Konfigurieren der Antwortverwaltung zum Senden von Syslog-Ereignissen an Splunk

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Funktion für das Management sicherer Analysemöglichkeiten konfigurieren, um Ereignisse per Syslog an einen Drittanbieter, z. B. Splunk, zu senden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sicheres Reaktionsmanagement für Netzwerkanalysen:
- Splunk-Syslog

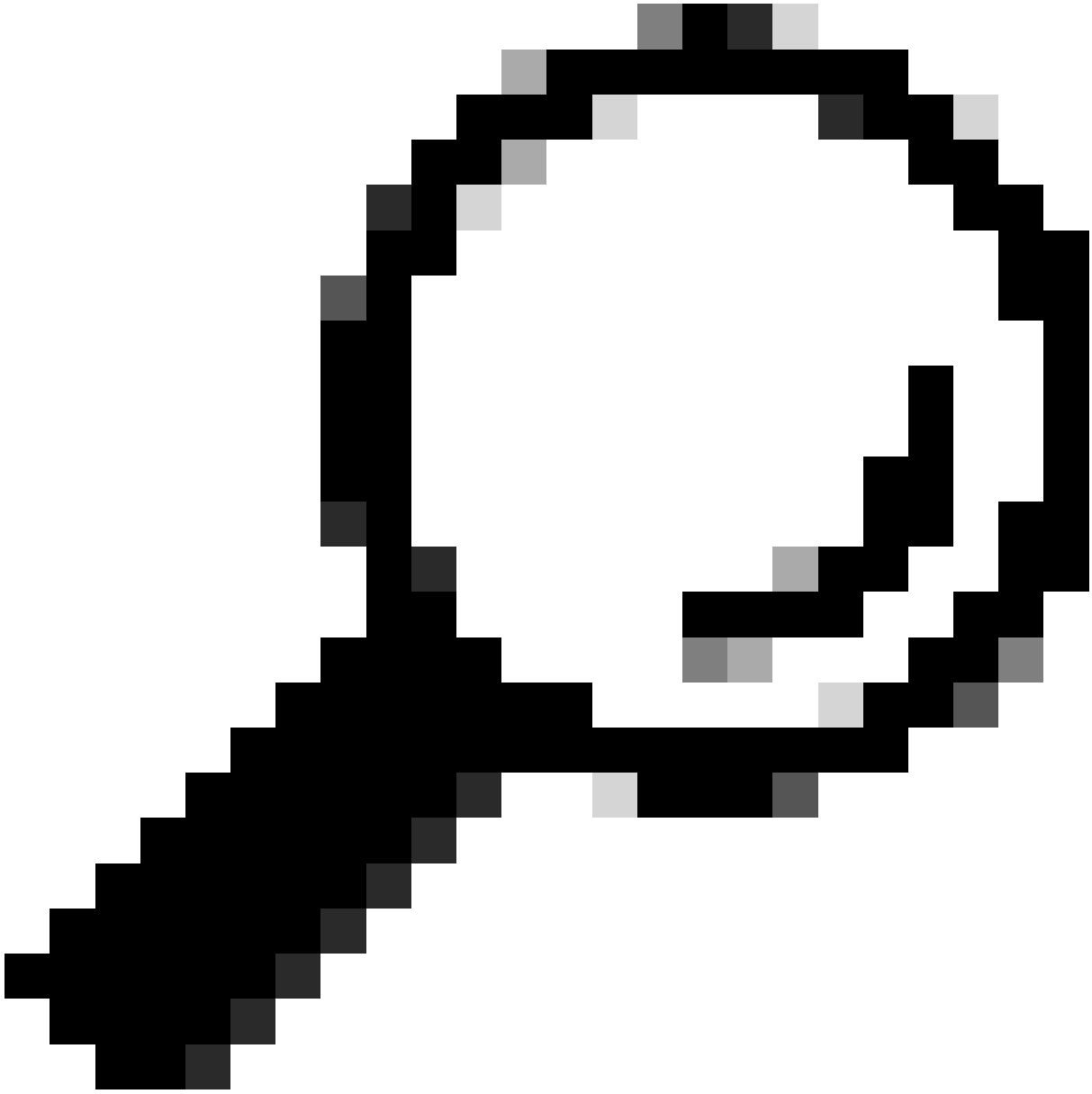
Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

- Bereitstellung von Secure Network Analytics (SNA), die mindestens eine Manager-Appliance

und eine FlowCollector-Appliance enthält.
- Splunk-Server installiert und über 443 Ports zugänglich.

Konfigurieren von Syslog auf SNA über UDP 514 oder einem benutzerdefinierten Port



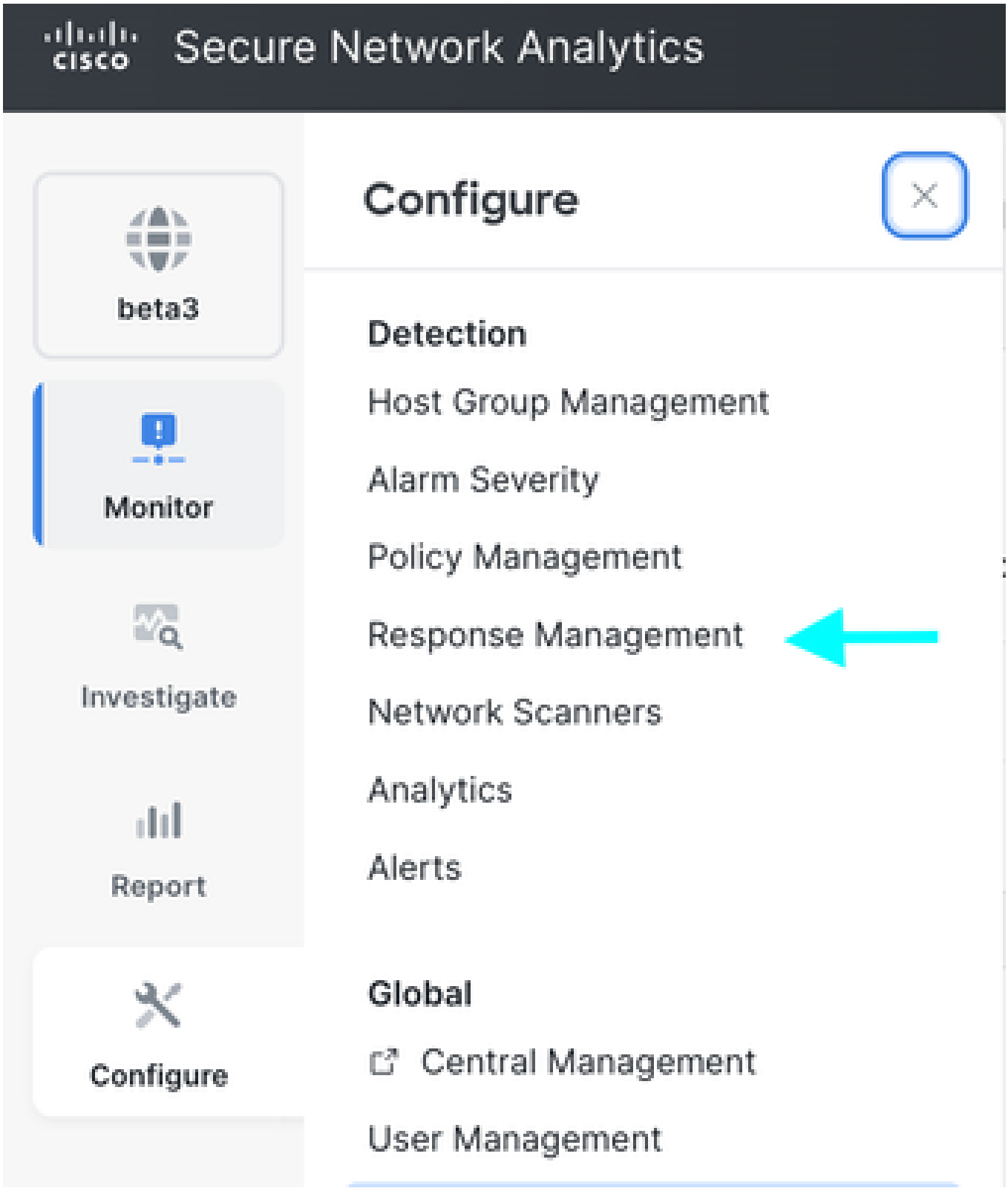
Tipp: Stellen Sie sicher, dass UDP/514, TCP/6514 oder jeder benutzerdefinierte Port, den Sie für Syslog auswählen, auf Firewalls oder zwischengeschalteten Geräten zwischen SNA und Splunk zugelassen ist.

1.SNA-Antwortmanagement

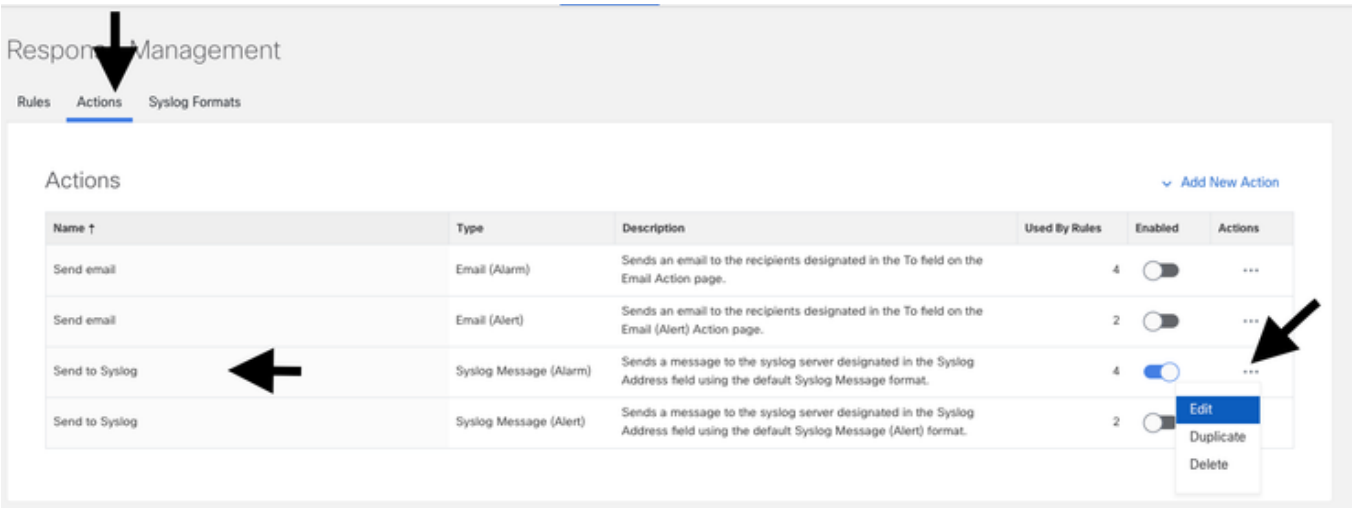
Mit der Response Management-Komponente von Secure Analytics (SA) können Regeln, Aktionen und Syslog-Ziele konfiguriert werden.

Diese Optionen müssen konfiguriert werden, um sichere Analysen an andere Ziele zu senden/weiterzuleiten.

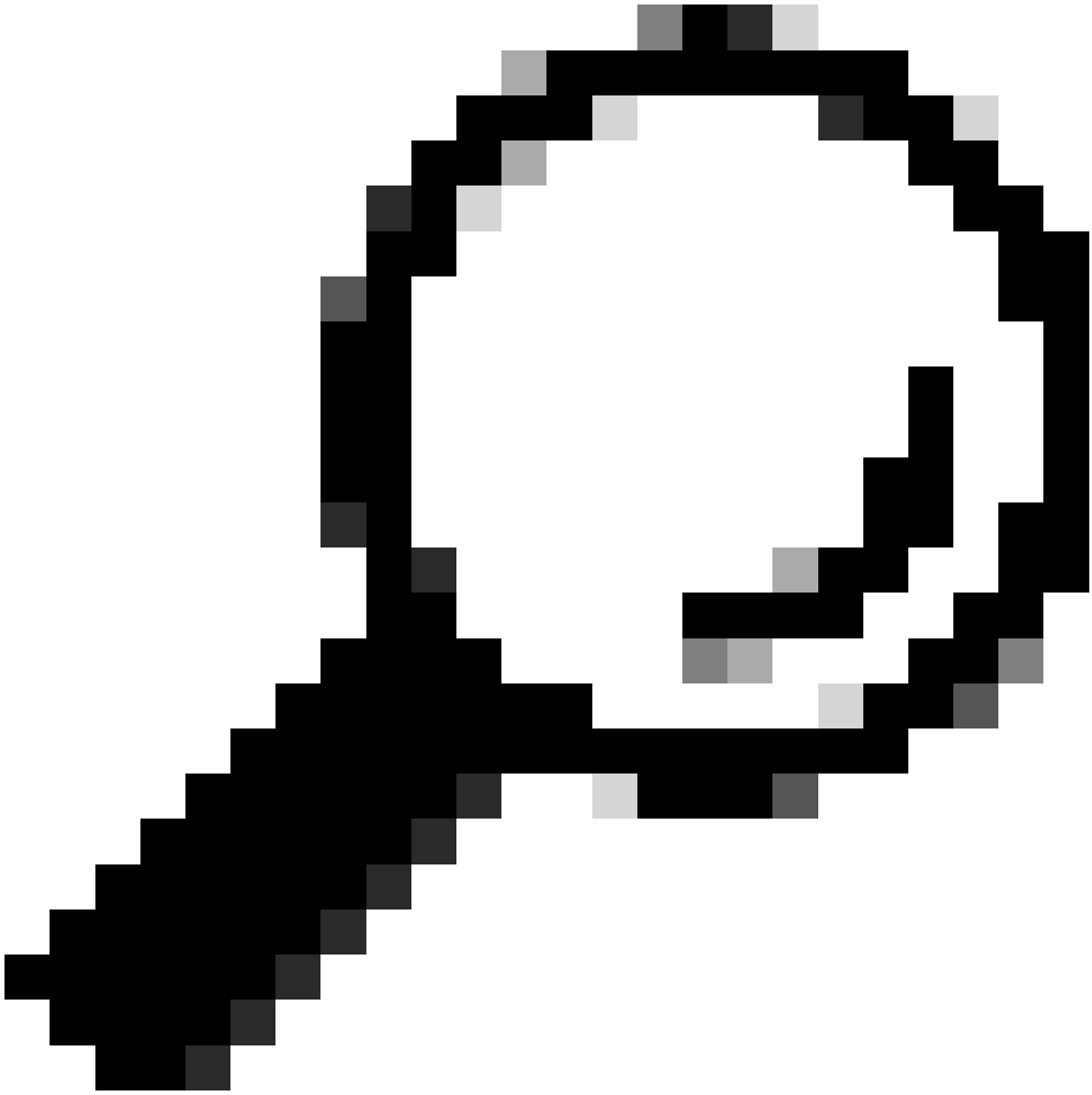
Schritt 1: Melden Sie sich bei der SA Manager-Appliance an, und navigieren Sie zu Configure > Detection Response Management.



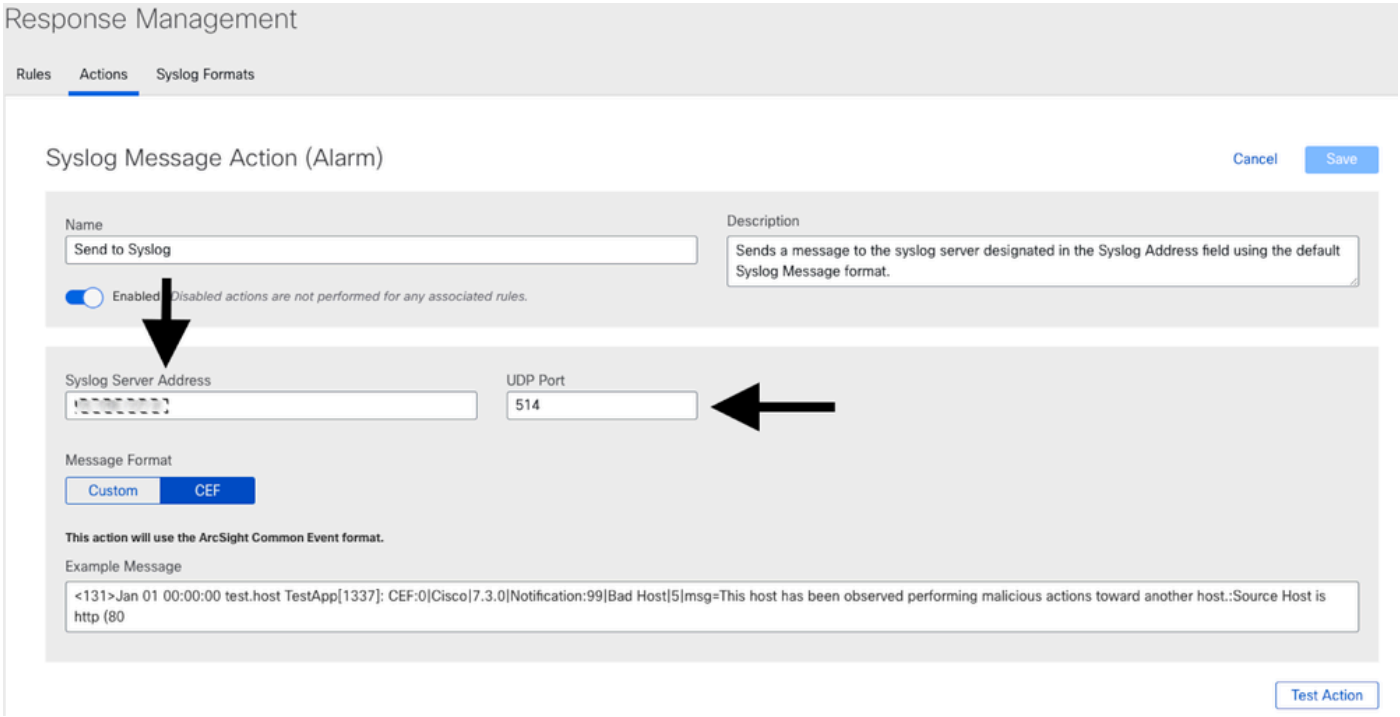
Phase 2: Navigieren Sie auf der neuen Seite zur Registerkarte Aktionen, suchen Sie nach dem standardmäßigen Posten An Syslog senden, und klicken Sie in der Spalte Aktion auf die Auslassungszeichen (...) und dann auf Bearbeiten.



Schritt 3: Geben Sie die gewünschte Zieladresse in das Feld Syslog-Serveradresse und den gewünschten Ziel-Empfangsport in das Feld UDP-Port ein. Wählen Sie im Nachrichtenformat die Option CEF aus.
Schritt 4: Klicken Sie abschließend auf die blaue Schaltfläche Speichern in der rechten oberen Ecke.



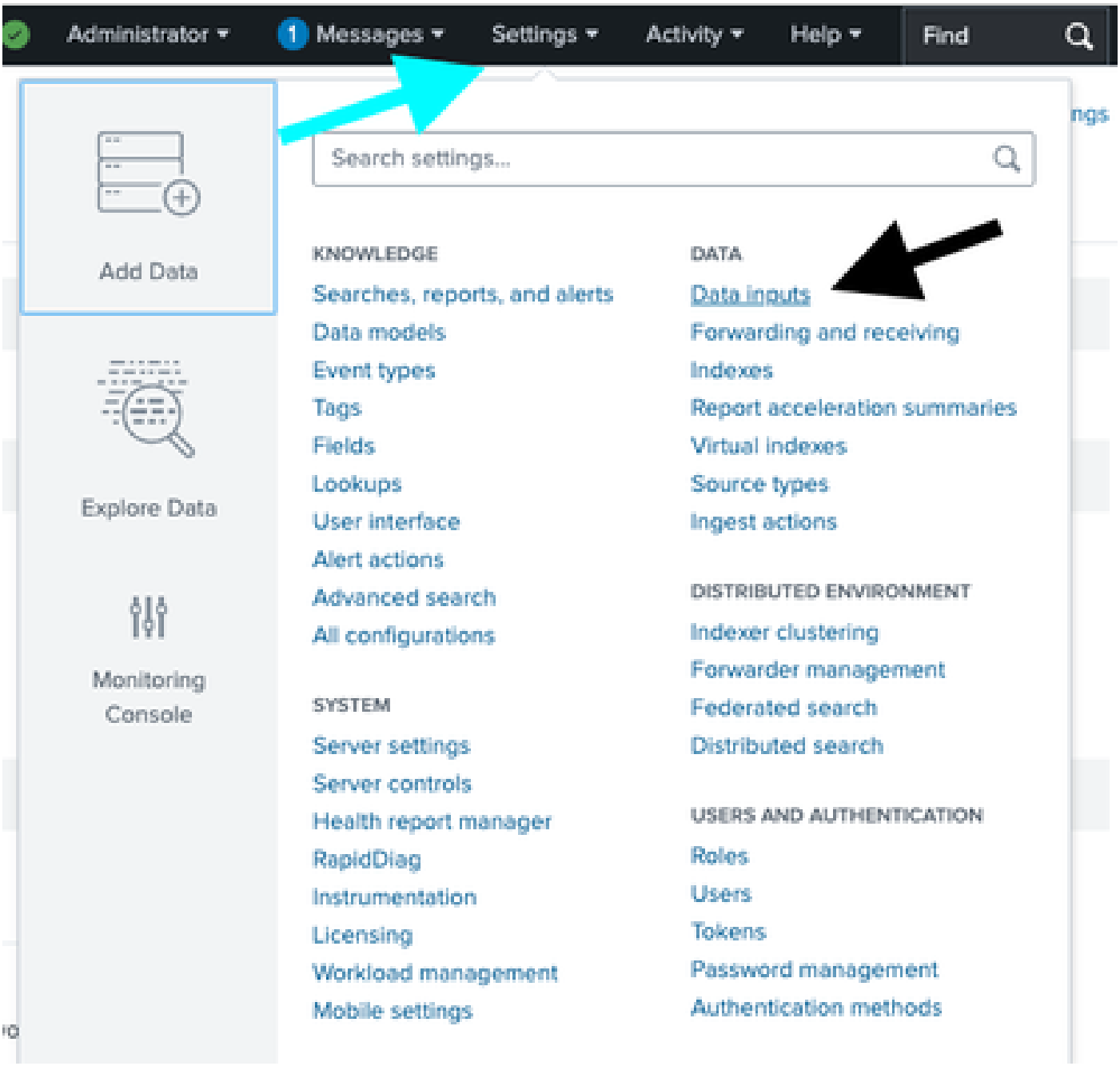
Tipp: Der Standard-UDP-Port für Syslog ist 514.



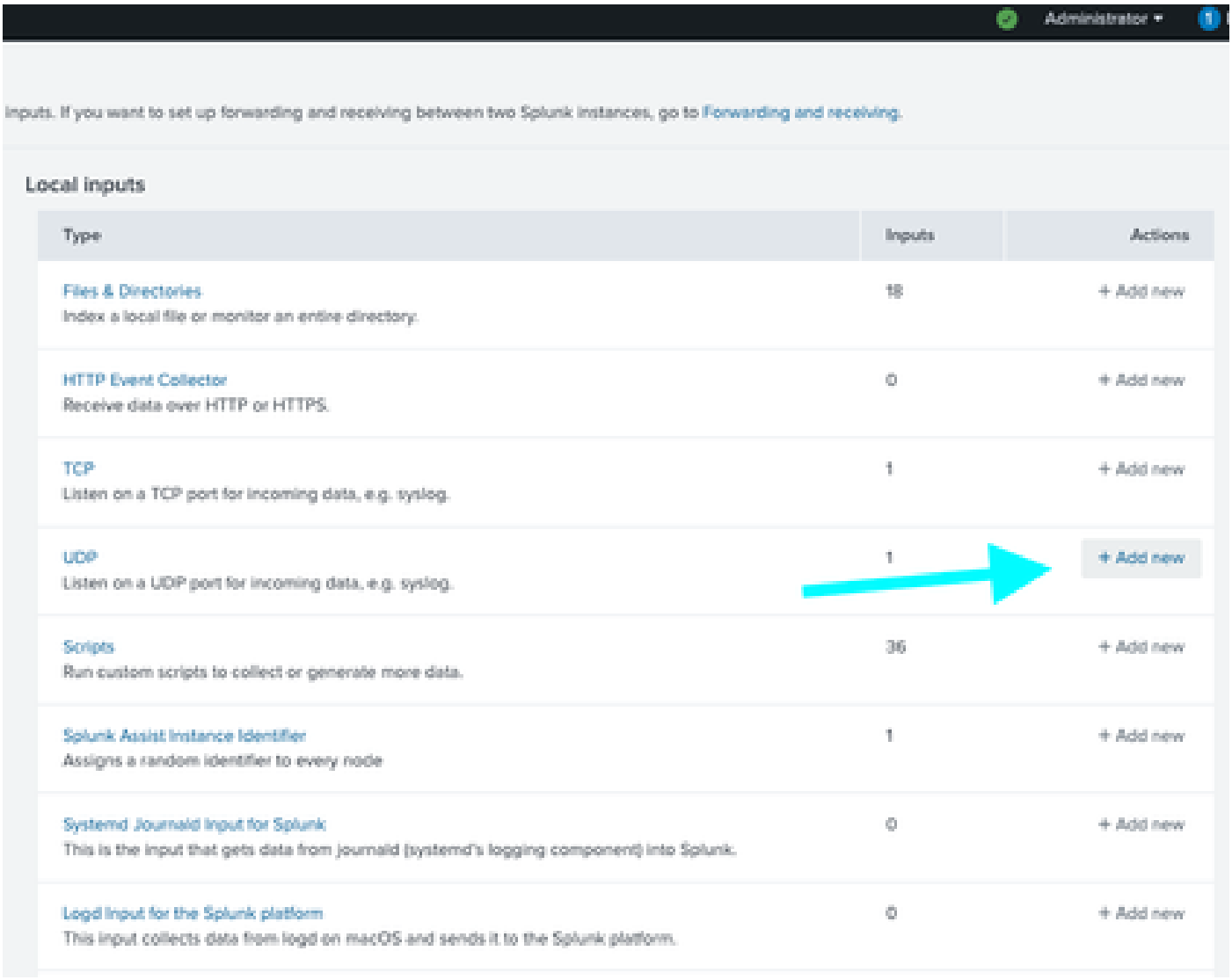
2.Konfigurieren von Splunk zum Empfangen von SNA-Syslogs über den UDP-Port

Nachdem Sie Ihre Änderungen auf die Webbenutzeroberfläche von Secure Network Analytics Manager angewendet haben, müssen Sie die Dateneingabe in Splunk konfigurieren.

Schritt 1: Melden Sie sich bei Splunk an, und navigieren Sie zu Einstellungen > Daten hinzufügen > DATEN-Eingaben.

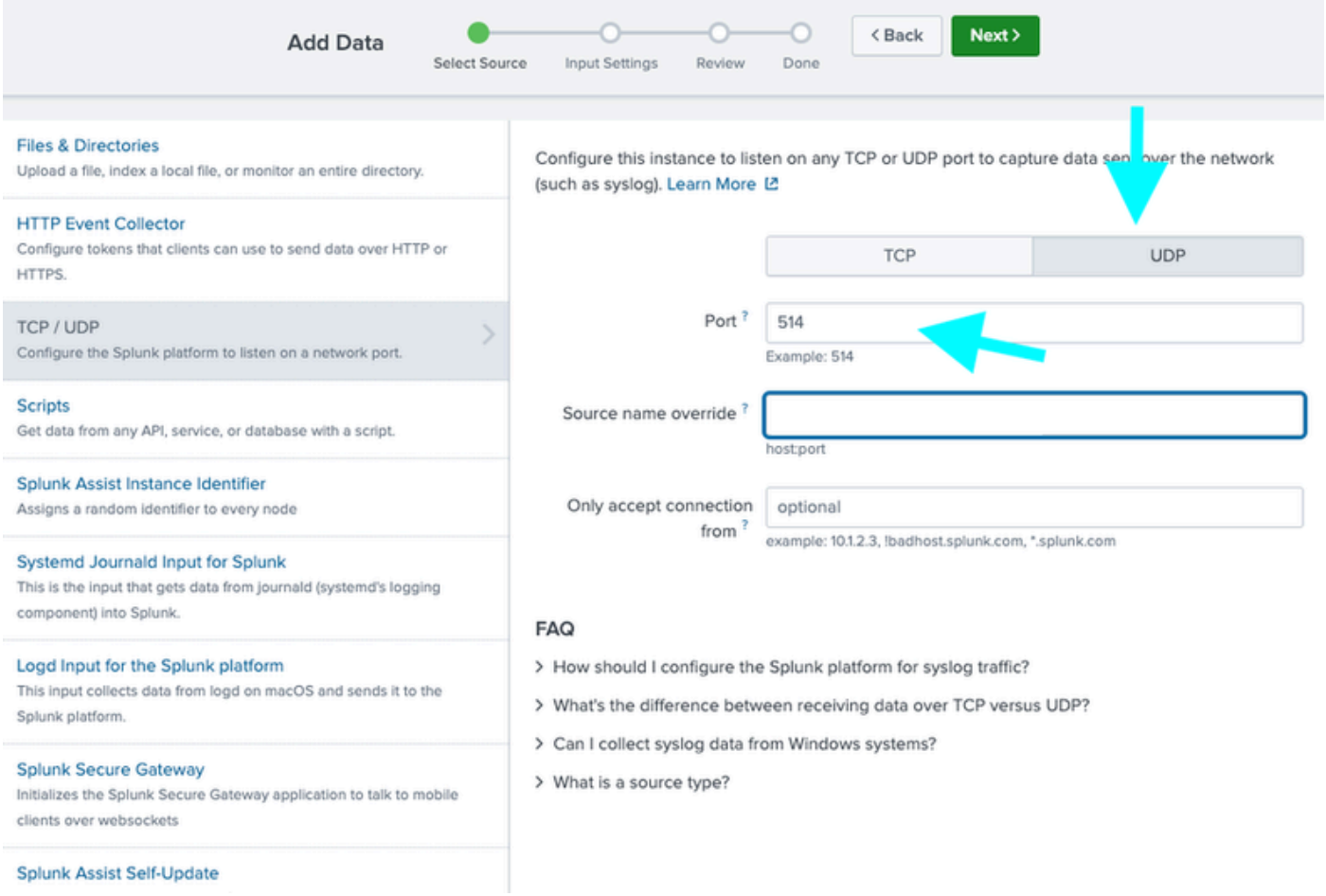


Phase 2: Suchen Sie die UDP-Leitung, und wählen Sie +Neu hinzufügen aus.



Schritt 3: Wählen Sie auf der neuen Seite UDP aus, und geben Sie den Empfangs-Port wie 514 in das Feld Port ein.
Schritt 4: Geben Sie im Feld Überschreiben des Quellnamens Folgendes ein: desired name of source.

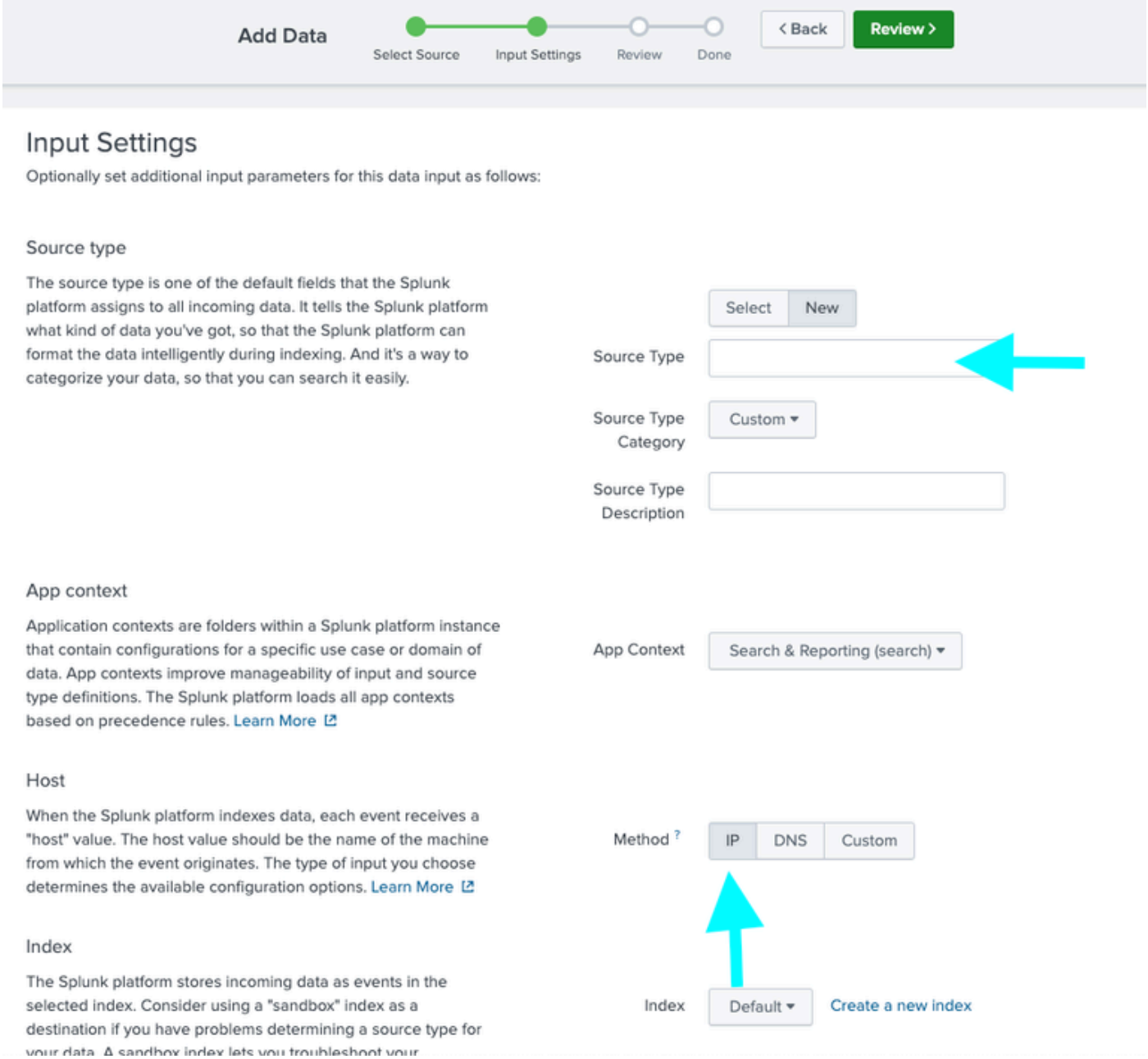
Schritt 5: Wenn Sie fertig sind, klicken Sie oben im Fenster auf die grüne Schaltfläche Weiter >.



Schritt 6: Wechseln Sie auf der nächsten Seite zur Option Neu, suchen Sie das Feld Quelltyp, und geben Sie desired source .

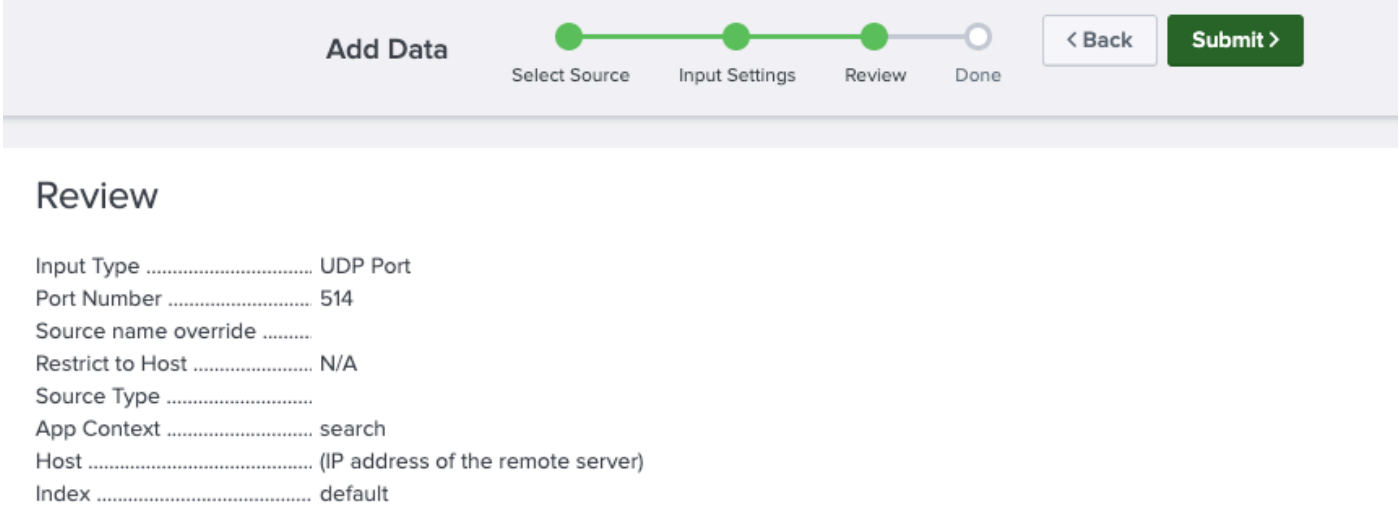
Schritt 7: Wählen Sie IP als Methodeaus.

Schritt 8: Klicken Sie oben im Bildschirm auf die grüne Schaltfläche Überprüfen >.

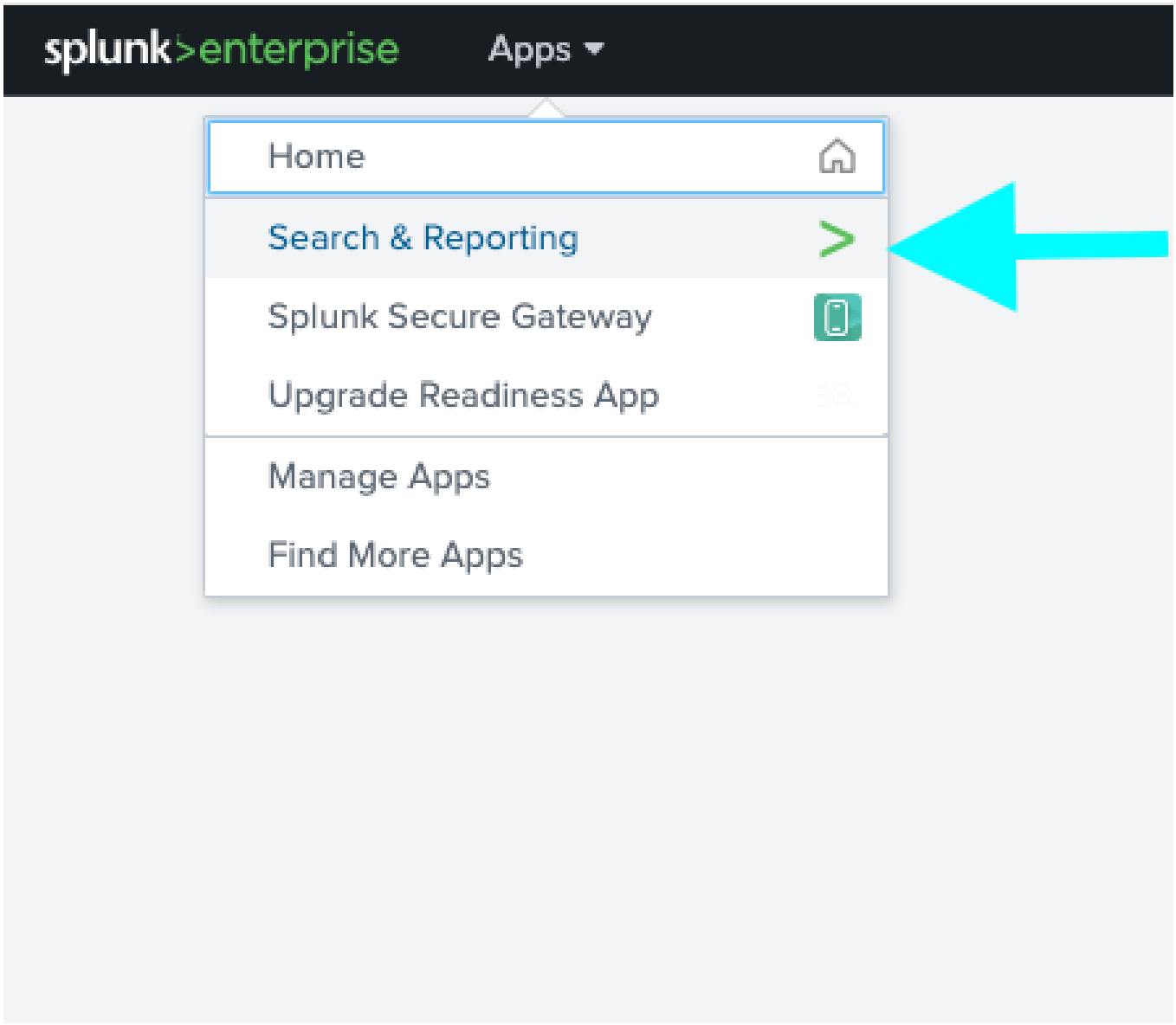


Schritt 9: Überprüfen Sie im nächsten Fenster Ihre Einstellungen, und bearbeiten Sie sie gegebenenfalls.

Phase 10: Klicken Sie nach der Validierung oben im Fenster auf die grüne Schaltfläche Submit > (Senden).

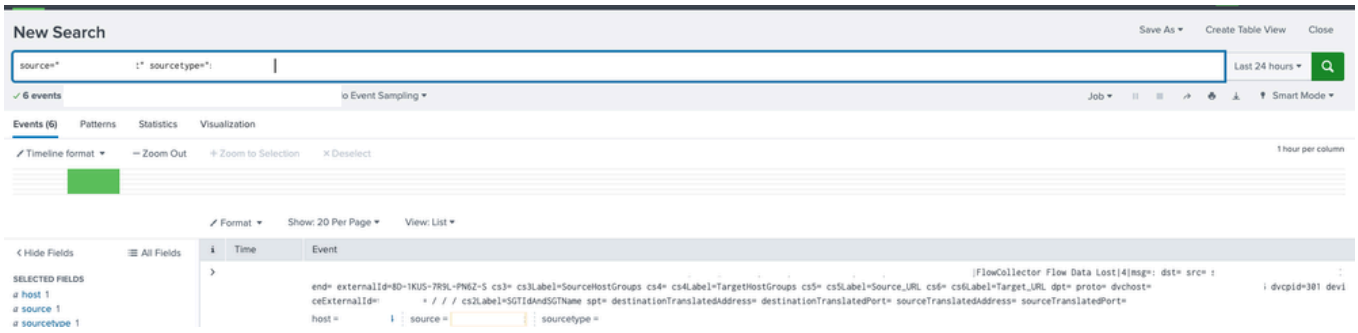


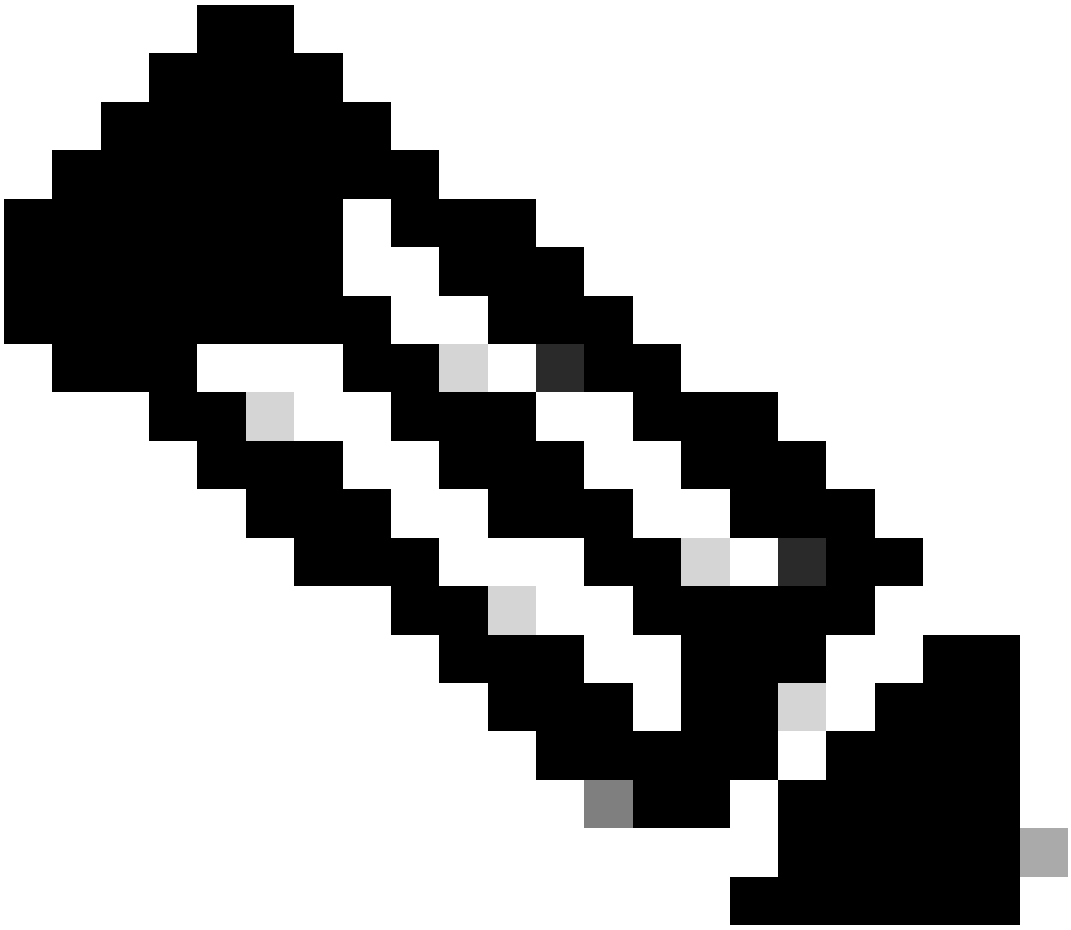
Phase 11: Navigieren Sie in der Webbenutzeroberfläche zu Apps > Search & Reporting.



Phase 12: Verwenden Sie auf der Seite "Suchen" den Filter`source="As_configured" sourcetype="As_configured",`

um nach empfangenen Protokollen zu suchen.



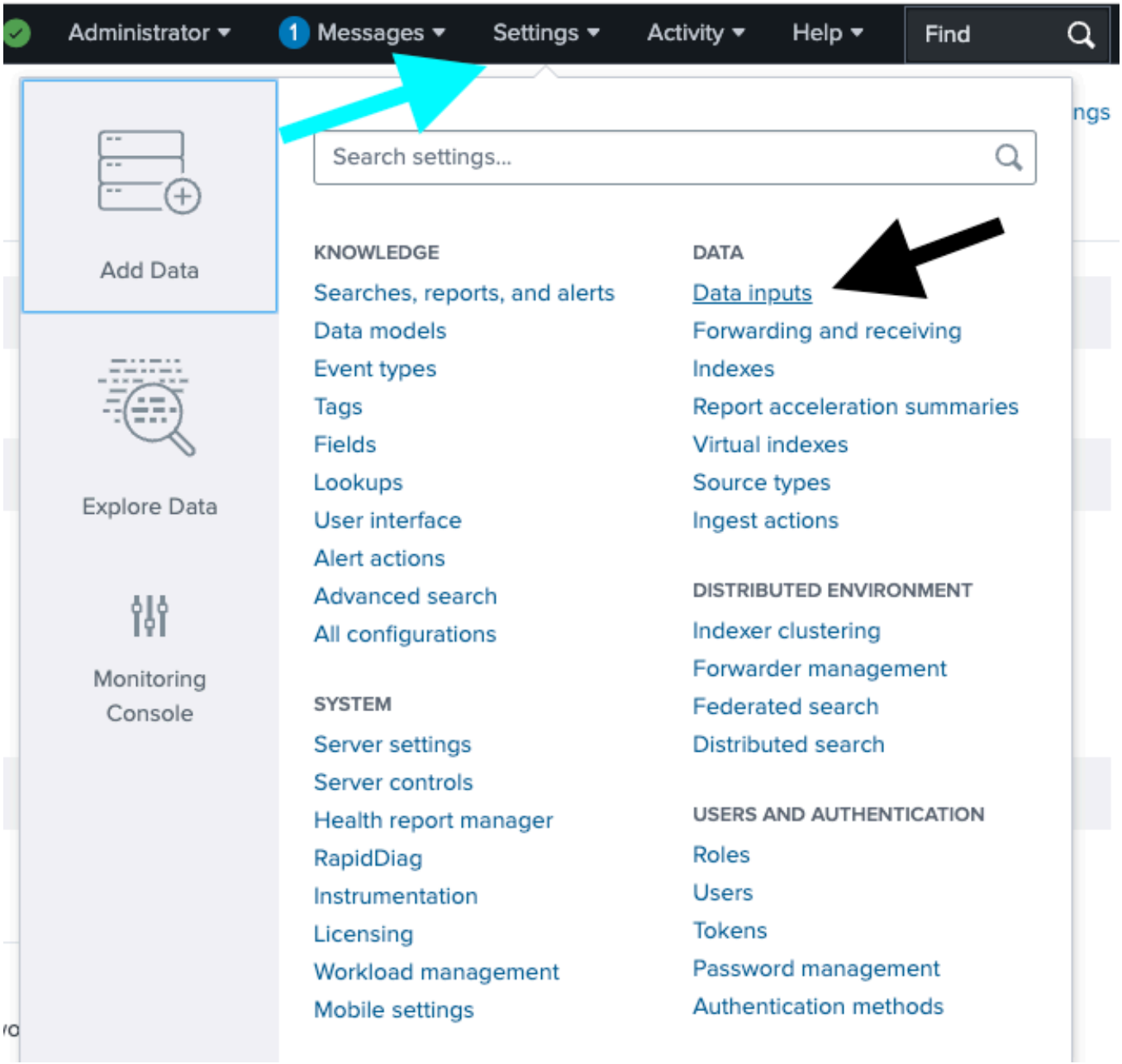


Anmerkung: Zur Quelle siehe Schritt 4
Informationen zu source_type finden Sie in Schritt 6.

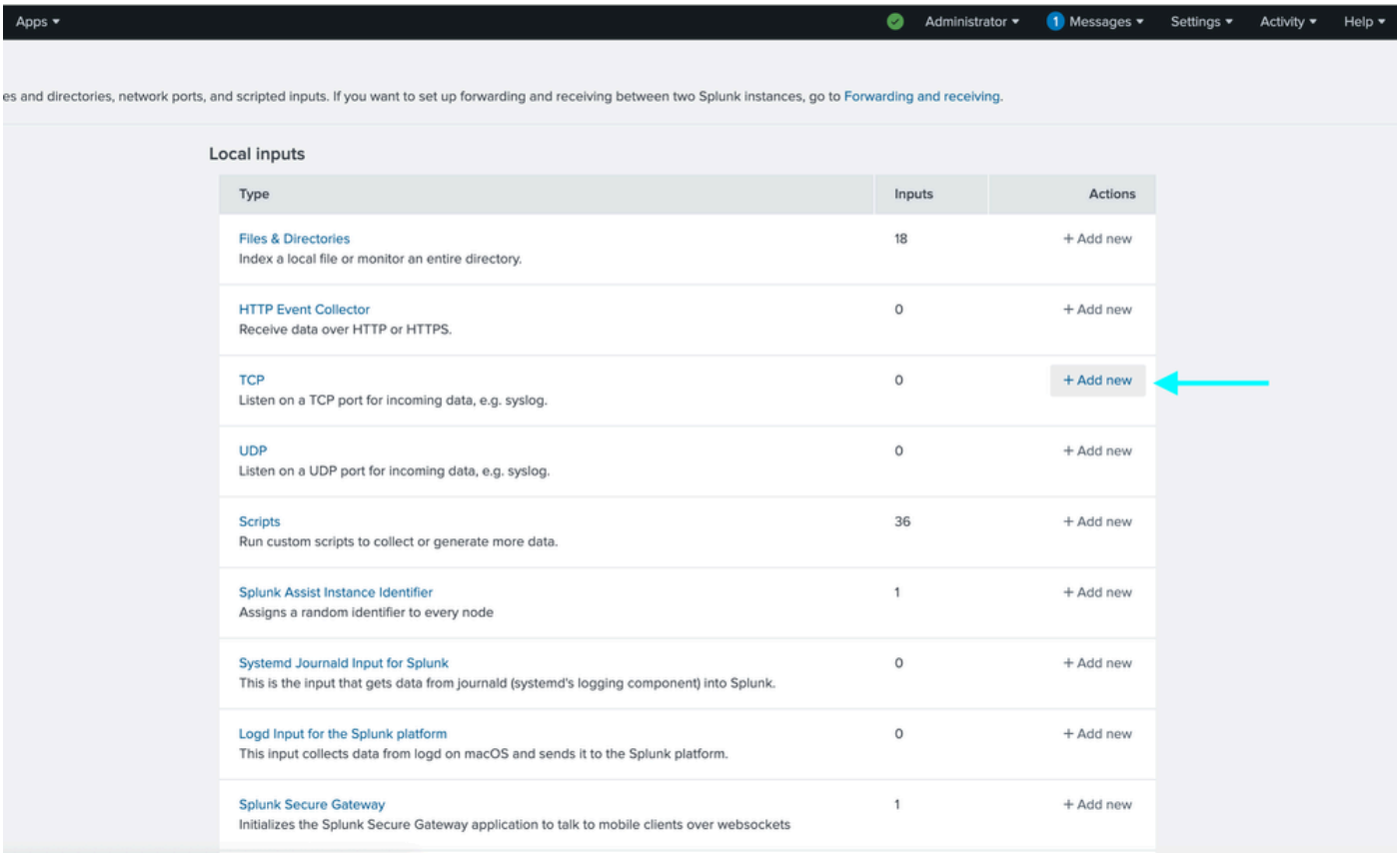
Konfiguration von Syslog auf SNA über TCP-Port 6514 oder benutzerdefinierten Port

1.Splunk für den Empfang von SNA-Audit-Protokollen über TCP-Port konfigurieren

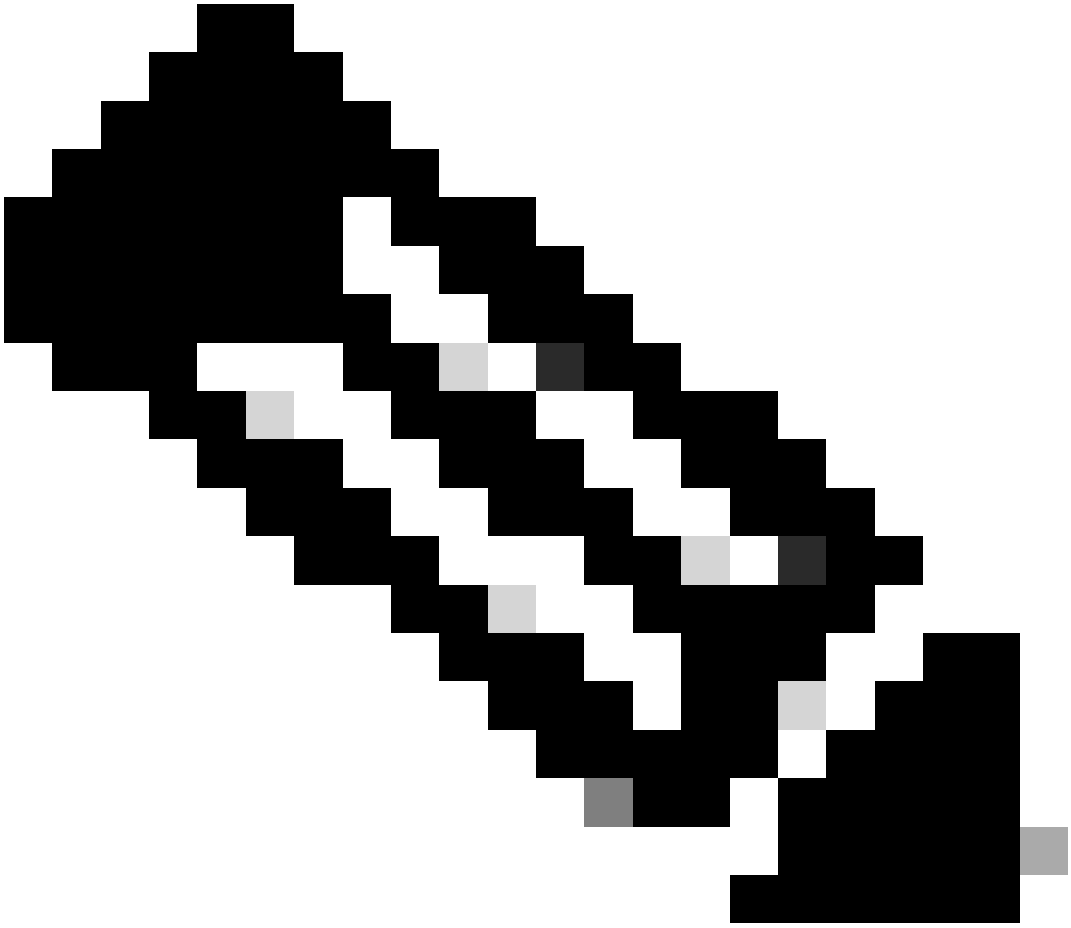
Schritt 1: Navigieren Sie in der Splunk-Benutzeroberfläche zu Einstellungen > Daten hinzufügen > Dateneingaben von DATEN.



Phase 2: Suchen Sie die TCP-Zeile, und wählen Sie + Neu hinzufügen aus.

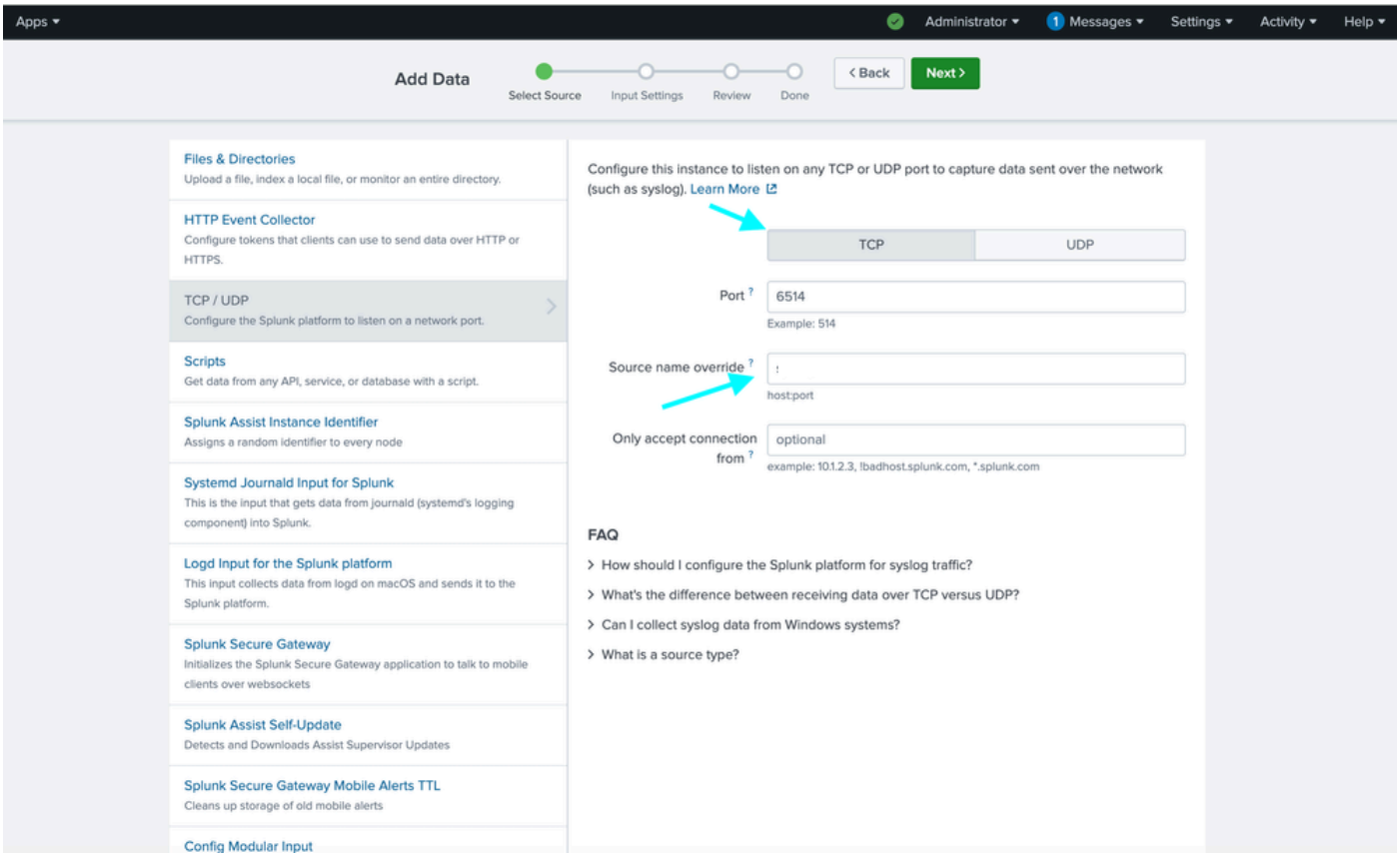


Schritt 3: Wählen Sie im neuen Fenster die Option TCP aus, geben Sie den gewünschten Empfangs-Port in das Beispielbild für den Port 6514 ein, und geben Sie im Feld Source name override (Quellname außer Kraft setzen) den gewünschten Namen ein.



Anmerkung: TCP 6514 ist der Standardport für Syslog über TLS

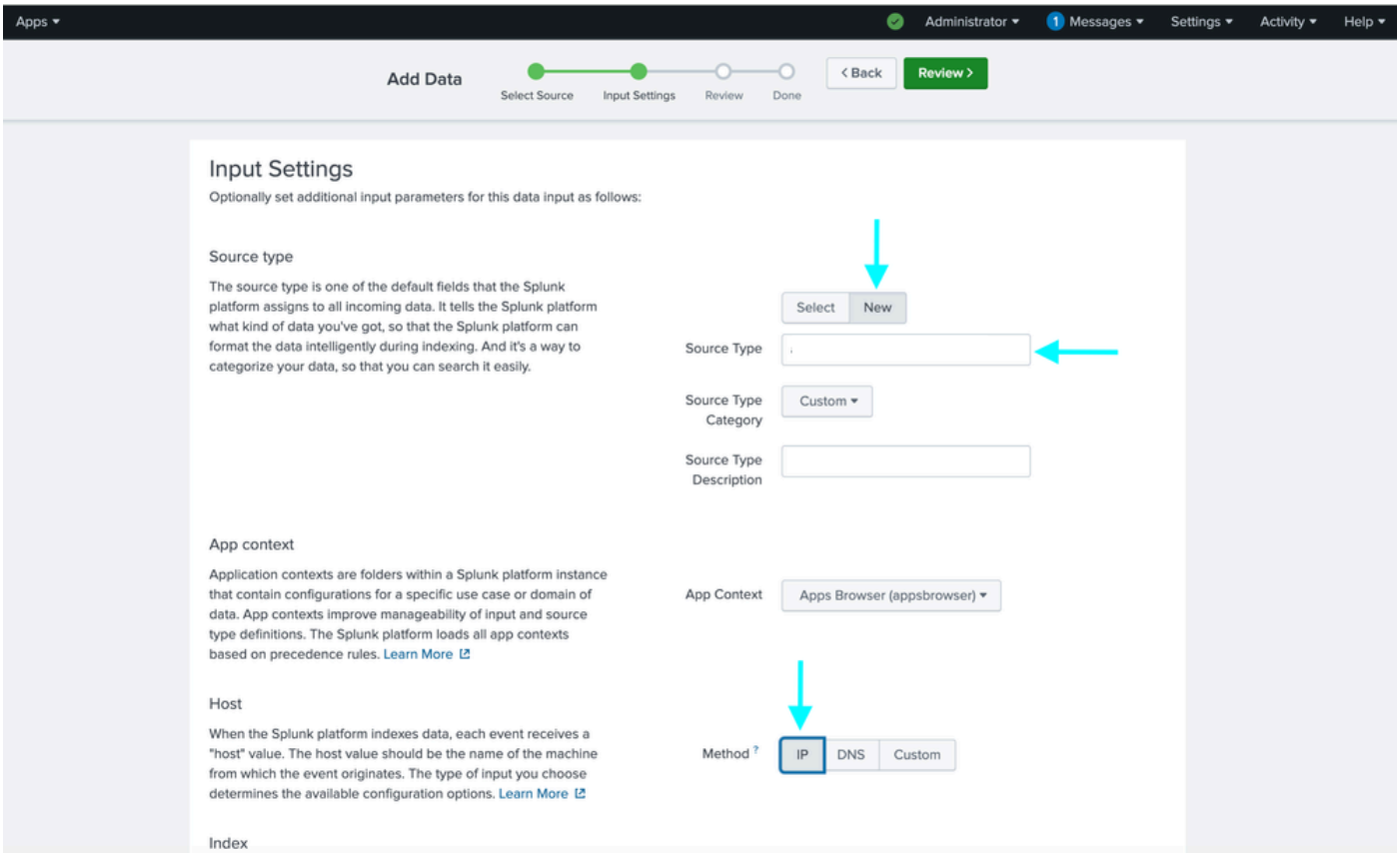
Schritt 4: Wenn Sie fertig sind, klicken Sie oben im Fenster auf die grüne Schaltfläche Weiter >.



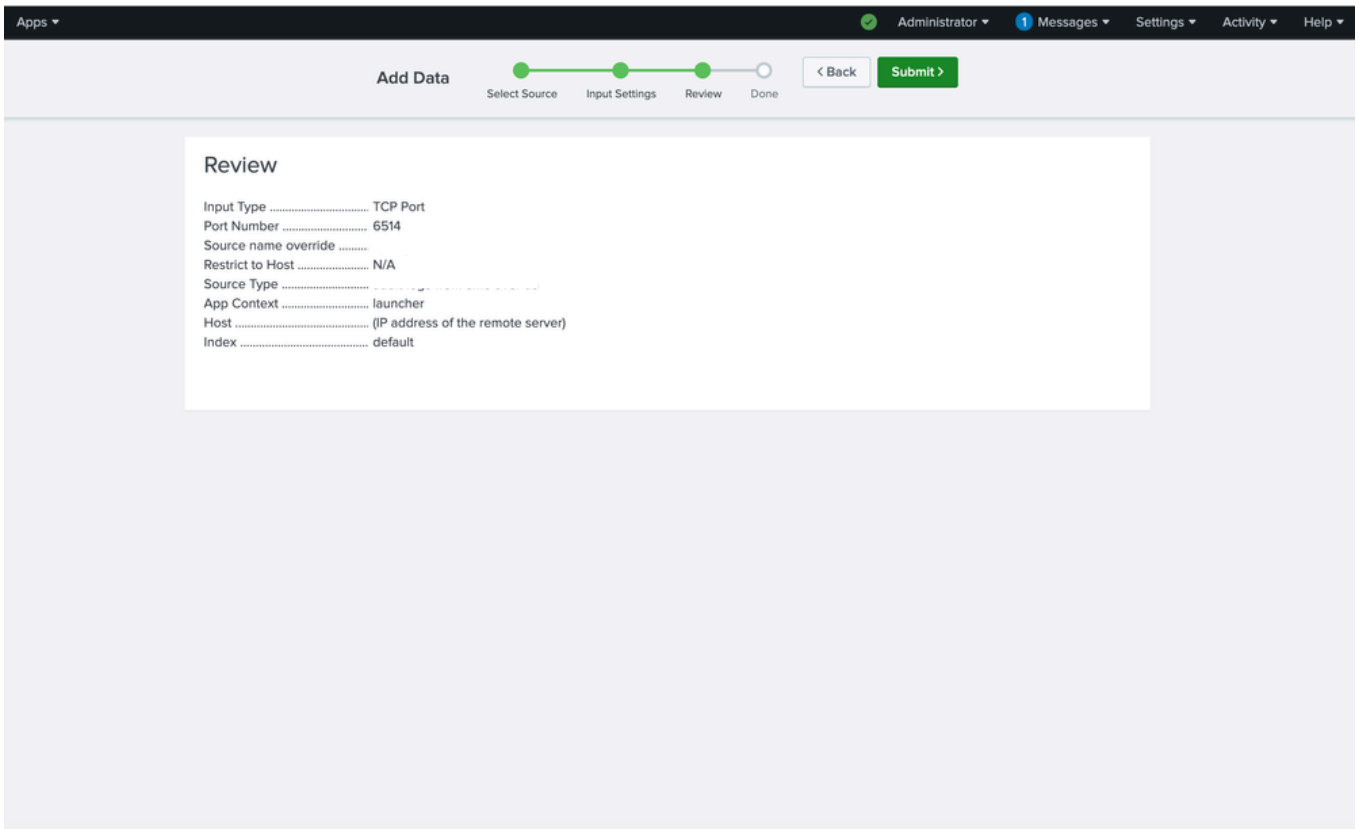
Schritt 5: Wählen Sie im Abschnitt Quellentyp im neuen Fenster die Option Neu aus, und geben Sie im Feld Quelltyp den gewünschten Namen ein.

Schritt 6: Wählen Sie im Host-Abschnitt IP als Methode aus.

Schritt 7: Wenn Sie fertig sind, klicken Sie oben im Fenster auf die grüne Schaltfläche Prüfen >.



Schritt 8: Überprüfen Sie im nächsten Fenster Ihre Einstellungen, und bearbeiten Sie sie gegebenenfalls. Klicken Sie nach der Validierung oben im Fenster auf die grüne Schaltfläche Submit > (Senden).



2.Zertifikat für Splunk generieren

Schritt 1: Führen Sie auf einem Computer, auf dem OpenSSL installiert ist, den`sudo openssl req -x509 -newkey rsa:4096 -keyout server_key.pem -out server_cert.pem -sha256 -days 3650 -subj /CN=10.106.127.4`Befehl aus, und ersetzen Sie dabei die Beispiel-IP-Adresse 10.106.127.4 durch die IP-Adresse des Splunk-Geräts. Sie werden zweimal aufgefordert, einen benutzerdefinierten Kennsatz einzugeben. In den Beispielen werden die Befehle von der Befehlszeile des Splunk-Computers ausgeführt.

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

Nach Abschluss des Befehls werden zwei Dateien generiert. Die Dateien server_cert.pem und server_key.pem.

```
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:
```

Phase 2: Wechseln Sie zum Root-Benutzer.

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

Schritt 3: Kopieren Sie das neu generierte Zertifikat in den `/opt/splunk/etc/auth/` .

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

Schritt 4: Anhängen der Datei "punkweb.cet" mit einem privaten Schlüssel.

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

Schritt 5: Ändern des Besitzes des Splunk-Zertifikats

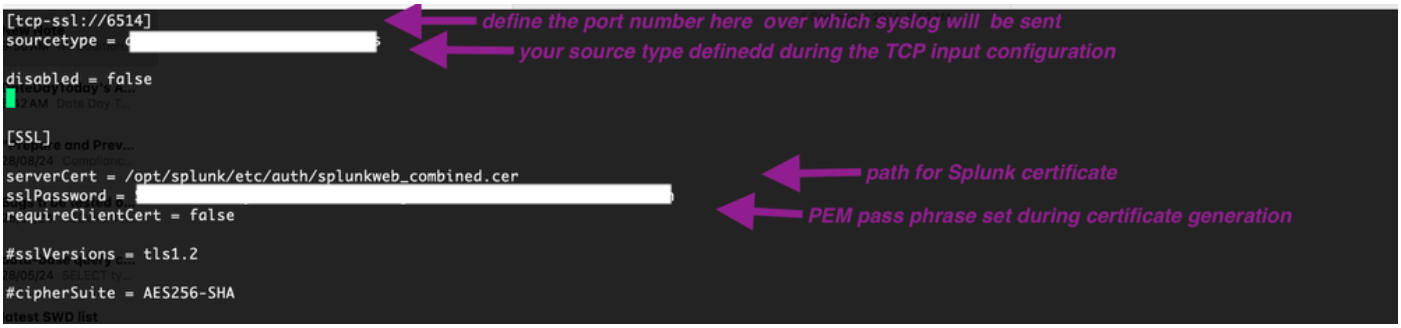
```
user@examplehost:~# chown 10777:10777/opt/splunk/etc/auth/splunkweb.cer
```

Schritt 6: Ändern der Berechtigung für das Splunk-Zertifikat

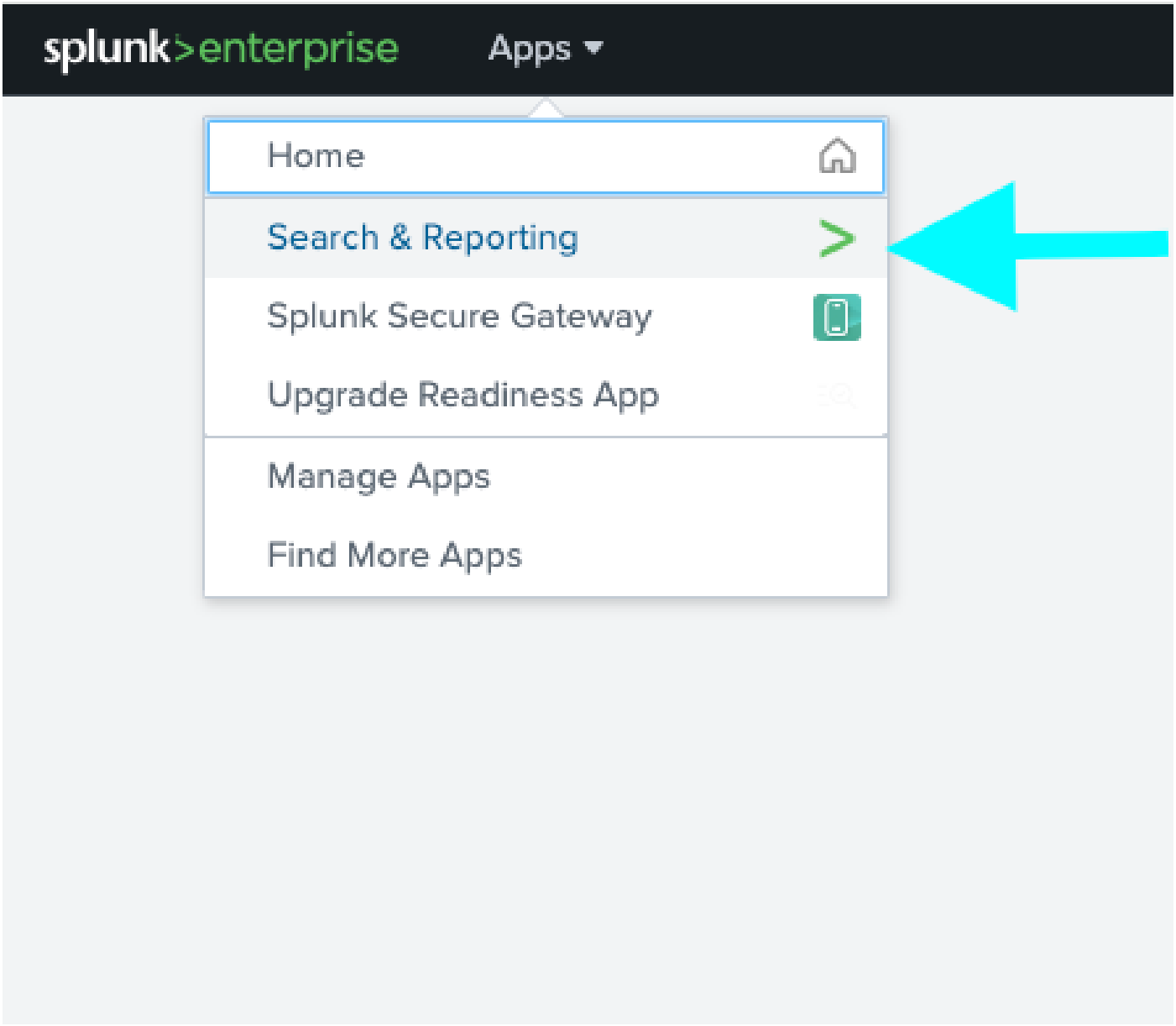
```
user@examplehost:~# chmod 600/opt/splunk/etc/auth/splunkweb.cer
```

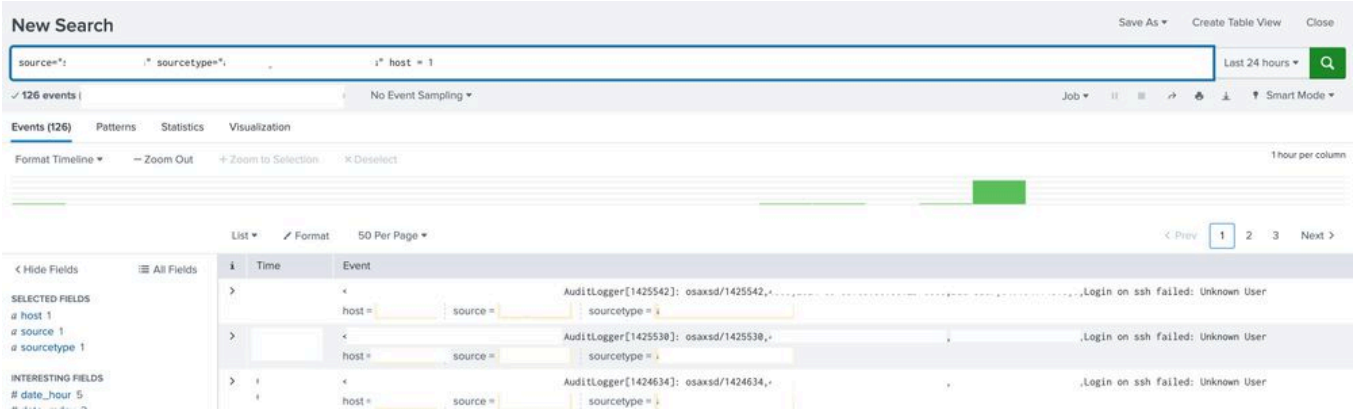
Schritt 7: Erstellen Sie eine neue Datei input.conf.

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



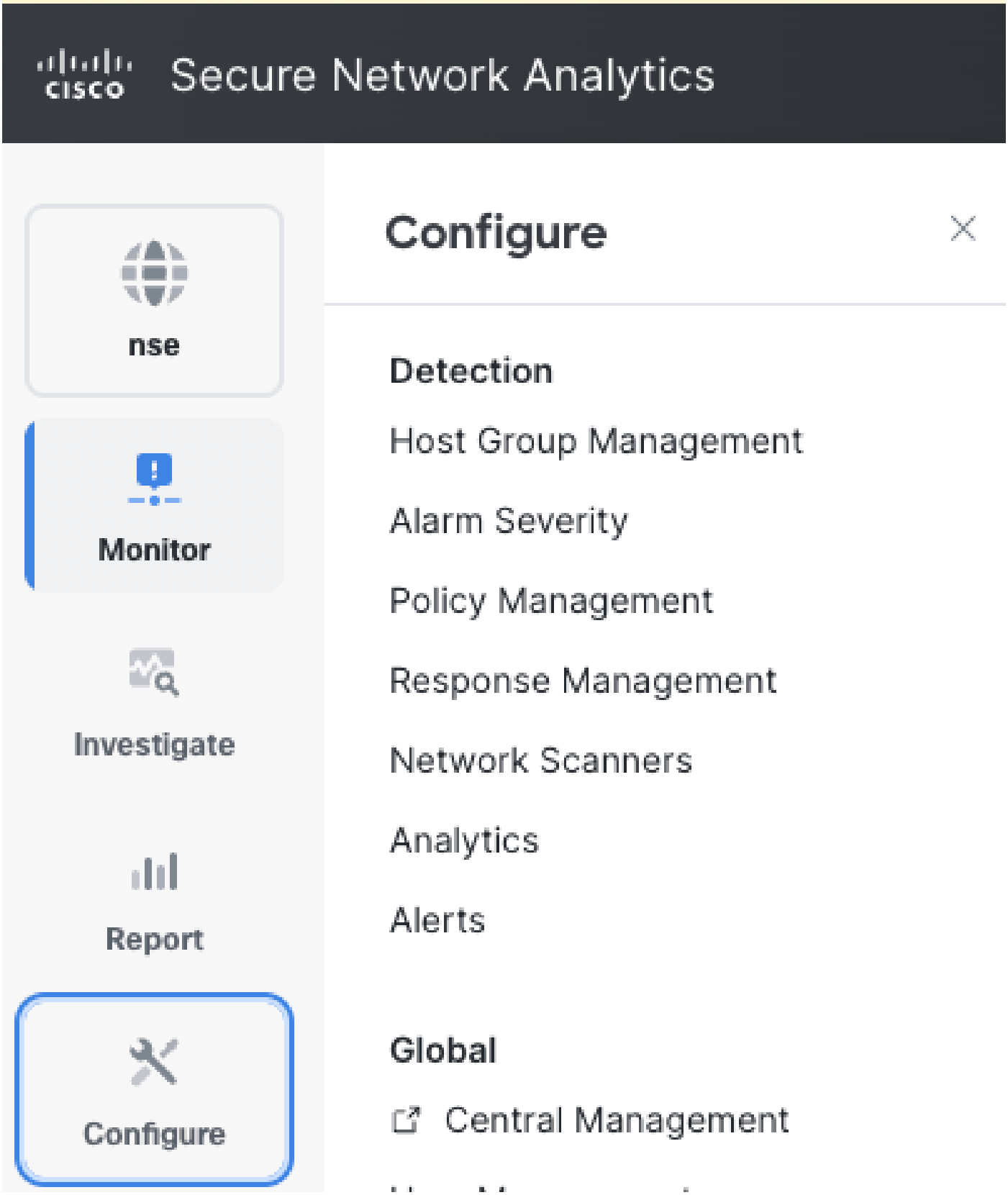
Schritt 8: Überprüfen Sie die Syslogs mithilfe der Suchfunktion.



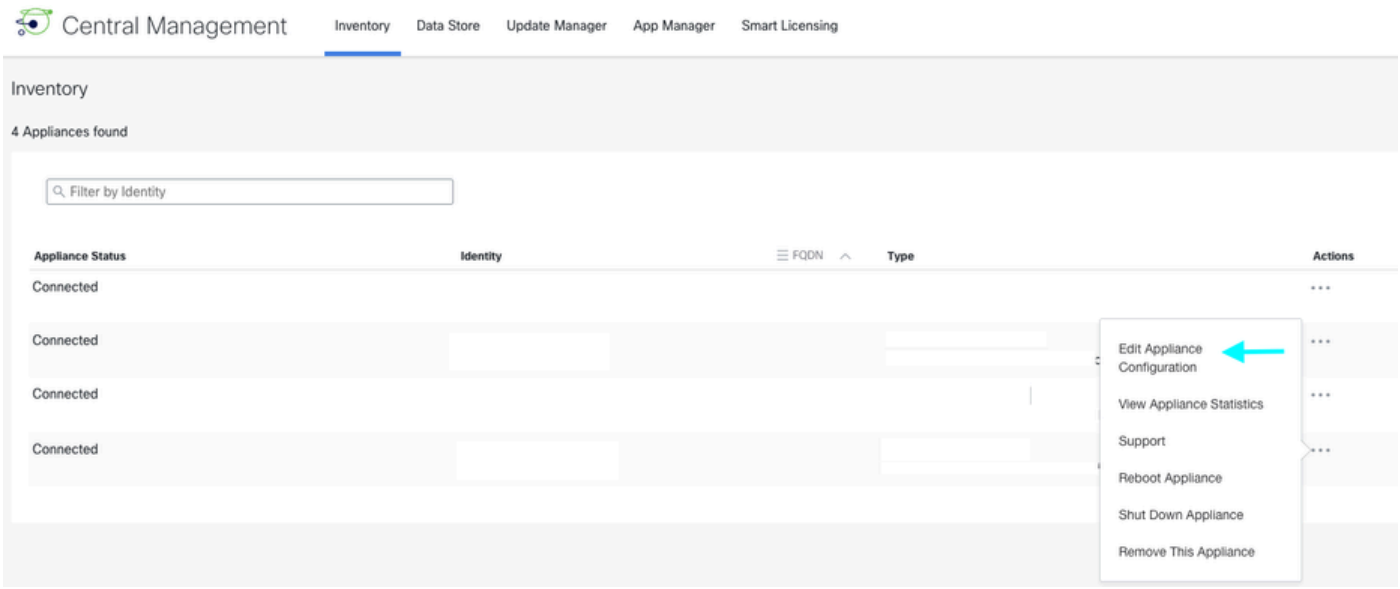


3.Konfigurieren des Prüfprotokollziels auf SNA

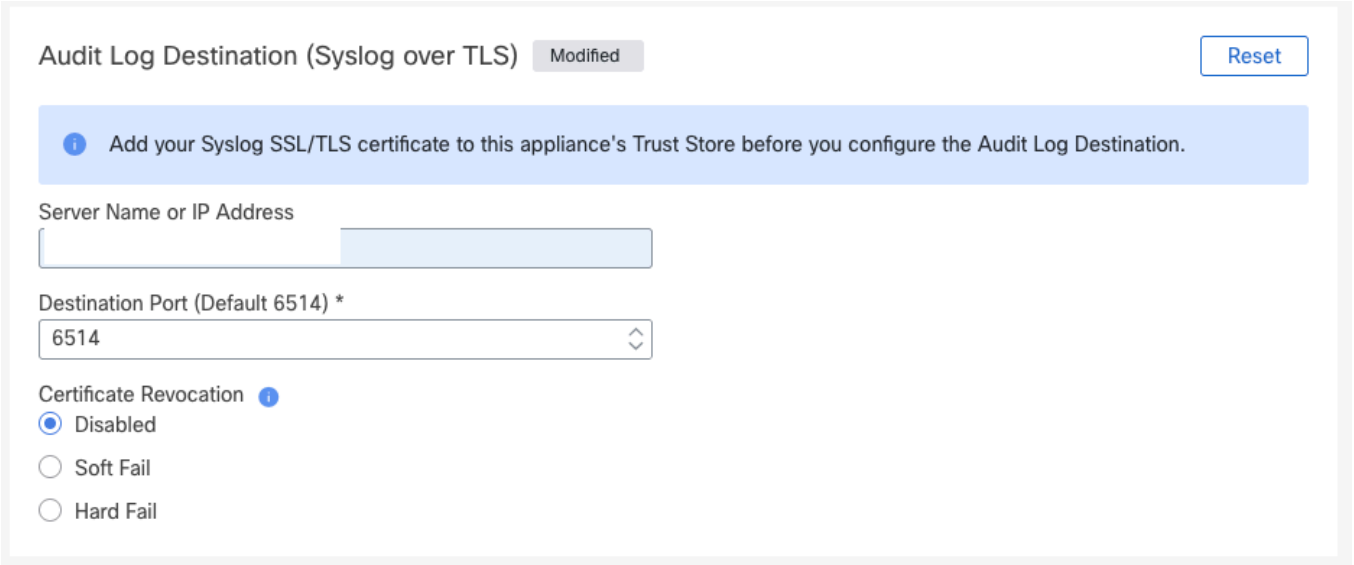
Schritt 1: Melden Sie sich bei der SMC-Benutzeroberfläche an, und navigieren Sie zu Configure > Central Management.



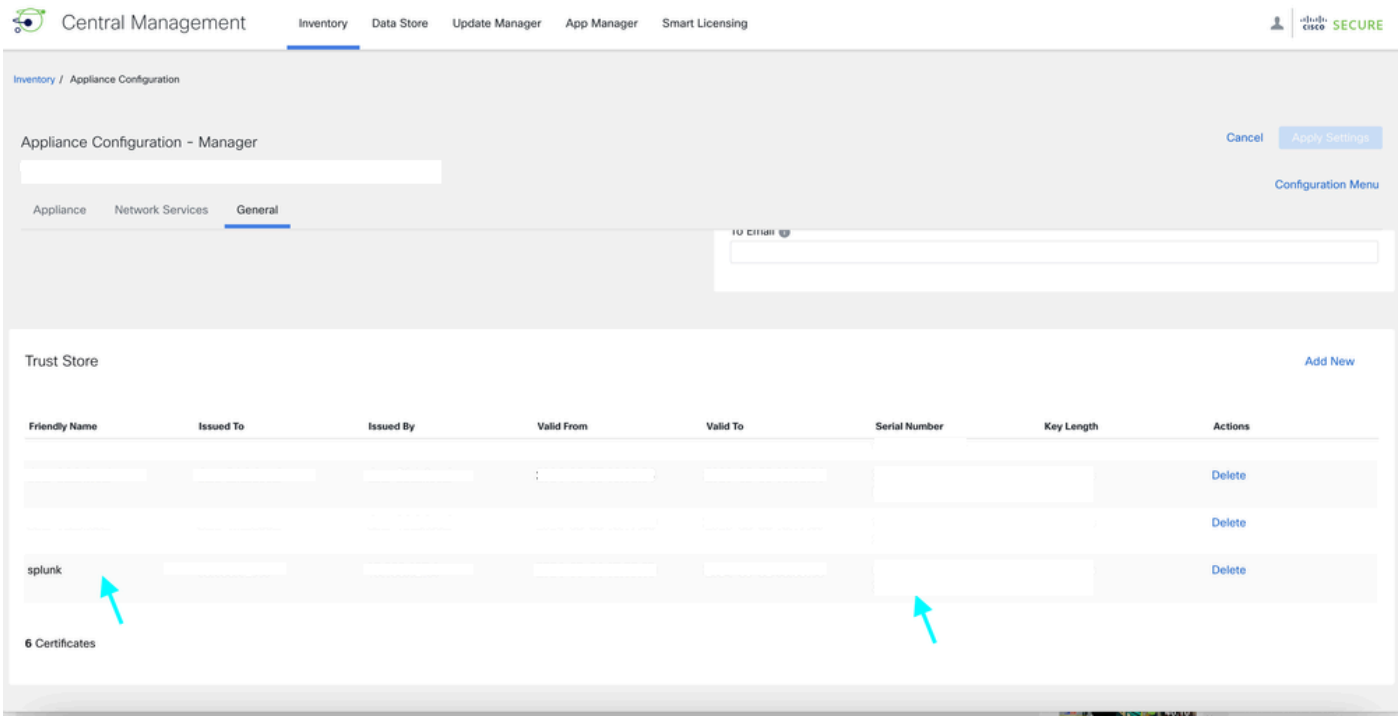
Phase 2: Klicken Sie auf das Auslassungszeichen-Symbol der gewünschten SNA-Appliance, und wählen Sie Einheit-Konfiguration bearbeiten aus.



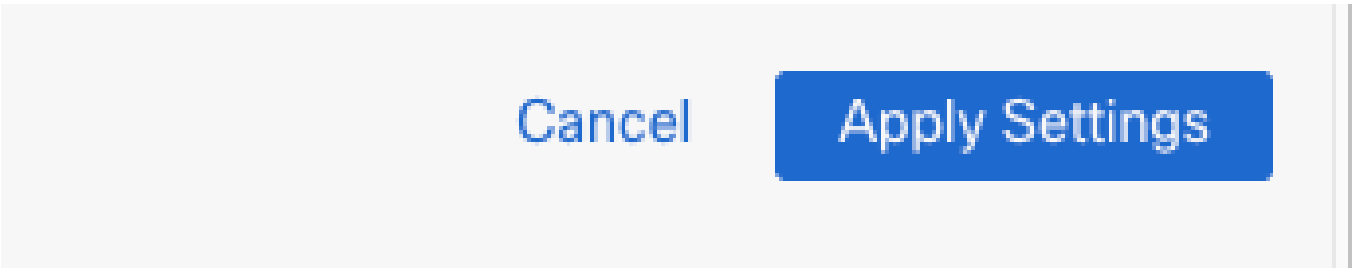
Schritt 3: Navigieren Sie zur Registerkarte Network Services (Netzwerkdienste), und geben Sie Details zum Ziel des Überwachungsprotokolls (Syslog über TLS) ein.



Schritt 4: Navigieren Sie zur Registerkarte General (Allgemein), scrollen Sie nach unten, und klicken Sie auf Add new (Neu hinzufügen), um das zuvor erstellte Splunk-Zertifikat mit dem Namen server_cert.pem hochzuladen.

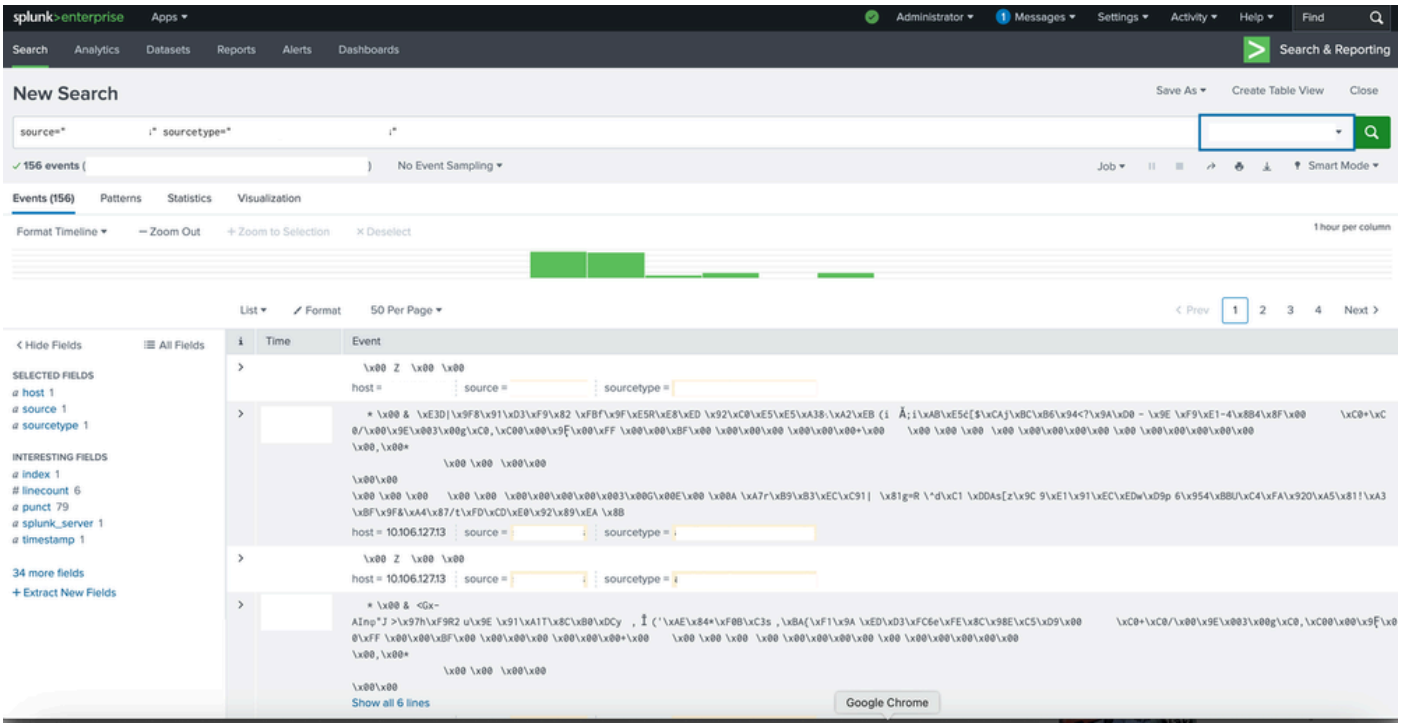


Schritt 5: Klicken Sie auf Einstellungen übernehmen.



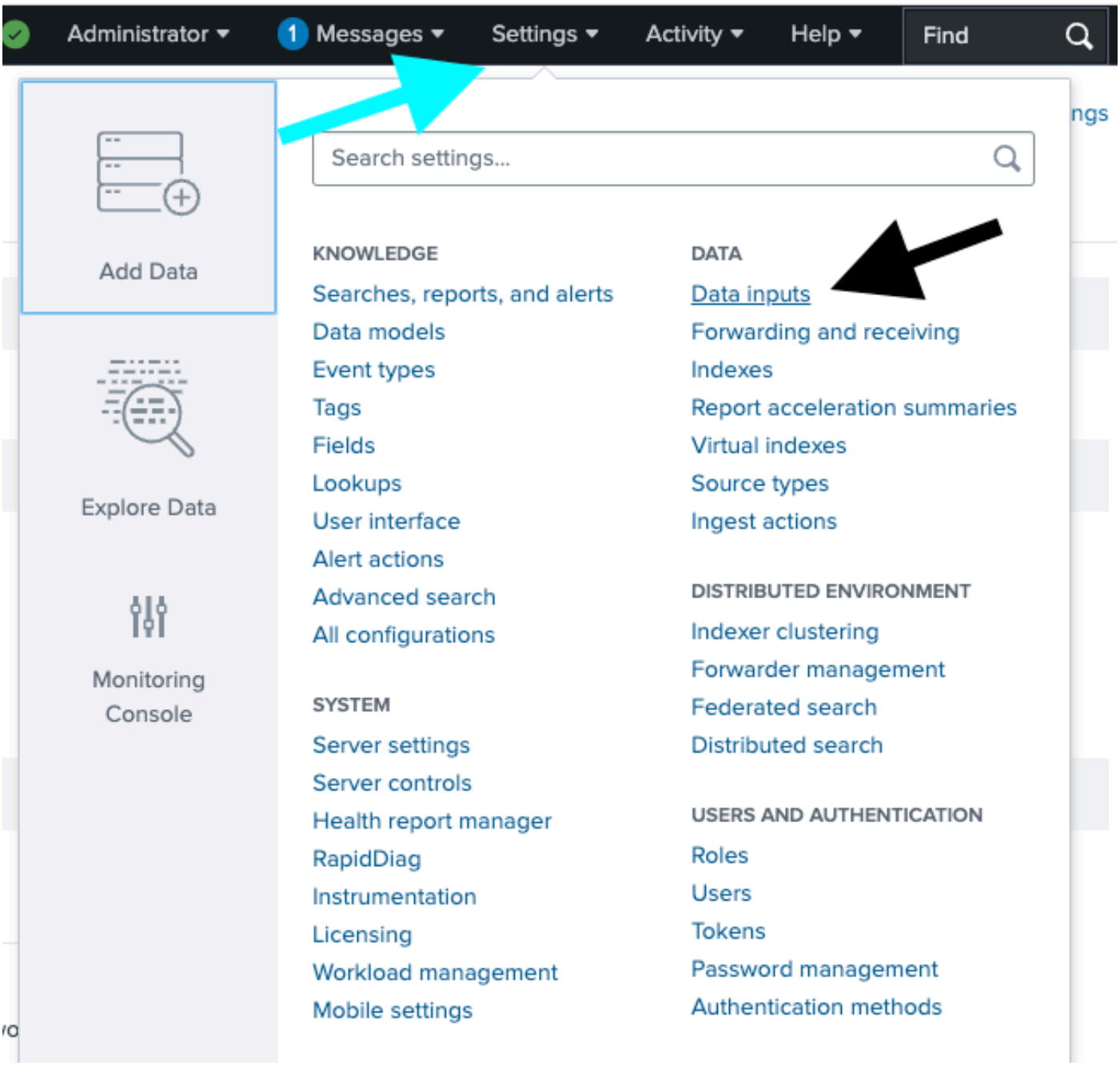
Fehlerbehebung

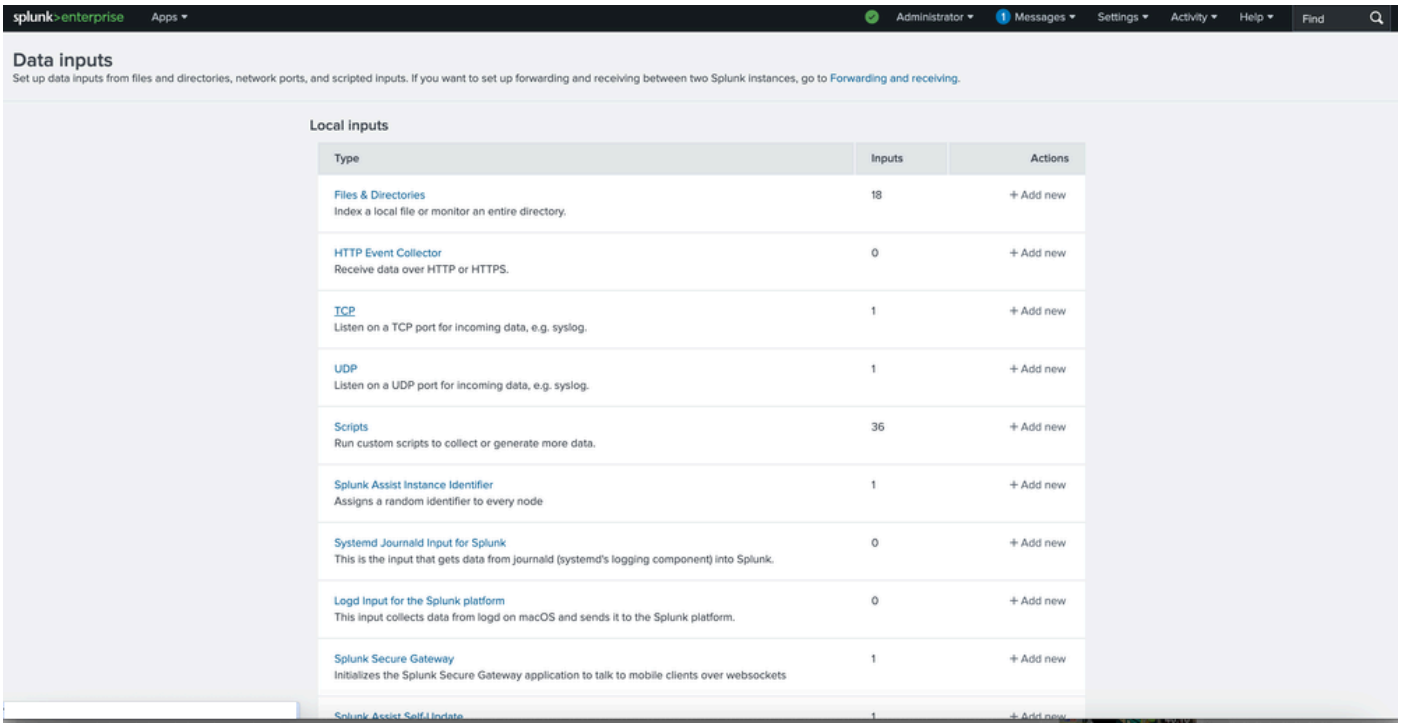
Es könnte komplettes Kauderwelsch auf der Suche sein.

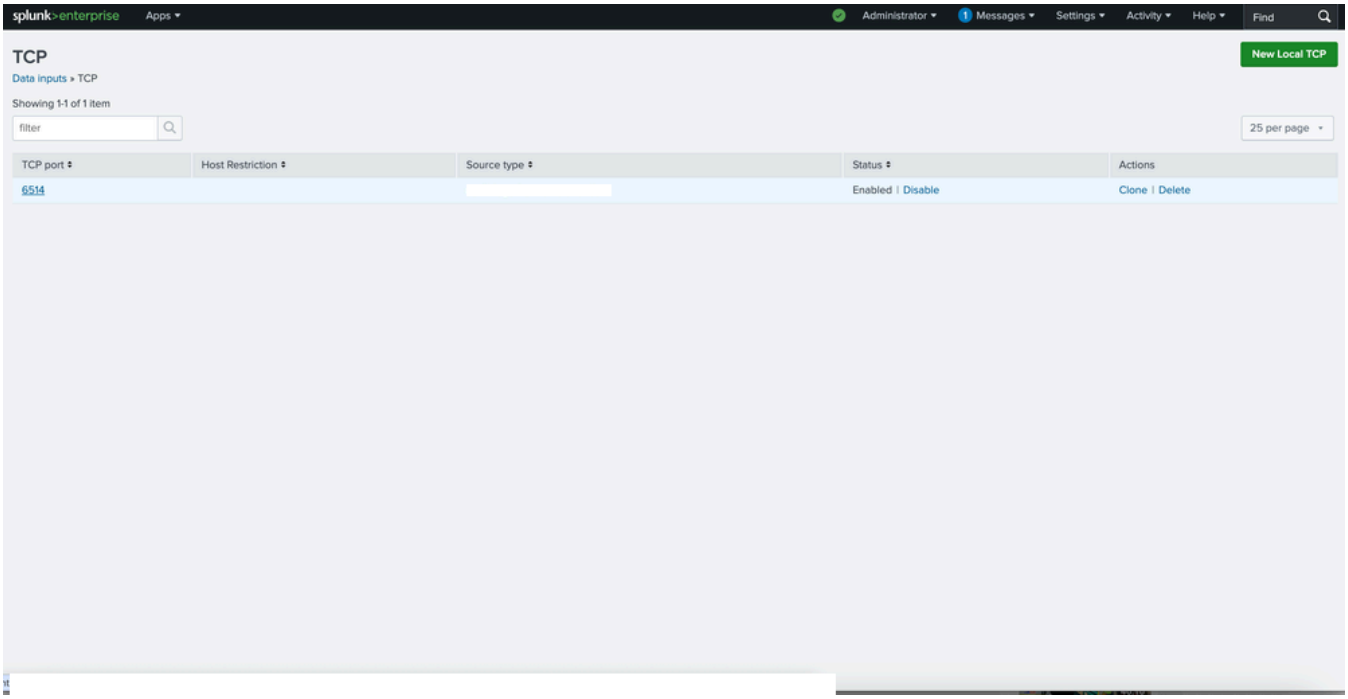


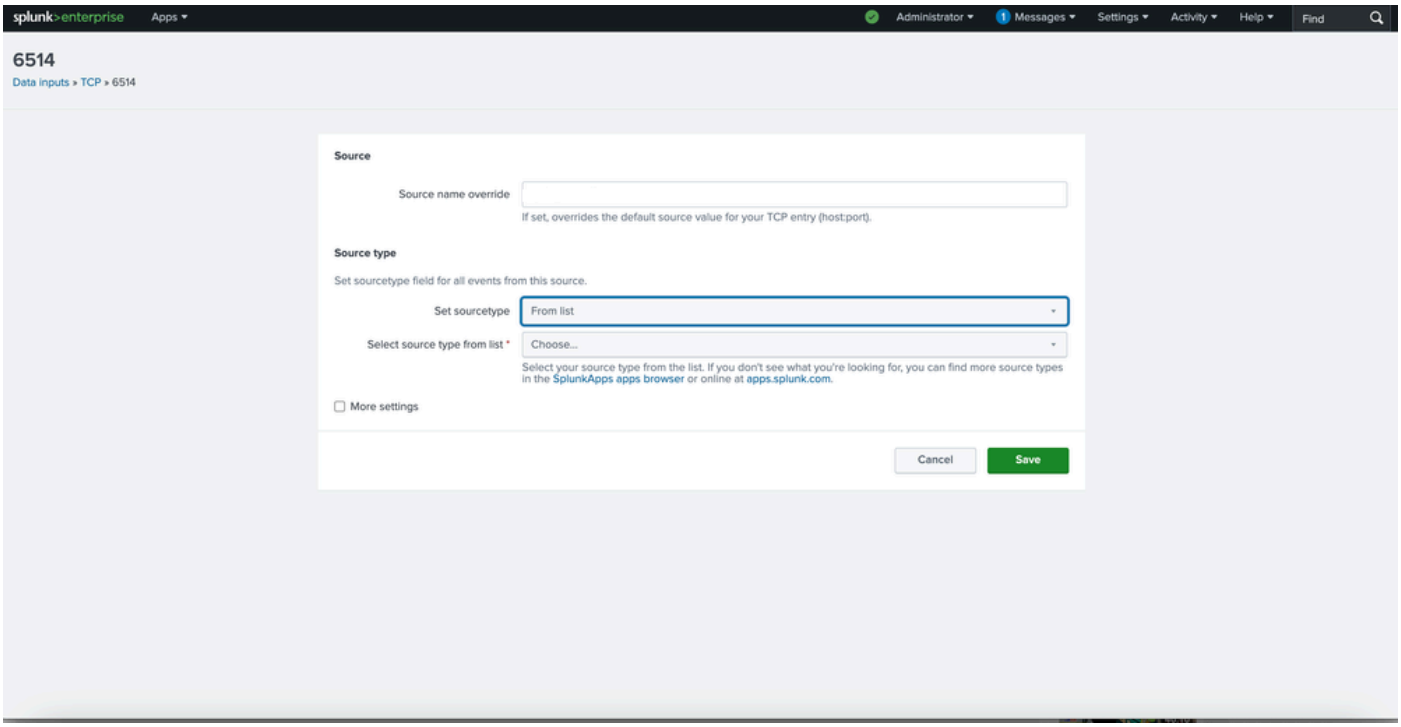
Lösung:

Ordnen Sie die Eingabe dem richtigen Quelltyp zu.


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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.