

Configure Response Management to Send Syslog Events to Splunk

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure syslog on SNA over UDP 514 or custom defined port](#)

[1.SNA Response Management](#)

[2.Configuring Splunk to Receive SNA Syslogs over UDP port](#)

[Configure syslog on SNA over TCP port 6514 or custom defined port](#)

[1.Configuring Splunk to Receive SNA Audit Logs over TCP port](#)

[2.Generate Certificate for Splunk](#)

[3.Configure Audit Log Destination on SNA](#)

[Troubleshoot](#)

Introduction

This document describes how to configure the Secure Analytics Response Management feature to send events via syslog to a 3rd party such as Splunk.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

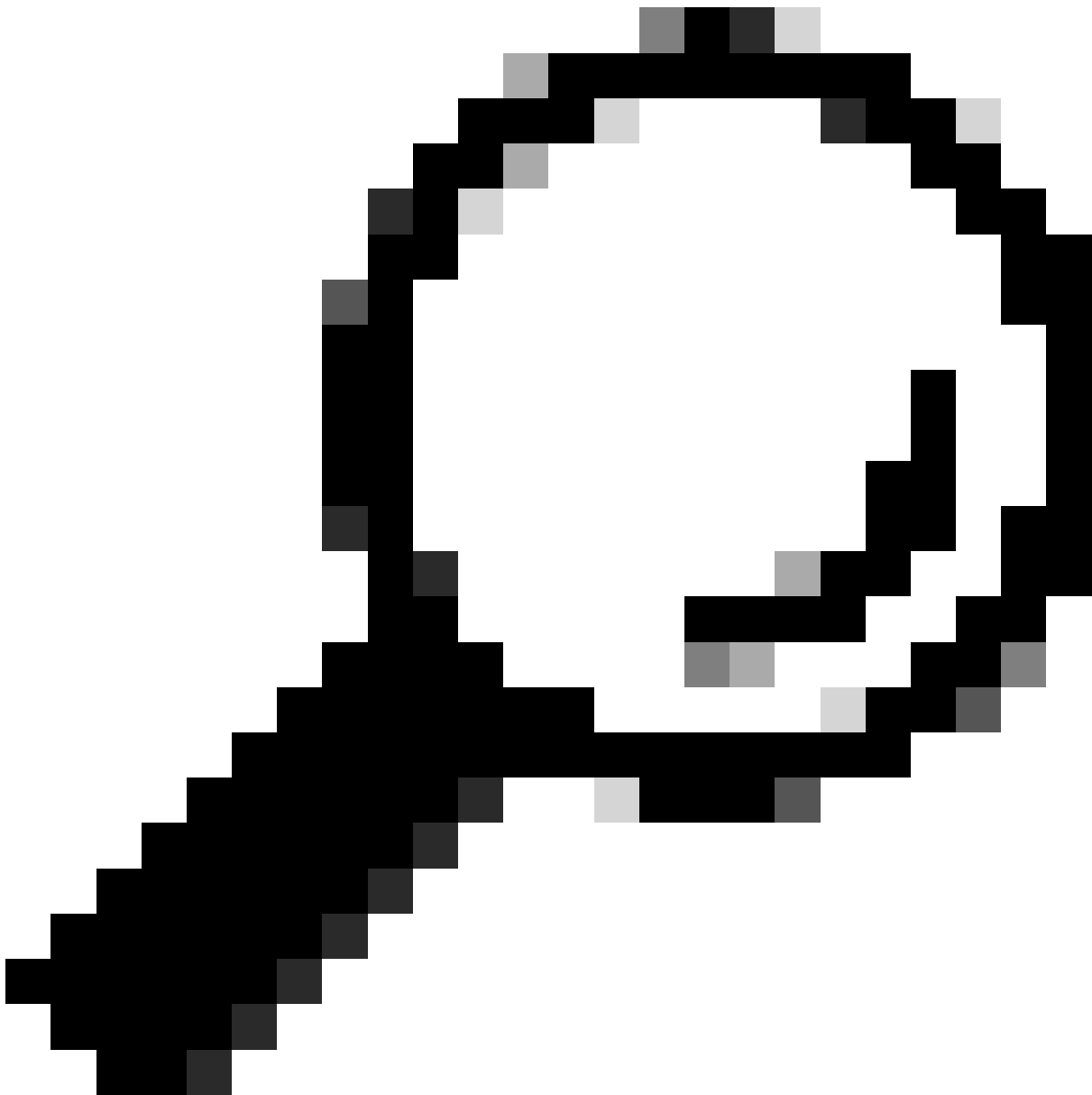
- Secure Network Analytics Response Management.
- Splunk Syslog

Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

- Secure Network Analytics (SNA) deployment that contains at least one Manager appliance and one Flow Collector appliance.
- Splunk server installed and accessible over 443 port.

Configure syslog on SNA over UDP 514 or custom defined port



Tip: Ensure that UDP/514, TCP/6514 or any custom port you choose for syslog is permitted on any firewalls or intermediate devices between SNA and Splunk.

1.SNA Response Management

The Response Management component of Secure Analytics (SA) can be used to configure Rules, Actions, and syslog Destinations.

These options must be configured to send/forward Secure Analytics alarms to other destinations.

Step1: Log into the SA Manager appliance and navigate to **Configure > Detection Response Management**.



beta3



Monitor



Investigate



Report



Configure

Configure



Detection

Host Group Management

Alarm Severity

Policy Management

Response Management

Network Scanners

Analytics

Alerts

Global

Central Management

User Management



Step 2: On the new page navigate to **Actions** tab, locate the default **Send to Syslog** line item and click the ellipsis (...) in the **Action** column, and then **Edit**.

Response Management

Rules Actions Syslog Formats

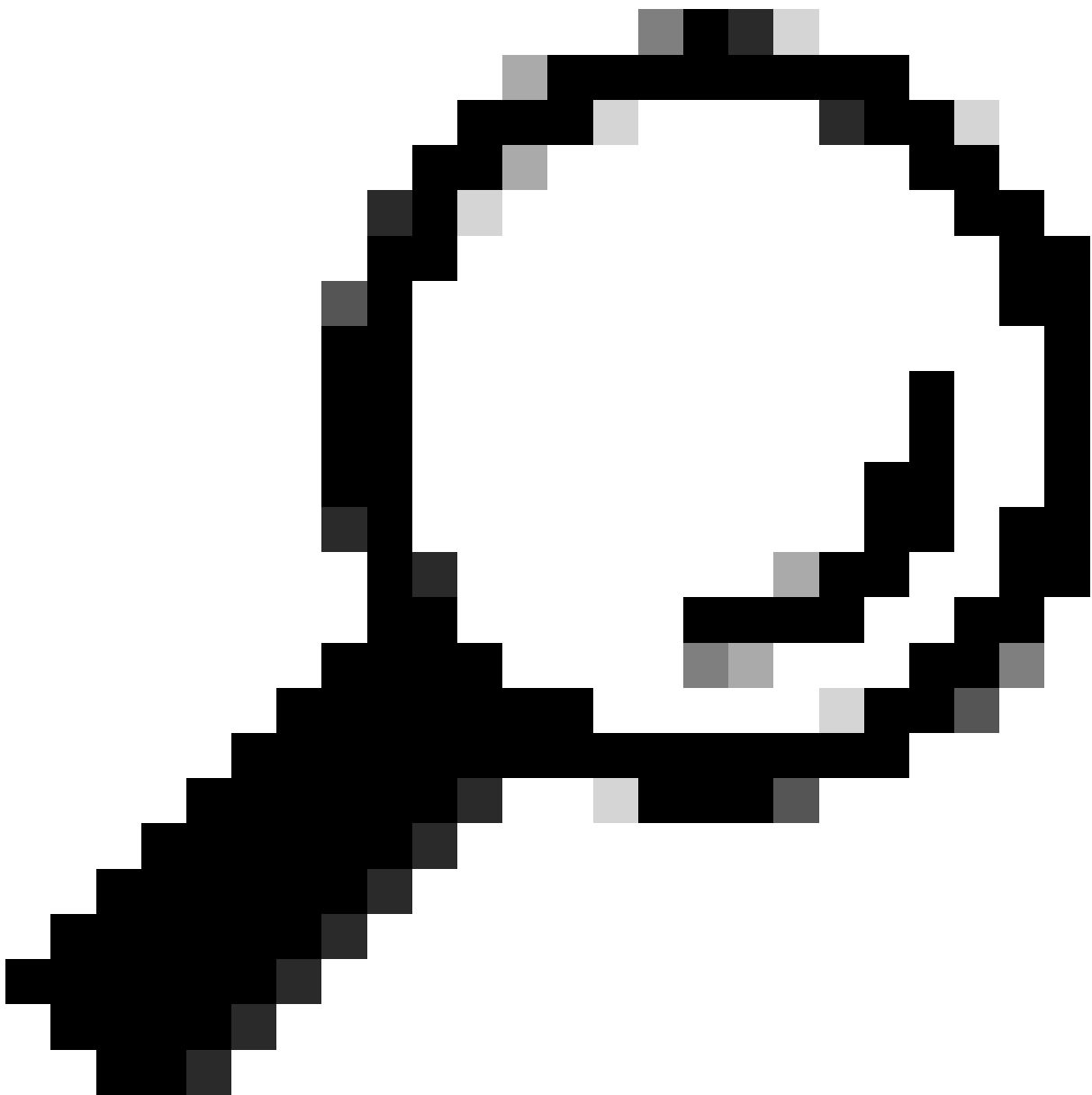
Actions

[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"/>	... Edit Duplicate Delete
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"/>	

Step 3: Enter the desired destination address in the **Syslog Server Address** field, and the desired destination receiving port in the **UDP Port** field. In the **Message Format** select **CEF**.

Step 4: When completed, click the blue **Save** button in the upper right corner.



Tip: The default UDP port for syslog is 514

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

10.10.10.10

UDP Port

514

Message Format

Custom

CEF

This action will use the ArcSight Common Event format.

Example Message

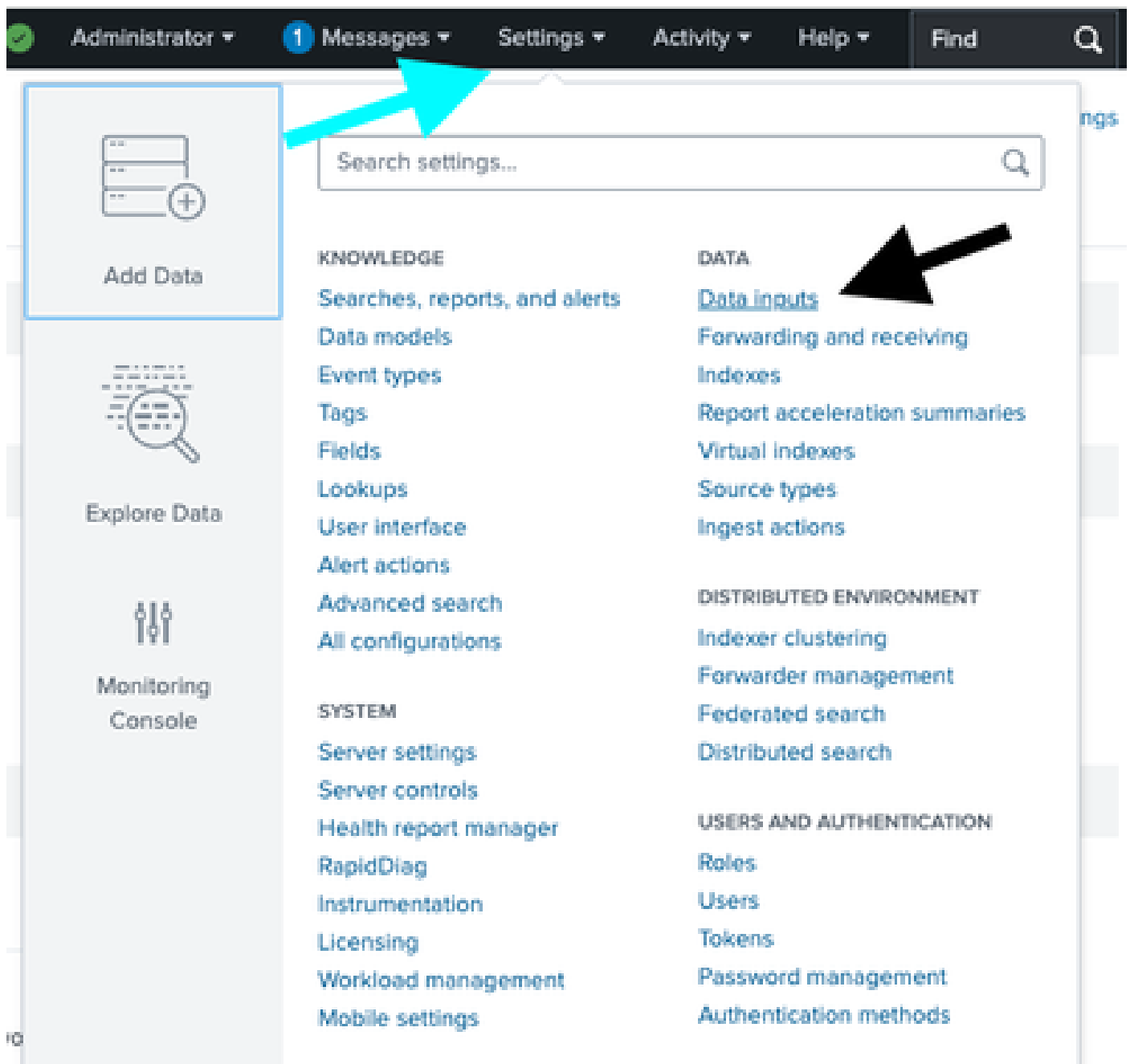
<131>Jan 01 00:00:00 test.host TestApp[1337]: CEF:0|Cisco|7.3.0|Notification:99|Bad Host|5|msg=This host has been observed performing malicious actions toward another host.:Source Host is http (80

Test Action

2. Configuring Splunk to Receive SNA Syslogs over UDP port

After applying your changes on Secure Network Analytics Manager Web UI , you must configure data input in Splunk.

Step 1: Log into Splunk and navigate to **Settings > Add Data > DATA Data Inputs**.



Step 2: Locate the **UDP** line and select **+Add new**.

Administrator

1

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

Step 3: On the new page select **UDP**, enter the receiving port such as 514 in the **Port** field.

Step 4: In the **Source name override** field, enter desired name of source.

Step 5: When complete, click the green **Next >** button on the top of the window.

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 Journal 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 ?

514

Example: 514

Source name override ?

host:port

Only accept connection from ?

optional

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?

Step 6: On the next page, switch to **New** option locate the **Source Type** field and enter desired source .

Step 7: Select **IP** for the **Method**.

Step 8: Click the green **Review** > button on the top of the screen.

Add Data

< Back

Review >

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

Select

New

Source Type Category

Custom ▾

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

Search & Reporting (search) ▾

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 ?

IP

DNS

Custom

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

Default ▾

Create a new index

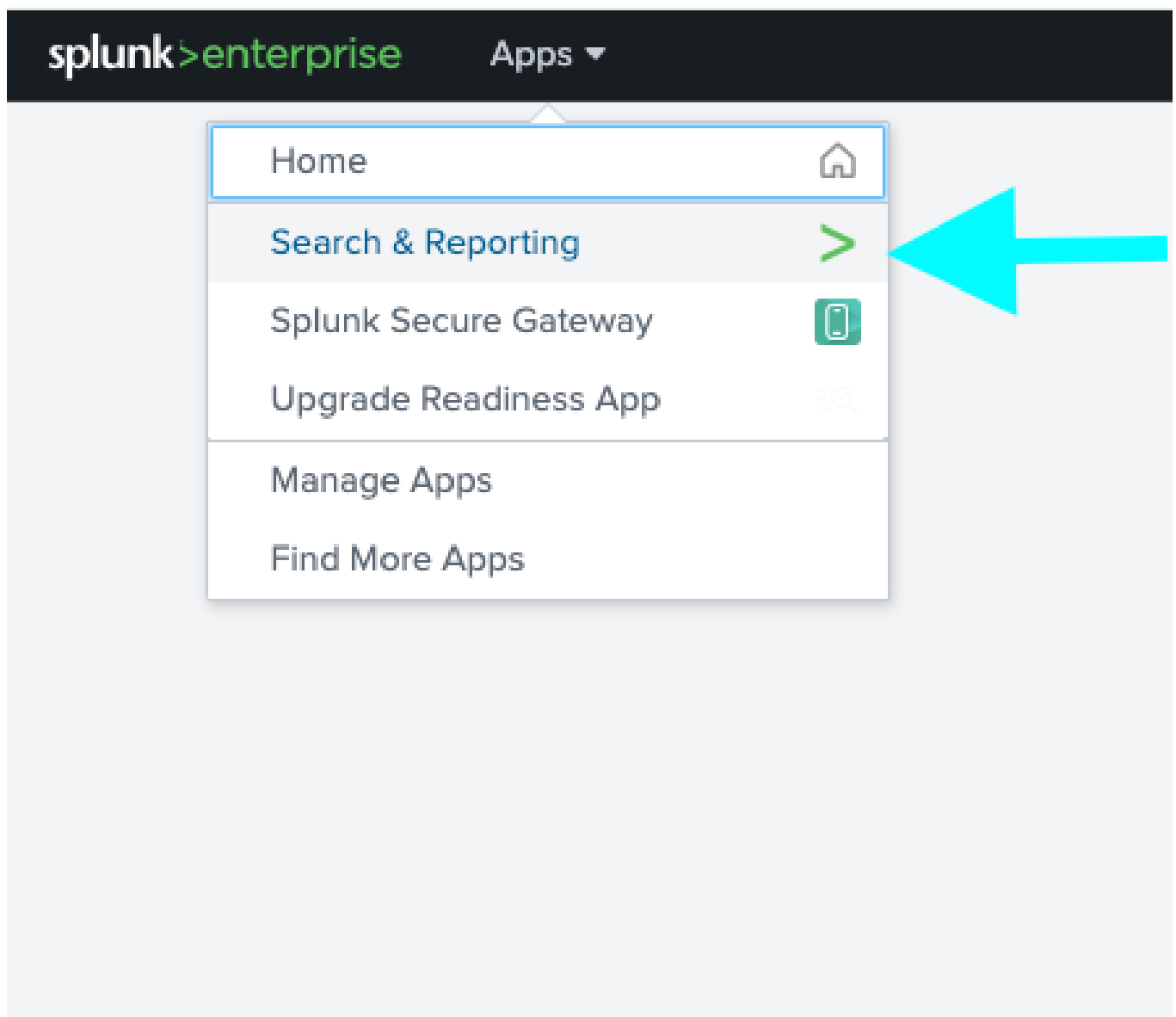
Step 9: On the next window, review your settings and edit if needed.

Step 10: Once validated, click the green **Submit** > button on the top of the window.

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

Step 11: Navigate to **Apps > Search & Reporting** in the Web UI.



Step 12: On the Search page, use the filter `source="As_configured" sourcetype="As_configured"` to find logs that have

been received.

New Search

Save AsCreate Table ViewClose

source*" i* sourcetype="1"Last 24 hours

6 eventsEvent SamplingJob

Events (6)PatternsStatisticsVisualizationTimeline formatZoom OutZoom to SelectionDeselect1 hour per column

FormatShow: 20 Per PageView: List

< Hide FieldsAll Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

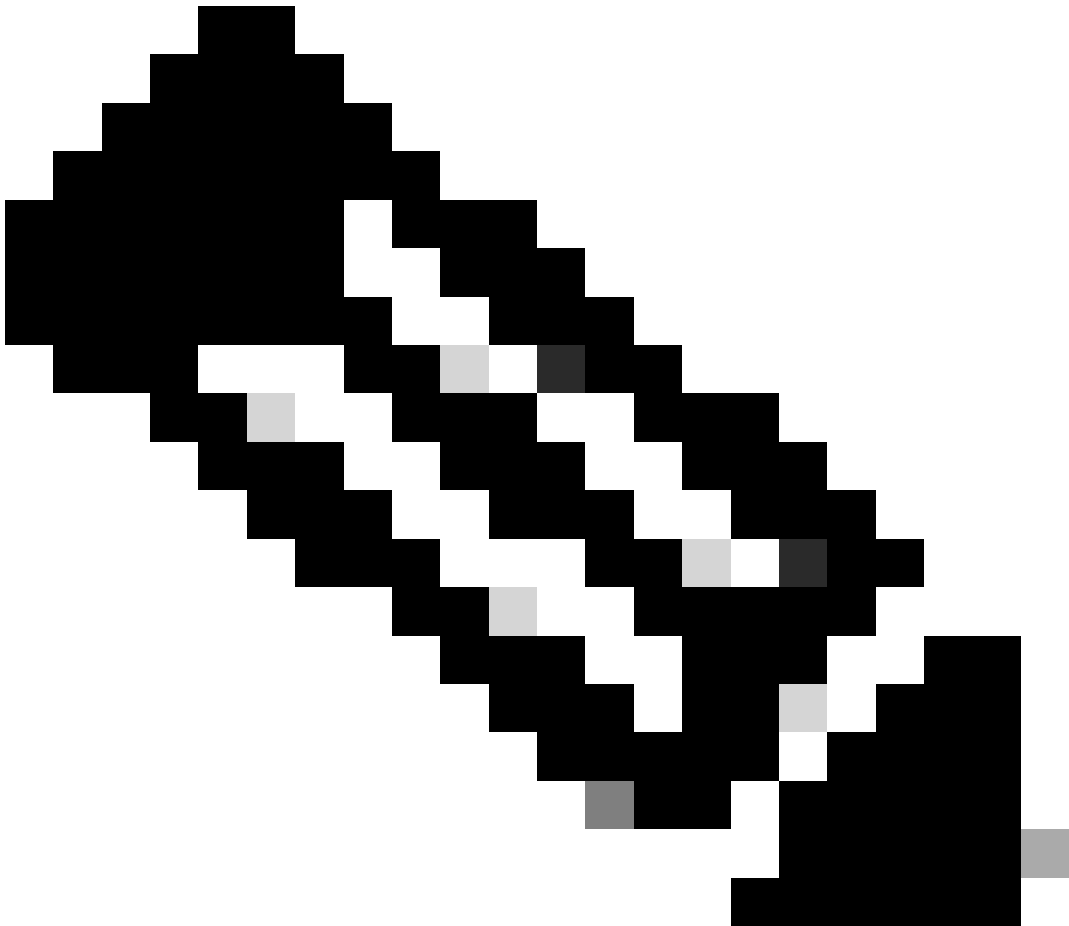
TimeEvent

>

end= externalId=8D-1KJ5-7R9L-PW6Z-5 cs3= cs3Label=SourceHostGroups cs4= cs4Label=TargetHostGroups cs5= cs5Label=Source_URL cs6= cs6Label=Target_URL dpt= proto= dvchost= i dvcpid=381 devi

ceExternalId= // cs2Label=SGTIDAndSGTName spt= destinationTranslatedAddress= destinationTranslatedPort= sourceTranslatedAddress= sourceTranslatedPort

host = source = sourcetype =

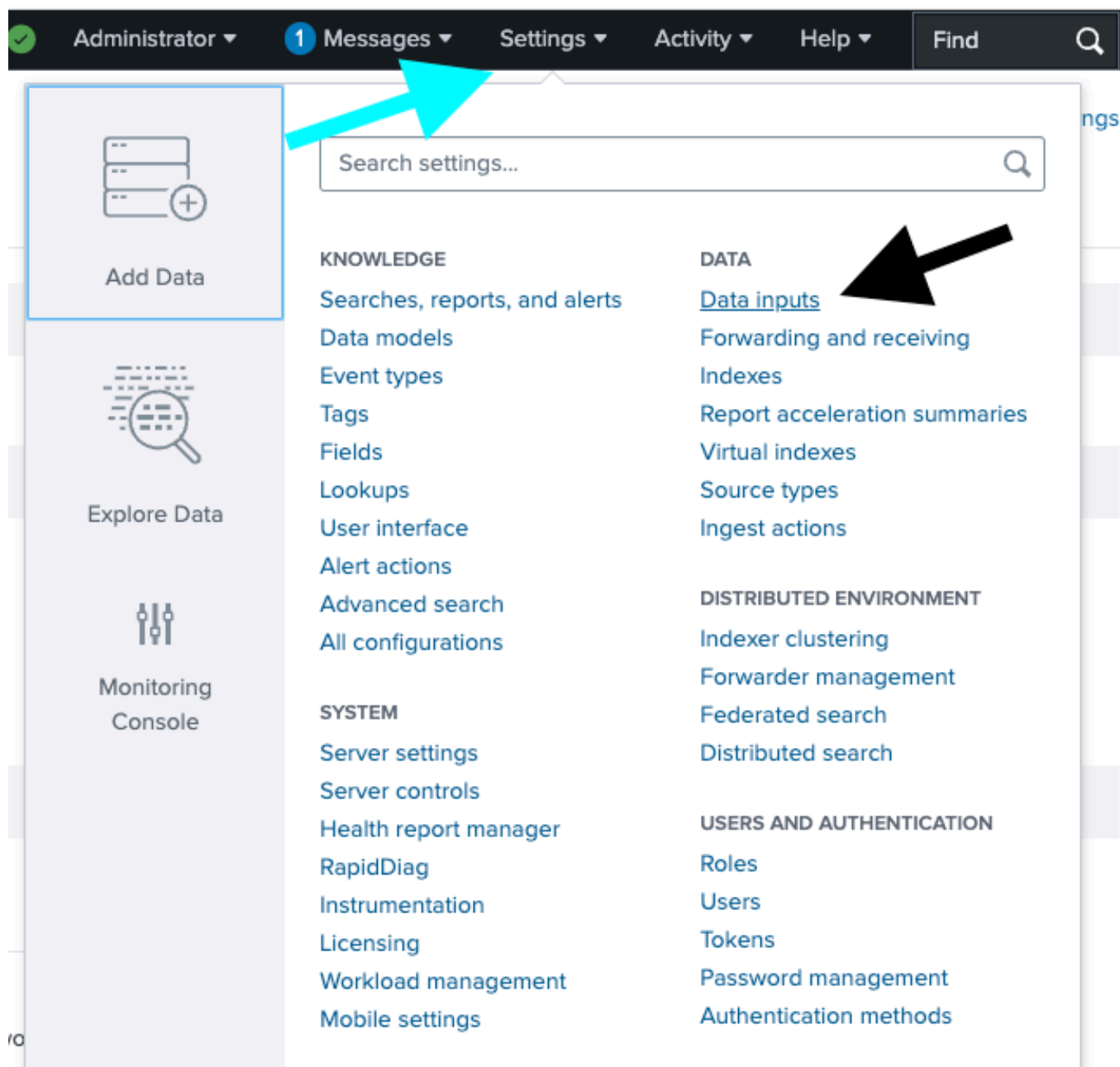


Note: For **source** see Step 4
For **source_type** see Step 6

Configure syslog on SNA over TCP port 6514 or custom defined port

1. Configuring Splunk to Receive SNA Audit Logs over TCP port

Step 1: In the Splunk UI, navigate to **Settings > Add Data > DATA Data Inputs**.



Step 2: Locate the **TCP** line and select + **Add new**.

Apps

Administrator1 MessagesSettingsActivityHelp

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
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.	0	+ Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	0	+ 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 Journal 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

Step 3: In the new window select **TCP**, enter the desired receiving port, in the example image port **6514**, and enter "desired name" in the **Source name override** field.



Note: TCP 6514 is default port for syslog over TLS

Step 4: When complete, click the green **Next >** button on the top of the window.

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
6514
Example: 514

Source name override
:
host:port

Only accept connection from
optional
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?

Step 5: In the new window select **New** in the **Source type** section, enter **desired name** in the **Source Type** field.

Step 6: Select **IP** for the **Method** in the **Host** section.

Step 7: When complete select the green **Review >** button on the top of the window.

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

Add Data ● ● ○ ○ < Back Review >

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 Select New

Source Type

Source Type Category Custom ▾

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 Apps Browser (appsbrowser) ▾

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 ? IP DNS Custom

Index

Step 8: On the next window, review your settings and edit if needed. Once validated click the green **Submit** > button on the top of the window.

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

Add Data ● ● ● ○ < Back Submit >

Review

Input Type TCP Port

Port Number 6514

Source name override

Restrict to Host N/A

Source Type

App Context launcher

Host (IP address of the remote server)

Index default

2.Generate Certificate for Splunk

Step 1: Using a machine that has openssl installed, run the `sudo openssl req -x509 -newkey rsa:4096 -keyout server_key.pem`

-out server_cert.pem -sha256 -days 3650 -subj /CN=10.106.127.4 command, replacing the example IP of 10.106.127.4 with the IP of the Splunk device. You are prompted twice to input a user defined pass phrase. In the examples, the commands are being ran from the command line of the Splunk machine.

```
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:
```

When the command completes, two files are generated. The `server_cert.pem` and `server_key.pem` files.

```
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:
```

Step 2: Switch to root user.

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

Step 3: Copy the newly generated certificate to the `/opt/splunk/etc/auth/`.

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

Step 4: Append the spunkweb.cet file with private key.

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

Step 5: Change the ownership of splunk certificate.

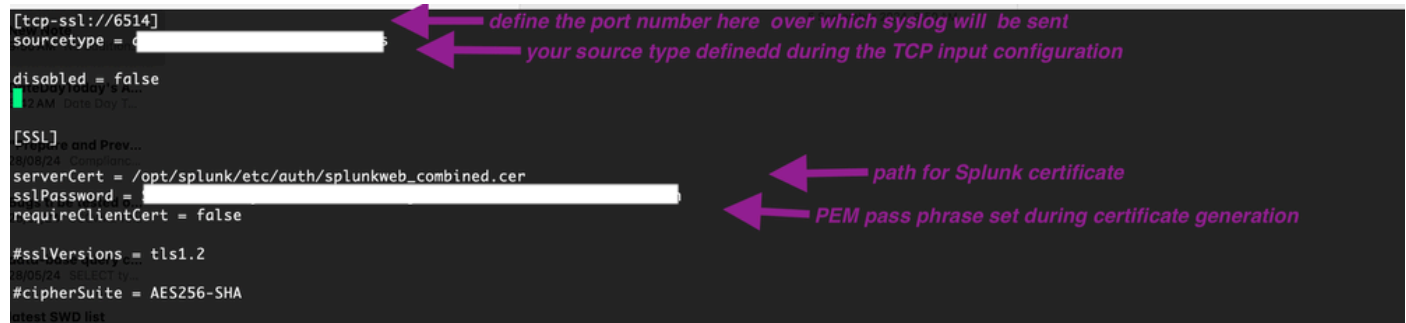
```
user@examplehost:~# chown 10777:10777/opt/splunk/etc/auth/splunkweb.cert
```

Step 6: Change the permission for splunk certificate.

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

Step 7: create a new input.conf file.

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



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

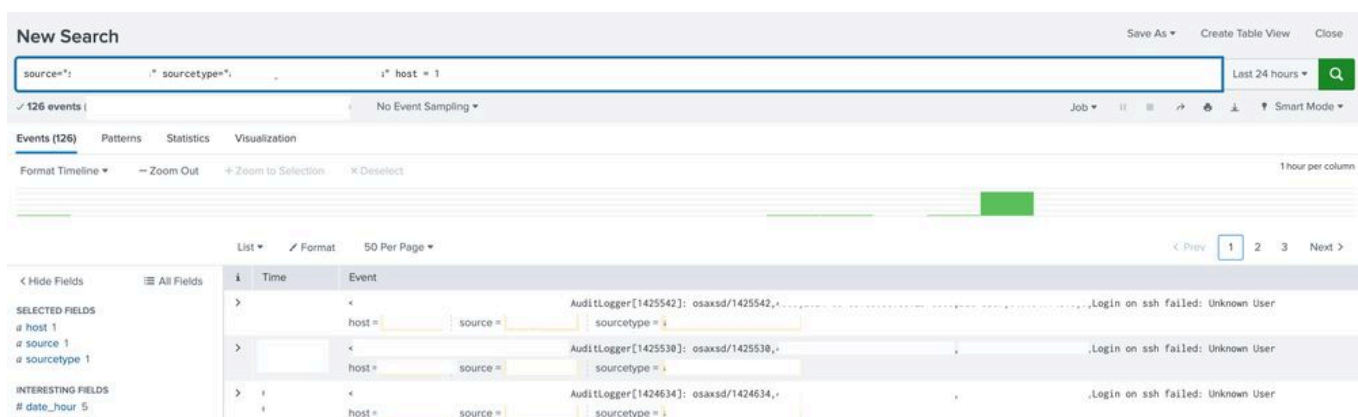
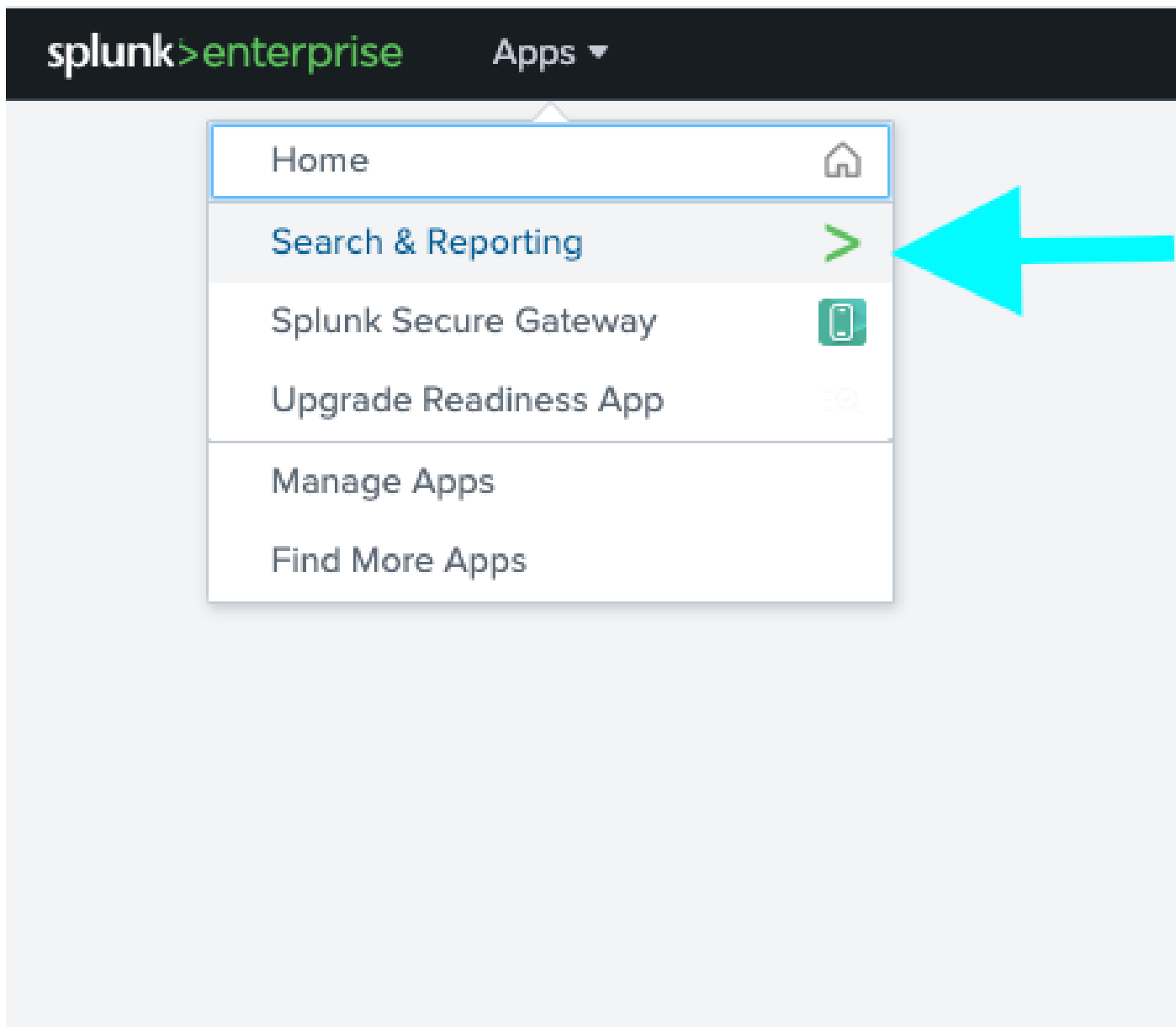
define the port number here over which syslog will be sent

your source type defined during the TCP input configuration

path for Splunk certificate

PEM pass phrase set during certificate generation

Step 8: Verify the syslogs using search.



3.Configure Audit Log Destination on SNA

Step 1: Log in to SMC UI navigate to **Configure > Central Management**.



nse



Monitor



Investigate



Report



Configure

Configure



Detection

Host Group Management

Alarm Severity

Policy Management

Response Management

Network Scanners

Analytics

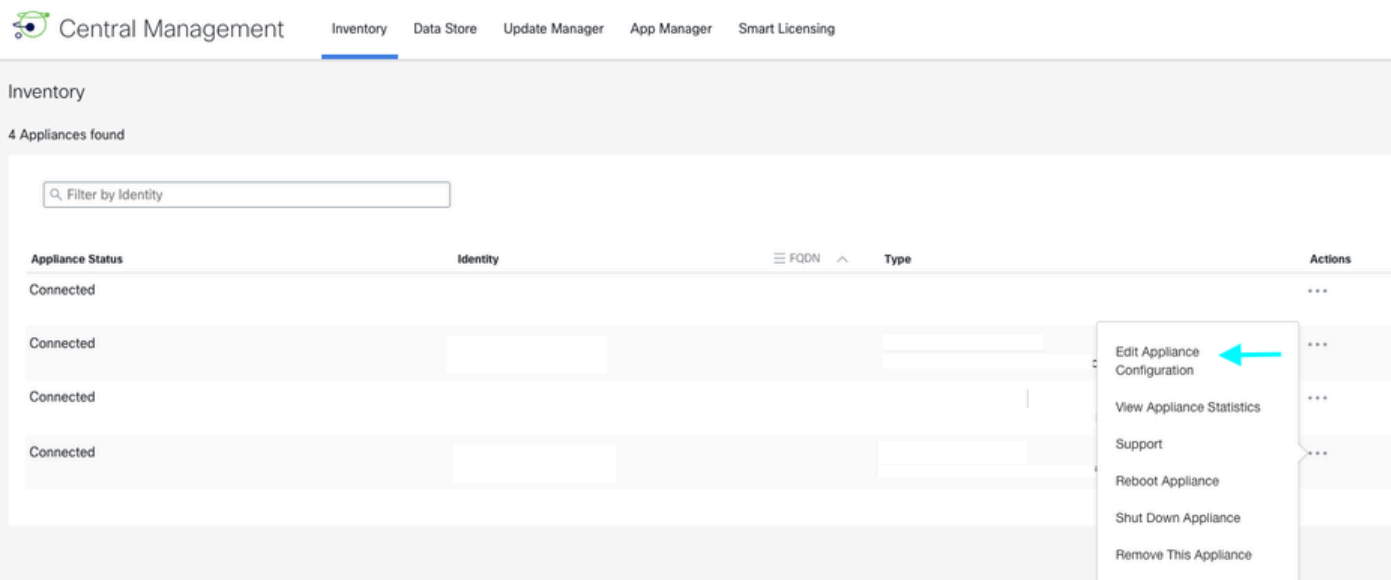
Alerts

Global

 Central Management

... ..

Step 2: Click ellipsis **icon** of your desired SNA appliance select Edit Appliance Configuration.



Step 3: Navigate to **Network Services** Tab and enter Audit Log Destination (Syslog over TLS) details.

Audit Log Destination (Syslog over TLS) Modified Reset

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

Step 4: Navigate to General tab, scroll down to the bottom Click **Add new** to upload the Splunk certificate created earlier named as server_cert.pem.

Central Management

InventoryData StoreUpdate ManagerApp ManagerSmart Licensing

Inventory / Appliance Configuration

Appliance Configuration - Manager

CancelApply Settings

Configuration Menu

ApplianceNetwork ServicesGeneral

TO EMAIL

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

Step 5: Click **Apply settings**.

Cancel

Apply Settings

Troubleshoot

There could be complete gibberish showing up on search.

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 🔍

Search Analytics Datasets Reports Alerts Dashboards **Search & Reporting**

New Search

Save As ▾ Create Table View Close

source=* :* sourcetype=* 🔍

✓ 156 events () No Event Sampling ▾ Job ▾ II ▾ ➔ ⬇️ ⬆️ Smart Mode ▾

Events (156) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 hour per column

List ▾ Format 50 Per Page ▾ < Prev 1 2 3 4 Next >

< Hide Fields All Fields

SELECTED FIELDS

host 1

source 1

sourcetype 1

INTERESTING FIELDS

index 1

linecount 6

punct 79

splunk_server 1

timestamp 1

34 more fields

+ Extract New Fields

i	Time	Event
>		<pre> \x00 Z \x00 \x00 host = source = sourcetype = </pre>
>		<pre> * \x00 & \xE3D \x9F8\x91\xD3\xF9\x82 \xF8F\x9F\xE5R\xE8\xED \x92\xC0\xE5\xE5\xA38:\xA2\xEB (i 0/\x00\x9E\x00J\x00g\xC0,\xC00\x00\x9F\x00\xFF \x00\x00\xBF\x00 \x00\x00\x00 \x00\x00\x00+\x00 \x00,\x00* \x00 \x00 \x00\x00 \x00\x00 \x00 \x00 \x00 \x00 \x00\x00\x00\x00\x003\x00G\x00E\x00 \x00A \xA7\xB9\xB3\xEC\xC91 \x81g=R \^d\xC1 \xD0As[z\x9C 9\xE1\x91\xEC\xEDw\xD9p 6\x954\x88U\xC4\xFA\x920\xA5\x81!\xA3 \x0F\x9F&\xA4\x87/t\xFD\xCD\xE0\x92\x89\xEA \x88 host = 10106.12713 source = sourcetype = </pre>
>		<pre> \x00 Z \x00 \x00 host = 10106.12713 source = sourcetype = </pre>
>		<pre> * \x00 & <GK- AInp"J >\x97h\xF9R2 u\x9E \x91\xATT\x8C\xB0\xDCY , Î (' \xAE\x84+\xF0B\xC3s , \xBA(\xF1\x9A \xED\xD3\xFC6\xFE\x8E\xC5\xD9\x00 0\xFF \x00\x00\x0F\x00 \x00\x00\x00 \x00\x00\x00+\x00 \x00 \x00 \x00 \x00\x00\x00\x00 \x00 \x00\x00\x00\x00\x00 \x00,\x00* \x00 \x00 \x00\x00 \x00\x00 </pre>

Show all 6 lines

Solution :

Map the input to its correct source type.



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
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

TCP

Data inputs > TCP

New Local TCP

Showing 1-1 of 1 item

filter

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