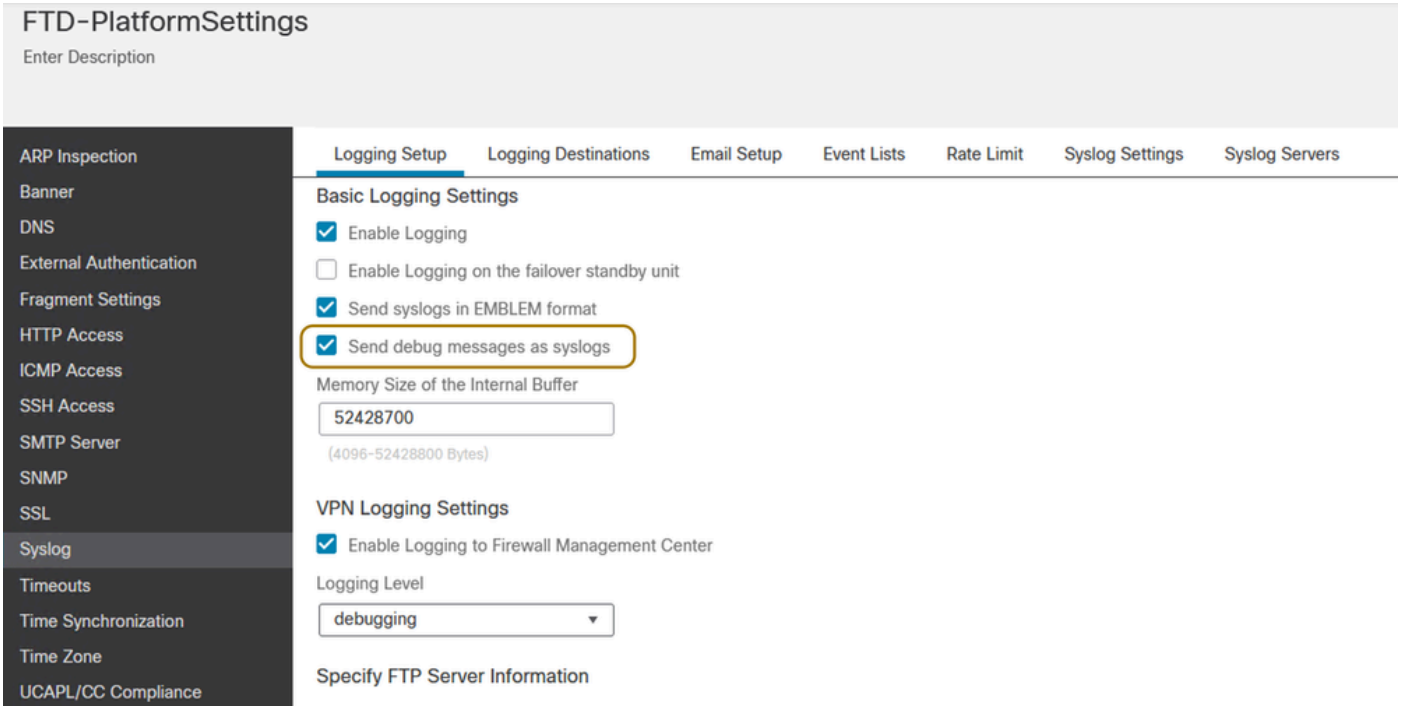


참고: 이 문서의 랩 환경에서는 별도의 전달자 및 인덱서 인스턴스가 필요하지 않습니다. Splunk Enterprise 인스턴스가 설치된 Windows 머신, 즉 syslog 서버는 인덱서 및 검색 헤드 역할을 합니다.

설정

FTD에 대한 Syslog 설정 구성

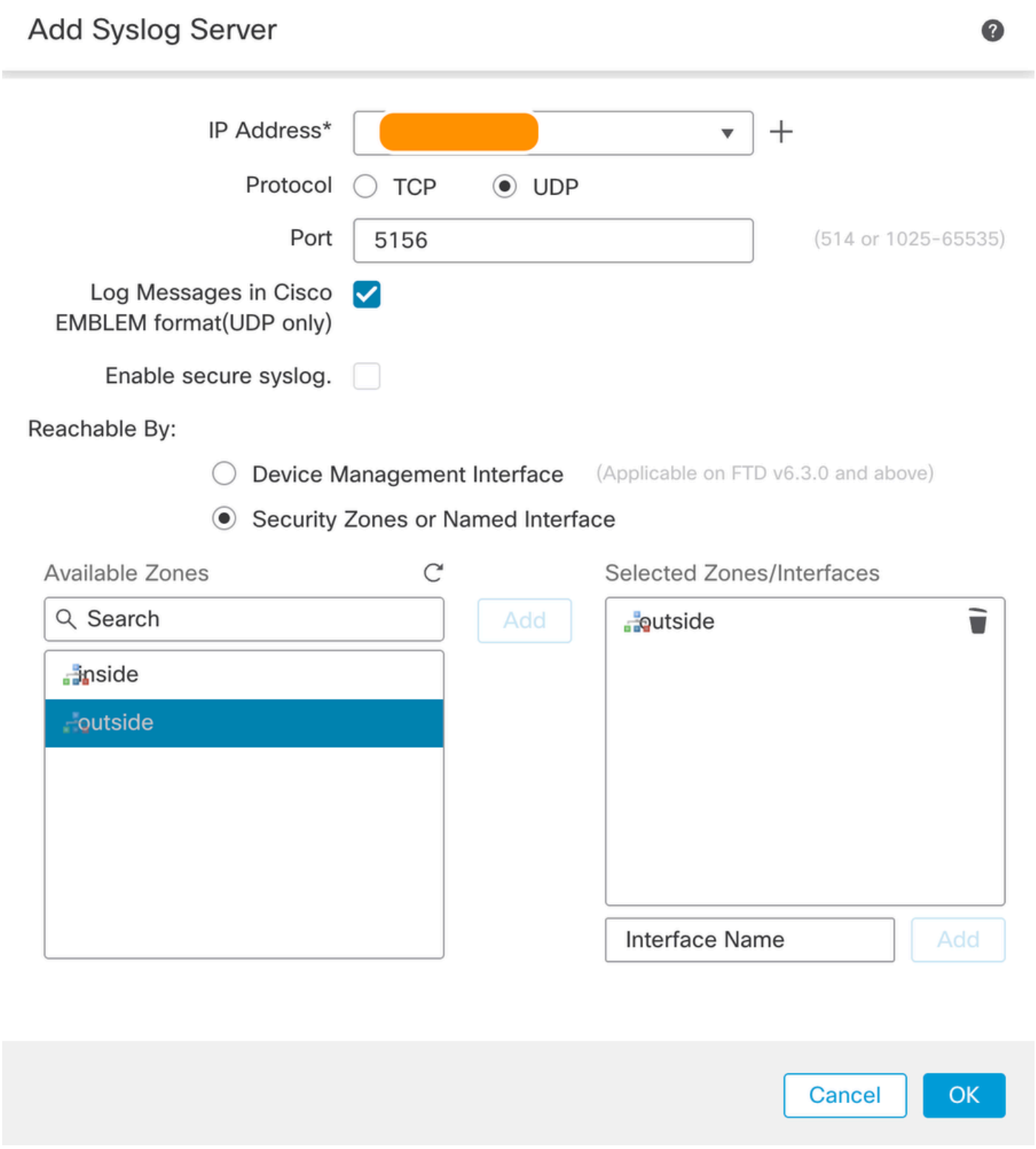
1단계. Splunk 인스턴스가 실행 중인 syslog 서버에 로그를 보내려면 Devices(디바이스) > Platform Settings(플랫폼 설정) 아래에서 FTD에 대한 FMC의 예비 syslog 설정을 구성합니다.



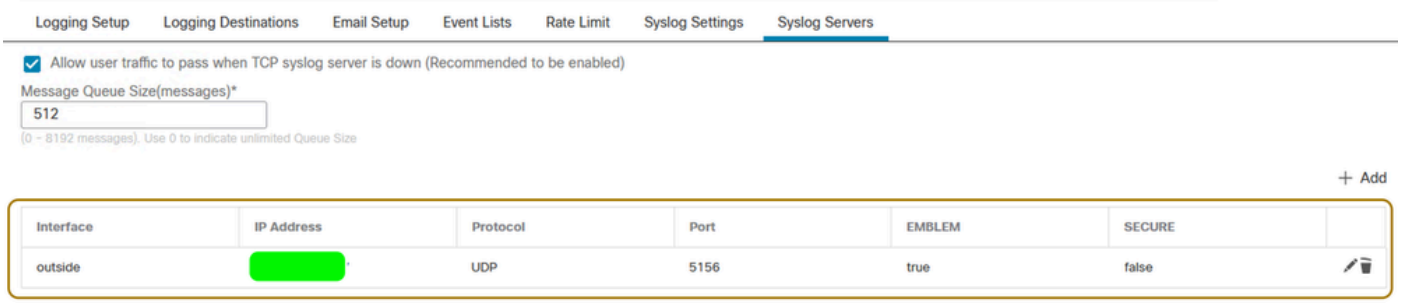
FTD의 플랫폼 설정 - Syslog

2단계. Splunk Enterprise 인스턴스가 설치되고 Syslog 서버로 실행되는 시스템의 IP 주소를 구성합니다. 해당 필드를 정의합니다.

```
IP Address: Fill in the IP address of the host acting as the syslog server
Protocol: TCP/UDP (usually UDP is preferred)
Port: You can choose any random high port. In this case 5156 is being used
Interface: Add the interface(s) through which you have connectivity to the server
```

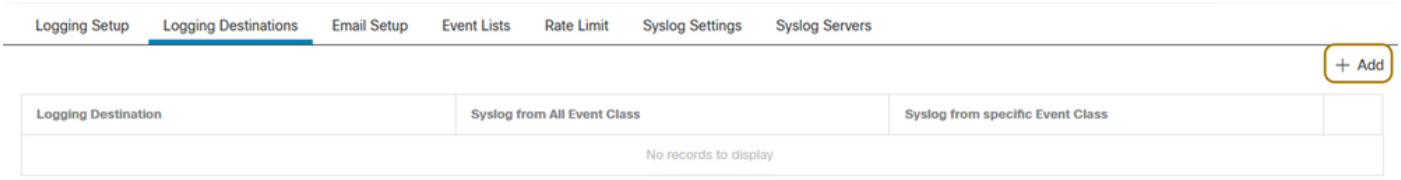


FTD의 플랫폼 설정 - Syslog 서버 추가

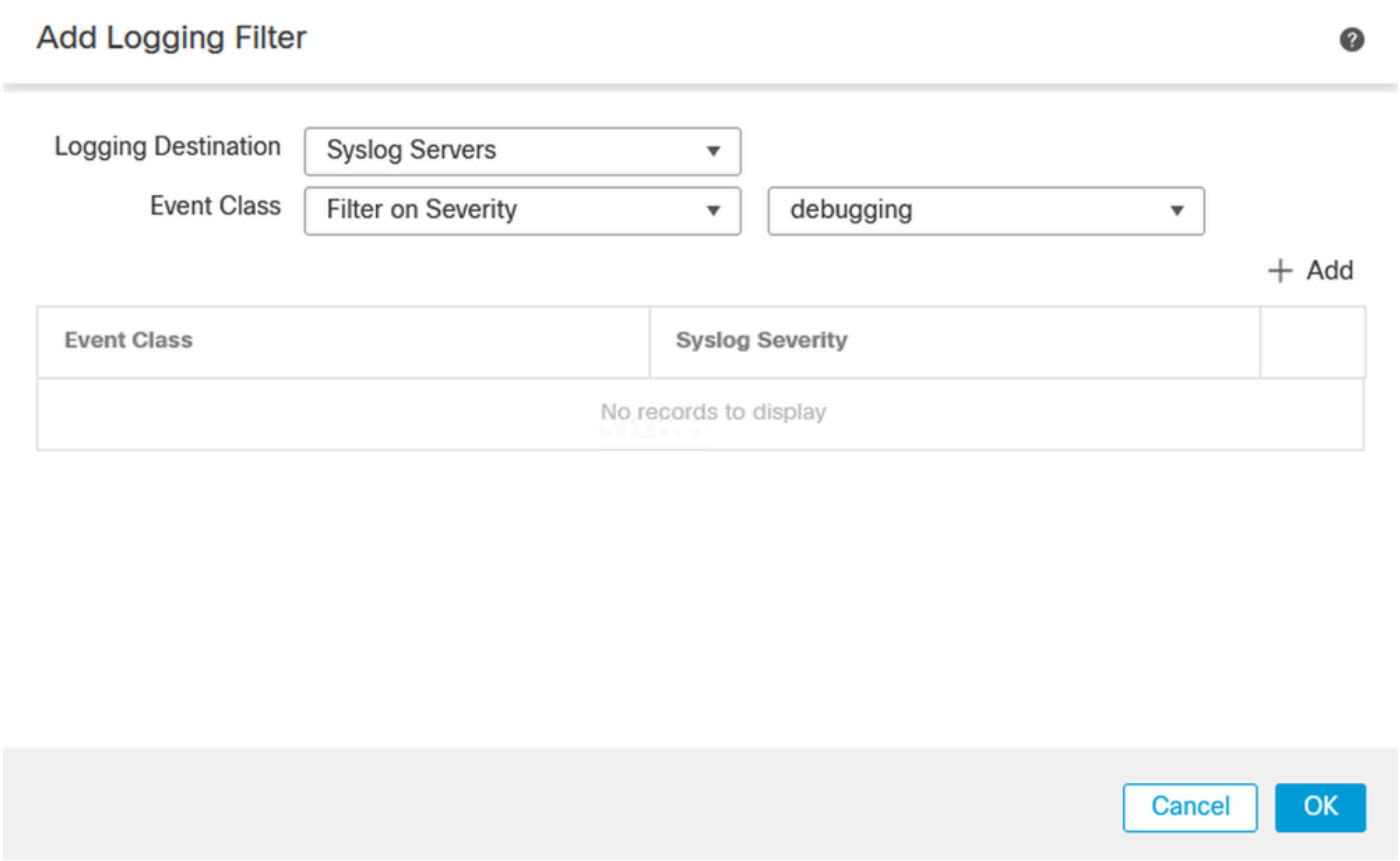


FTD의 플랫폼 설정 - Syslog 서버 추가됨

3단계. Syslog 서버에 대한 로깅 대상을 추가합니다. 로깅 레벨은 선택 또는 활용 사례에 따라 설정할 수 있습니다.



FTD의 플랫폼 설정 - 로깅 대상 추가



FTD의 플랫폼 설정 - 로깅 대상에 대한 심각도 수준 설정

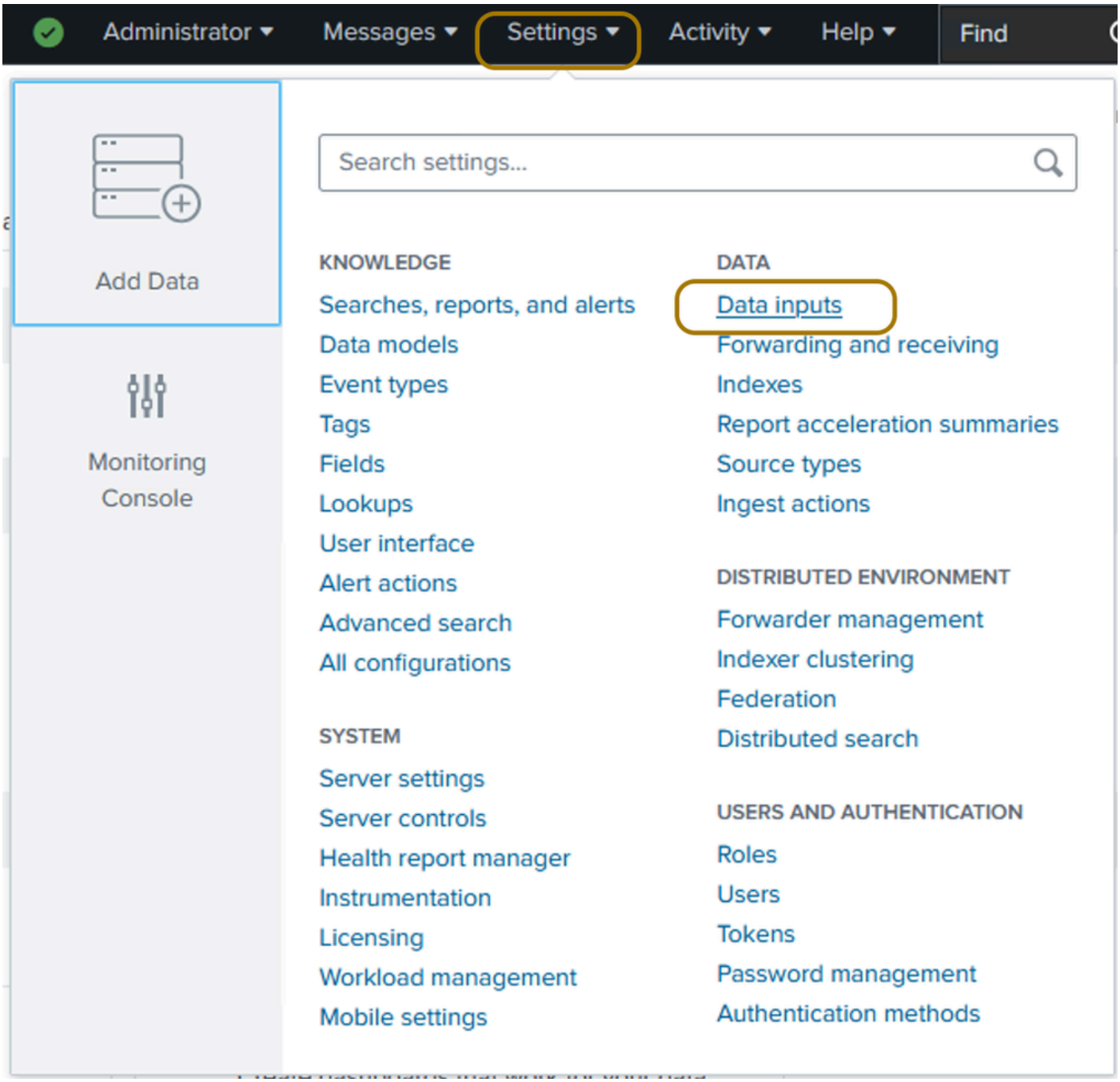
이 단계를 완료한 후 플랫폼 설정 변경 사항을 FTD에 배포합니다.

Splunk 엔터프라이즈 인스턴스에서 데이터 입력 구성

1단계. Splunk Enterprise 인스턴스 웹 인터페이스에 로그인합니다.

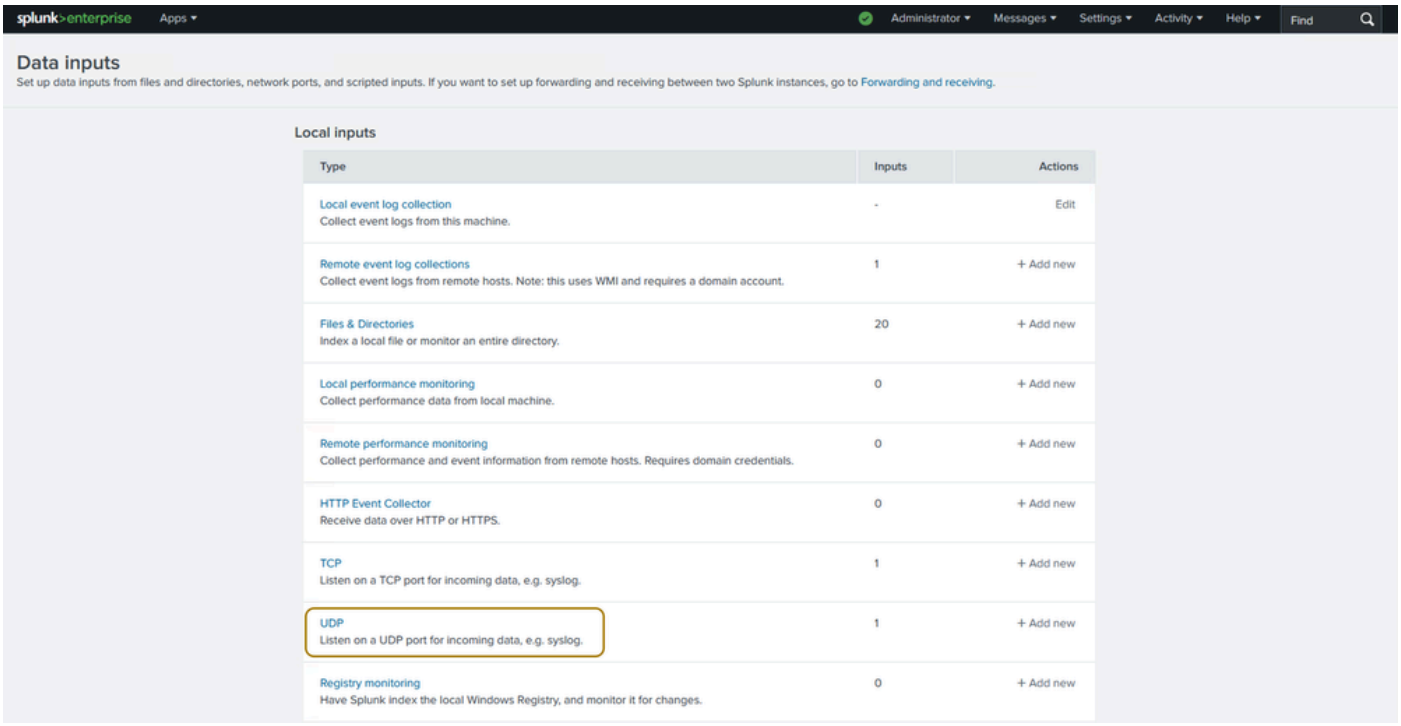
Splunk 웹 인터페이스 로그인 페이지

2단계. Splunk에 syslog를 저장하고 인덱싱할 수 있도록 데이터 입력을 정의해야 합니다. 로그인한 후 Settings(설정) > Data(데이터) > Data Inputs(데이터 입력)로 이동합니다.

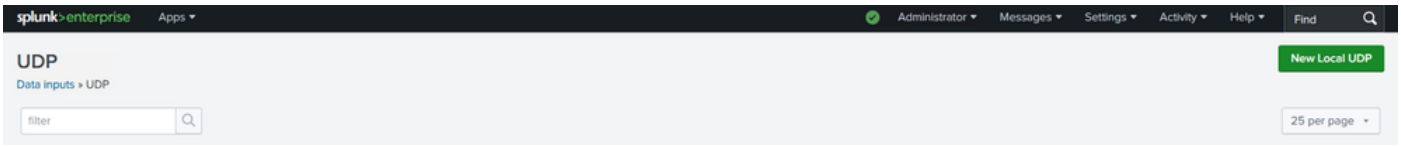


Splunk의 데이터 입력으로 이동

3단계. UDP를 선택한 다음 나타나는 다음 페이지에서 New Local UDP를 클릭합니다.

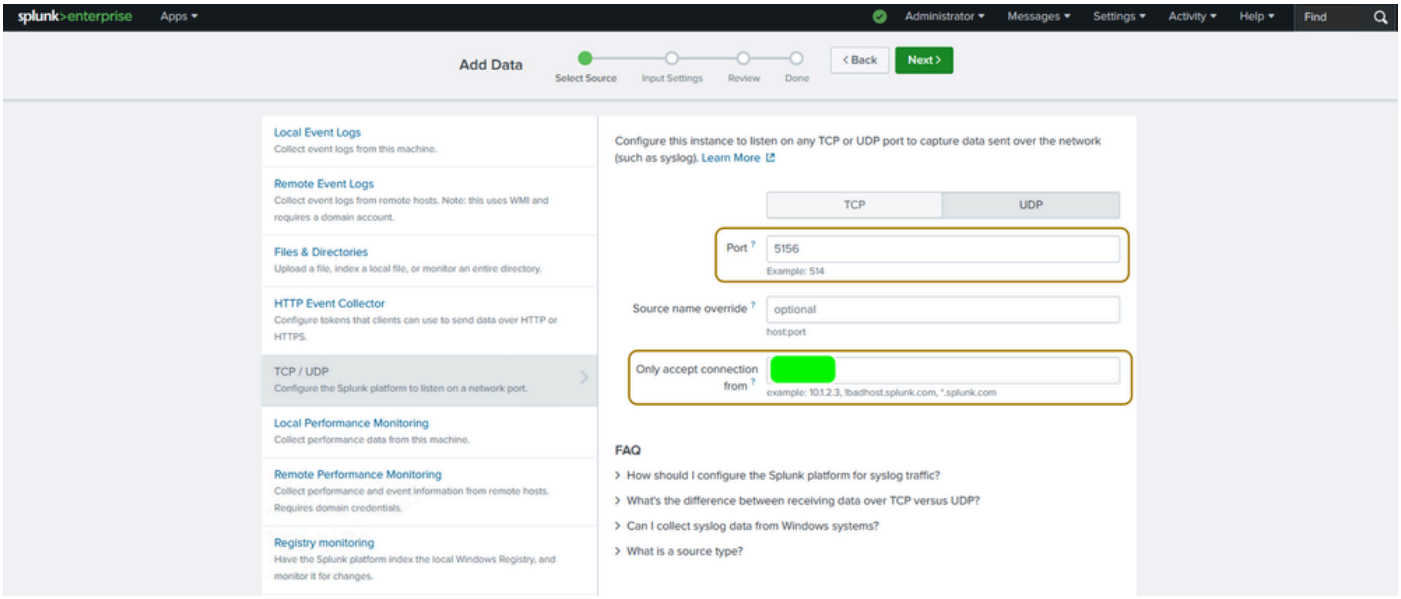


UDP 데이터 입력에 대해 'UDP'를 클릭합니다.



'새 로컬 UDP' 입력 만들기

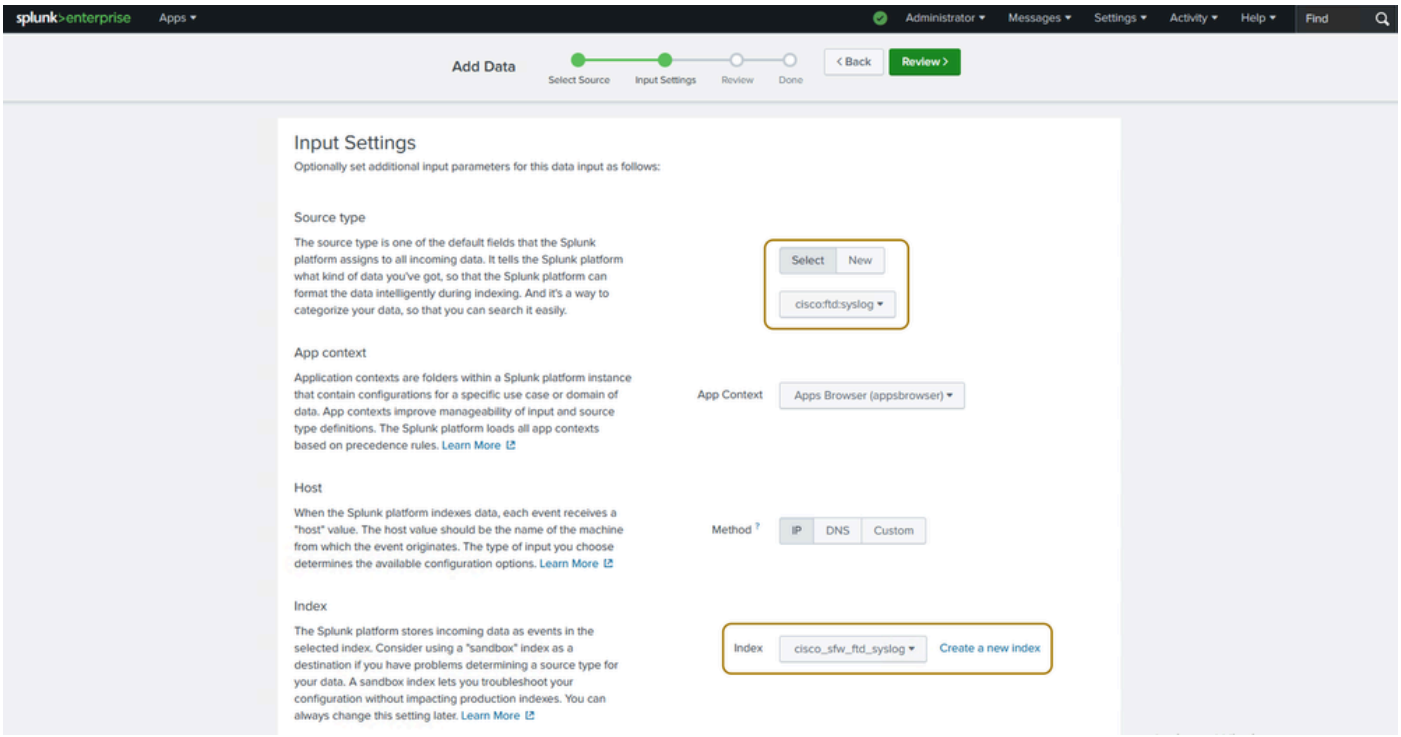
4단계. syslog가 전송되는 포트를 입력합니다. FTD syslog 설정에 구성된 포트(이 경우 5156)와 동일해야 합니다. 한 소스(FTD)의 syslog만 수락하려면 Only Accept Connection From 필드를 Splunk 서버와 통신하는 FTD의 인터페이스 IP로 설정합니다. Next(다음)를 클릭합니다.



포트 및 FTD IP 주소 지정

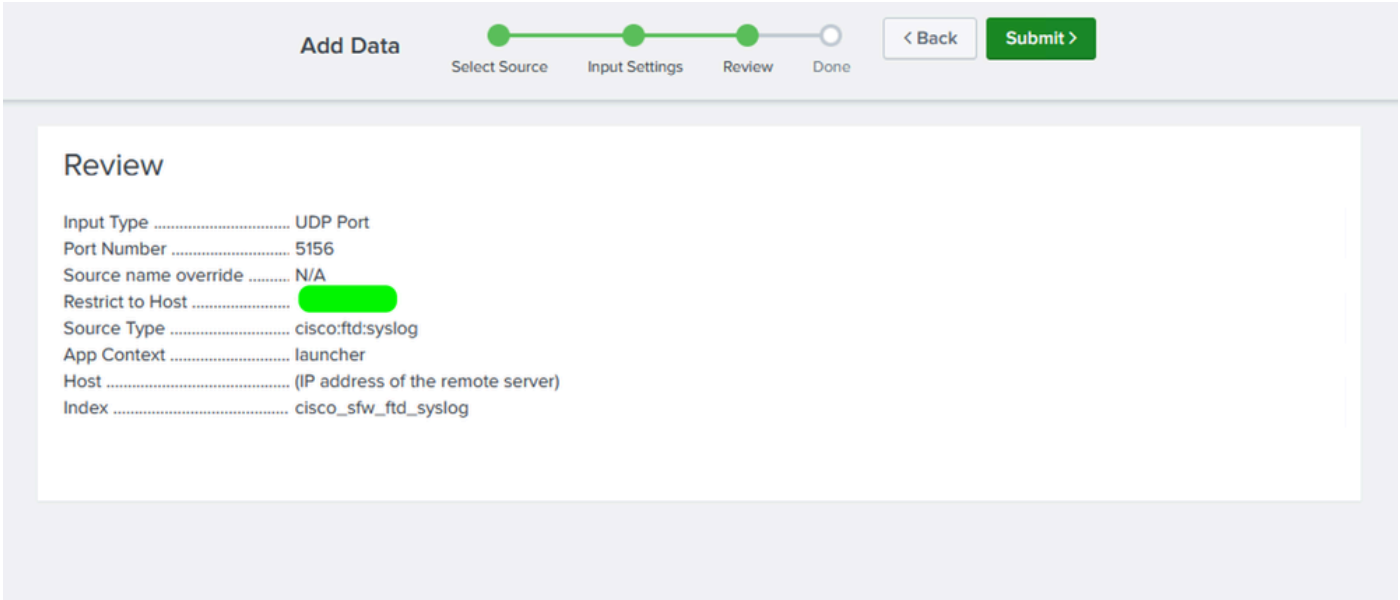
5단계. 다음 이미지에서 강조 표시된 대로 Splunk에 미리 정의된 소스 유형 및 인덱스 필드 값을 검

색하고 선택할 수 있습니다. 나머지 필드에는 기본 설정을 사용할 수 있습니다.



데이터 입력 설정 구성

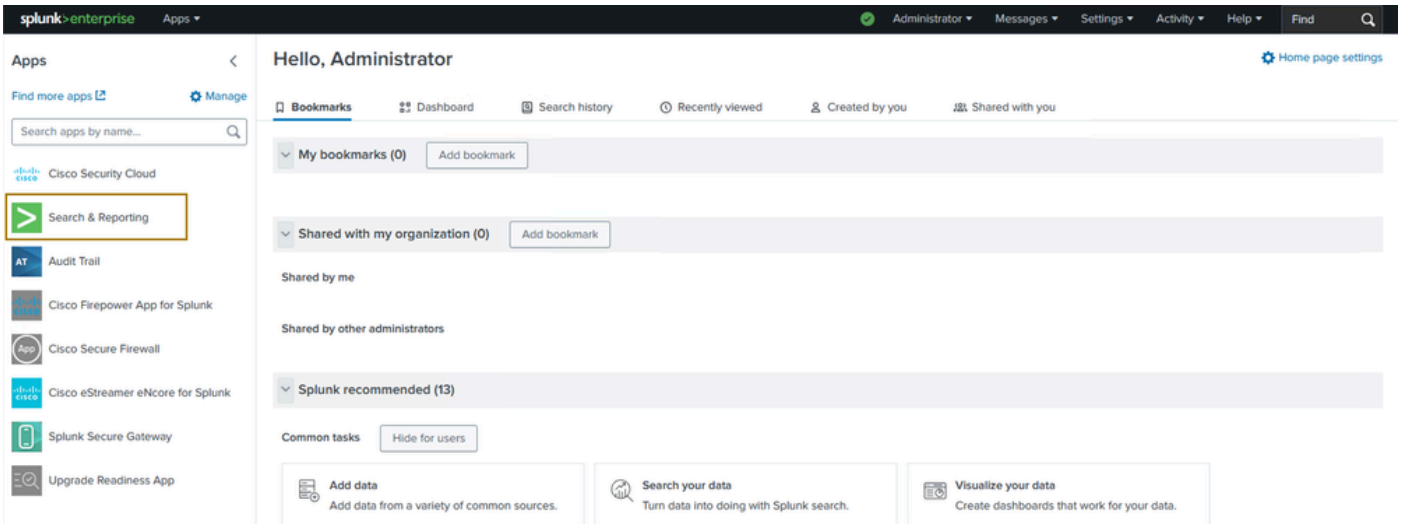
6단계. 설정을 검토하고 Submit(제출)을 클릭합니다.



데이터 입력 설정 검토

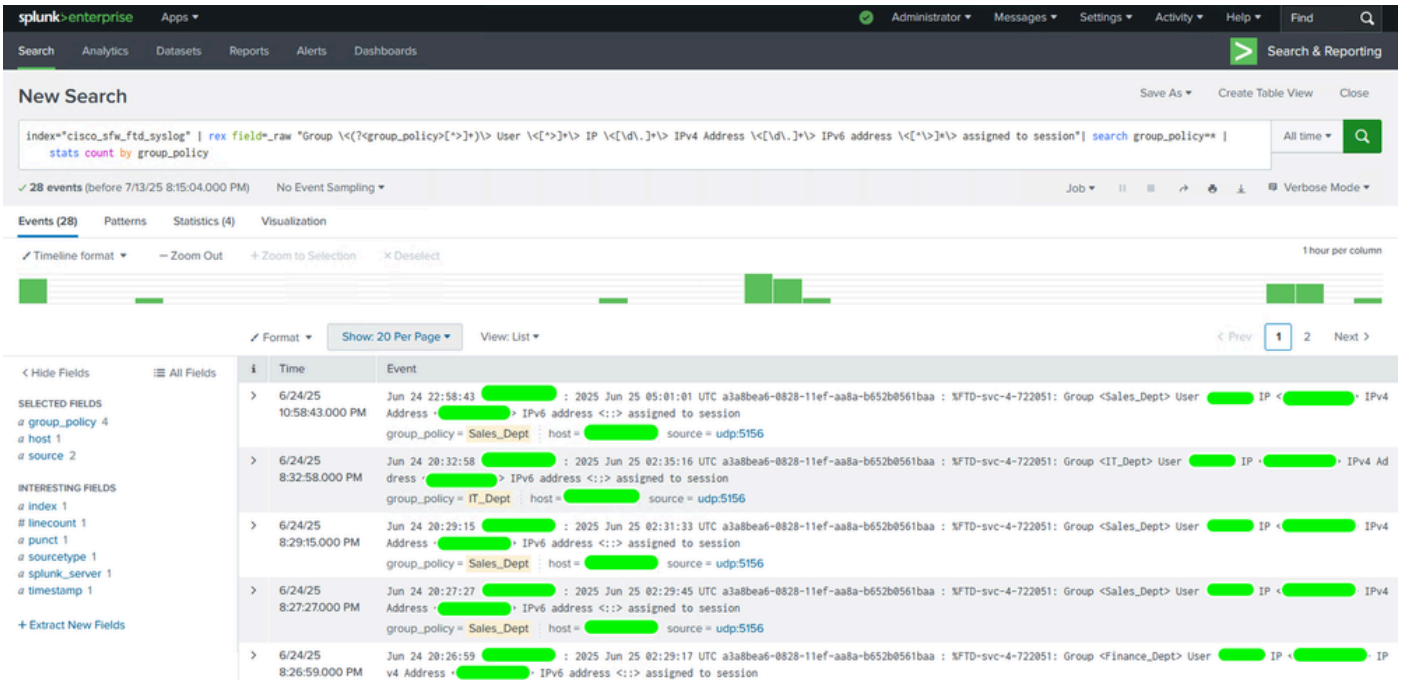
SPL 쿼리 실행 및 대시보드 생성

1단계. Splunk에서 Search and Reporting 앱으로 이동합니다.

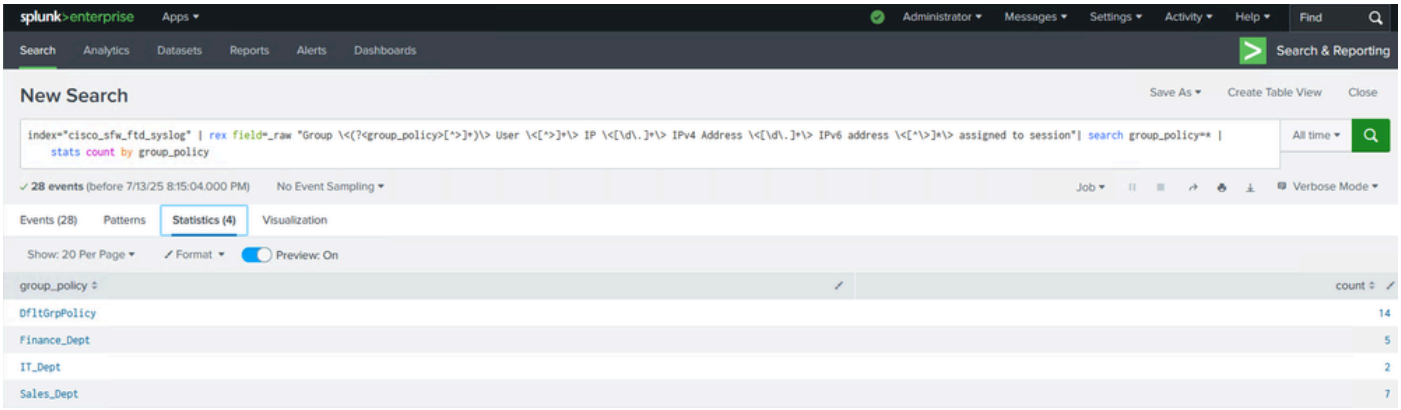


검색 및 보고 앱으로 이동

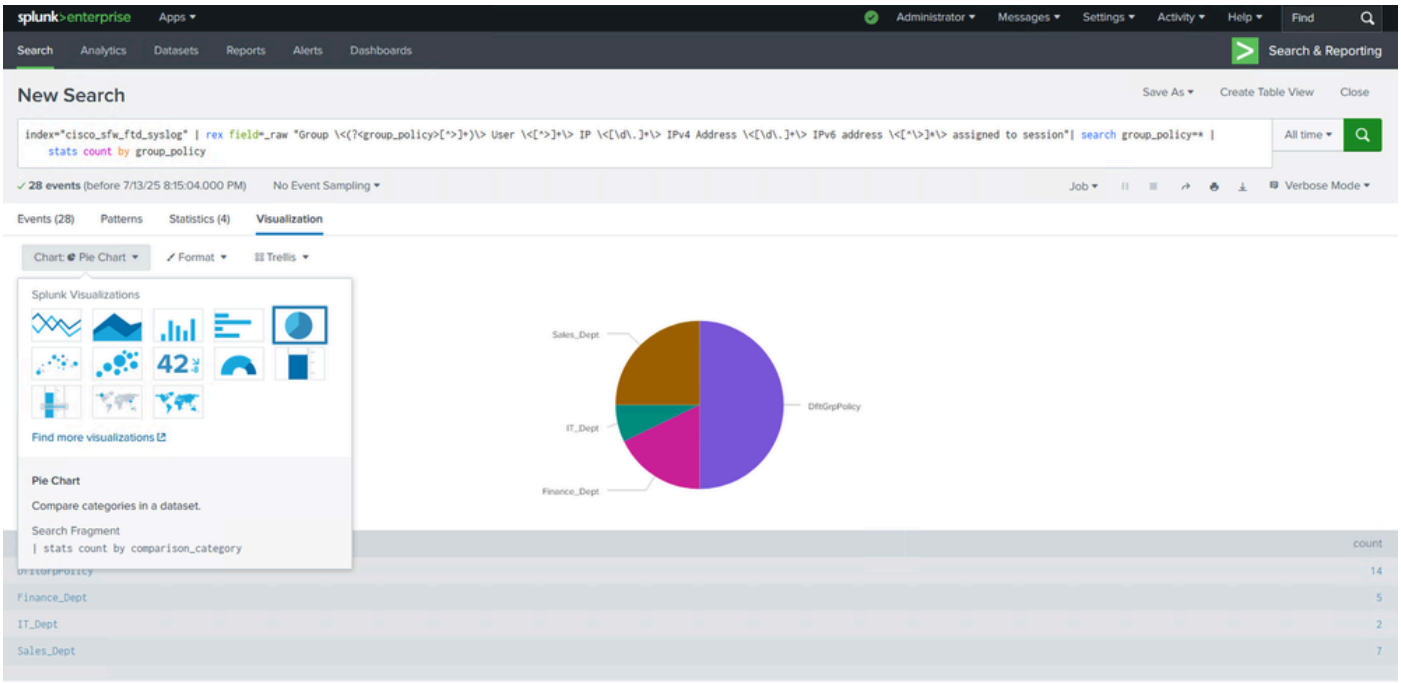
2단계. 시각화할 데이터에 따라 SPL 쿼리를 작성하고 실행합니다. Events(이벤트) 탭의 각 로그, Statistics(통계) 탭의 그룹 정책당 연결 수, 자세한 정보 표시 모드에서 각 로그를 완전히 확인하고 Visualization(시각화) 탭의 이러한 통계를 사용하여 이 데이터를 시각화할 수 있습니다.



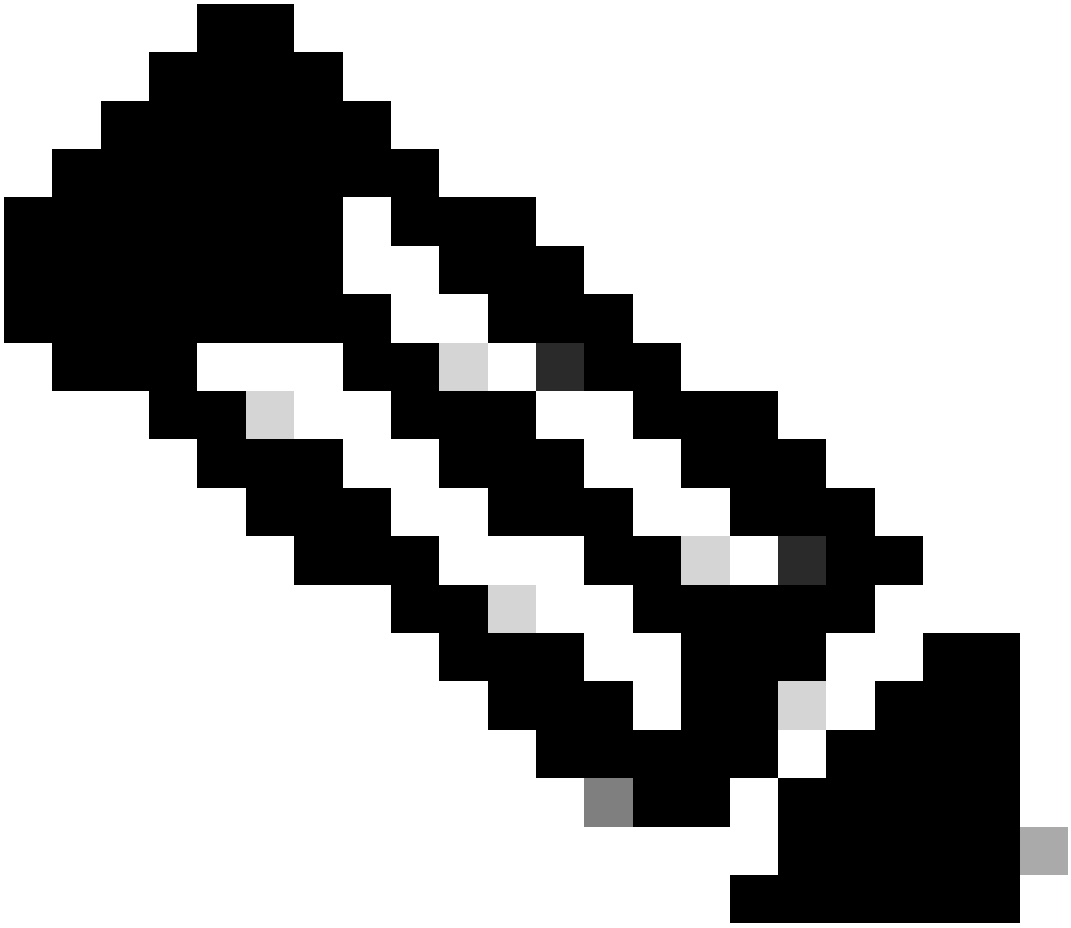
SPL 쿼리를 사용하여 이벤트 검색



Statistics(통계) 탭 확인

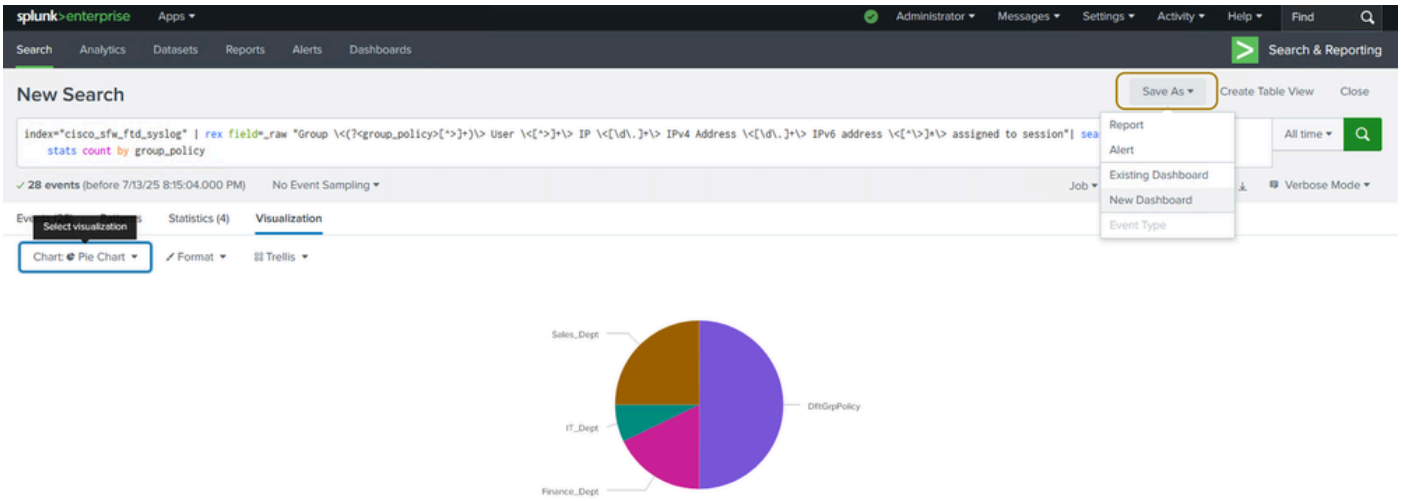


Visualization(시각화) 탭에는 그래프/차트가 표시됩니다.



참고: 이 예에서 쿼리는 서로 다른 그룹 정책 전반에서 성공적인 원격 액세스 VPN 연결을 위해 로그를 가져오는 중입니다. 그룹 정책당 성공한 연결의 수 및 백분율을 시각화하기 위해 파이 차트가 사용되었습니다. 요구 사항 및 환경 설정에 따라 막대 그래프와 같은 다른 유형의 시각화를 사용하도록 선택할 수도 있습니다.

3단계. 다른 이름으로 저장을 클릭하고 이 패널을 추가할 대시보드가 이미 있는지 아니면 새 대시보드를 생성할지 여부에 따라 신규 또는 기존 대시보드를 선택합니다. 이 예에서는 두 대시보드를 보여 줍니다.



대시보드에 패널 저장

4단계. 생성 중인 대시보드에 제목을 지정하고 원 그래프가 포함된 패널의 제목을 지정합니다.

Save Panel to New Dashboard

Dashboard Title: FTD_Dashboard

ftd_dashboard — Edit ID

Description: Optional

Permissions: Private

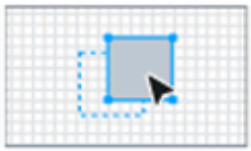
How do you want to build your dashboard? What's this?

Classic Dashboards
The traditional Splunk dashboard builder

Dashboard Studio NEW
A new builder to create visually-rich, customizable dashboards

Select layout mode

Absolute
Full layout control



Grid
Quick organization

Panel Title: Successful RAVPN Connections Per Group Policy

Visualization Type: Pie Chart | Statistics Table

> Advanced Panel Settings

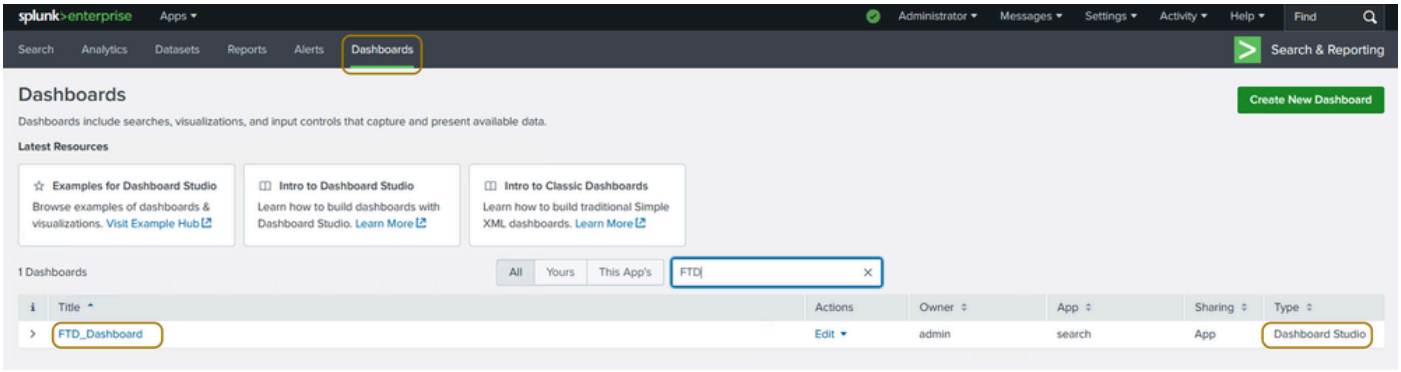
Cancel | Save to Dashboard

새 대시보드에 대한 설정

으로 설정할 수 있습니다. 또한 대시보드의 패널 설정과 레이아웃을 세부적으로 제어할지 여부에 따라 Classic(클래식) 또는 Dashboard Studio(대시보드 스튜디오) 모드를 선택하여 대시보드를 구성합니다.

5단계(선택 사항) 앞서 언급한 단계를 사용하여 요구 사항에 따라 더 많은 SPL 쿼리를 이 대시보드에 패널로 실행하고 저장합니다.

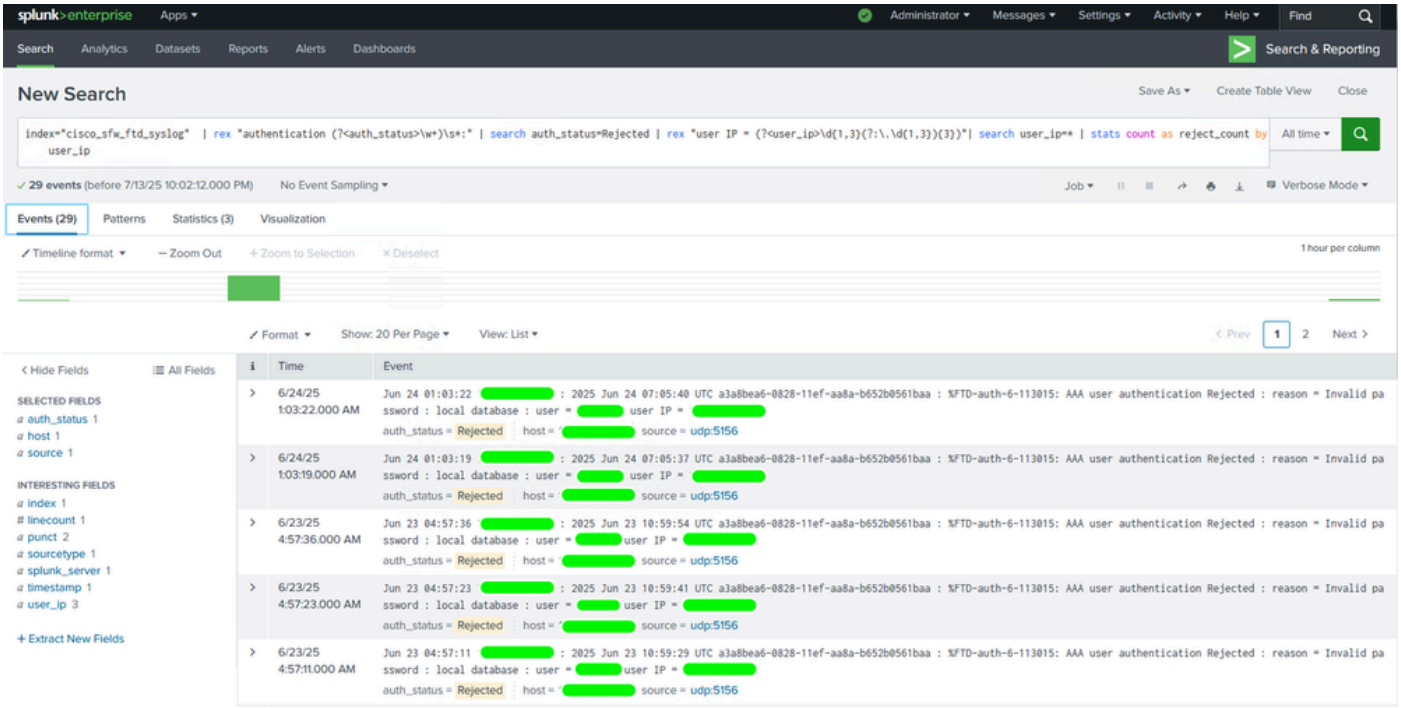
6단계. 생성한 대시보드를 검색하고 선택하려면 대시보드 탭으로 이동합니다. 패널을 보거나 편집하거나 다시 정렬하려면 클릭합니다.



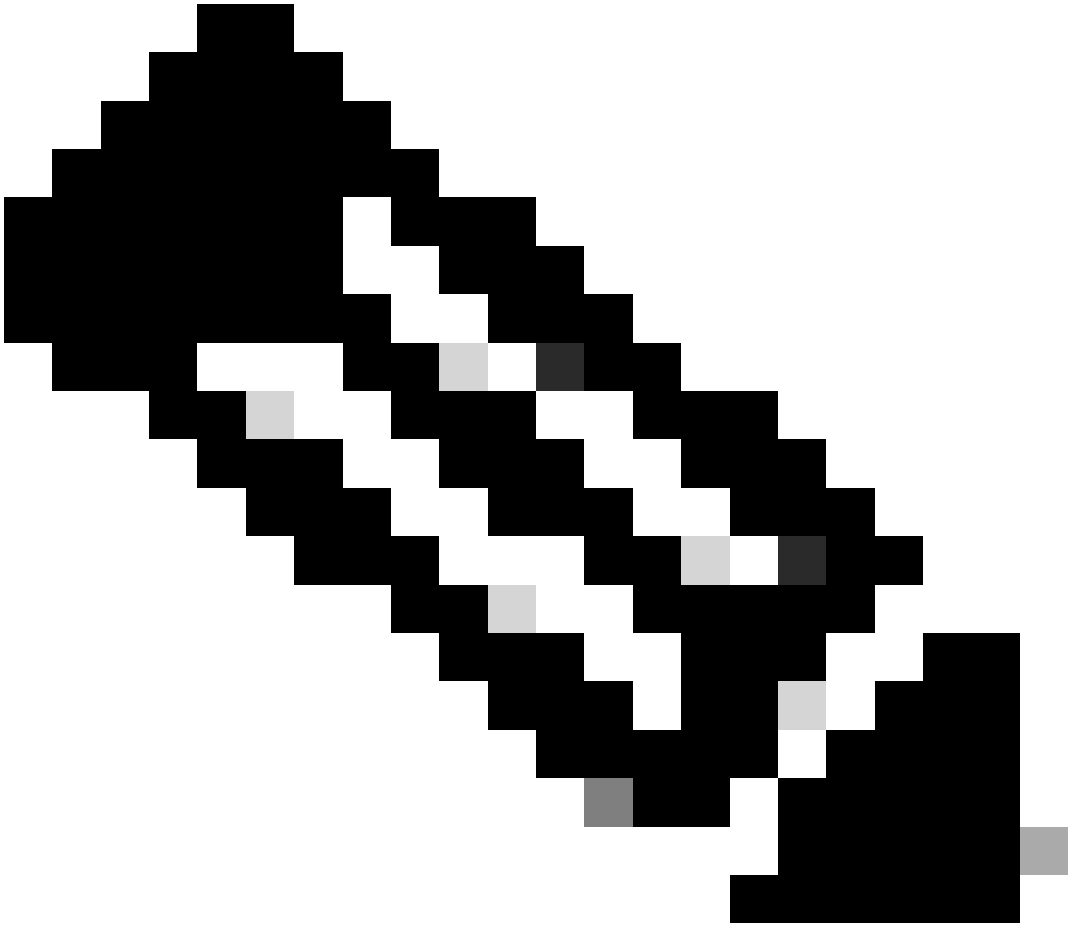
대시보드를 보는 방법

SPL 쿼리를 기반으로 알림 구성

1단계. Search and Reporting 앱으로 이동하여 SPL 쿼리를 구성하고 실행하여 경고를 트리거하는 데 사용할 올바른 로그를 가져오는지 확인합니다.



개별 경고 생성을 위한 SPL 쿼리 실행



참고: 이 예에서는 쿼리가 원격 액세스 VPN에 대한 실패한 인증 로그를 가져와서 특정 시간 내에 실패한 시도 횟수가 특정 임계값을 초과할 경우 경고를 트리거하는 데 사용됩니다.

3단계. Save As(다른 이름으로 저장)를 클릭하고 Alert(경고)를 선택합니다.

경고 저장

4단계. Alert(경고)의 이름을 Title(제목)으로 지정합니다. 알림을 구성하는 데 필요한 기타 세부 정보 및 매개변수를 모두 입력하고 Save(저장)를 클릭합니다. 이 알림에 사용되는 설정에 대해 설명했습니다.

<#root>

Permissions: Shared in App.
Alert Type: Real-time (allows failed user authentications in the last 10 minutes can be tracked continu
Trigger Conditions: A

custom

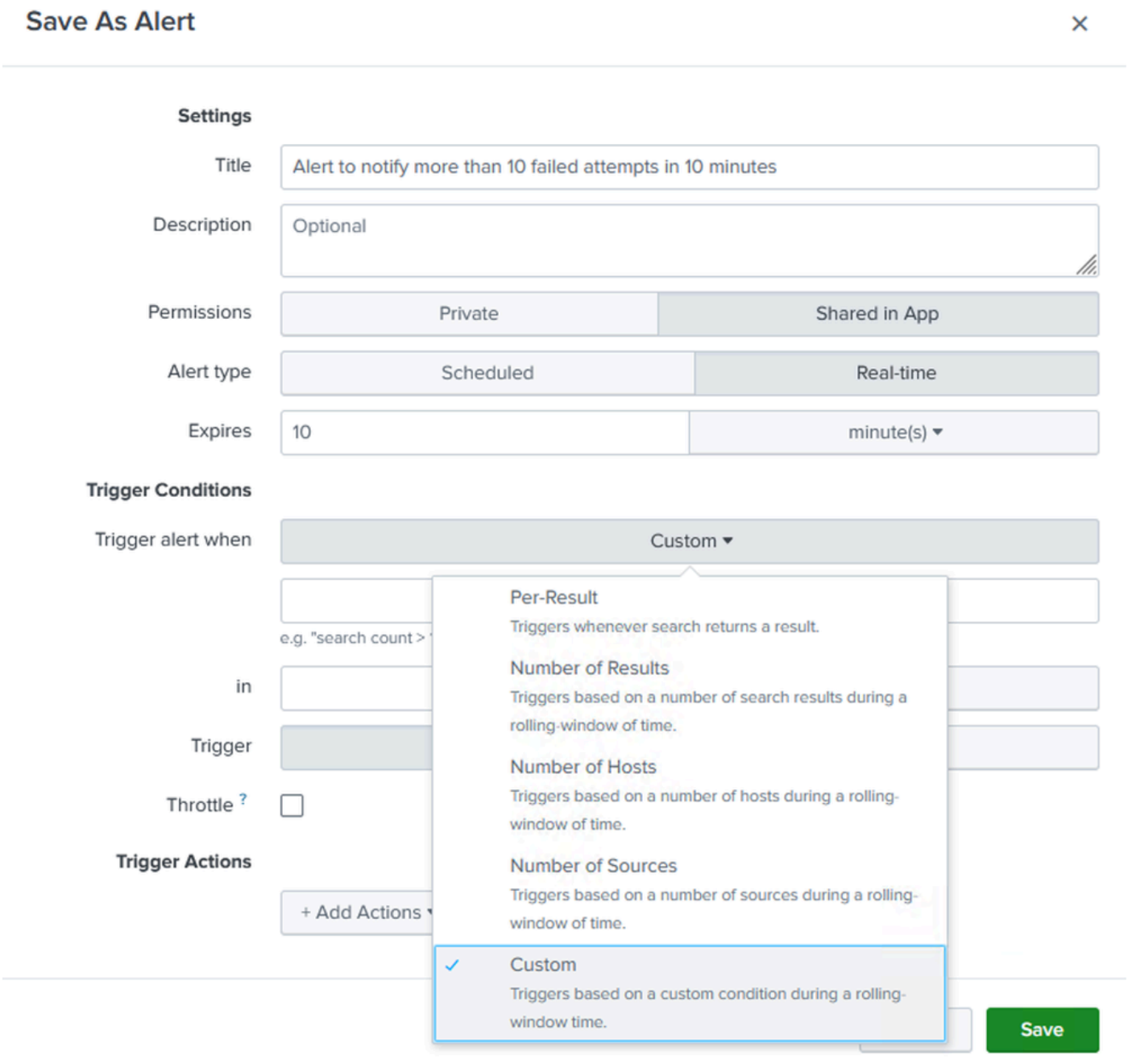
 condition is used to search if the

reject_count

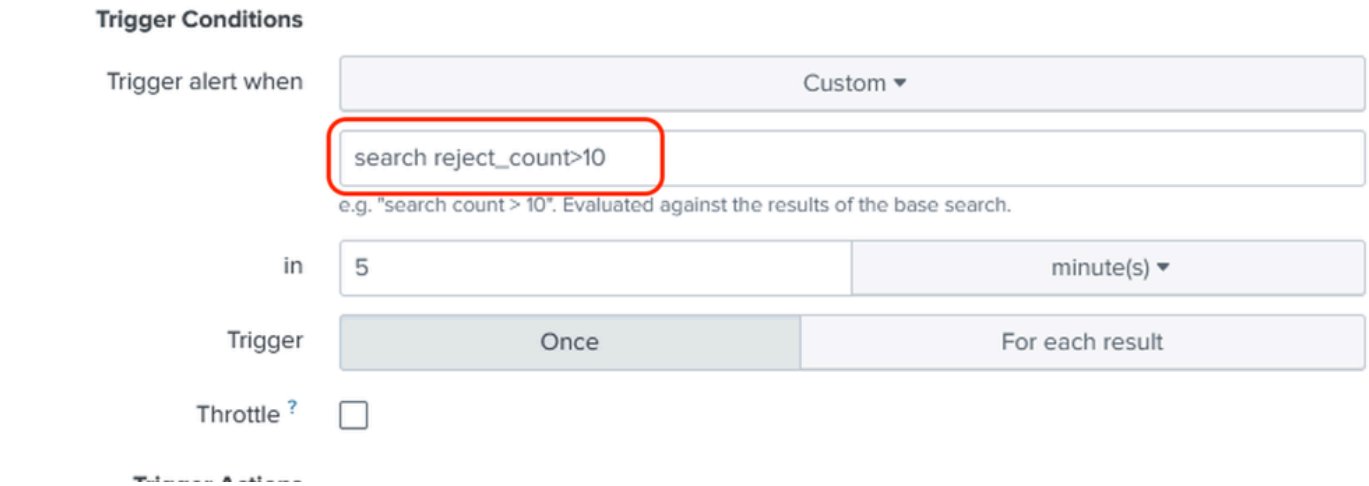
counter from the SPL query has exceeded 10 in the last 5 minutes for any IP address.
Trigger Actions: Set a trigger action such as

Add to Triggered Alerts, Send email, etc.

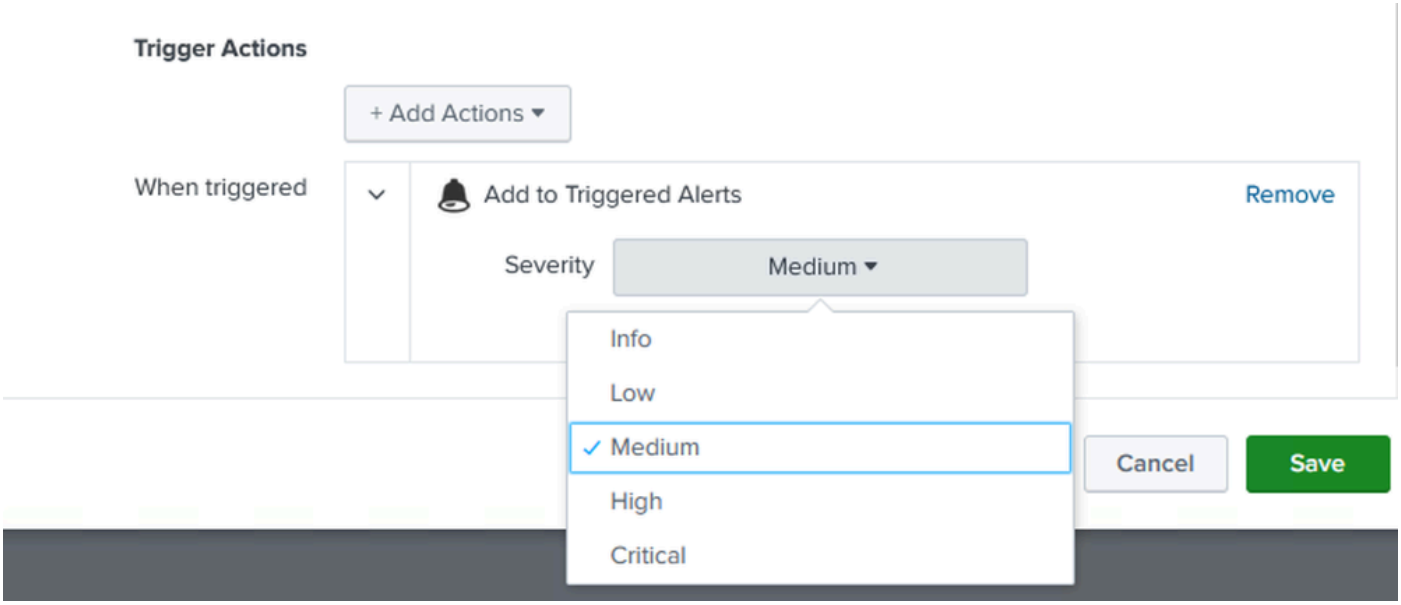
and set the alert severity as per your requirement.



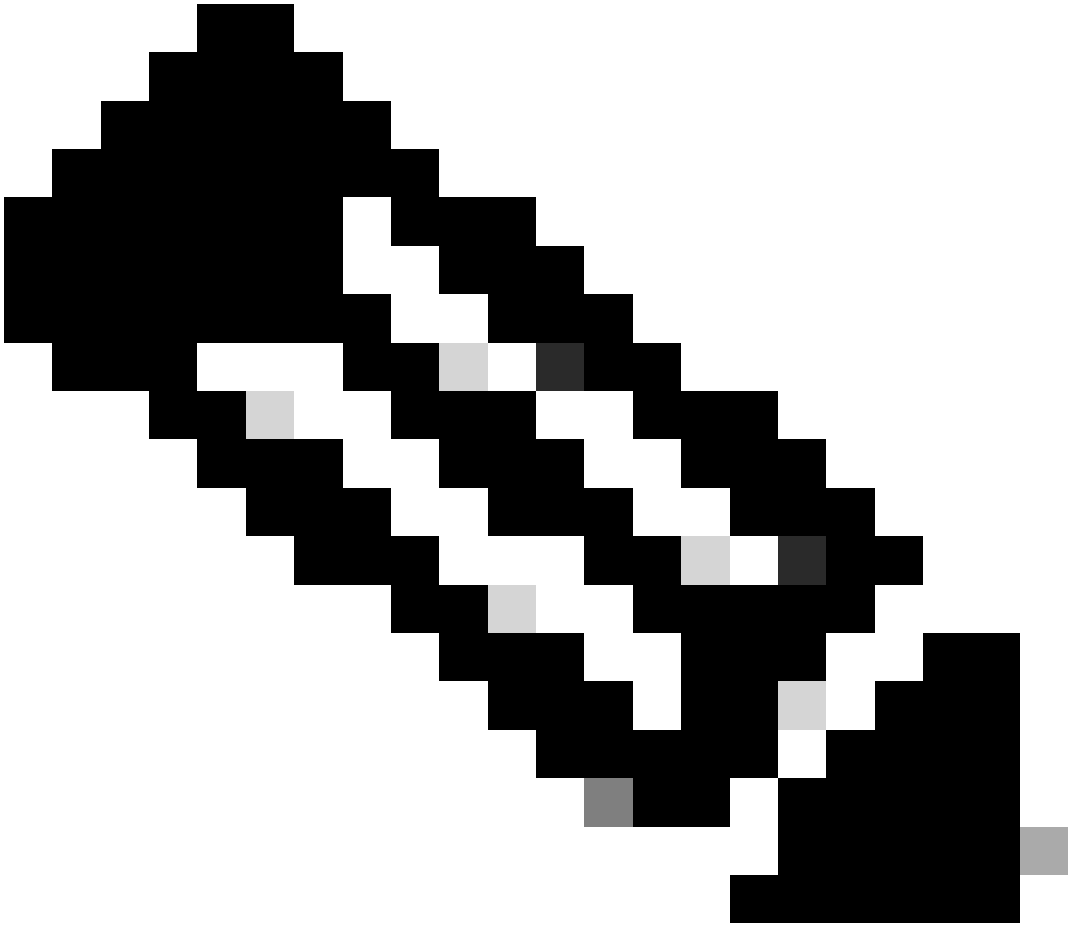
경고 생성을 위한 추가 설정



경고 생성을 위한 추가 설정



경고 생성을 위한 추가 설정



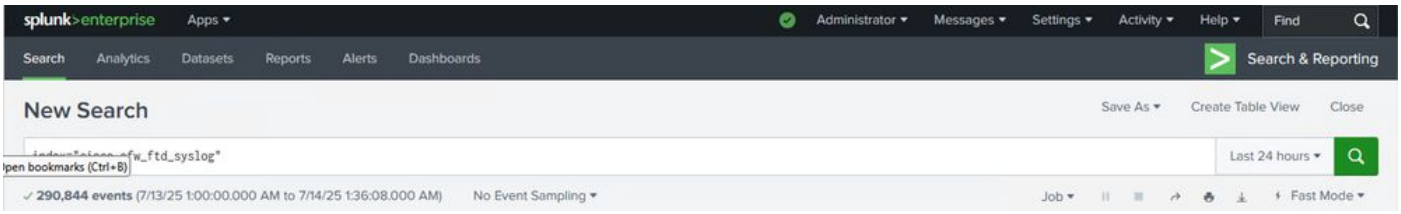
참고: 각 결과에 대해 알림을 트리거하려면 조정 설정도 그에 따라 정의해야 합니다.

다음을 확인합니다.

대시보드와 알림을 생성한 후에는 이 섹션에 제공된 지침을 사용하여 컨피그레이션, 데이터 흐름, 대시보드 및 실시간 알림을 확인할 수 있습니다.

로그 보기

방화벽에서 전송한 로그를 수신하여 splunk 검색 헤드에 표시하는지 확인하기 위해 검색 앱을 사용할 수 있습니다. 이는 인덱스화된 최신 로그(검색 인덱스 = "cisco_sfw_ftd_syslog")와 그와 연결된 타임스탬프를 확인하여 확인할 수 있습니다.

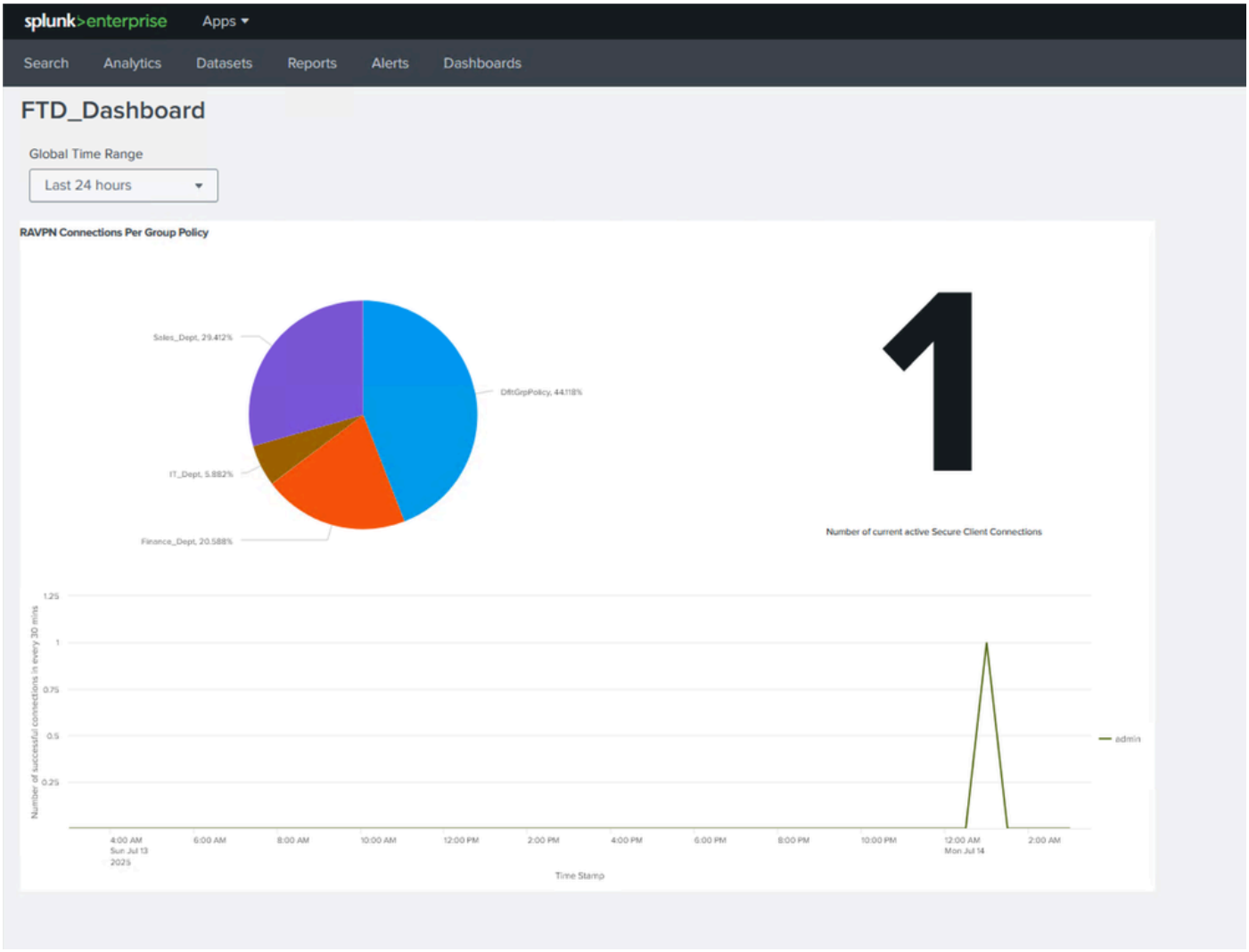


로그 확인 및 보기

로그 확인 및 보기

실시간 대시보드 보기

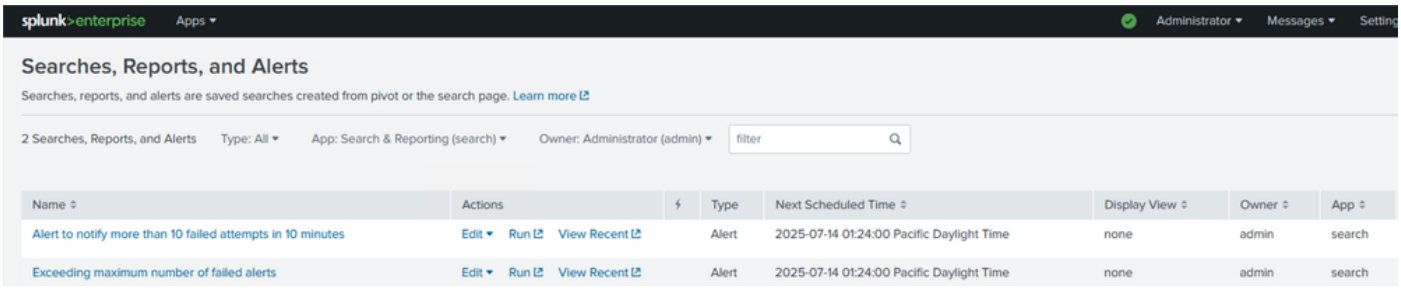
생성한 사용자 지정 대시보드로 이동하여 FTD에서 새 데이터 및 로그가 생성될 때 각 패널의 변경 사항을 확인할 수 있습니다.



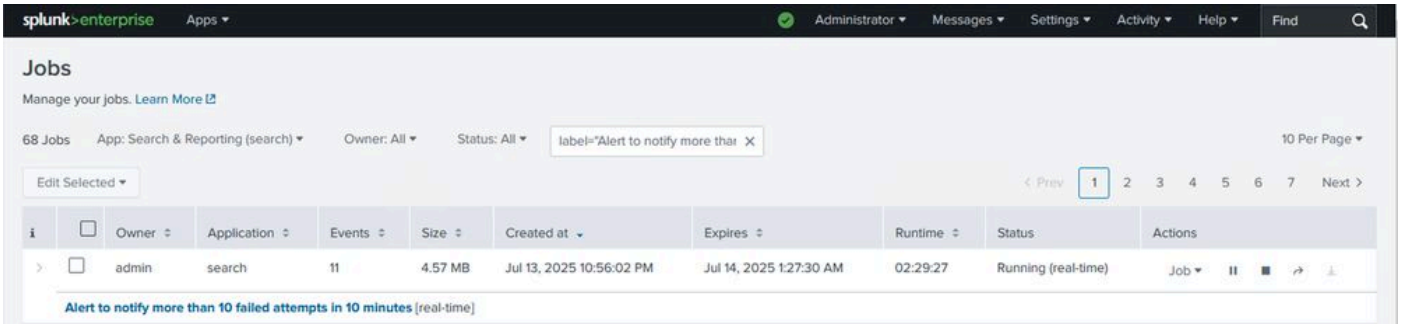
대시보드 보기

경보가 트리거되었는지 확인

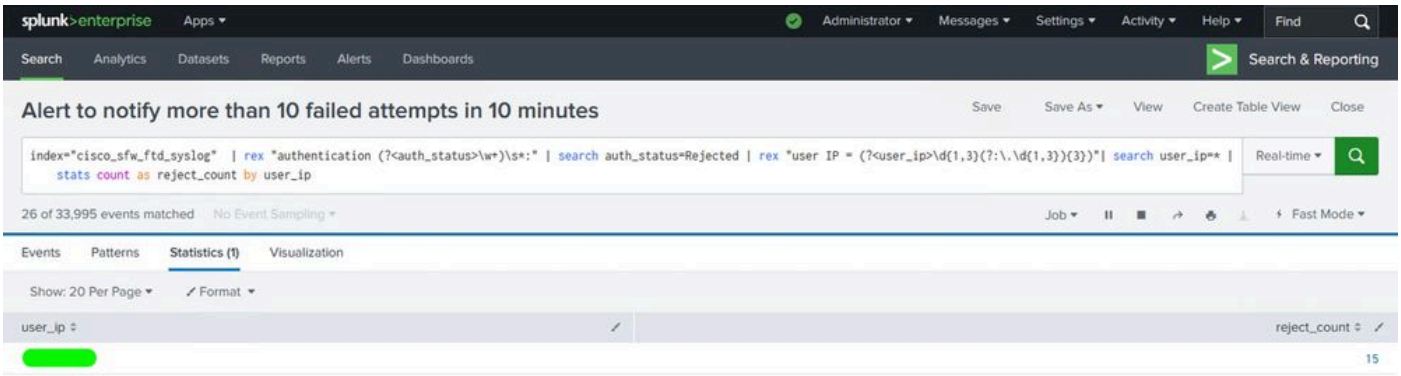
경고문에 대한 정보를 확인하려면 검색, 보고서 및 경고문 섹션으로 이동하여 최근 경고문 정보를 확인할 수 있습니다. 작업 및 검색에 대해 자세히 확인하려면 최근 보기를 누릅니다.



알림 확인 및 보기



알림 확인 및 보기



트리거된 경고에 대한 통계 확인

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.