Splunk에 Syslog 이벤트를 전송하도록 응답 관리 구성

목차

소개

이 문서에서는 syslog를 통해 Splunk와 같은 서드파티에 이벤트를 전송하도록 보안 분석 응답 관리 기능을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

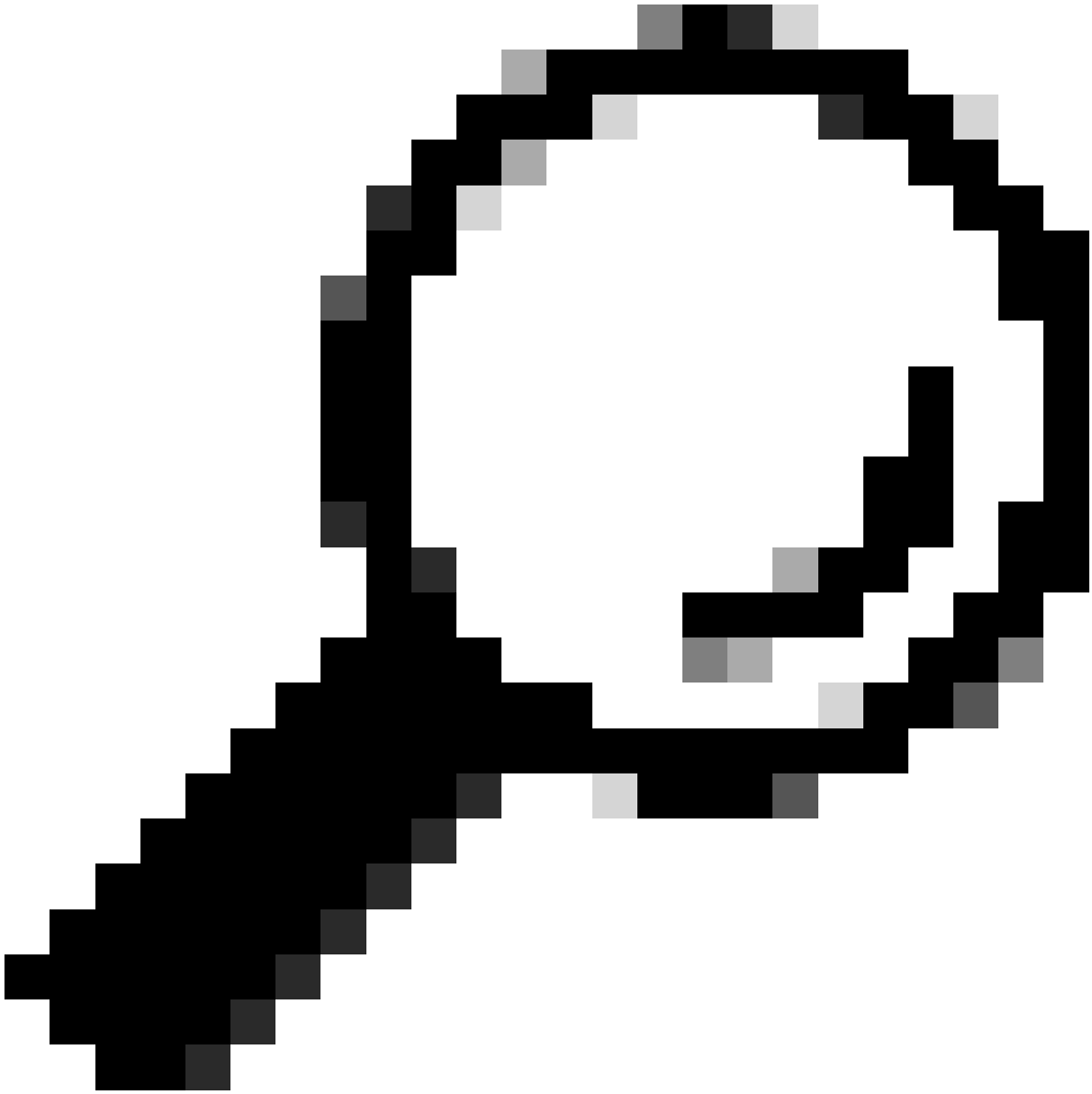
- 보안 네트워크 분석 응답 관리.
- Splunk Syslog

사용되는 구성 요소

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

- 하나 이상의 Manager 어플라이언스와 하나의 Flow Collector 어플라이언스가 포함된 SNA(Secure Network Analytics) 구축.
- Splunk 서버가 설치되어 있으며 443개 포트를 통해 액세스할 수 있습니다.

UDP 514 또는 사용자 정의 포트를 통해 SNA에 syslog 구성



팁: SNA와 Splunk 사이의 방화벽 또는 중간 디바이스에서 syslog에 대해 선택한 UDP/514,TCP/6514 또는 사용자 지정 포트가 허용되는지 확인합니다.

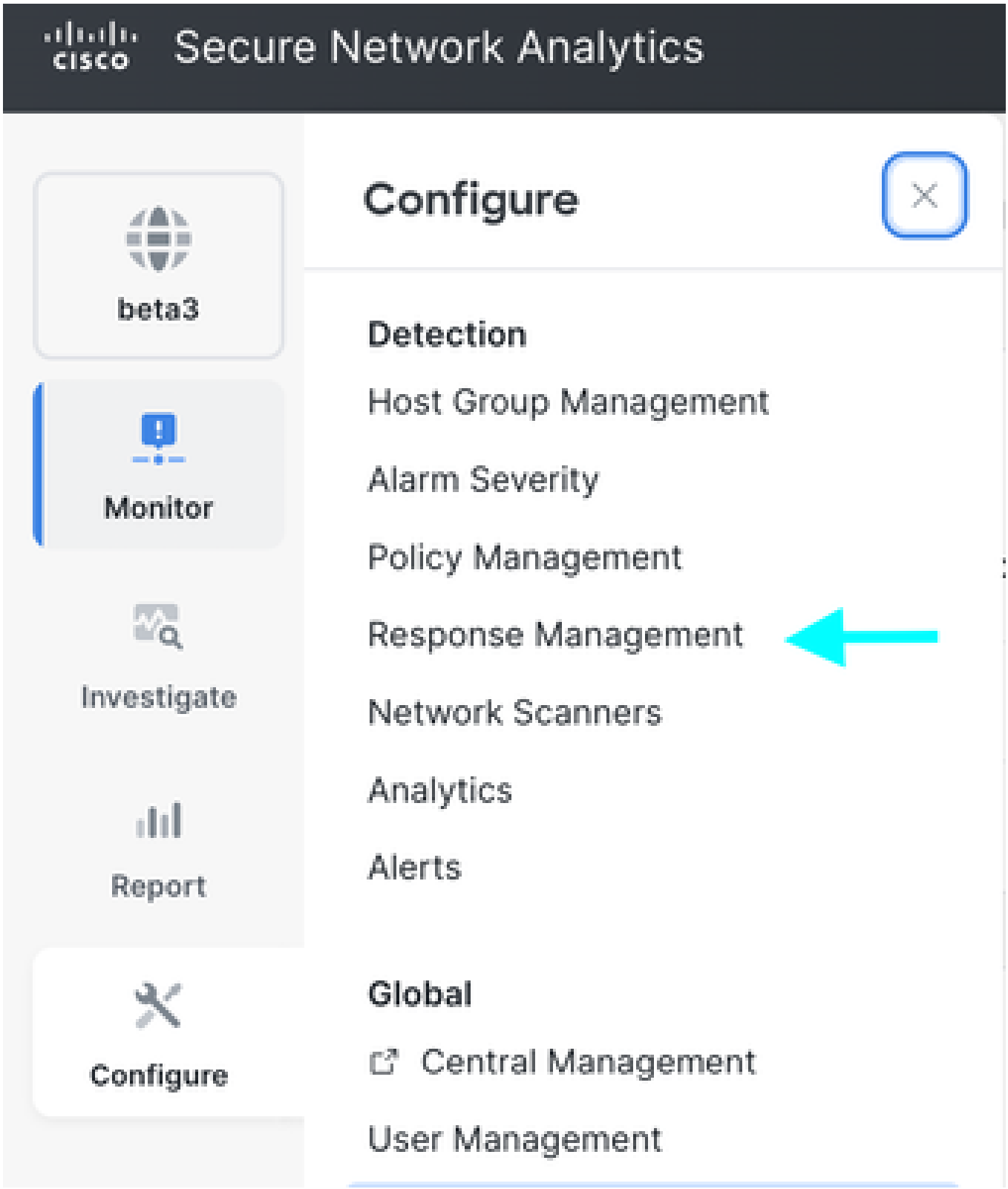
1.SNA 응답 관리

SA(Secure Analytics)의 응답 관리 구성 요소를 사용하여 규칙, 작업 및 syslog 대상을 구성할 수 있습니다.

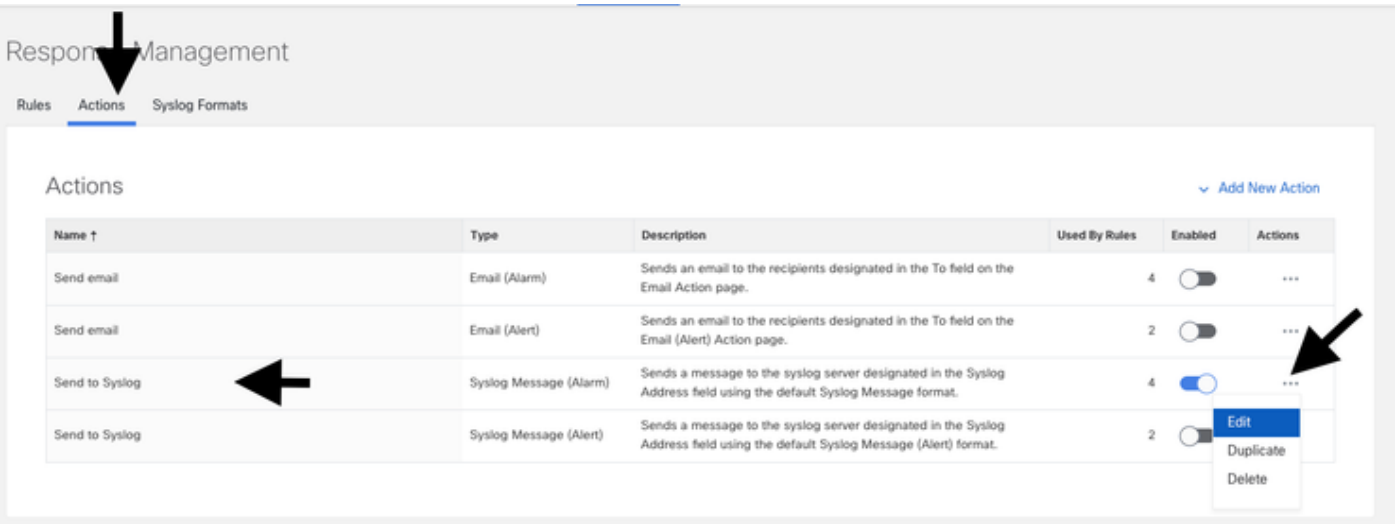
이러한 옵션은 Secure Analytics 경보를 다른 대상으로 전송/전달하도록 구성해야 합니다.

1단계: SA Manager Appliance에 로그인하고 Configure(구성) > Detection Response

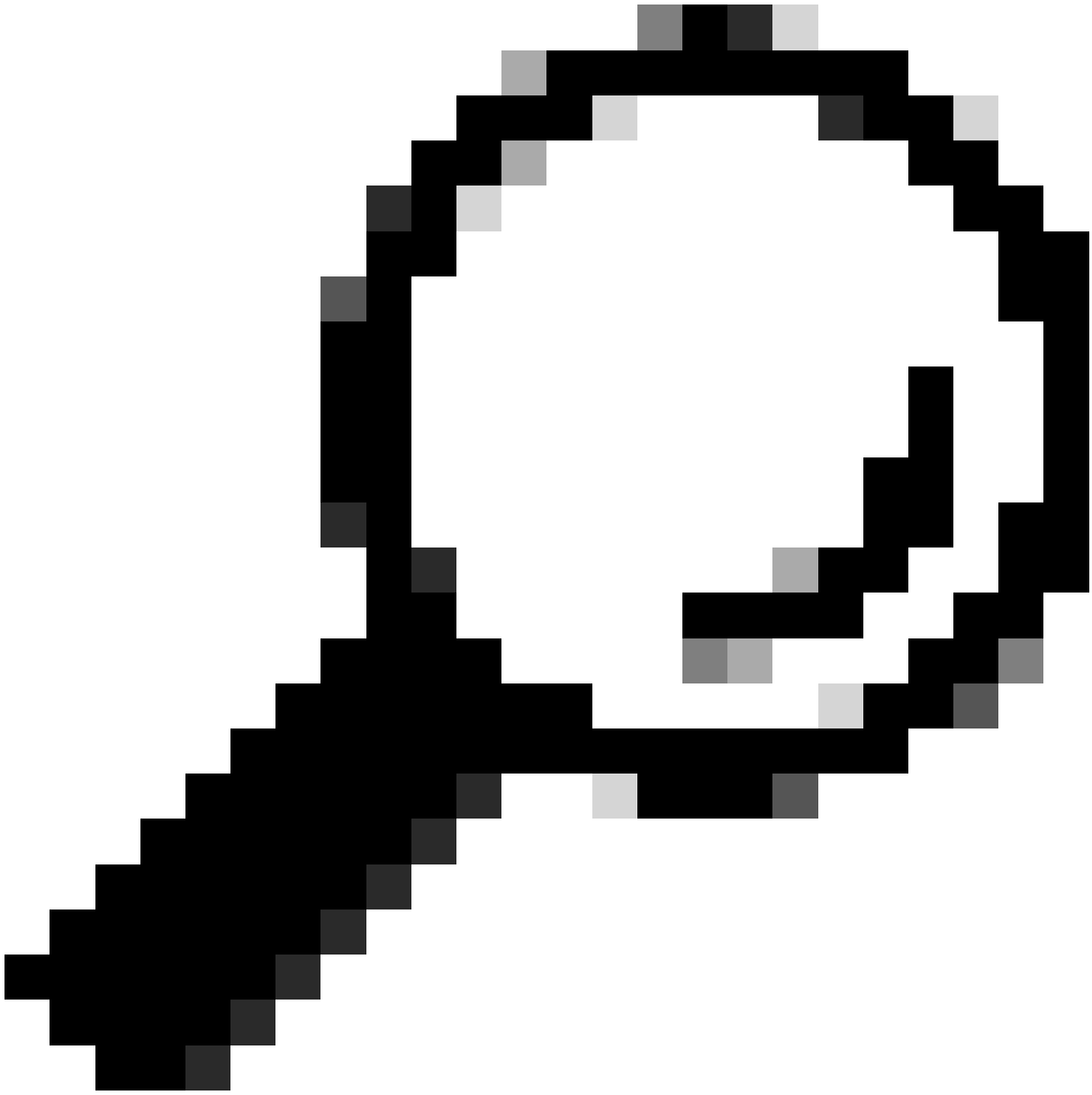
Management(탐지 응답 관리)로 이동합니다.



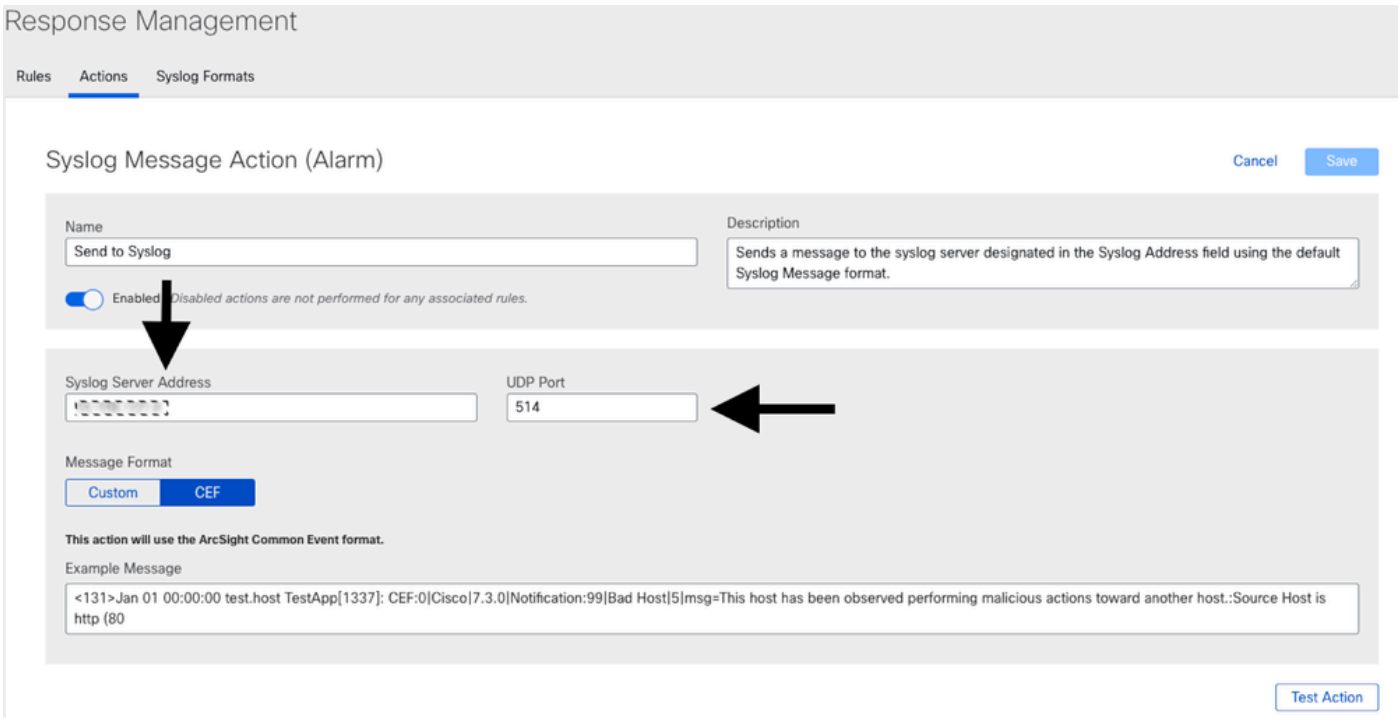
2단계: 새 페이지에서 Actions(작업) 탭으로 이동하여 기본 Send to Syslog(Syslog로 보내기) 행 항목을 찾고 Action(작업) 열에서 줄임표(...)를 클릭한 다음 Edit(수정)를 클릭합니다.



3단계: Syslog Server Address 필드에 원하는 목적지 주소를 입력하고, UDP Port 필드에 원하는 목적지 수신 포트를 입력합니다. 메시지 형식에서 CEF를 선택합니다.
4단계: 완료되면 오른쪽 상단의 파란색 Save(저장) 버튼을 클릭합니다.



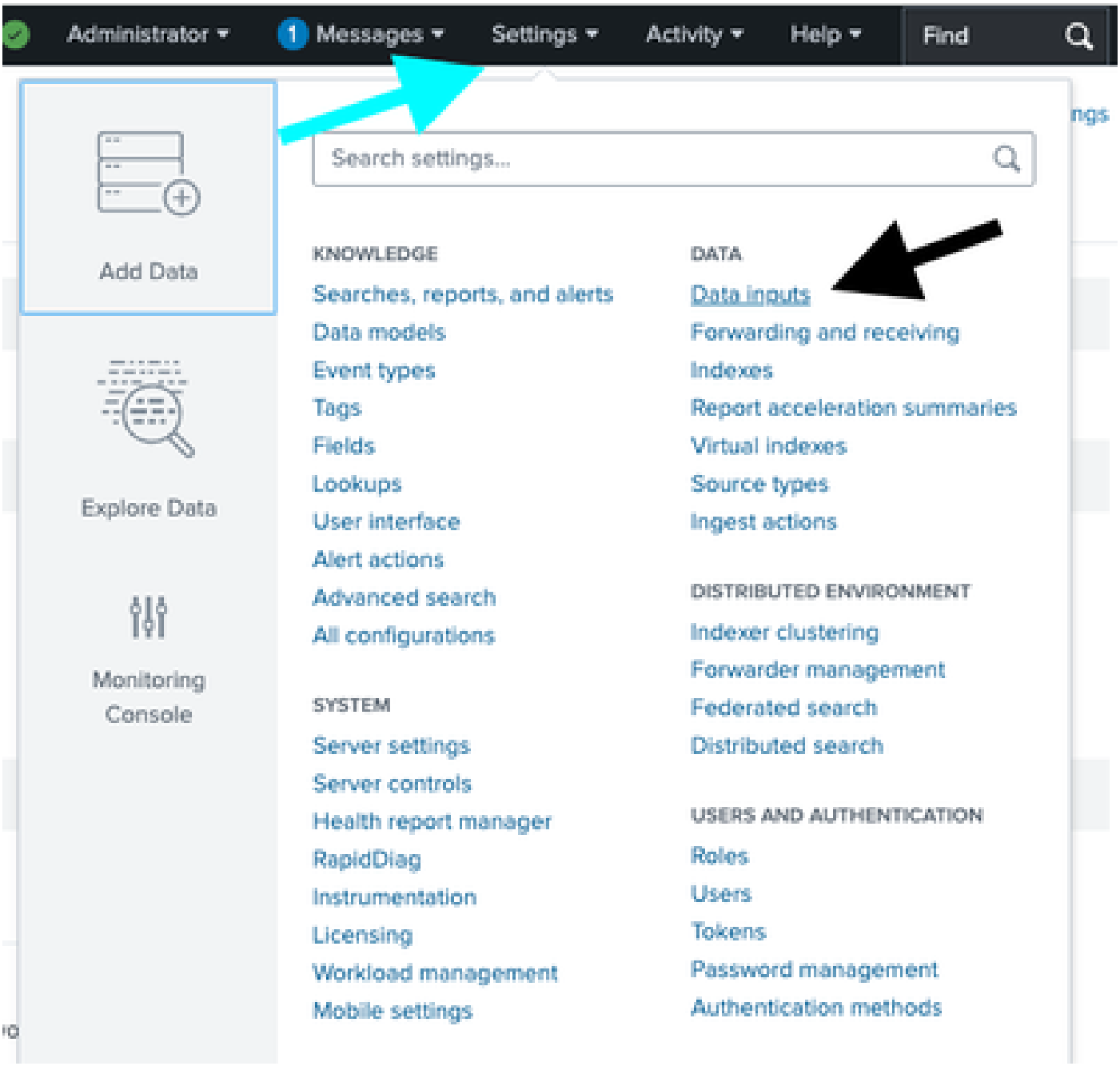
팁: syslog의 기본 UDP 포트는 514입니다



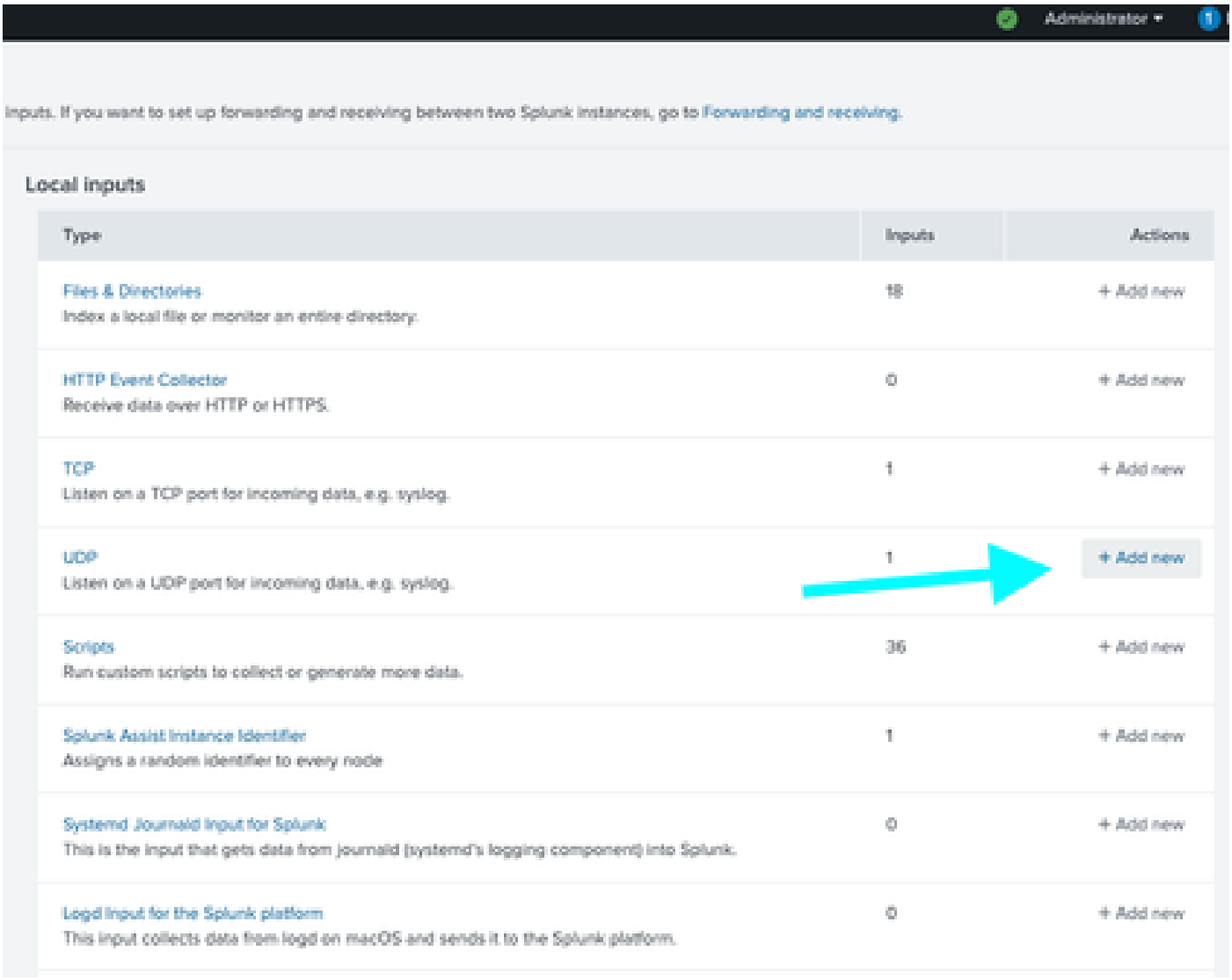
2. UDP 포트를 통해 SNA Syslog를 수신하도록 Splunk 구성

Secure Network Analytics Manager 웹 UI에서 변경 사항을 적용한 후 Splunk에서 데이터 입력을 구성해야 합니다.

1단계: Splunk에 로그인하고 Settings(설정) > Add Data(데이터 추가) > DATA Data Inputs(데이터 입력)로 이동합니다.

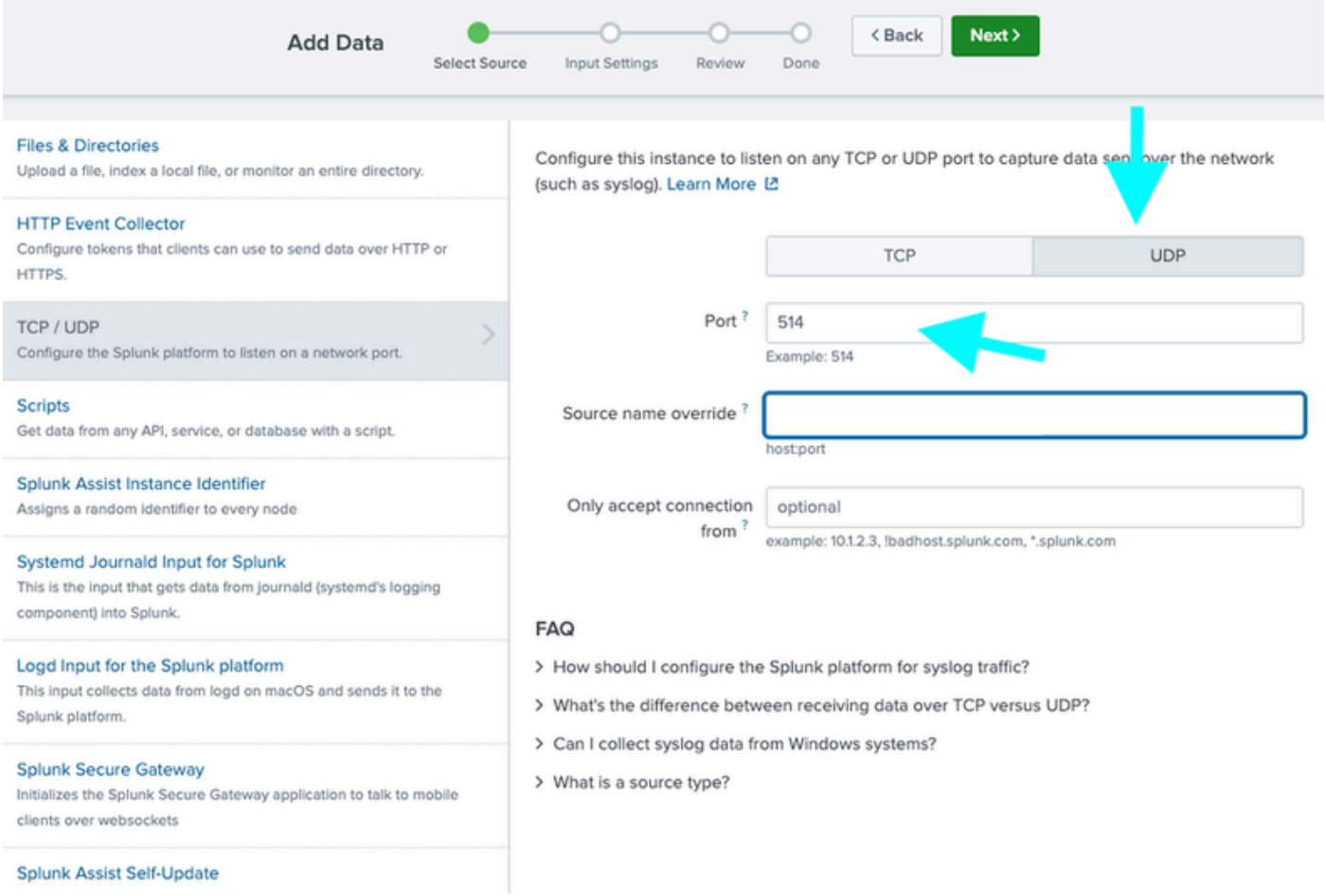


2단계: UDP 회선을 찾고 +Add new(+새로 추가)를 선택합니다.



3단계: 새 페이지에서 UDP를 선택하고 Port(포트) 필드에 수신 포트(예: 514)를 입력합니다.
4단계: Source name override(소스 이름 재정의) 필드에 desired name of source.

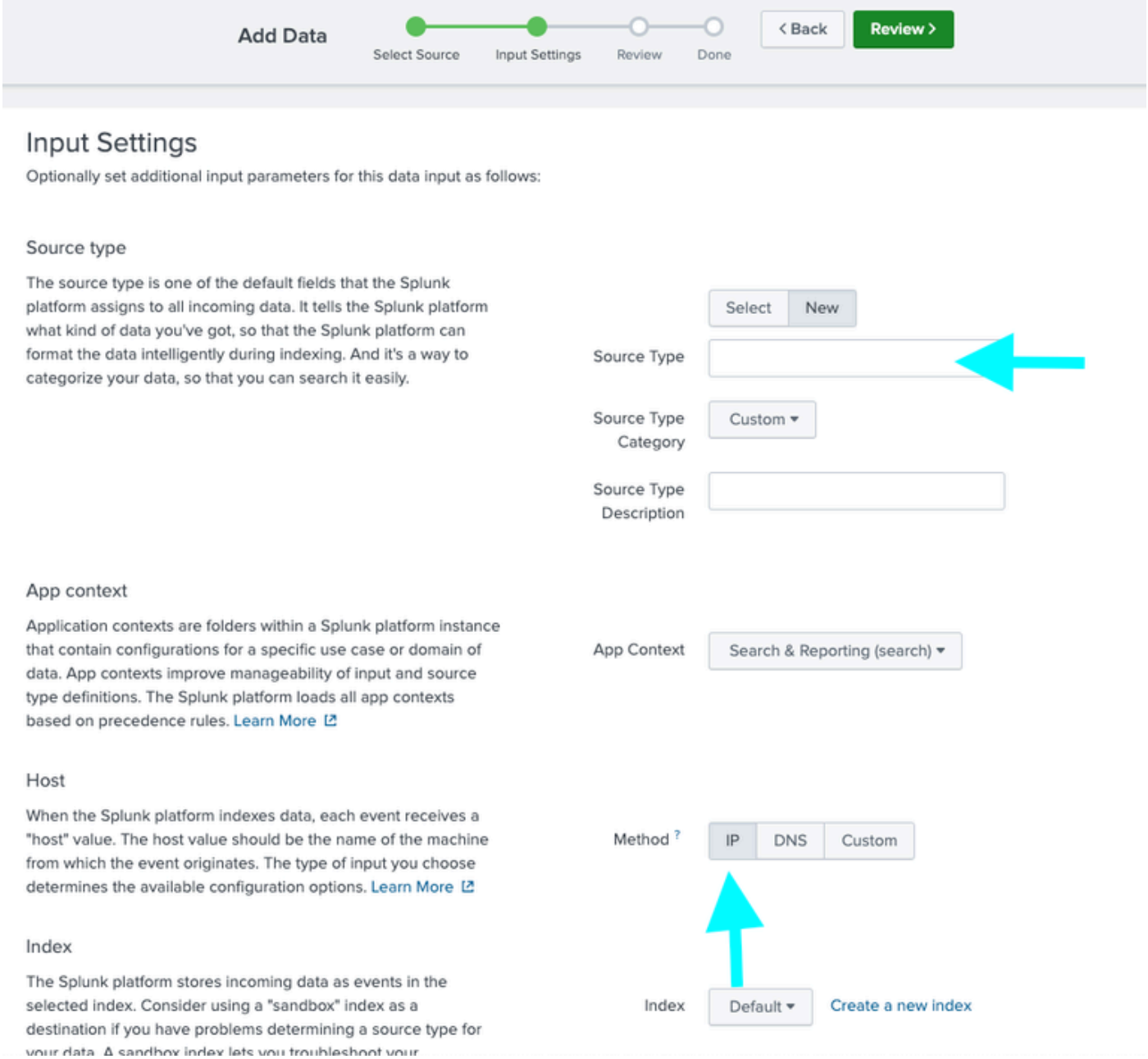
5단계: 완료되면 창 상단의 녹색 다음 > 버튼을 클릭합니다.



6단계: 다음 페이지에서 [새로 만들기]로 전환한 다음 [소스 유형] 필드를 찾아 다음을 입력합니다 desired source .

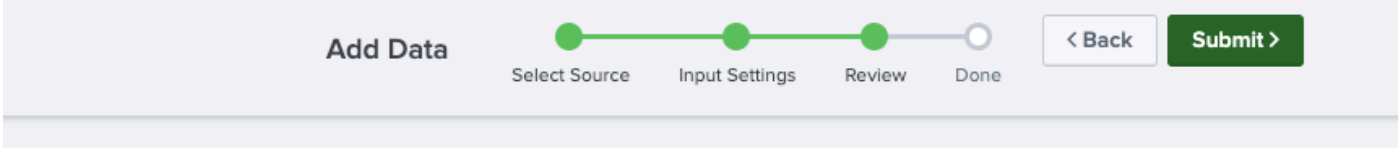
7단계: 메서드의 IP를 선택합니다.

8단계: 화면 상단의 녹색 Review(검토) > 버튼을 클릭합니다.



9단계: 다음 창에서 설정을 검토하고 필요한 경우 수정합니다.

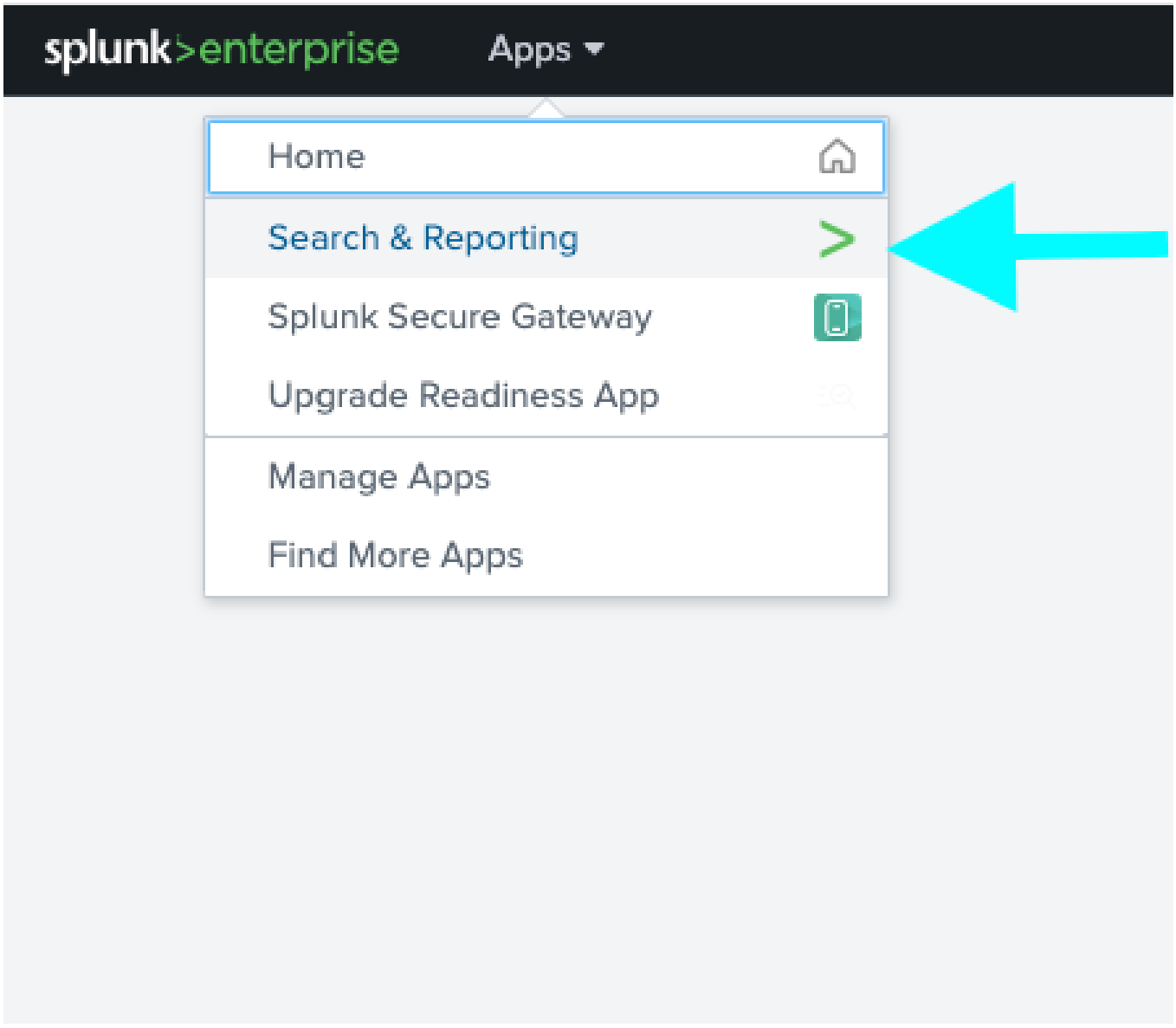
10단계: 검증이 완료되면 창 상단에서 녹색 Submit > 버튼을 클릭합니다.



Review

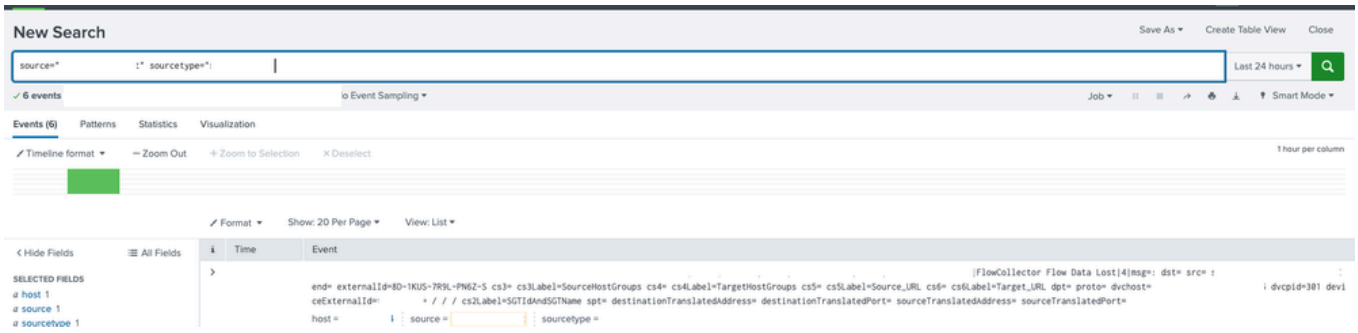
Input Type ..... UDP Port
Port Number 514
Source name override .....
Restrict to Host ..... N/A
Source Type .....
App Context ..... search
Host ..... (IP address of the remote server)
Index ..... default

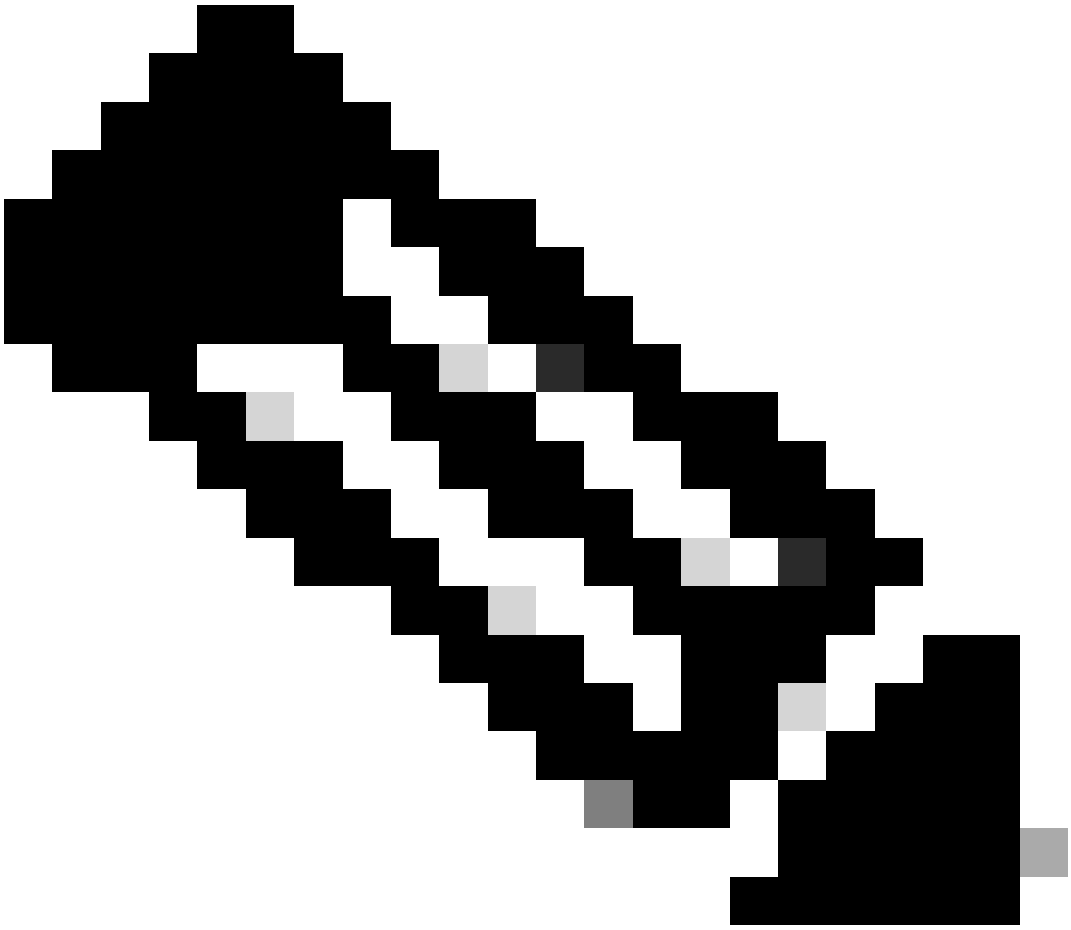
11단계: 웹 UI에서 Apps(앱) > Search & Reporting(검색 및 보고)으로 이동합니다.



12단계: Search(검색) 페이지에서 필터를 사용하여source="As_configured" sourcetype="As_configured"수신된 로

그를 찾습니다.



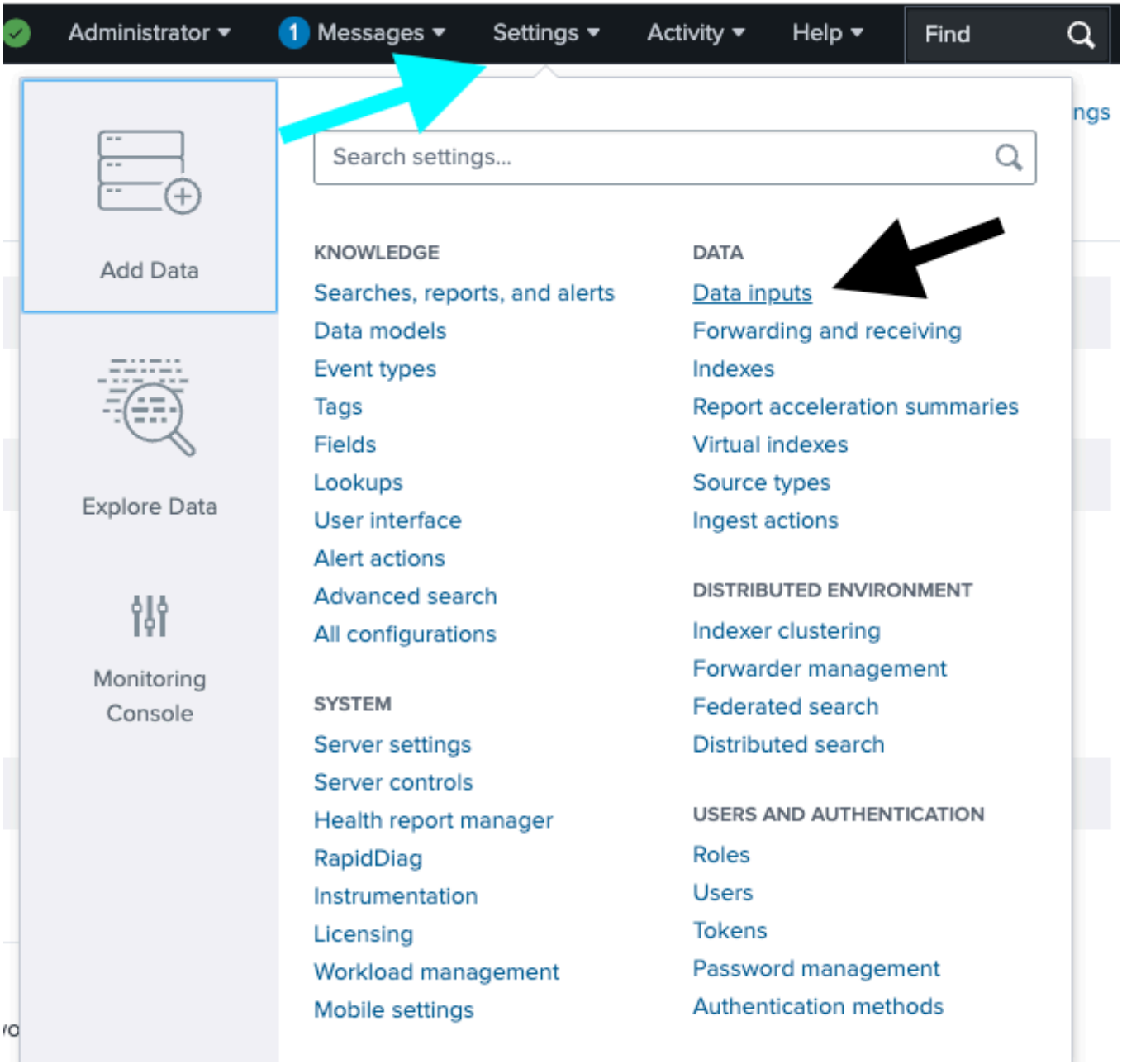


참고: 소스에 대해서는 4단계를 참조하십시오.
source_type의 경우 6단계를 참조하십시오.

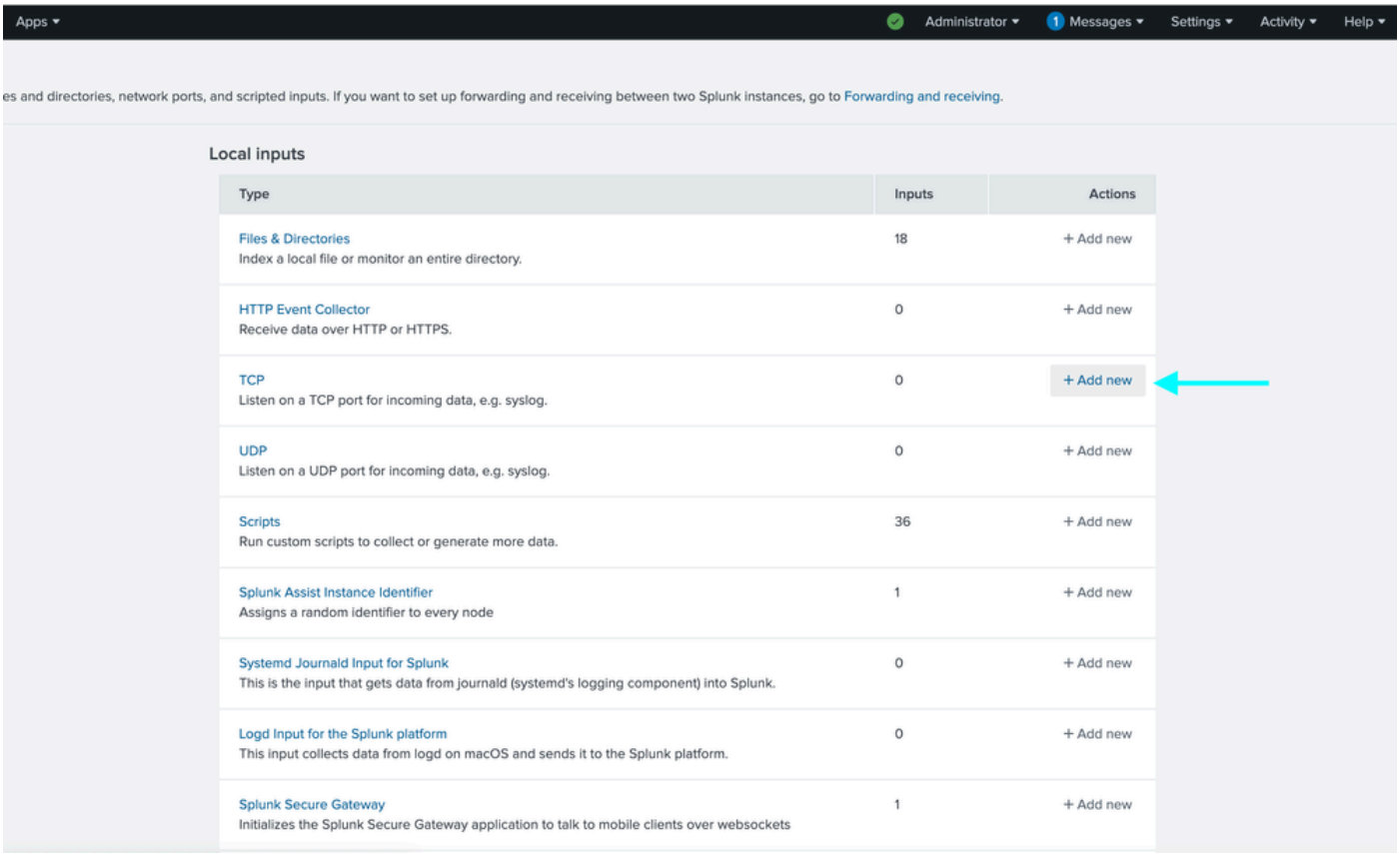
TCP 포트 6514 또는 사용자 정의 포트를 통해 SNA에서 syslog 구성

1. TCP 포트를 통해 SNA 감사 로그를 수신하도록 Splunk 구성

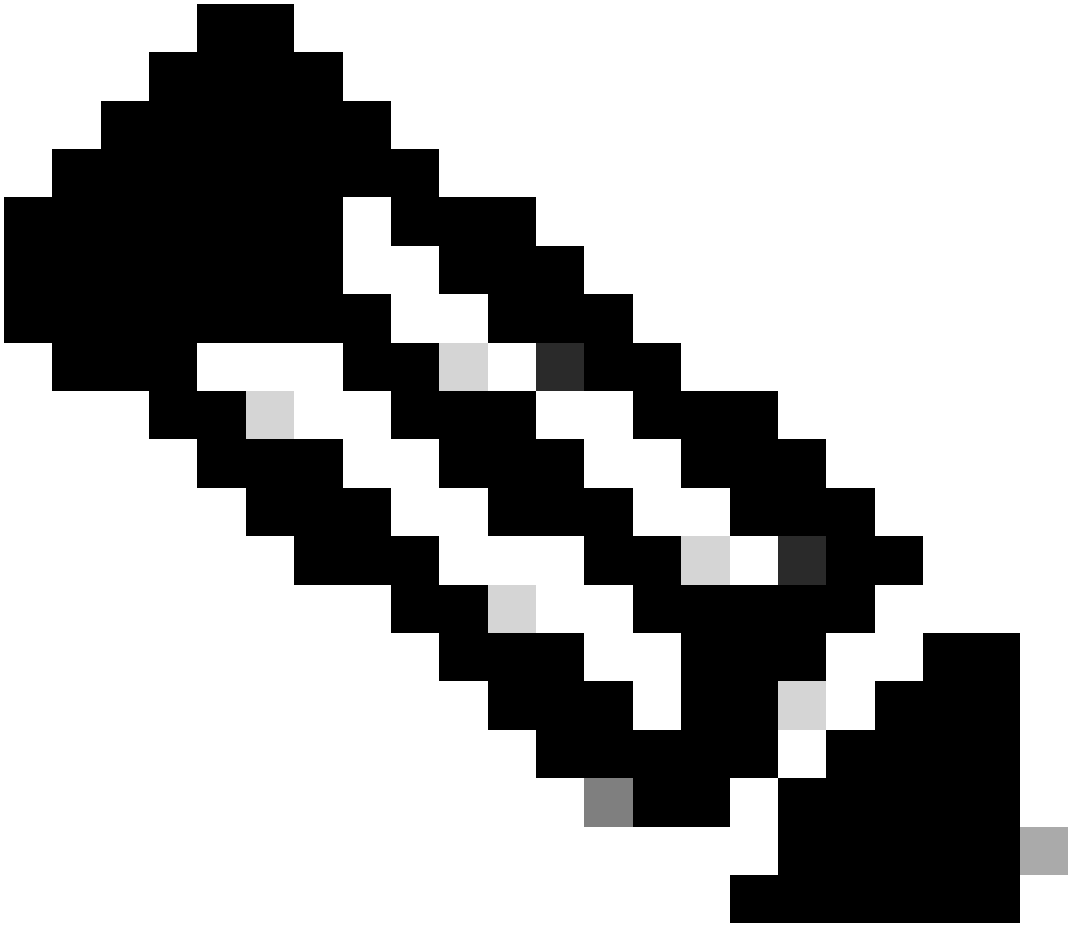
1단계: Splunk UI에서 Settings(설정) > Add Data(데이터 추가) > DATA Data Inputs(데이터 입력)로 이동합니다.



2단계: TCP 행을 찾고 + Add new(새로 추가)를 선택합니다.

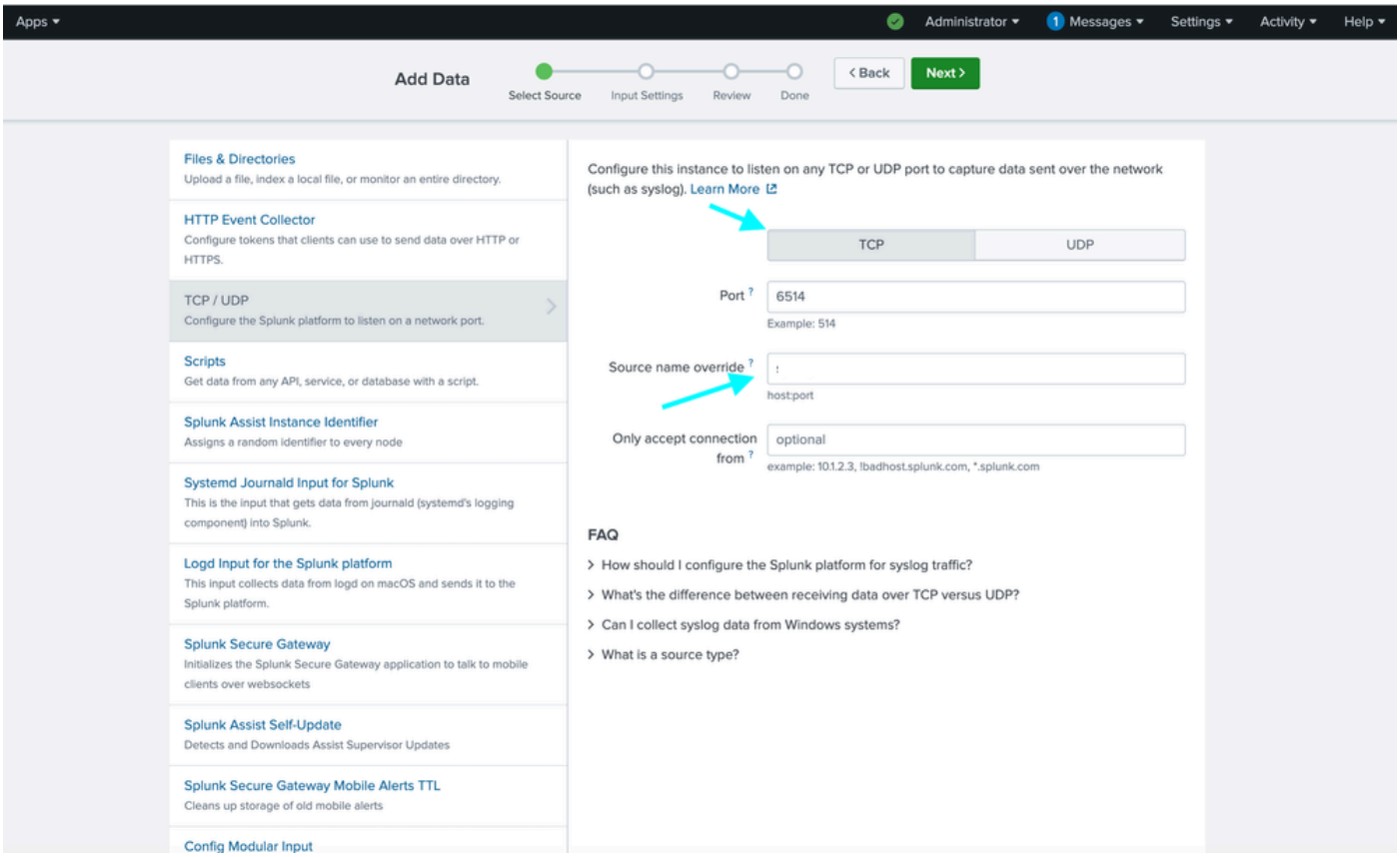


3단계: 새 창에서 TCP를 선택하고, 원하는 수신 포트를 예제 이미지 포트 6514에 입력하고, Source name override 필드에 "desired name"을 입력합니다.



참고: TCP 6514는 TLS를 통한 syslog의 기본 포트입니다

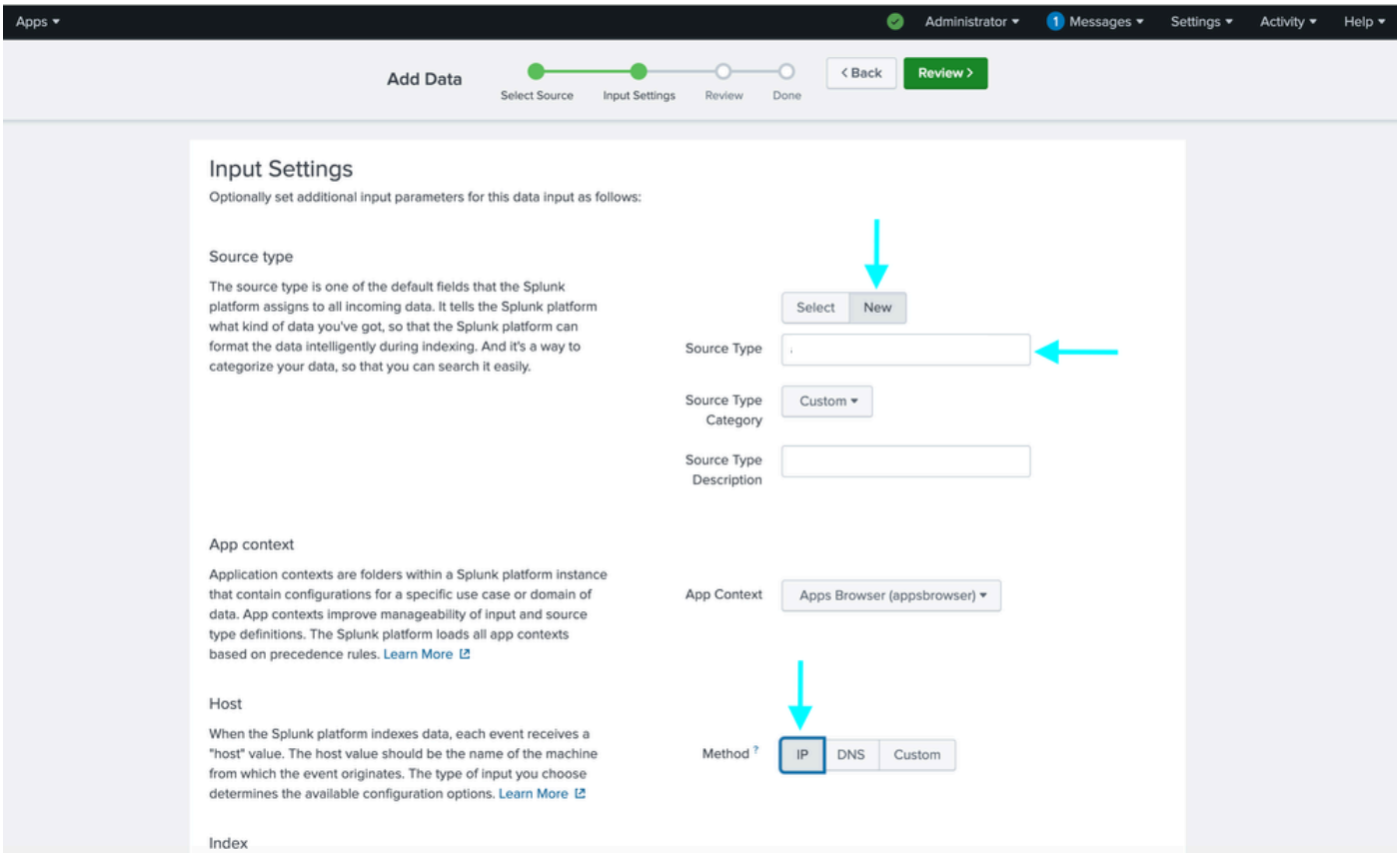
4단계: 완료되면 창 상단의 녹색 다음 > 버튼을 클릭합니다.



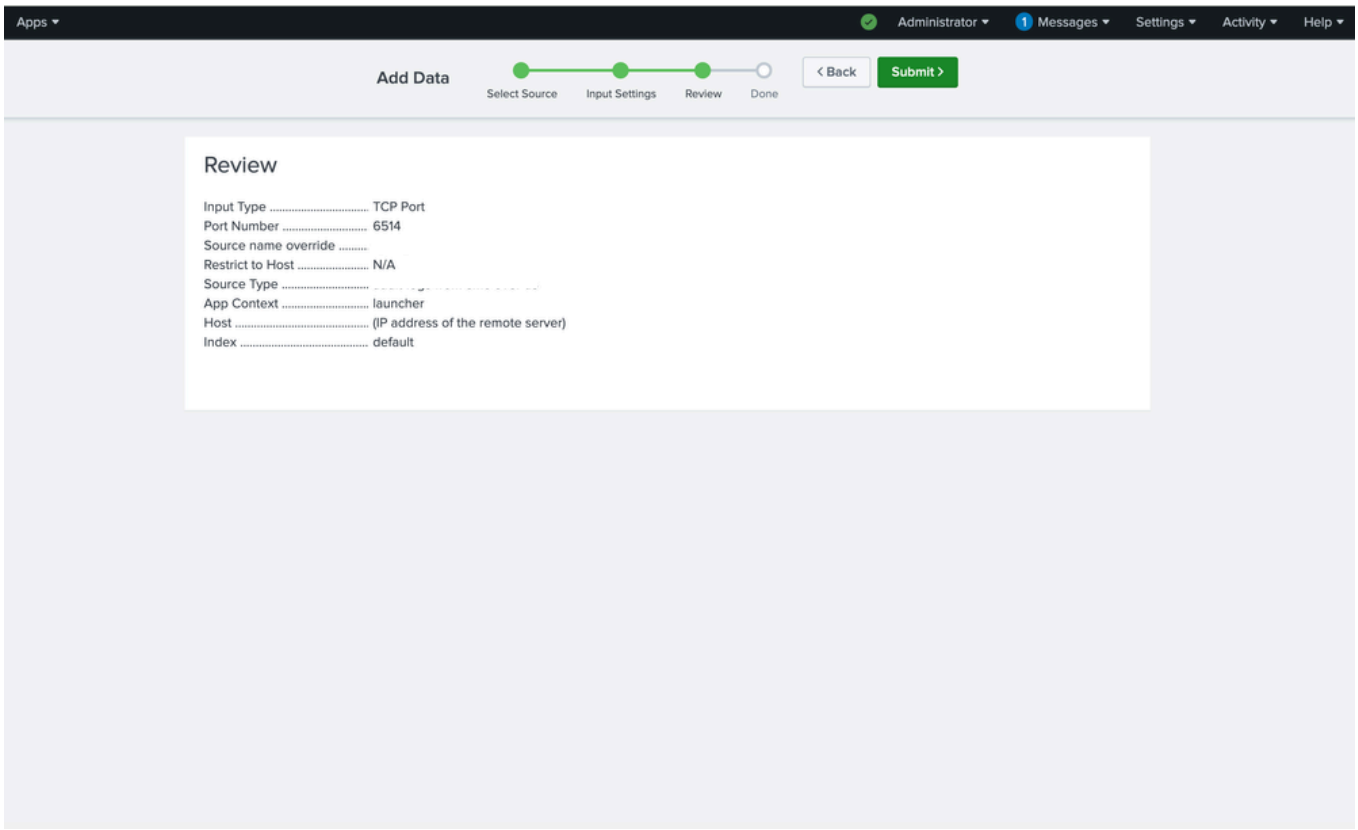
5단계: 새 창의 소스 유형 섹션에서 새로 만들기를 선택하고 소스 유형 필드에 원하는 이름을 입력합니다.

6단계: Host(호스트) 섹션에서 Method(메서드)에 대한 IP를 선택합니다.

7단계: 완료되면 창 상단의 녹색 검토 > 버튼을 선택합니다.



8단계: 다음 창에서 설정을 검토하고 필요한 경우 수정합니다. 검증이 완료되면 창 상단의 녹색 Submit(제출) > 버튼을 클릭합니다.



2. Splunk용 인증서 생성

1단계: openssl이 설치된 시스템을 사용하여 명령을 실행하고sudo openssl req -x509 -newkey rsa:4096 -keyout server_key.pem -out server_cert.pem -sha256 -days 3650 -subj /CN=10.106.127.410.106.127.4의 예 IP를 Splunk 디바이스의 IP로 교체합니다. 사용자 정의 암호를 입력하라는 메시지가 두 번 표시됩니다. 이 예에서는 Splunk 시스템의 명령줄에서 명령을 실행합니다.

```
user@examplehost: sudo openssl req -x509 -newkey rsa:4096 -keyout server_key.pem -out server_cert.pem -
..+...+..+.+...+..+...........+.............+.+.....+.+......+..+.+..........+...+++++++++++++++++
....+.......+..+...+...+.+......+...+.........+...........+.....+...+..+...+...+...+...+.........+..
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
user@examplehost:
```

명령이 완료되면 두 개의 파일이 생성됩니다. server_cert.pem 및 server_key.pem 파일

```
user@examplehost: ll server*
-rw-r--r-- 1 root root 1814 Dec 20 19:02 server_cert.pem
-rw------- 1 root root 3414 Dec 20 19:02 server_key.pem
user@examplehost:
```

2단계: 루트 사용자로 전환합니다.

```
user@examplehost:~$ sudo su
[sudo] password for examplehost:
```

3단계: 새로 생성된 인증서를에 /opt/splunk/etc/auth/ 복사합니다.

```
user@examplehost:~# cat /home/examplehost/server_cert.pem > /opt/splunk/etc/auth/splunkweb.cer
```

4단계: 개인 키와 함께 spunkweb.cet 파일을 추가합니다.

```
user@examplehost:~# cat /home/examplehost/server_key.pem >> /opt/splunk/etc/auth/splunkweb.cer
```

5단계: splunk 인증서의 소유권을 변경합니다.

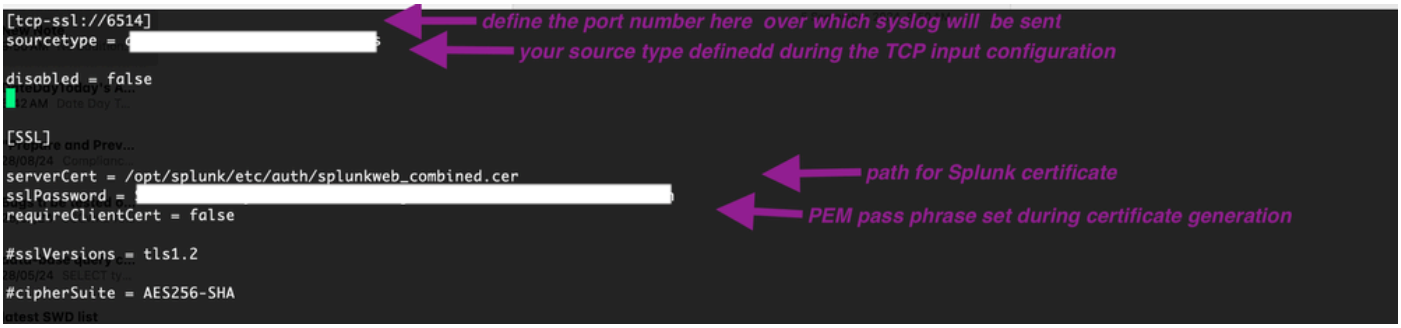
```
user@examplehost:~# chown 10777:10777/opt/splunk/etc/auth/splunkweb.cer
```

6단계: splunk 인증서에 대한 권한을 변경합니다.

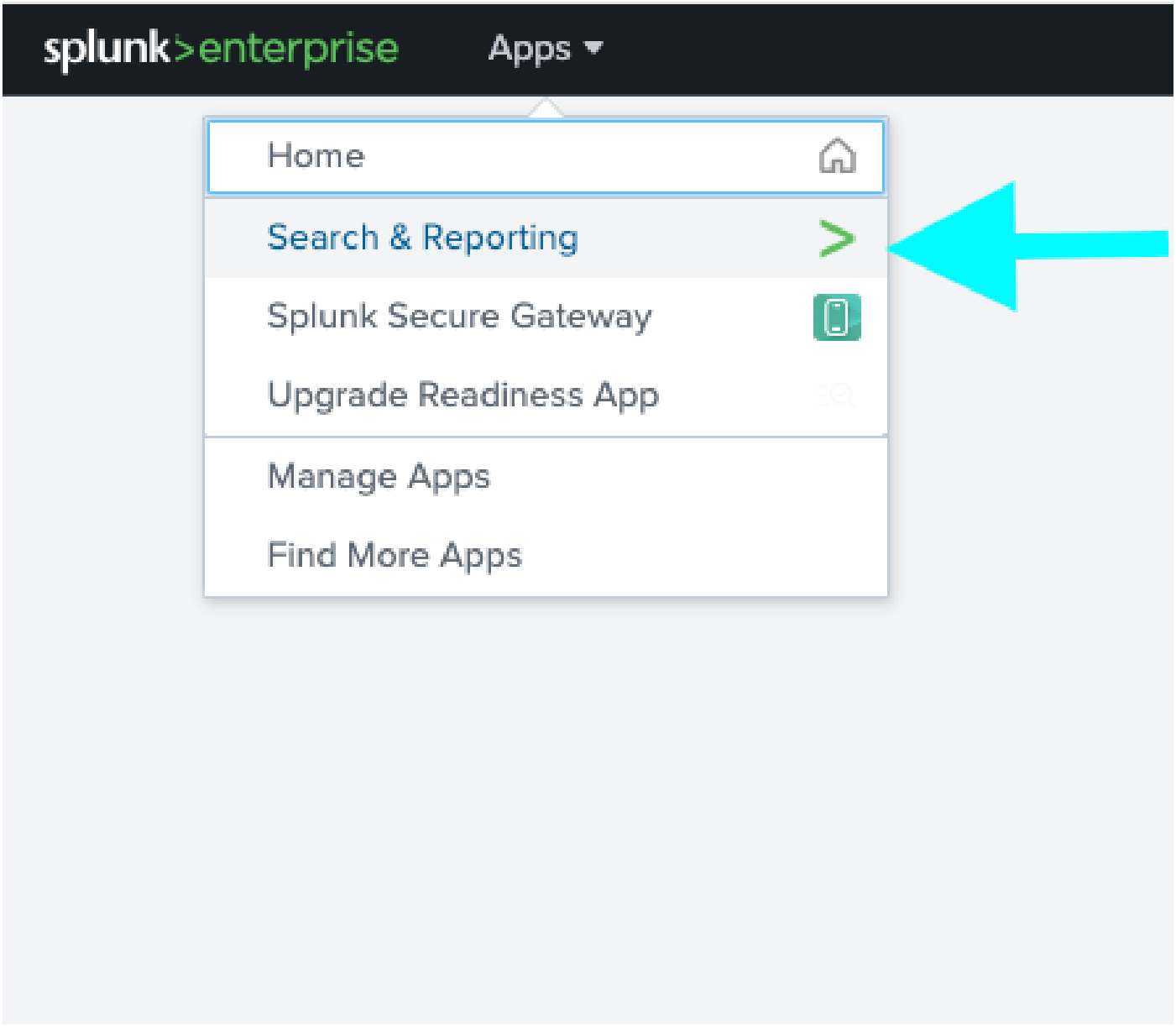
```
user@examplehost:~# chmod 600/opt/splunk/etc/auth/splunkweb.cer
```

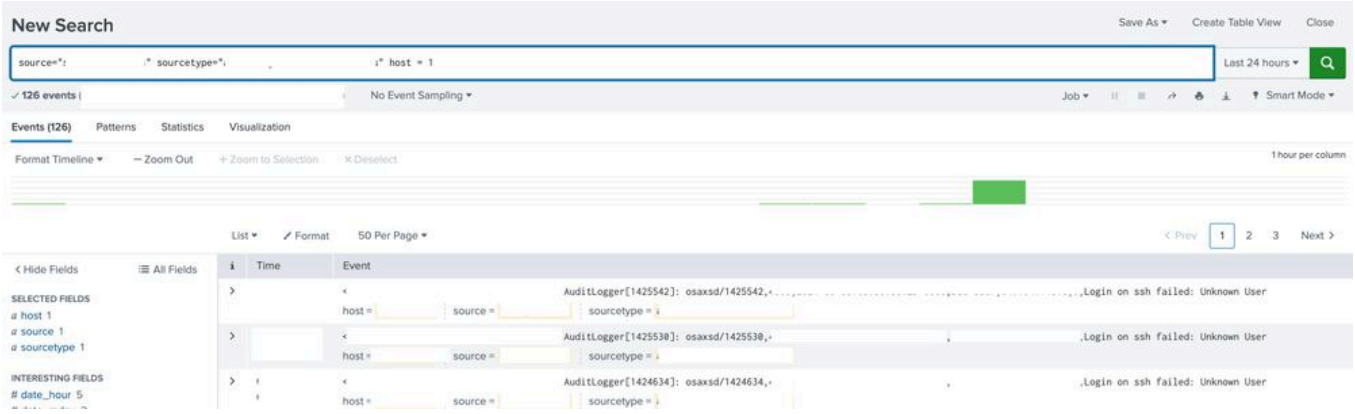
7단계: 새 input.conf 파일을 만듭니다.

```
user@examplehost:~# vim /opt/splunk/etc/system/local/inputs
```



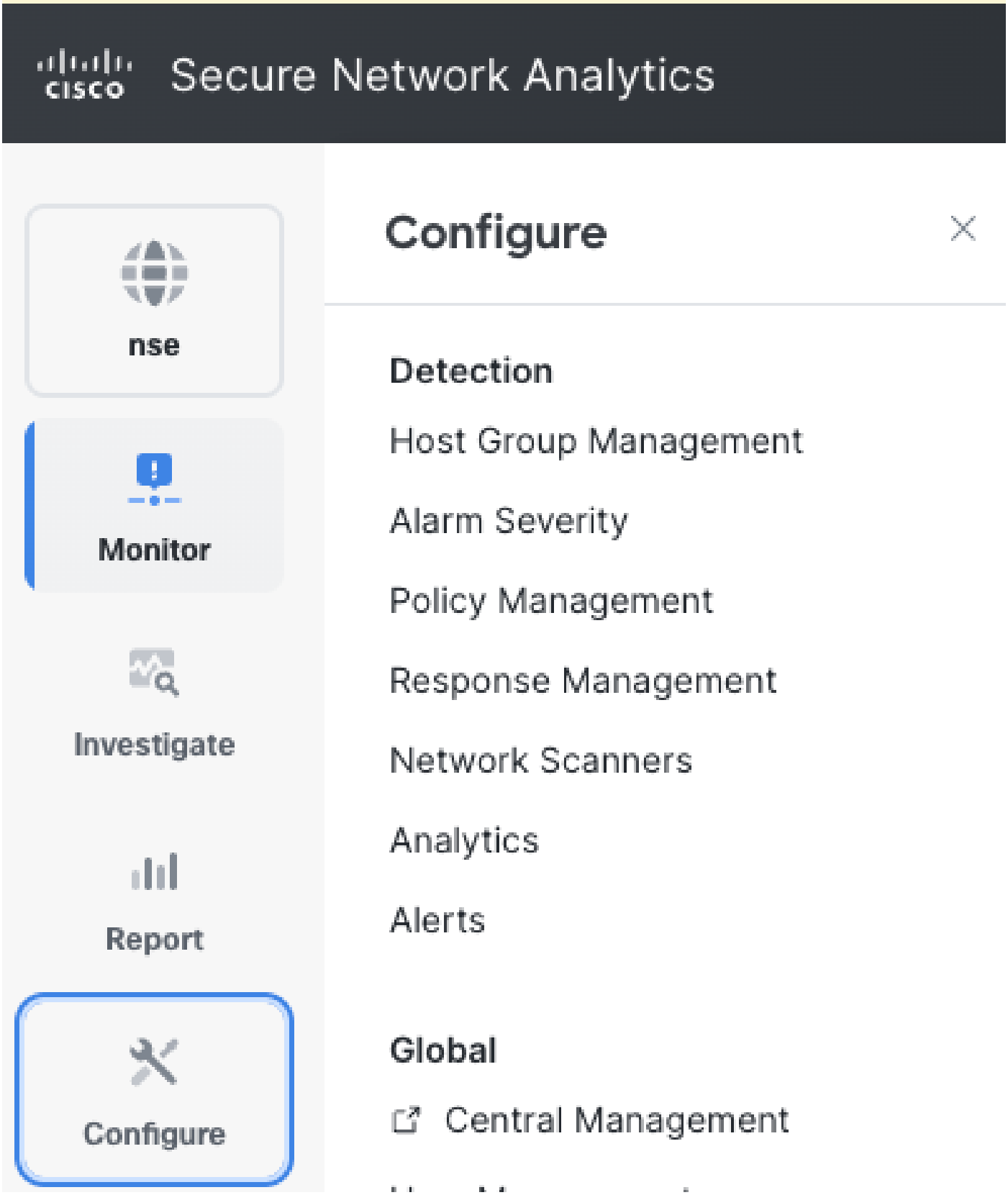
8단계: 검색을 사용하여 syslog를 확인합니다.



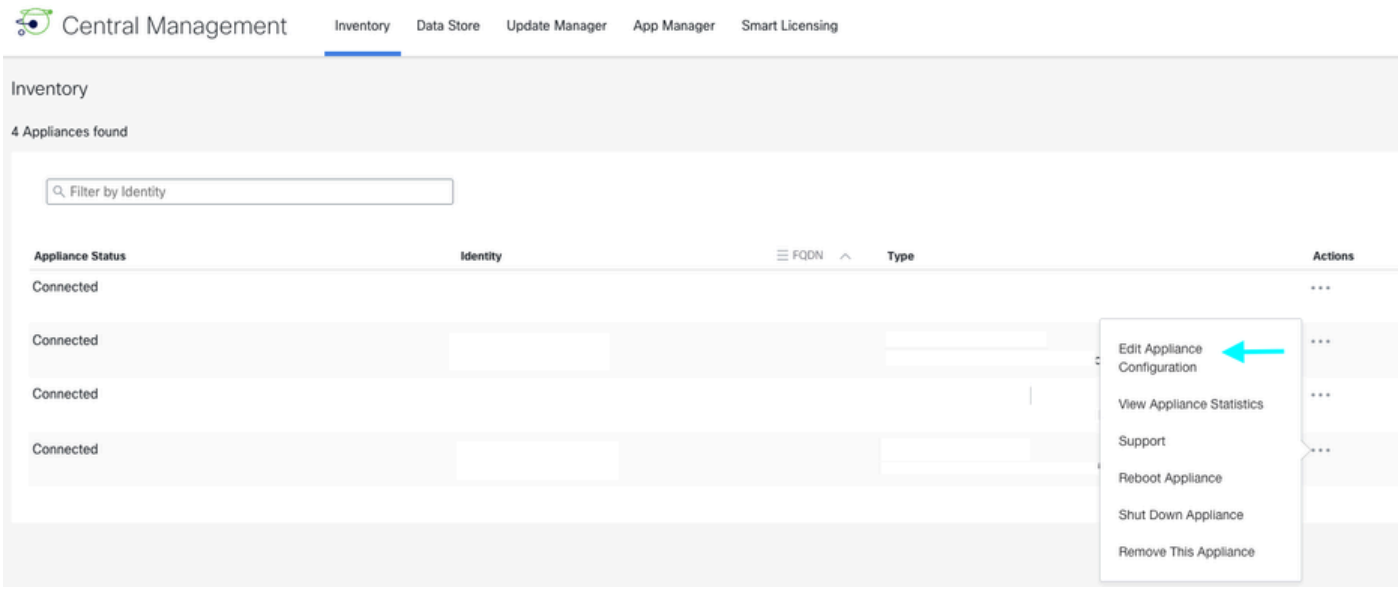


3. SNA에서 감사 로그 대상 구성

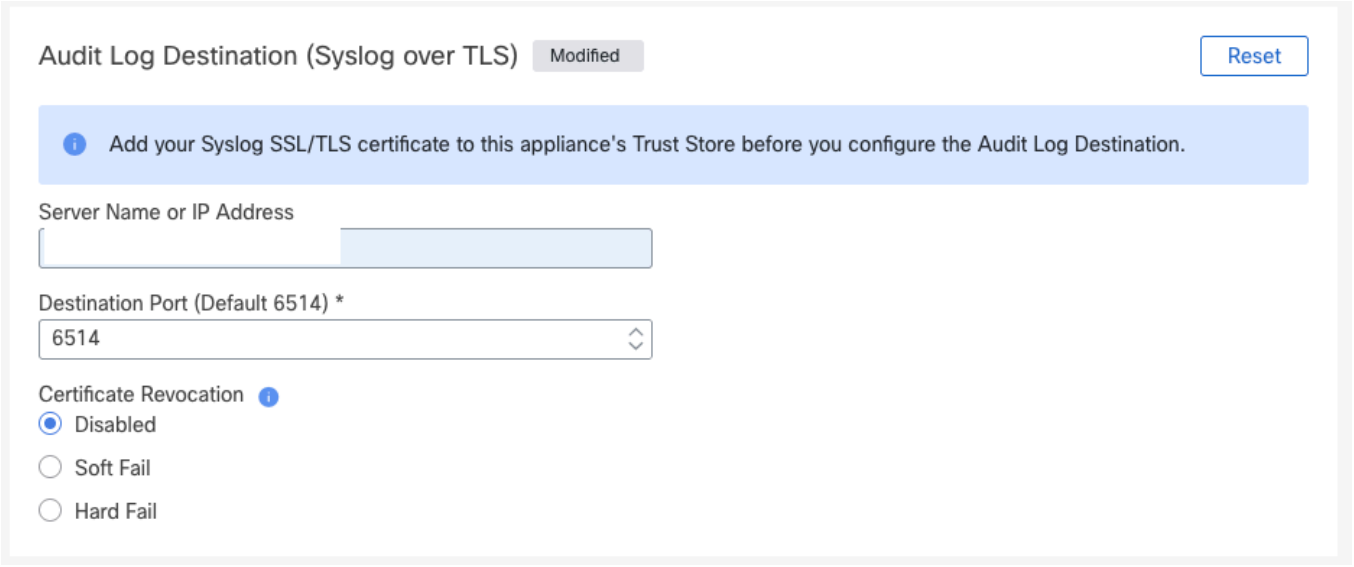
1단계: SMC UI에 로그인하고 Configure(구성) > Central Management(중앙 관리)로 이동합니다.



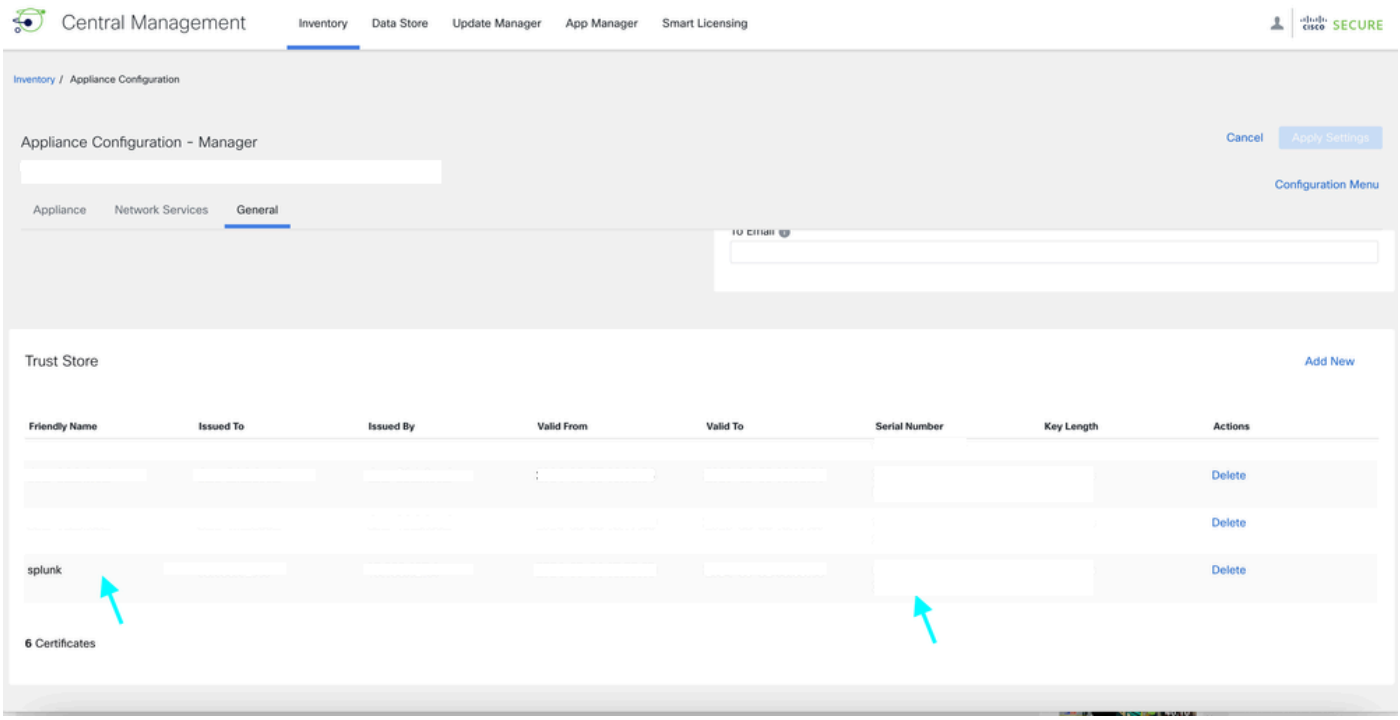
2단계: 원하는 SNA 어플라이언스의 생략 기호 아이콘을 클릭하고 Edit Appliance Configuration(어플라이언스 컨피그레이션 수정)을 선택합니다.



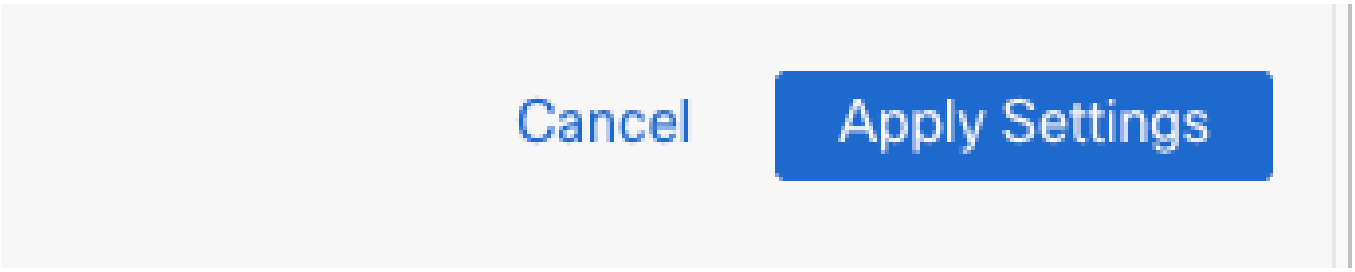
3단계: Network Services(네트워크 서비스) 탭으로 이동하고 Audit Log Destination (Syslog over TLS) 세부 정보를 입력합니다.



4단계: General(일반) 탭으로 이동하고 아래쪽으로 스크롤하여 Add new(새로 추가)를 클릭하여 이전에 생성한 server_cert.pem이라는 Splunk 인증서를 업로드합니다.

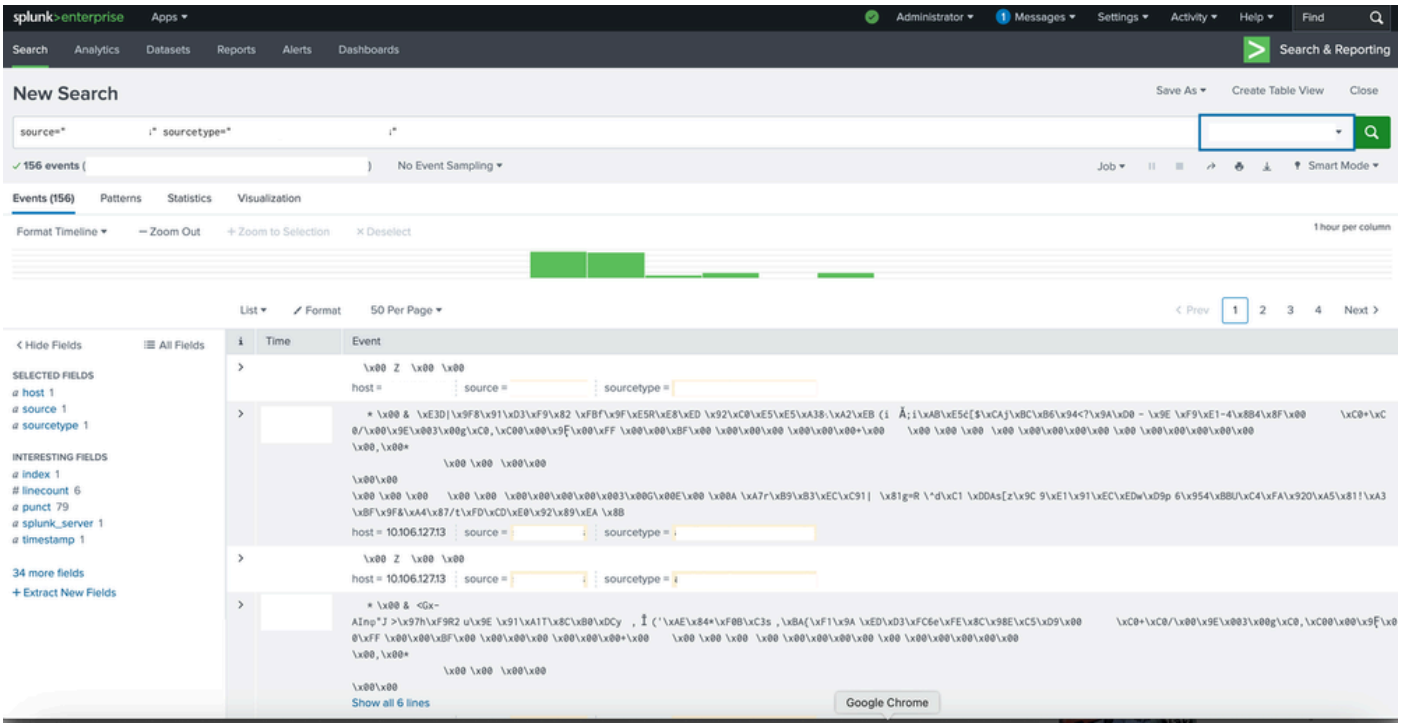


5단계: Apply settings(설정 적용)를 클릭합니다.



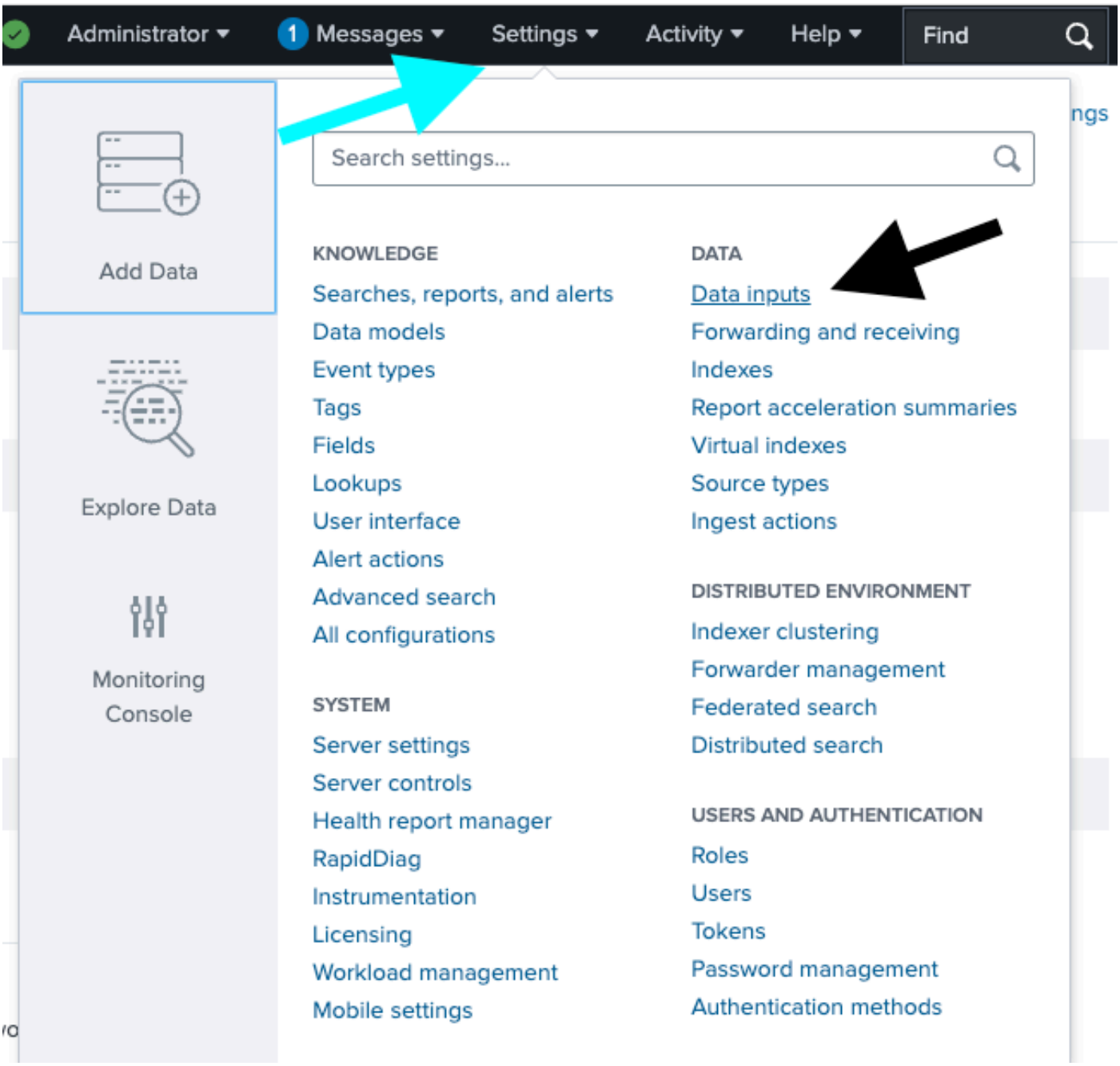
문제 해결

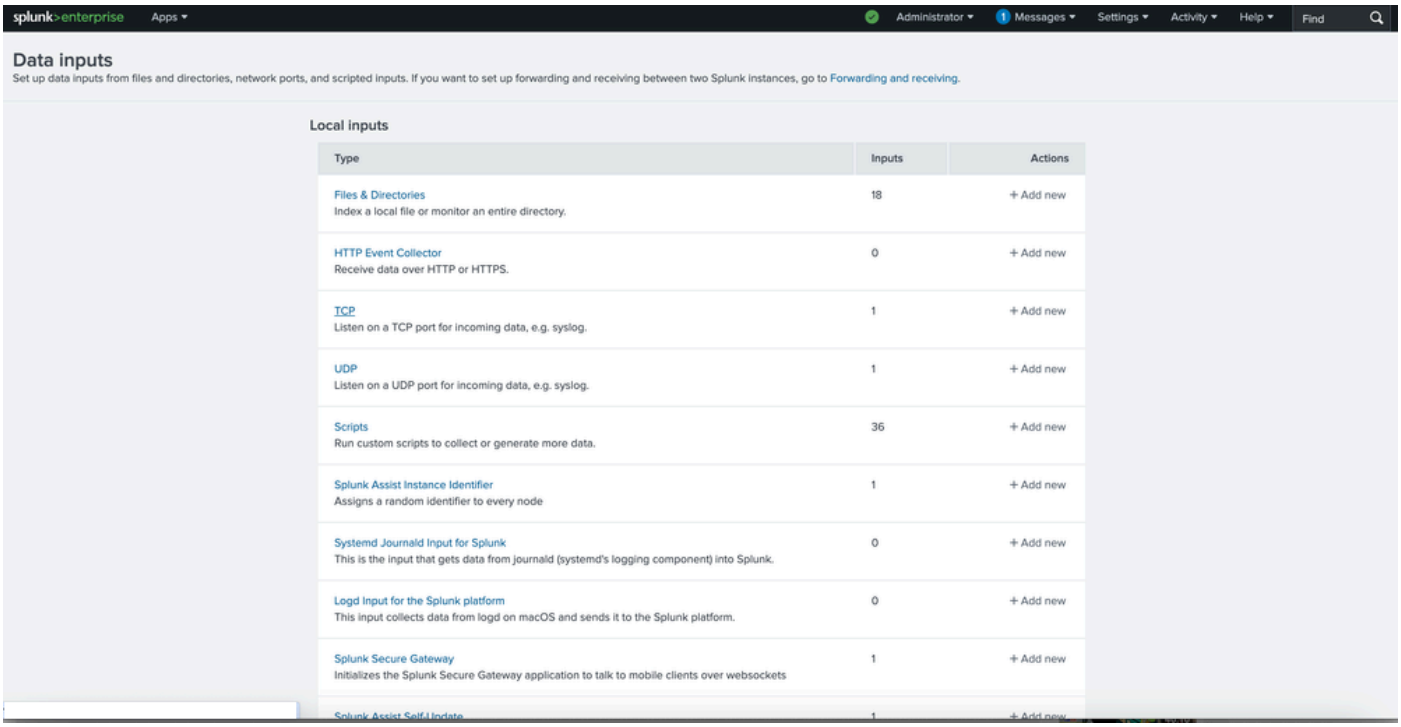
수색 중에 완전한 횡설수설적인 것이 나타날 수도 있다.

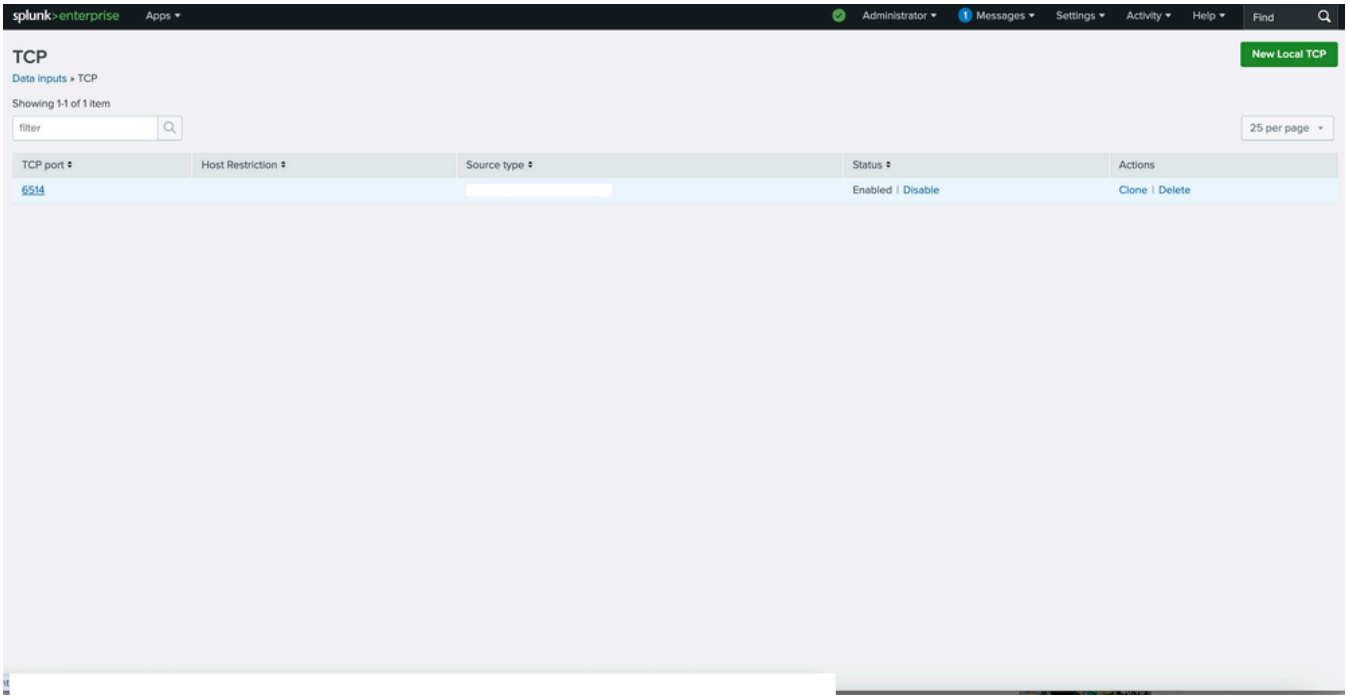


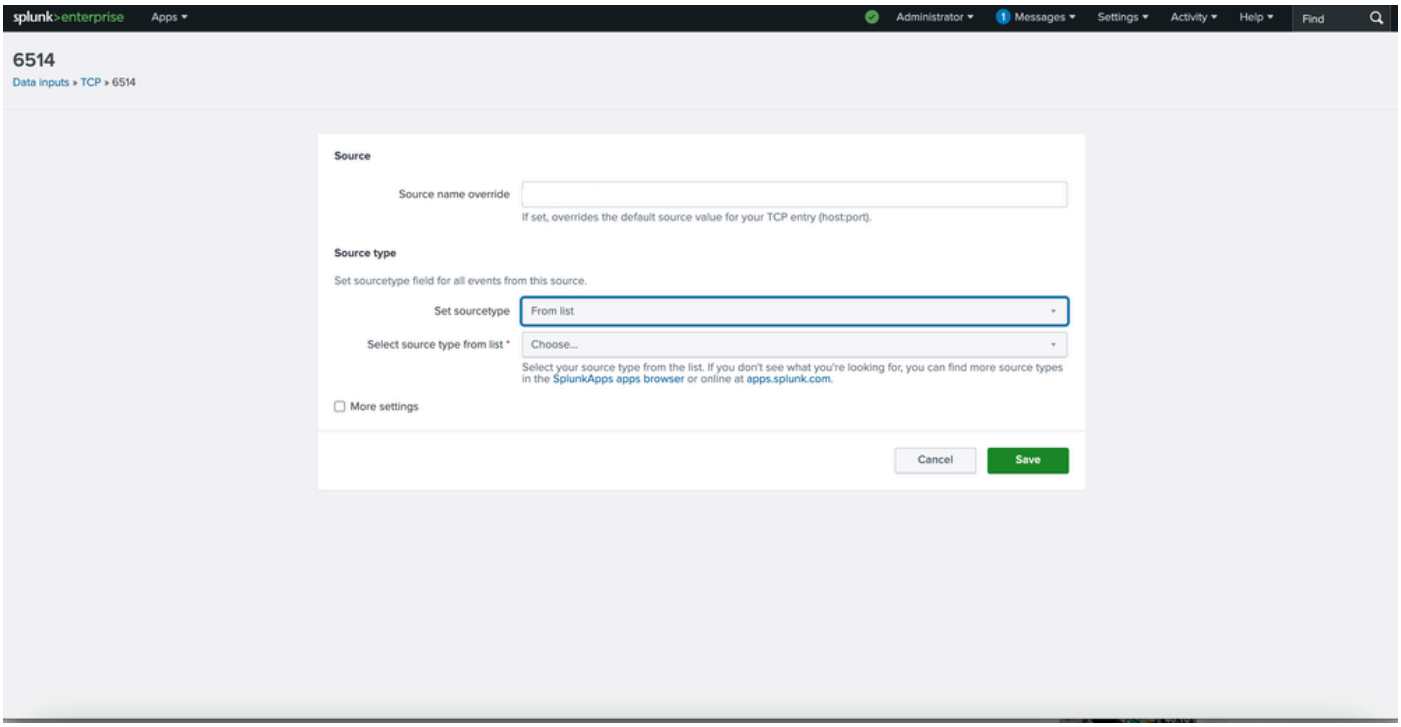
해결책:

입력을 올바른 소스 유형에 매핑합니다.


Administrator
1 Messages
Settings
Activity
Help
Find
Add Data
Explore Data
Monitoring Console
Search settings...
KNOWLEDGE
Searches, reports, and alerts
Data models
Event types
Tags
Fields
Lookups
User interface
Alert actions
Advanced search
All configurations
SYSTEM
Server settings
Server controls
Health report manager
RapidDiag
Instrumentation
Licensing
Workload management
Mobile settings
DATA
Data inputs
Forwarding and receiving
Indexes
Report acceleration summaries
Virtual indexes
Source types
Ingest actions
DISTRIBUTED ENVIRONMENT
Indexer clustering
Forwarder management
Federated search
Distributed search
USERS AND AUTHENTICATION
Roles
Users
Tokens
Password management
Authentication methods


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Data inputs
Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to Forwarding and receiving.
Local inputs
Type
Inputs
Actions
Files & Directories
Index a local file or monitor an entire directory.
18
+ Add new
HTTP Event Collector
Receive data over HTTP or HTTPS.
0
+ Add new
TCP
Listen on a TCP port for incoming data, e.g. syslog.
1
+ Add new
UDP
Listen on a UDP port for incoming data, e.g. syslog.
1
+ Add new
Scripts
Run custom scripts to collect or generate more data.
36
+ Add new
Splunk Assist Instance Identifier
Assigns a random identifier to every node
1
+ Add new
Systemd Journald Input for Splunk
This is the input that gets data from journald (systemd's logging component) into Splunk.
0
+ Add new
Logd Input for the Splunk platform
This input collects data from logd on macOS and sends it to the Splunk platform.
0
+ Add new
Splunk Secure Gateway
Initializes the Splunk Secure Gateway application to talk to mobile clients over websockets
1
+ Add new
Splunk Assist Self-Update
1
+ Add new


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
TCP
New Local TCP
Data inputs › TCP
Showing 1-1 of 1 item
filter
25 per page
TCP port
Host Restriction
Source type
Status
Actions
6514
Enabled | Disable
Clone | Delete


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
6514
Data inputs » TCP » 6514
Source
Source name override
If set, overrides the default source value for your TCP entry (host:port).
Source type
Set sourcetype field for all events from this source.
Set sourcetype
From list
Select source type from list *
Choose...
Select your source type from the list. If you don't see what you're looking for, you can find more source types in the SplunkApps apps browser or online at apps.splunk.com.
More settings
Cancel
Save

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.