

# Splunk에 Syslog 이벤트를 전송하도록 응답 관리 구성

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[UDP 514 또는 사용자 정의 포트를 통해 SNA에 syslog 구성](#)

[1.SNA 응답 관리](#)

[2. UDP 포트를 통해 SNA Syslog를 수신하도록 Splunk 구성](#)

[TCP 포트 6514 또는 사용자 정의 포트를 통해 SNA에서 syslog 구성](#)

[1. TCP 포트를 통해 SNA 감사 로그를 수신하도록 Splunk 구성](#)

[2. Splunk용 인증서 생성](#)

[3. SNA에서 감사 로그 대상 구성](#)

[문제 해결](#)

---

## 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

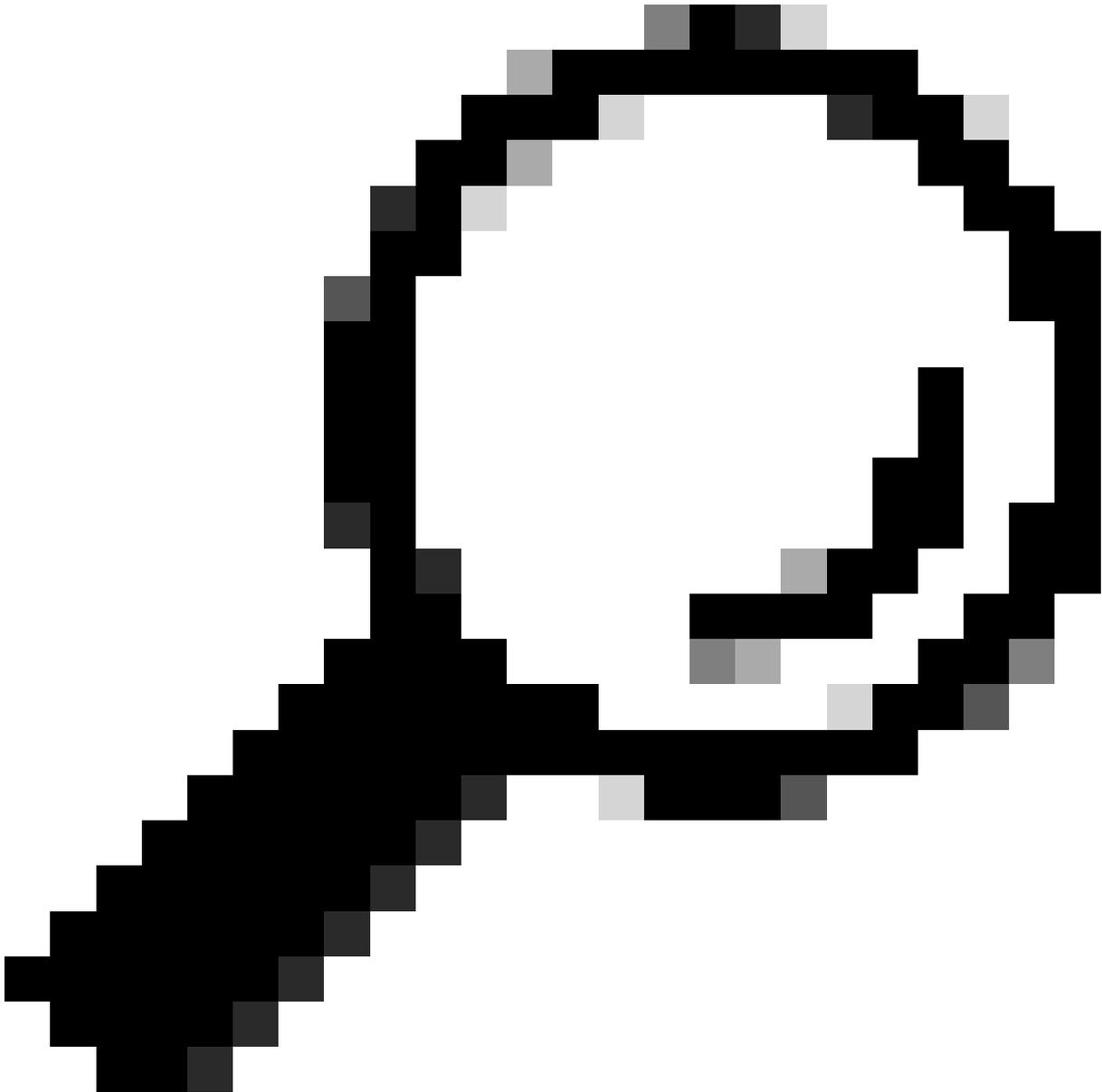
### 사용되는 구성 요소

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.

---

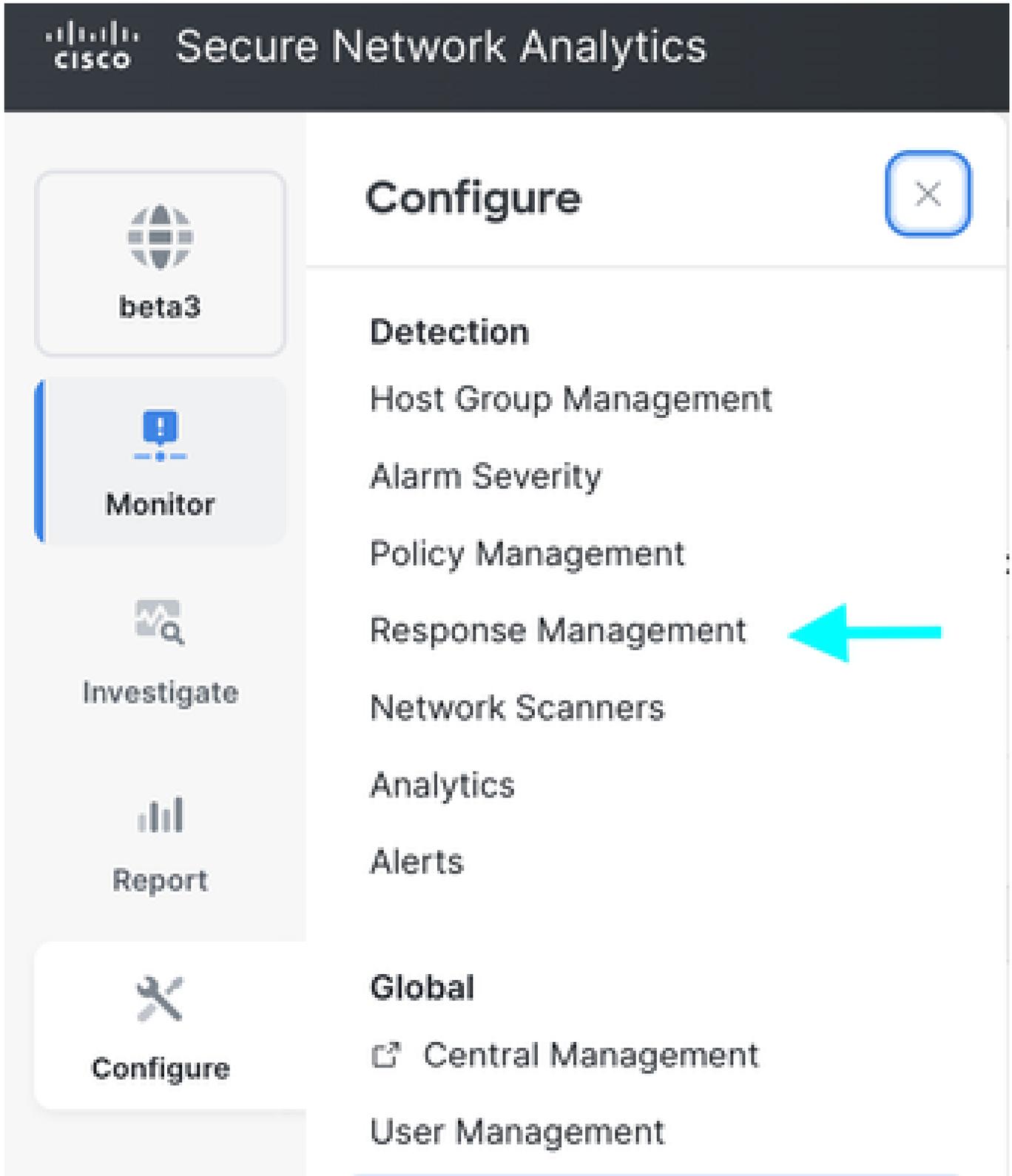
## 1.SNA 응답 관리

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.

Response Management

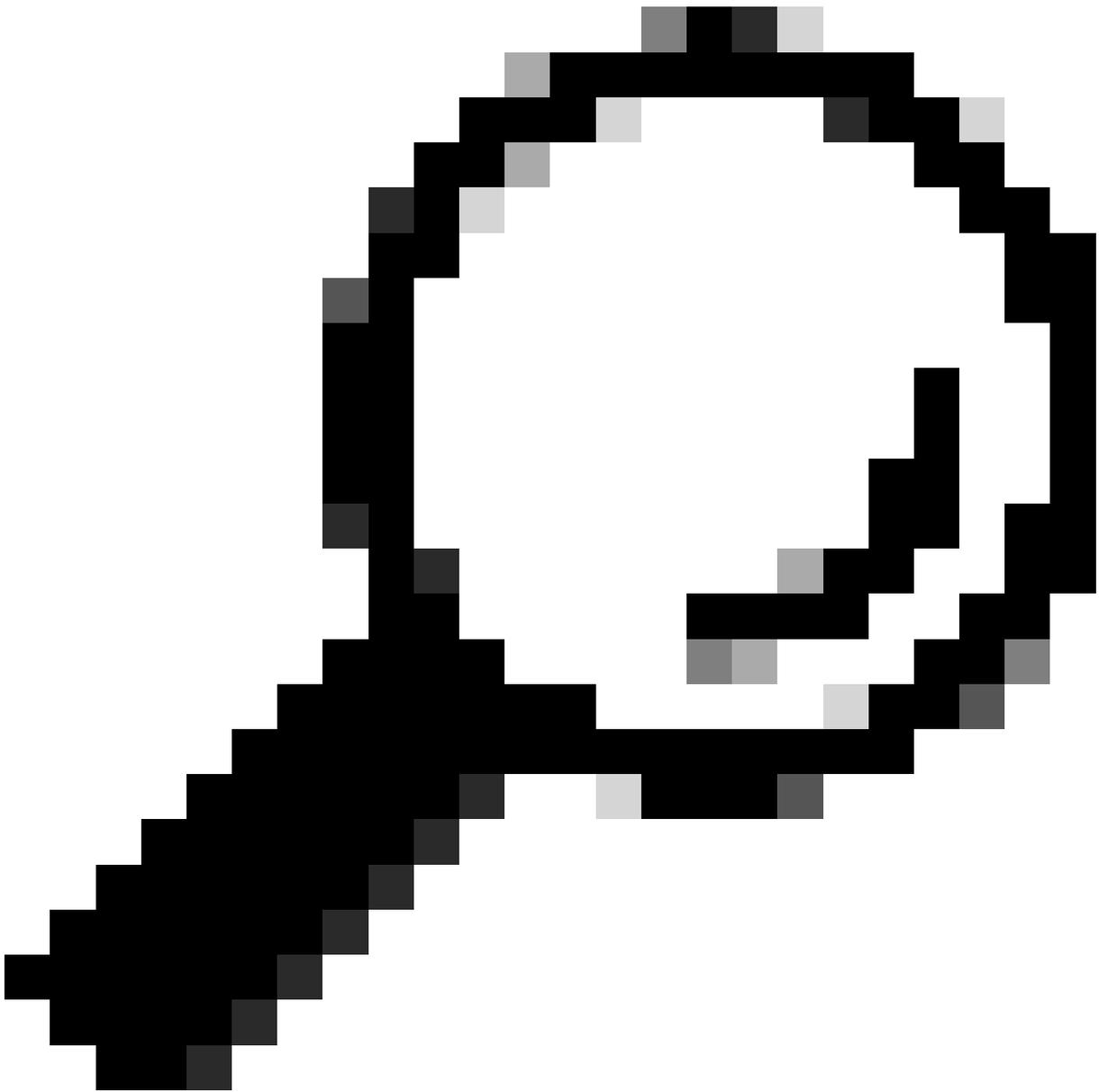
Rules **Actions** Syslog Formats

Actions Add New Action

Name ↑	Type	Description	Used By Rules	Enabled	Actions
Send email	Email (Alarm)	Sends an email to the recipients designated in the To field on the Email Action page.	4	<input type="checkbox"/>	...
Send email	Email (Alert)	Sends an email to the recipients designated in the To field on the Email (Alert) Action page.	2	<input type="checkbox"/>	...
Send to Syslog	Syslog Message (Alarm)	Sends a message to the syslog server designated in the Syslog Address field using the default Syslog Message format.	4	<input checked="" type="checkbox"/>	...
Send to Syslog	Syslog Message (Alert)	Sends a message to the syslog server designated in the Syslog Address field using the default Syslog Message (Alert) format.	2	<input type="checkbox"/>	<div style="border: 1px solid #ccc; padding: 2px;"> <span>Edit</span>  <span>Duplicate</span>  <span>Delete</span> </div>

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

---

## Response Management

Rules **Actions** Syslog Formats

### Syslog Message Action (Alarm)

Cancel

Save

Name

Send to Syslog

Description

Sends a message to the syslog server designated in the Syslog Address field using the default Syslog Message format.



Enabled Disabled actions are not performed for any associated rules.

Syslog Server Address

[Redacted]

UDP Port

514

Message Format

Custom

**CEF**

This action will use the ArcSight Common Event format.

Example Message

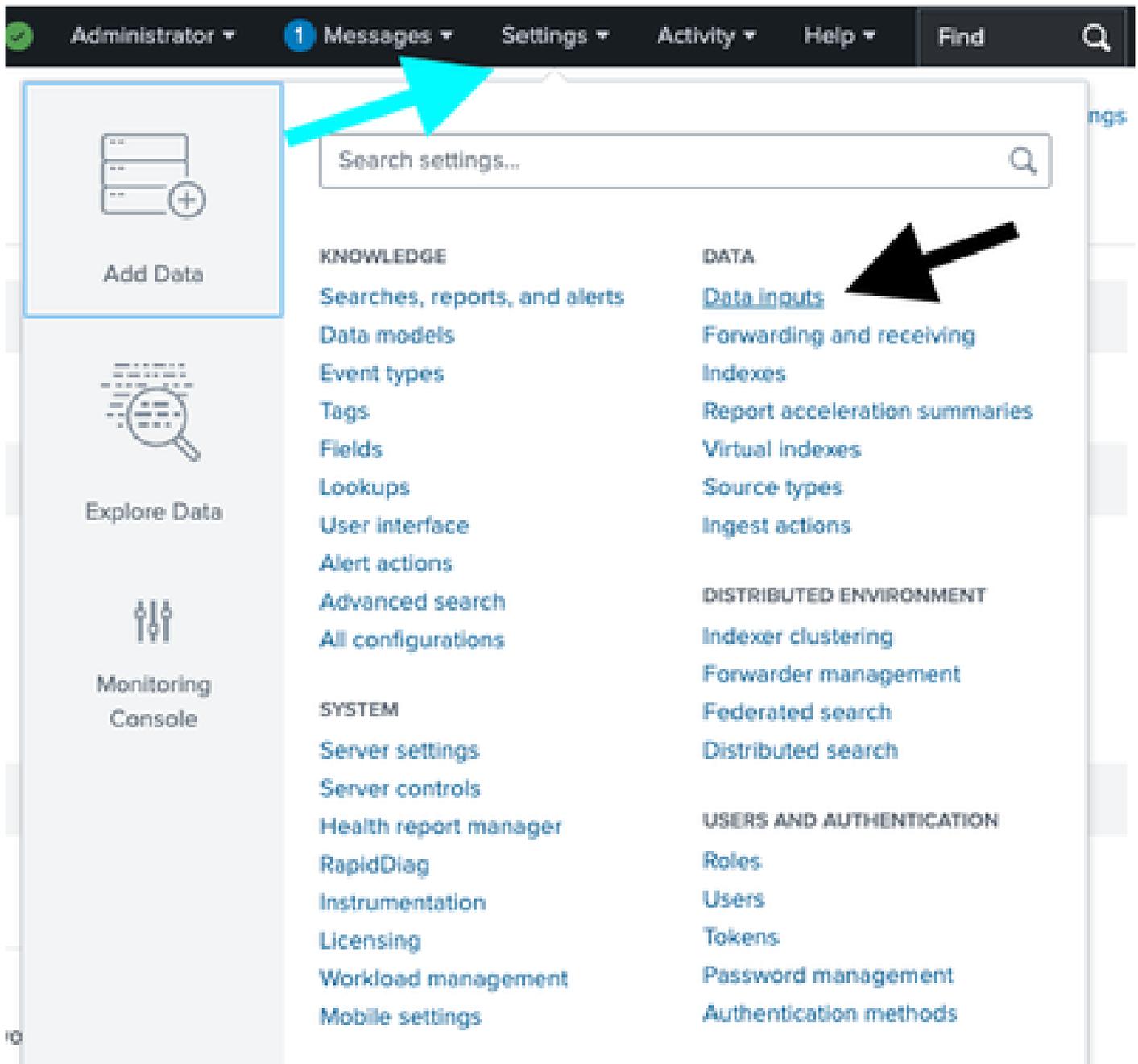
<131>Jan 01 00:00:00 test.host TestApp[1337]: CEF:0|Cisco|7.3.0|Notification:99|Bad Host|5|msg=This host has been observed performing malicious actions toward another host.:Source Host is http (80

Test Action

## 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.

inputs. If you want to set up forwarding and receiving between two Splunk instances, go to [Forwarding and receiving](#).

### Local Inputs

Type	Inputs	Actions
<b>Files &amp; Directories</b> Index a local file or monitor an entire directory.	18	+ Add new
<b>HTTP Event Collector</b> Receive data over HTTP or HTTPS.	0	+ Add new
<b>TCP</b> Listen on a TCP port for incoming data, e.g. syslog.	1	+ Add new
<b>UDP</b> Listen on a UDP port for incoming data, e.g. syslog.	1	+ Add new
<b>Scripts</b> Run custom scripts to collect or generate more data.	36	+ Add new
<b>Splunk Assist Instance Identifier</b> Assigns a random identifier to every node	1	+ Add new
<b>Systemd Journald input for Splunk</b> This is the input that gets data from journald (systemd's logging component) into Splunk.	0	+ Add new
<b>Logd input for the Splunk platform</b> This input collects data from logd on macOS and sends it to the Splunk platform.	0	+ Add new

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.

**Add Data** Select Source Input Settings Review Done < Back Next >

**Files & Directories**  
Upload a file, index a local file, or monitor an entire directory.

**HTTP Event Collector**  
Configure tokens that clients can use to send data over HTTP or HTTPS.

**TCP / UDP** >  
Configure the Splunk platform to listen on a network port.

**Scripts**  
Get data from any API, service, or database with a script.

**Splunk Assist Instance Identifier**  
Assigns a random identifier to every node

**Systemd Journald Input for Splunk**  
This is the input that gets data from journald (systemd's logging component) into Splunk.

**Logd Input for the Splunk platform**  
This input collects data from logd on macOS and sends it to the Splunk platform.

**Splunk Secure Gateway**  
Initializes the Splunk Secure Gateway application to talk to mobile clients over websockets

**Splunk Assist Self-Update**

Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). [Learn More](#)

TCP
UDP

Port ?   
Example: 514

Source name override ?

Only accept connection from ?   
example: 10.1.2.3, lbadhost.splunk.com, \*.splunk.com

**FAQ**

- > How should I configure the Splunk platform for syslog traffic?
- > What's the difference between receiving data over TCP versus UDP?
- > Can I collect syslog data from Windows systems?
- > What is a source type?

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.

## Input Settings

Optionally set additional input parameters for this data input as follows:

### Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Source Type

Source Type Category

Source Type Description

### App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. [Learn More](#)

App Context

### Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

Method ?

### Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your

Index  [Create a new index](#)

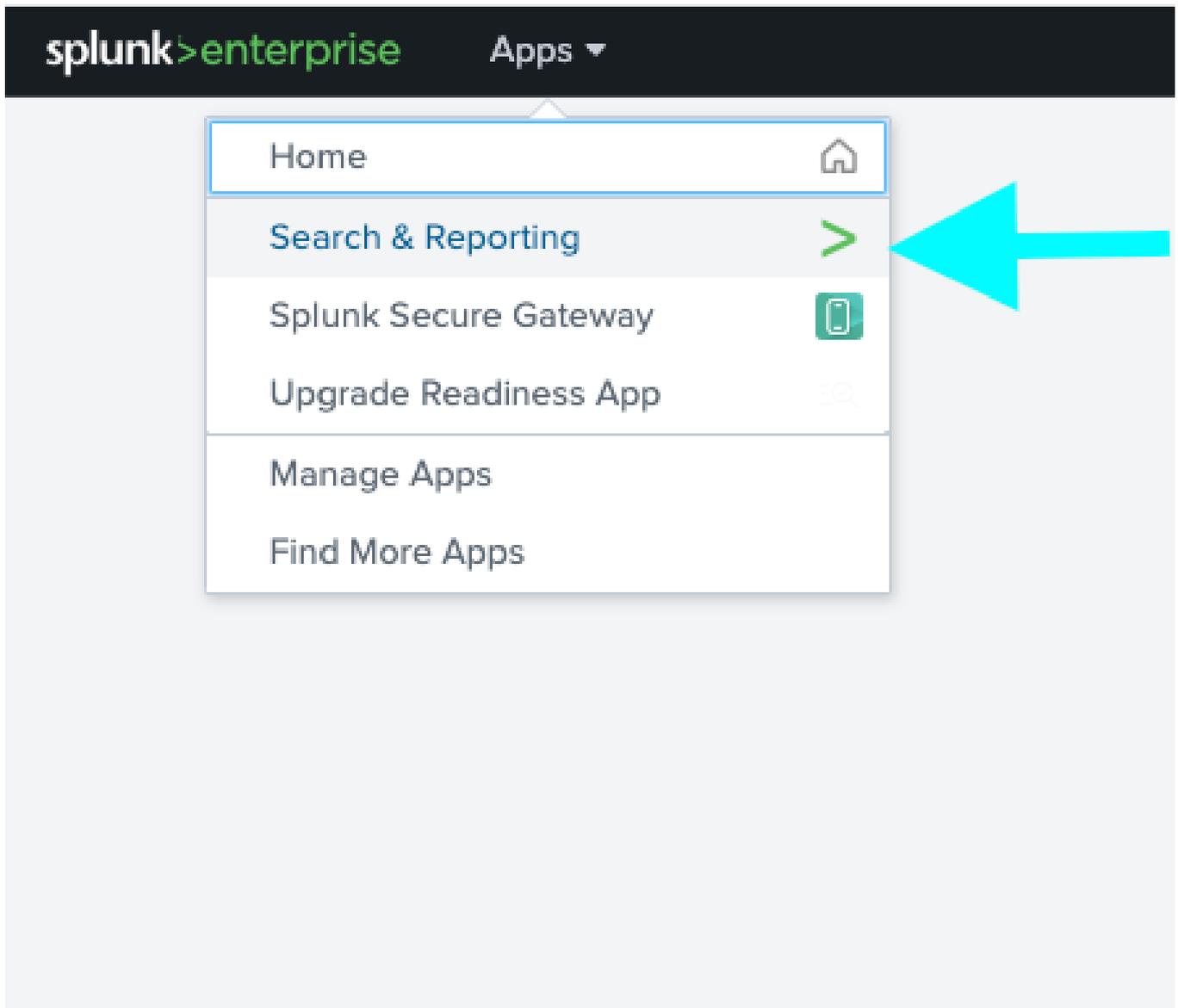
9단계: 다음 창에서 설정을 검토하고 필요한 경우 수정합니다.

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

## Review

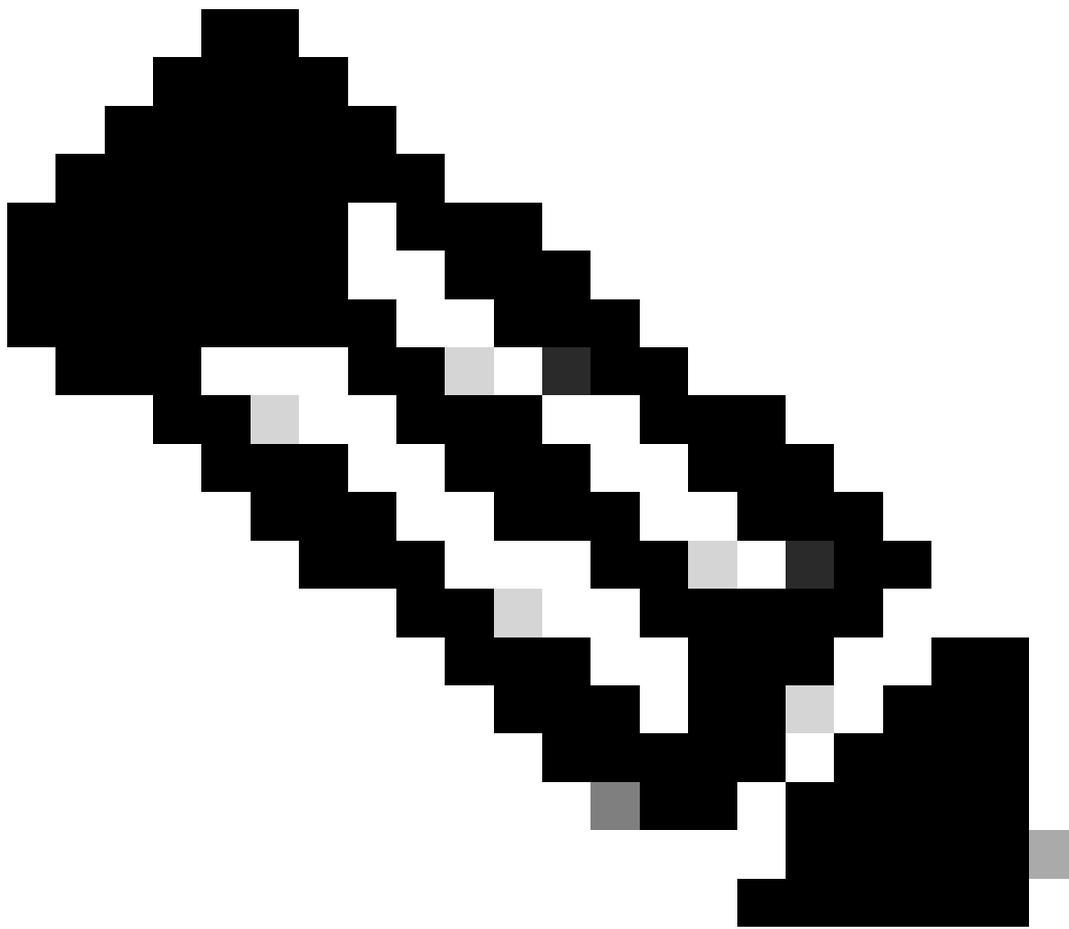
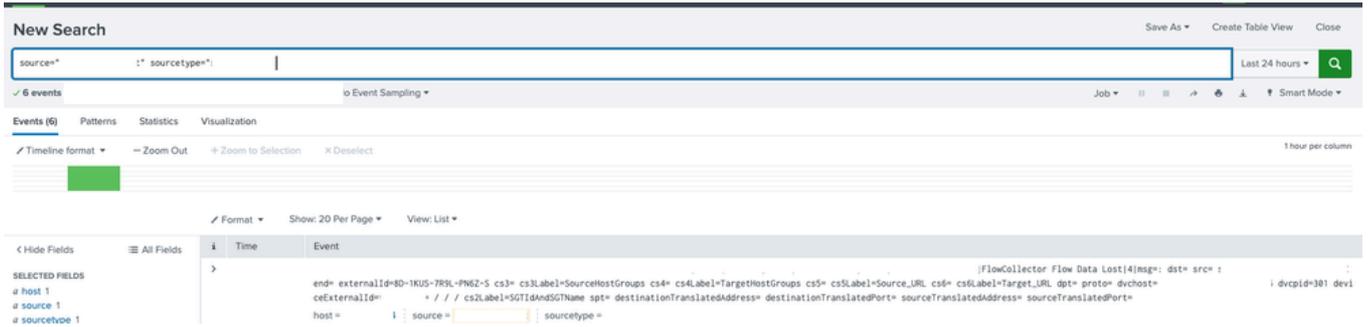
Input Type ..... UDP Port  
Port Number ..... 514  
Source name override .....  
Restrict to Host ..... N/A  
Source Type .....  
App Context ..... search  
Host ..... (IP address of the remote server)  
Index ..... default

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



12단계: Search(검색) 페이지에서 필터를 사용하여 `source="As_configured" sourcetype="As_configured"` 수신된 로

그를 찾습니다.

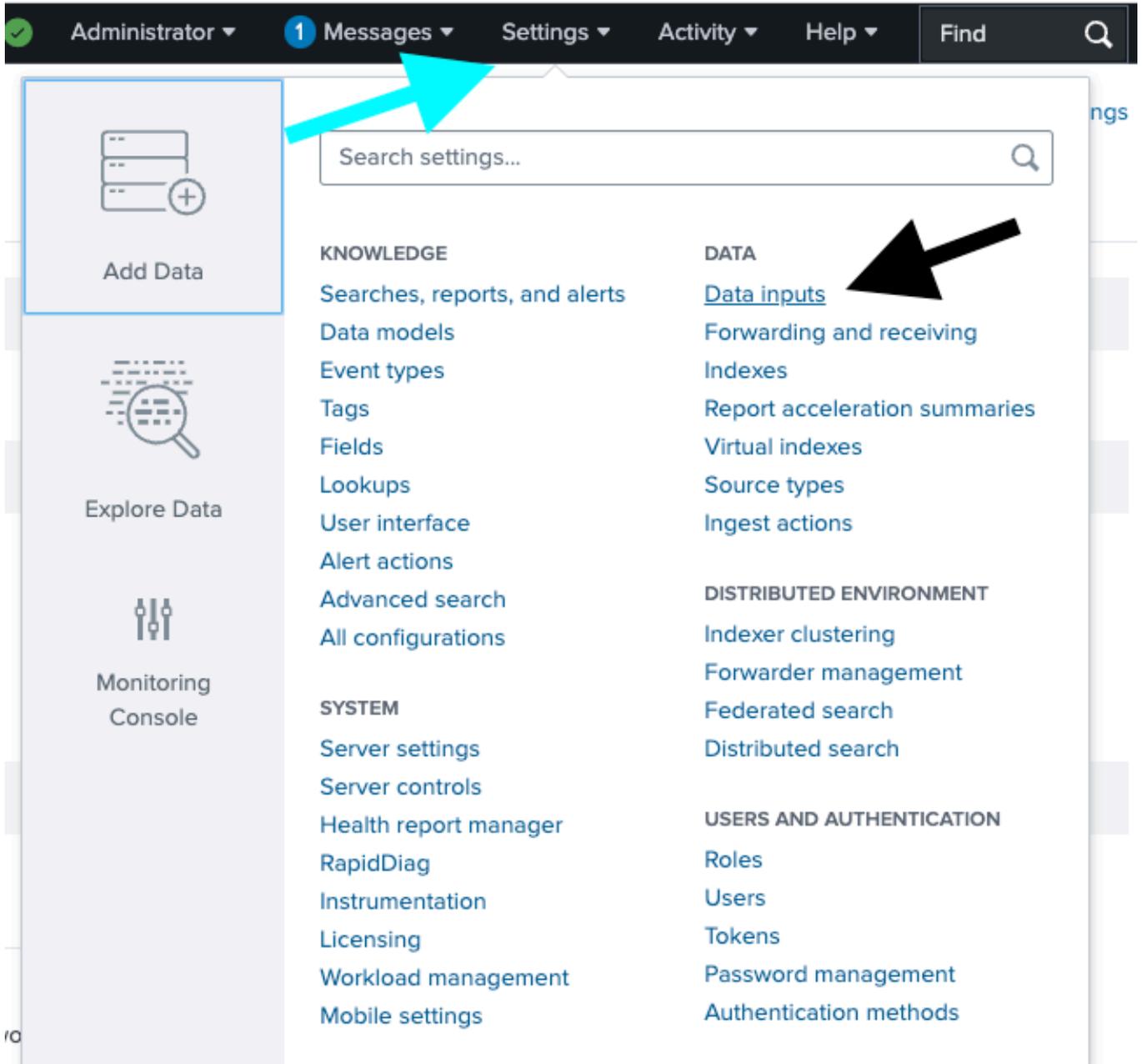


참고: 소스에 대해서는 4단계를 참조하십시오.  
source\_type의 경우 6단계를 참조하십시오.

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.

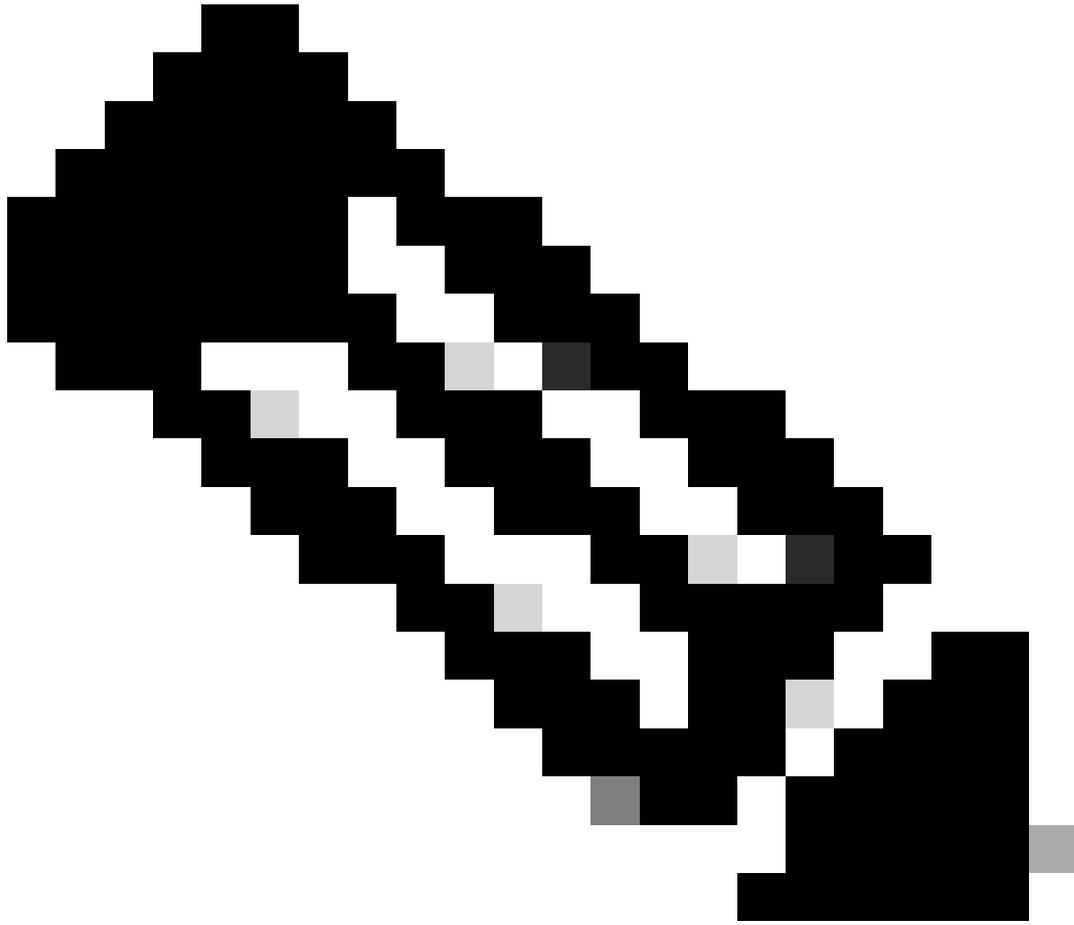
es and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to [Forwarding and receiving](#).

### Local inputs

Type	Inputs	Actions
<b>Files &amp; Directories</b> Index a local file or monitor an entire directory.	18	+ Add new
<b>HTTP Event Collector</b> Receive data over HTTP or HTTPS.	0	+ Add new
<b>TCP</b> Listen on a TCP port for incoming data, e.g. syslog.	0	+ Add new
<b>UDP</b> Listen on a UDP port for incoming data, e.g. syslog.	0	+ Add new
<b>Scripts</b> Run custom scripts to collect or generate more data.	36	+ Add new
<b>Splunk Assist Instance Identifier</b> Assigns a random identifier to every node	1	+ Add new
<b>Systemd Journal Input for Splunk</b> This is the input that gets data from journald (systemd's logging component) into Splunk.	0	+ Add new
<b>Logd Input for the Splunk platform</b> This input collects data from logd on macOS and sends it to the Splunk platform.	0	+ Add new
<b>Splunk Secure Gateway</b> Initializes the Splunk Secure Gateway application to talk to mobile clients over websockets	1	+ Add new



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.

Apps ▾ Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾

**Add Data**    Select Source    Input Settings    Review    Done    < Back    Next >

**Files & Directories**  
Upload a file, index a local file, or monitor an entire directory.

**HTTP Event Collector**  
Configure tokens that clients can use to send data over HTTP or HTTPS.

**TCP / UDP** >  
Configure the Splunk platform to listen on a network port.

**Scripts**  
Get data from any API, service, or database with a script.

**Splunk Assist Instance Identifier**  
Assigns a random identifier to every node

**Systemd Journald Input for Splunk**  
This is the input that gets data from journald (systemd's logging component) into Splunk.

**Logd Input for the Splunk platform**  
This input collects data from logd on macOS and sends it to the Splunk platform.

**Splunk Secure Gateway**  
Initializes the Splunk Secure Gateway application to talk to mobile clients over websockets

**Splunk Assist Self-Update**  
Detects and Downloads Assist Supervisor Updates

**Splunk Secure Gateway Mobile Alerts TTL**  
Cleans up storage of old mobile alerts

**Config Modular Input**

Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). [Learn More](#)

TCP    UDP

Port ?   
Example: 514

Source name override ?   
host:port

Only accept connection from ?   
example: 10.1.2.3, lbadhost.splunk.com, \*.splunk.com

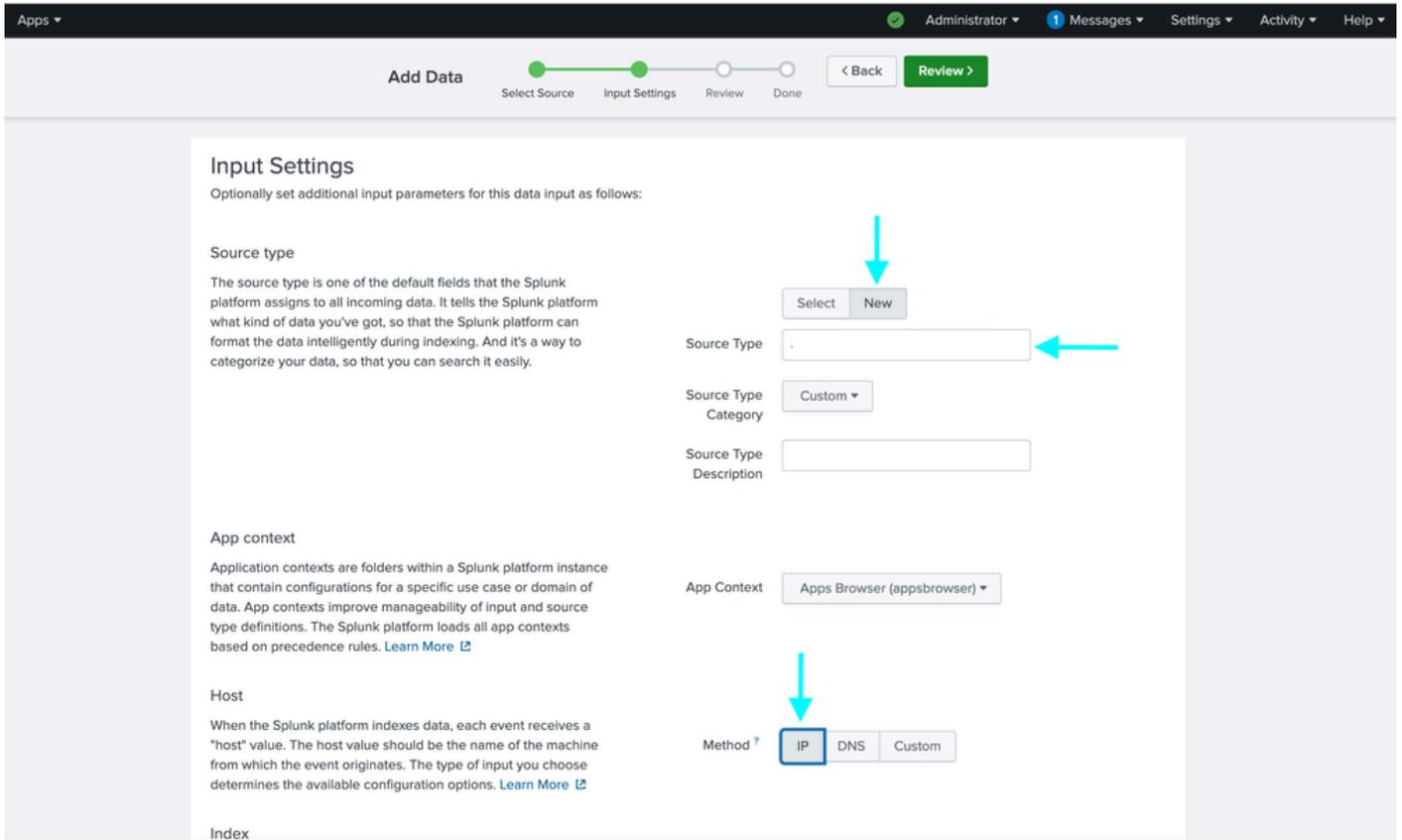
**FAQ**

- > How should I configure the Splunk platform for syslog traffic?
- > What's the difference between receiving data over TCP versus UDP?
- > Can I collect syslog data from Windows systems?
- > What is a source type?

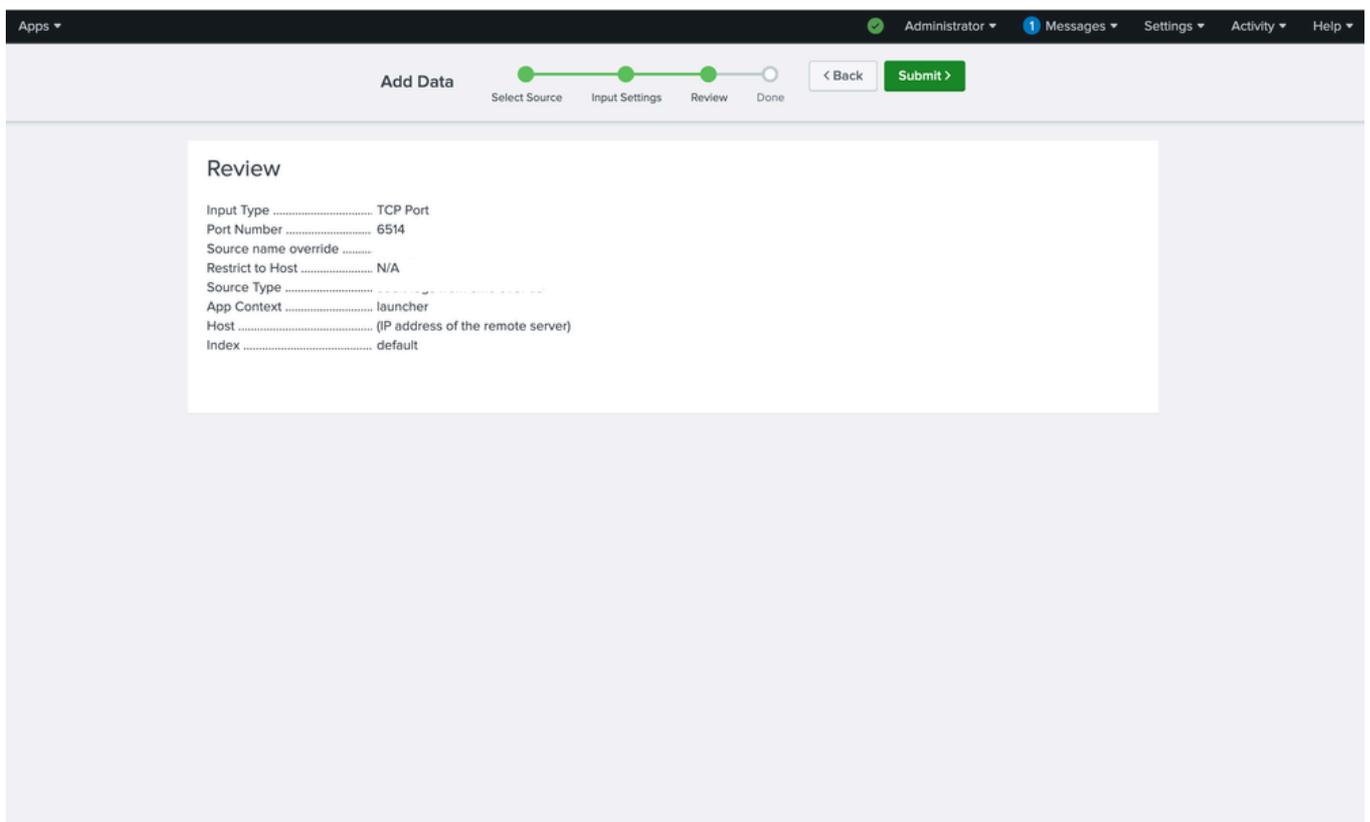
5단계: 새 창의 소스 유형 섹션에서 새로 만들기를 선택하고 소스 유형 필드에 원하는 이름을 입력합니다.

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



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

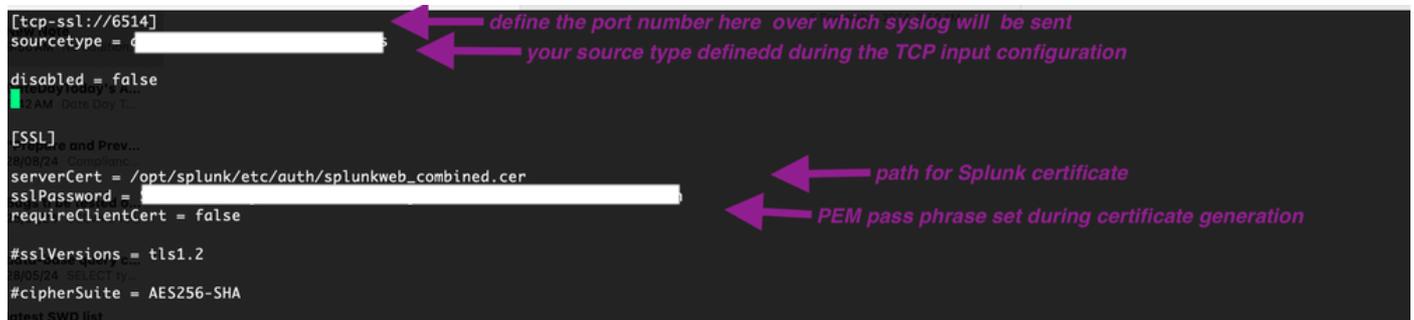
6단계: splunk 인증서에 대한 권한을 변경합니다.

```
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
```

```
[tcp-ssl://6514]
sourcetype = [redacted]
disabled = false
[SSL]
serverCert = /opt/splunk/etc/auth/splunkweb_combined.cer
sslPassword = [redacted]
requireClientCert = false
#sslVersions = tls1.2
#cipherSuite = AES256-SHA
```

A screenshot of a terminal window showing the configuration of a Splunk input. The configuration is for a TCP-SSL listener on port 6514. The 'sourcetype' is set to a redacted value. The 'disabled' flag is set to false. Under the [SSL] section, 'serverCert' is set to '/opt/splunk/etc/auth/splunkweb\_combined.cer', 'sslPassword' is set to a redacted value, and 'requireClientCert' is set to false. Below this, 'sslVersions' is set to 'tls1.2' and 'cipherSuite' is set to 'AES256-SHA'. Four purple arrows point to specific parts of the configuration with explanatory text: one points to the port number '6514' with the text 'define the port number here over which syslog will be sent'; another points to the 'sourcetype' field with the text 'your source type defined during the TCP input configuration'; a third points to the 'serverCert' path with the text 'path for Splunk certificate'; and a fourth points to the 'sslPassword' field with the text 'PEM pass phrase set during certificate generation'.

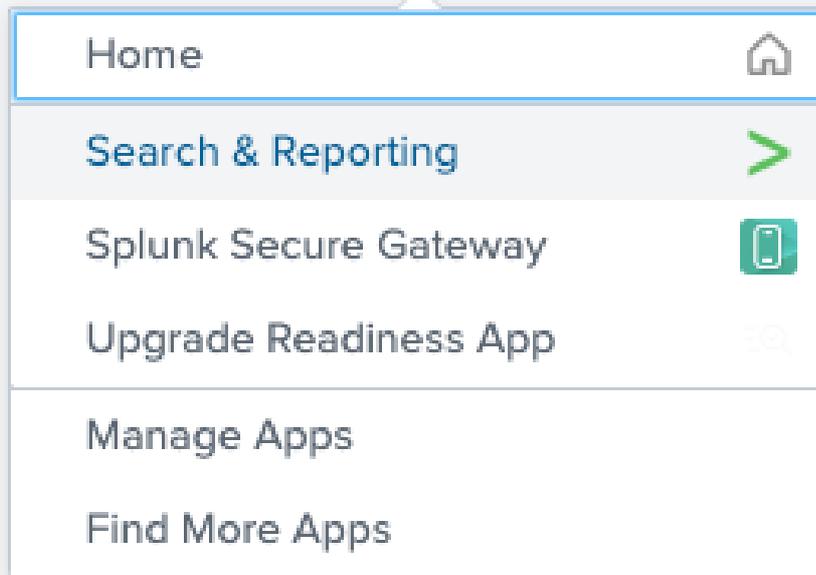
*define the port number here over which syslog will be sent*

*your source type defined during the TCP input configuration*

*path for Splunk certificate*

*PEM pass phrase set during certificate generation*

8단계: 검색을 사용하여 syslog를 확인합니다.



New Search

source="\*" \* sourcetype="\*" \* host = 1

126 events | No Event Sampling

Events (126) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

List Format 50 Per Page

Time	Event
>	< AuditLogger[1425542]: osaxsd/1425542,.....Login on ssh failed: Unknown User
>	< AuditLogger[1425538]: osaxsd/1425538,.....Login on ssh failed: Unknown User
>	< AuditLogger[1424634]: osaxsd/1424634,.....Login on ssh failed: Unknown User

### 3. SNA에서 감사 로그 대상 구성

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



nse



Monitor



Investigate



Report



Configure

## Configure ×

### Detection

Host Group Management

Alarm Severity

Policy Management

Response Management

Network Scanners

Analytics

Alerts

### Global

Central Management

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

Inventory

4 Appliances found

Filter by Identity

Appliance Status	Identity	FQDN	Type	Actions
Connected				...
Connected				<ul style="list-style-type: none"> <li>Edit Appliance Configuration</li> <li>View Appliance Statistics</li> <li>Support</li> <li>Reboot Appliance</li> <li>Shut Down Appliance</li> <li>Remove This Appliance</li> </ul>
Connected				...
Connected				...

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

**Audit Log Destination (Syslog over TLS)** Modified Reset

**i** Add your Syslog SSL/TLS certificate to this appliance's Trust Store before you configure the Audit Log Destination.

Server Name or IP Address

Destination Port (Default 6514) \*

Certificate Revocation **i**

Disabled

Soft Fail

Hard Fail

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

Central Management Inventory Data Store Update Manager App Manager Smart Licensing SECURE

Inventory / Appliance Configuration

Appliance Configuration - Manager Cancel Apply Settings

Configuration Menu

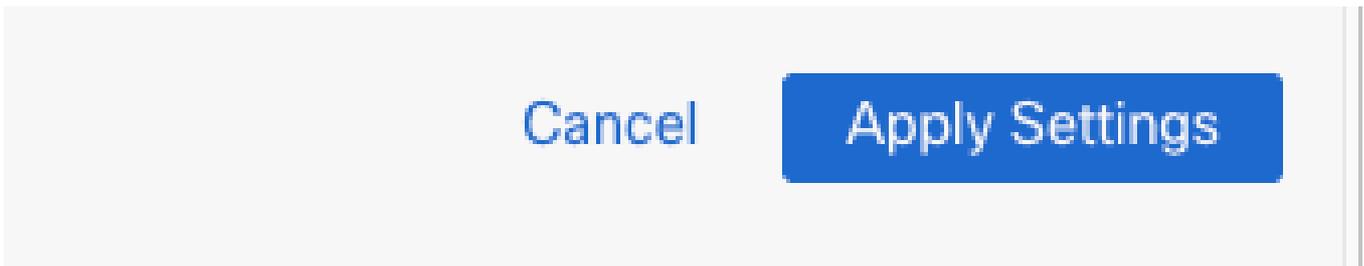
Appliance Network Services General

Trust Store Add New

Friendly Name	Issued To	Issued By	Valid From	Valid To	Serial Number	Key Length	Actions
							Delete
							Delete
splunk							Delete

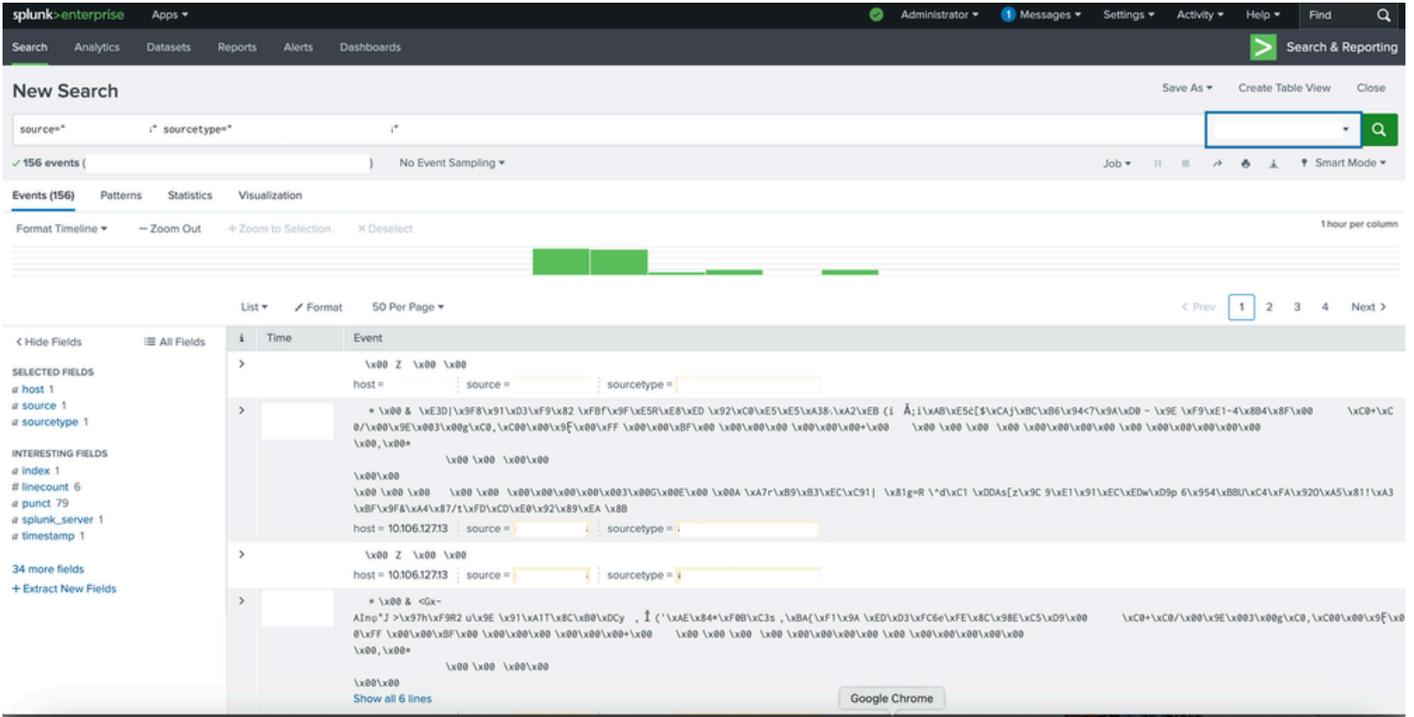
6 Certificates

5단계: Apply settings(설정 적용)를 클릭합니다.



## 문제 해결

수색 중에 완전한 횡설수설적인 것이 나타날 수도 있다.



해결책:

입력을 올바른 소스 유형에 매핑합니다.

  
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



## 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
<a href="#">Files &amp; Directories</a> Index a local file or monitor an entire directory.	18	+ Add new
<a href="#">HTTP Event Collector</a> Receive data over HTTP or HTTPS.	0	+ Add new
<a href="#">TCP</a> Listen on a TCP port for incoming data, e.g. syslog.	1	+ Add new
<a href="#">UDP</a> Listen on a UDP port for incoming data, e.g. syslog.	1	+ Add new
<a href="#">Scripts</a> Run custom scripts to collect or generate more data.	36	+ Add new
<a href="#">Splunk Assist Instance Identifier</a> Assigns a random identifier to every node	1	+ Add new
<a href="#">Systemd Journald Input for Splunk</a> This is the input that gets data from journald (systemd's logging component) into Splunk.	0	+ Add new
<a href="#">Logd Input for the Splunk platform</a> This input collects data from logd on macOS and sends it to the Splunk platform.	0	+ Add new
<a href="#">Splunk Secure Gateway</a> Initializes the Splunk Secure Gateway application to talk to mobile clients over websockets	1	+ Add new
<a href="#">Splunk Assist Self Update</a>	1	+ Add new

## TCP

Data inputs > TCP

New Local TCP

Showing 1-1 of 1 item

25 per page

TCP port	Host Restriction	Source type	Status	Actions
6514			Enabled   Disable	Clone   Delete

# 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

Select source type from list \*

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.