## 1. Introduction to Splunk Enterprise

Splunk Enterprise is a SIEM platform to collect, analyze, and monitor data from a variety of network devices (not only IP phones).

Please visit the following link for a brief overview of the platform:

https://www.splunk.com/en_us/software/splunk-enterprise/features.html

For integration with the VOIP-500/600 Series IP Call Station, Splunk Enterprise uses the Syslog protocol to collect and parse data. The parsed data is then used for triggering various events (programmable) and network administrators can be notified via email in real-time.

Splunk Enterprise also offers a dashboard which is customizable for a variety of monitoring needs. Various events associated with devices can be viewed in real-time through this dashboard.

Below are a couple snapshot examples of a customized dashboard for the VOIP-500/VOIP-600 Series IP Call Stations:

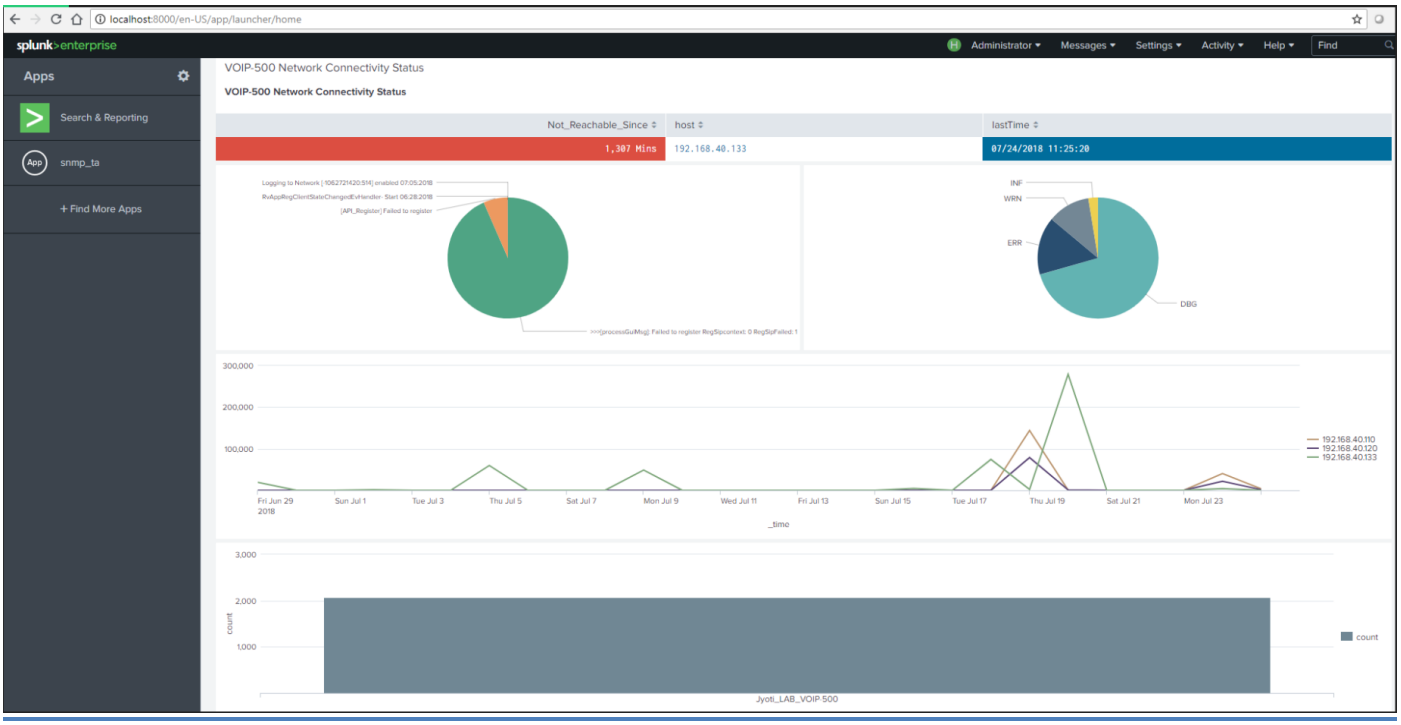


**Figure 1. Example of a Splunk Enterprise dashboard.**

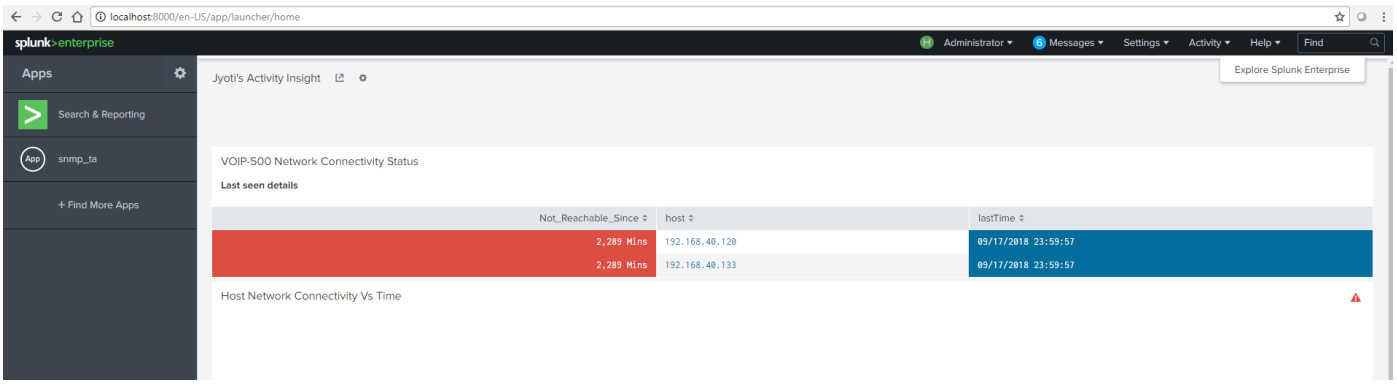


**Figure 2. Example of a Splunk Enterprise dashboard.**

## 2. Configuring the VOIP-500/VOIP-600 Series IP Call Station for Syslog

For the VOIP-500/VOIP-600 IP Call Stations to be able to send Syslog messages to the Splunk Enterprise server, logging must be enabled as shown below.

The **"Logging Level"** will depend on the amount of details which need to be sent to the server. The **"Debug"** level sends the most information while the **"Error"** level sends the least.


**Figure 3. Configuration of VOIP-500/VOIP-600 for Syslog.**

To configure the VOIP-500/VOIP-600 Series IP Call Station for Syslog, please carry out the following:

1. Connect to the VOIP-500/VOIP-600 unit using a supported web browser.
2. Go to **Maintenance > Logging**.
3. Select **Network** under **Send log messages to:**
4. Enter the **Splunk Enterprise server IP address** under **Logging Server IP Address**.
5. Set the **Logging Level** to **Debug**.
6. Click **Apply** to save changes.

## 3. Configuration of Splunk Enterprise Server

1. Log into the Splunk Enterprise server as an administrator.
2. **Create Index.**
    a) Go to **Settings > Data > Indexes**.
    b) Create a custom **Index** to tag all Syslog data originating from the VOIP-500/VOIP-600 Series IP Call Stations.
    c) Assign an **Index Name** and leave all other fields to default values.

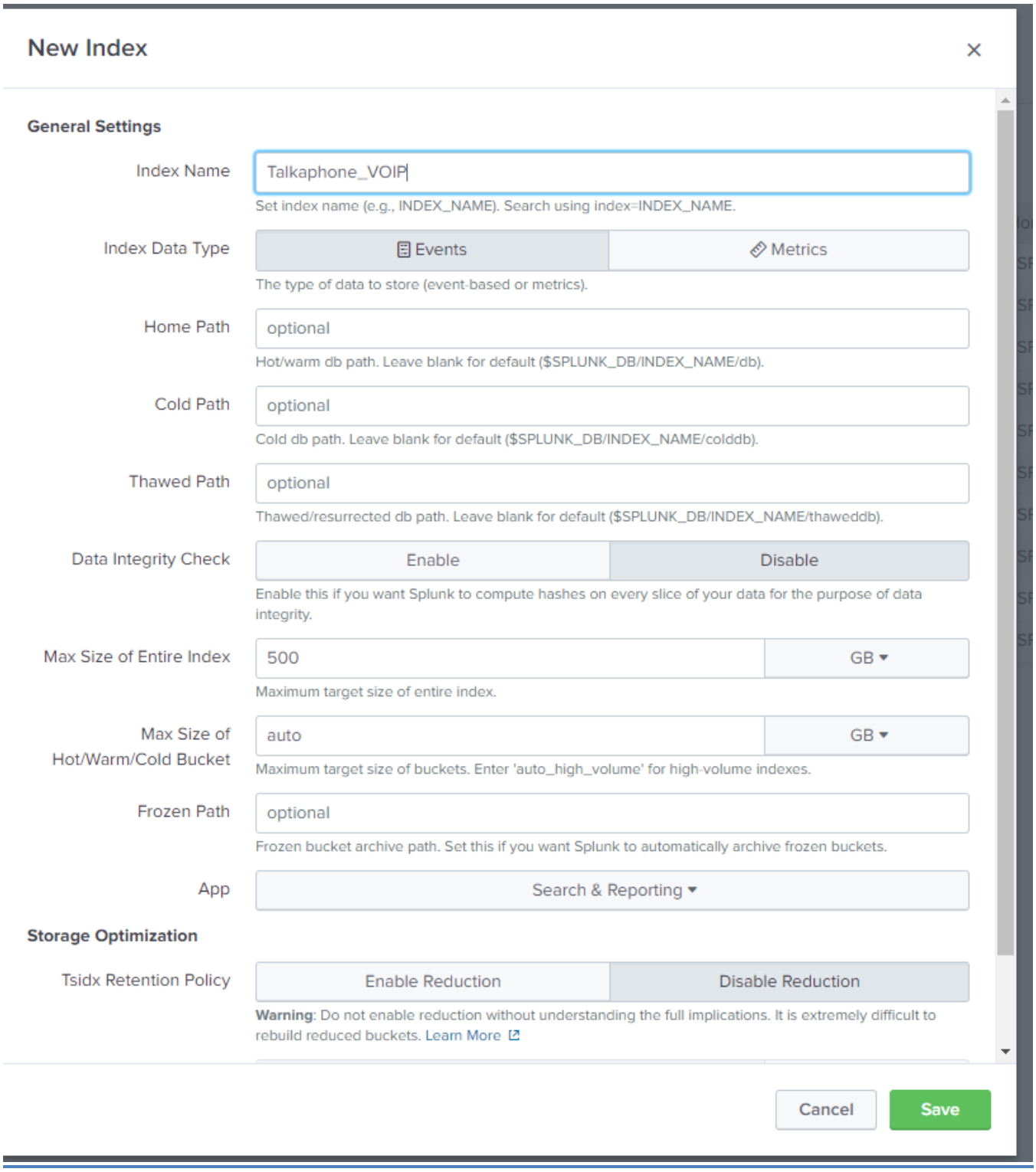


**Figure 4. Index configuration -- Splunk Enterprise.**

### 3. Add Source Type.

a) Add a **Source Type** for each VOIP-500/VOIP-600 Series IP Call Station as shown.

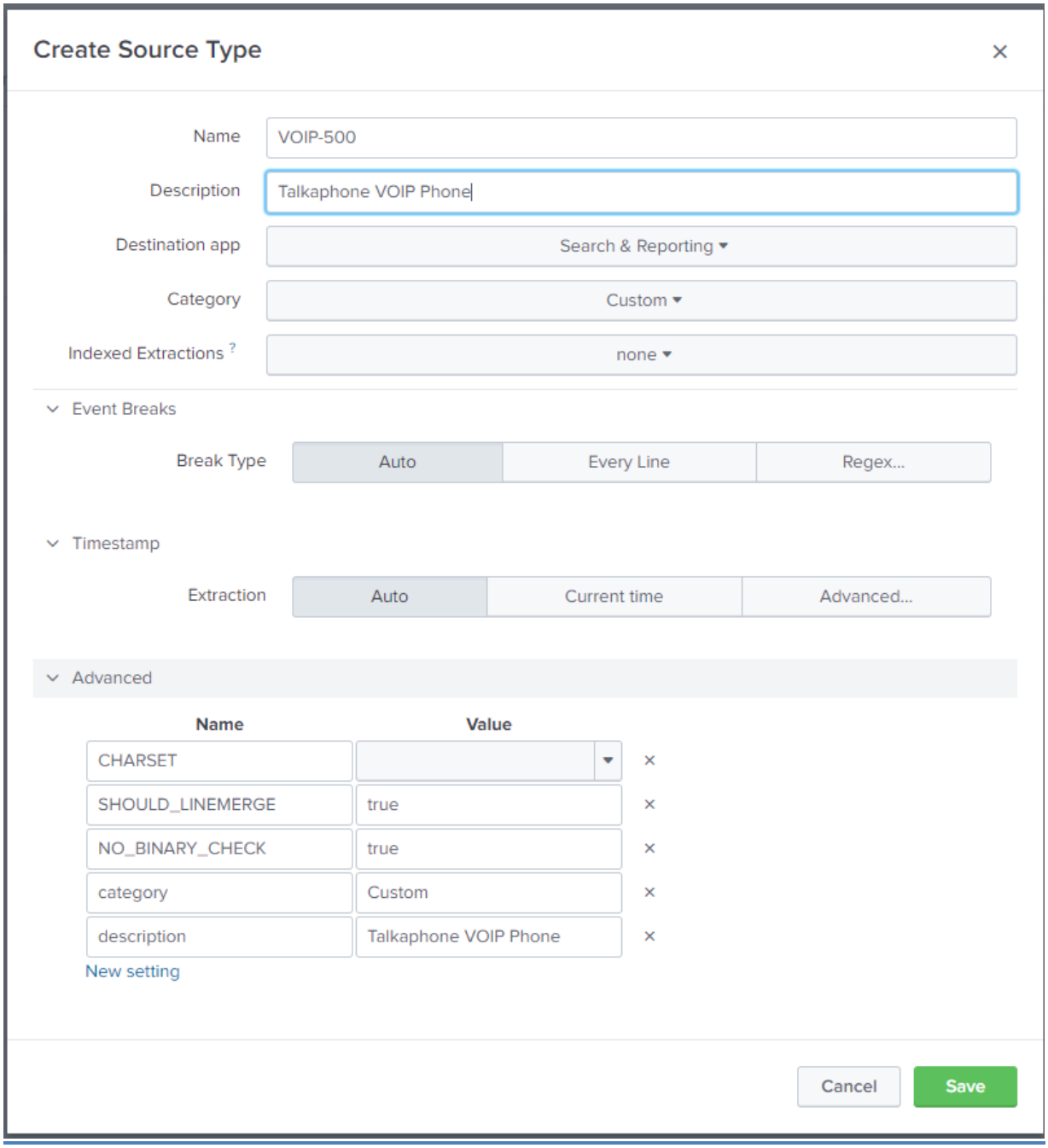


**Figure 5. Adding a source type -- Splunk Enterprise.**

## 4. Add Data Inputs.

a) Go to **Settings > Data > Data Inputs > UDP**.

b) Add a **UDP Port** to listen for Syslog messages. This port must match the port configured on the VOIP-500/VOIP-600 unit.

c) Click **Next**.

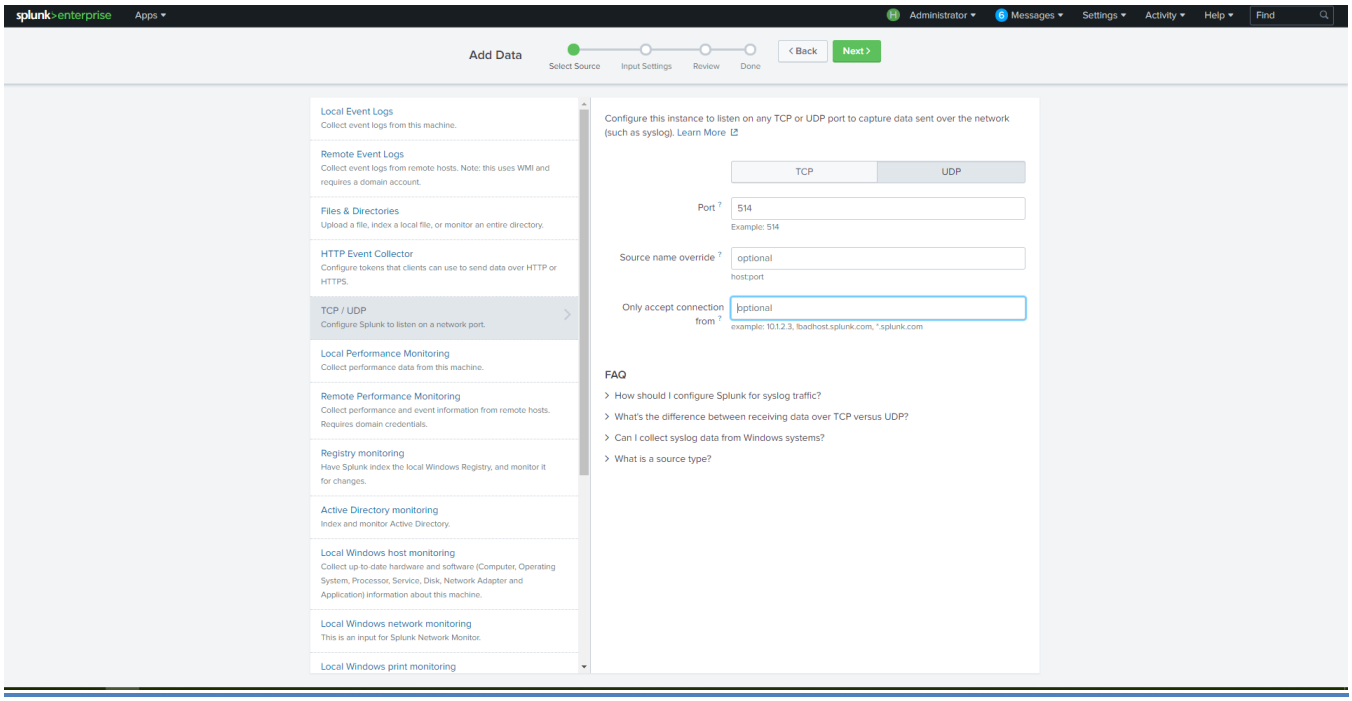


**Figure 6. Configuring a data input -- Splunk Enterprise.**

d) Specify the **Source Type** as **VOIP-500** as shown below.

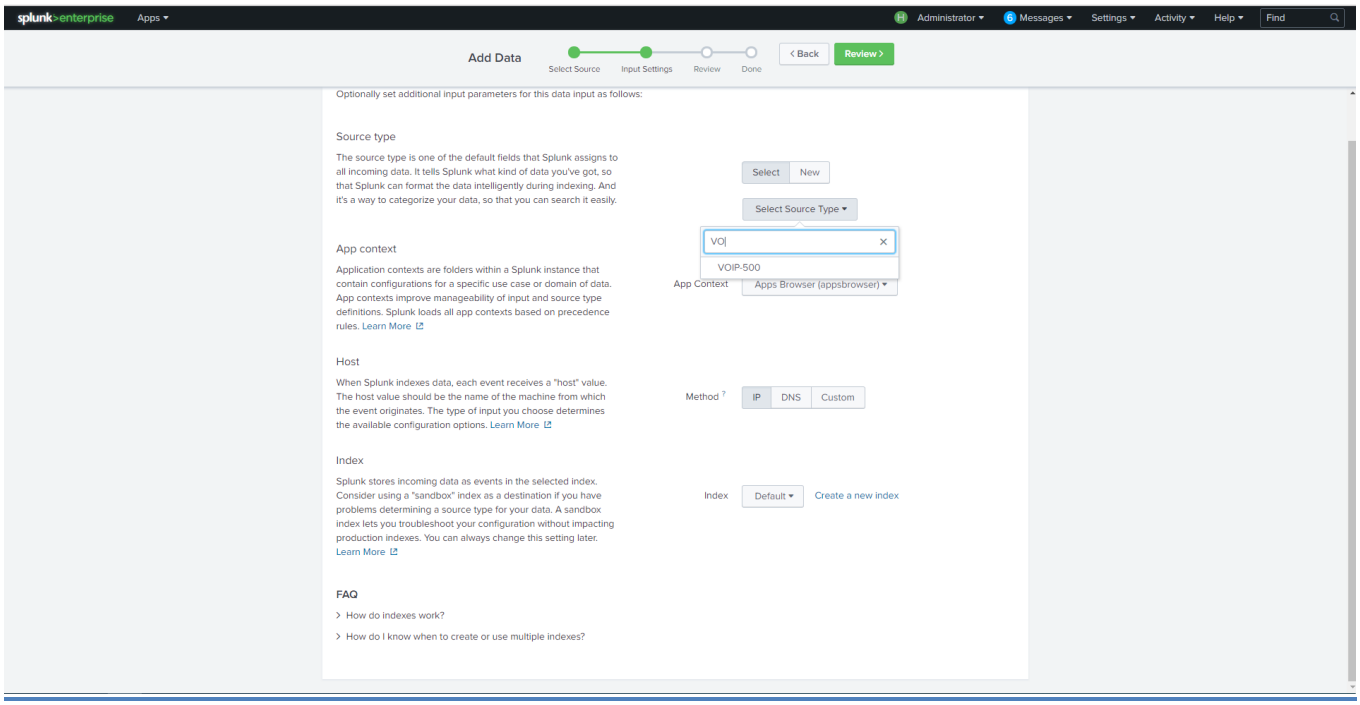


**Figure 7. Specifying source type -- Splunk Enterprise.**

e) Click **Review**.

f) Click **Submit**.

## 5. Configuring Receive Data.

a) Go to **Settings > Data > Forwarding and Receiving > Receive Data**.

b) Add a **New Receiving Port**. This port should match the port configured on the VOIP-500/VOIP-600 unit for sending data to the network.

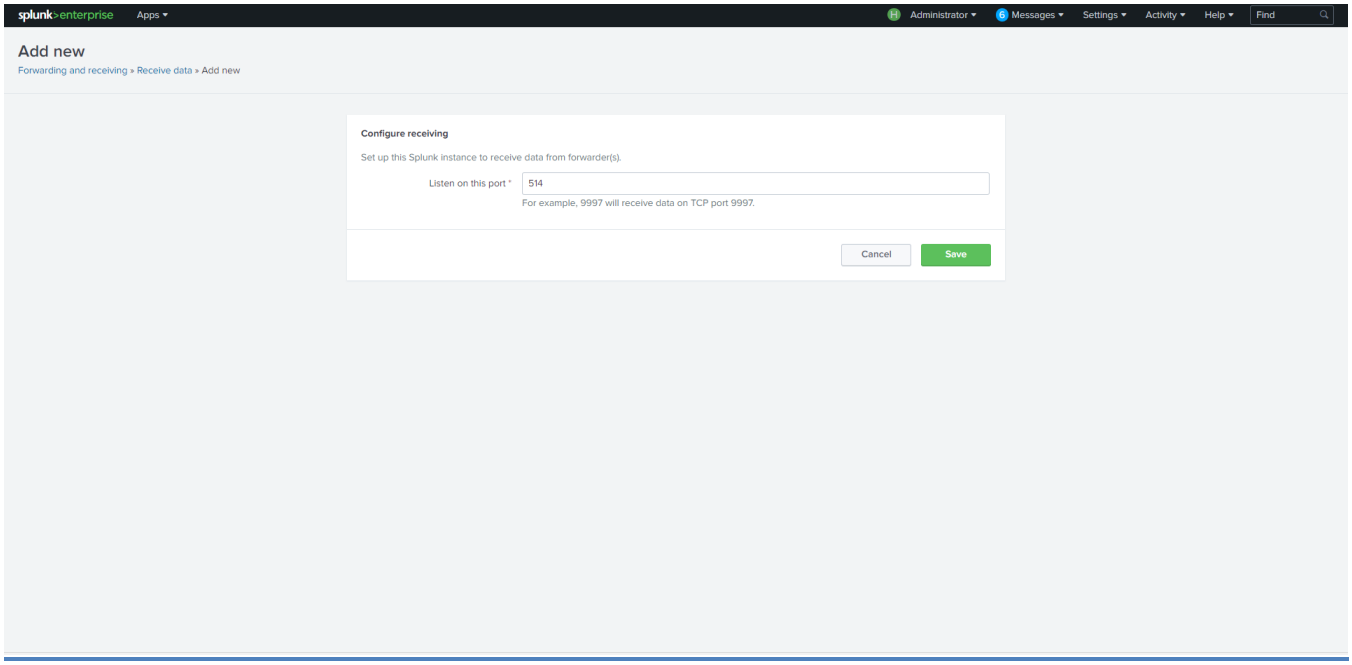


**Figure 8. Adding a new receiving port -- Splunk Enterprise.**

c) Add a universal forwarder port of **9997**.

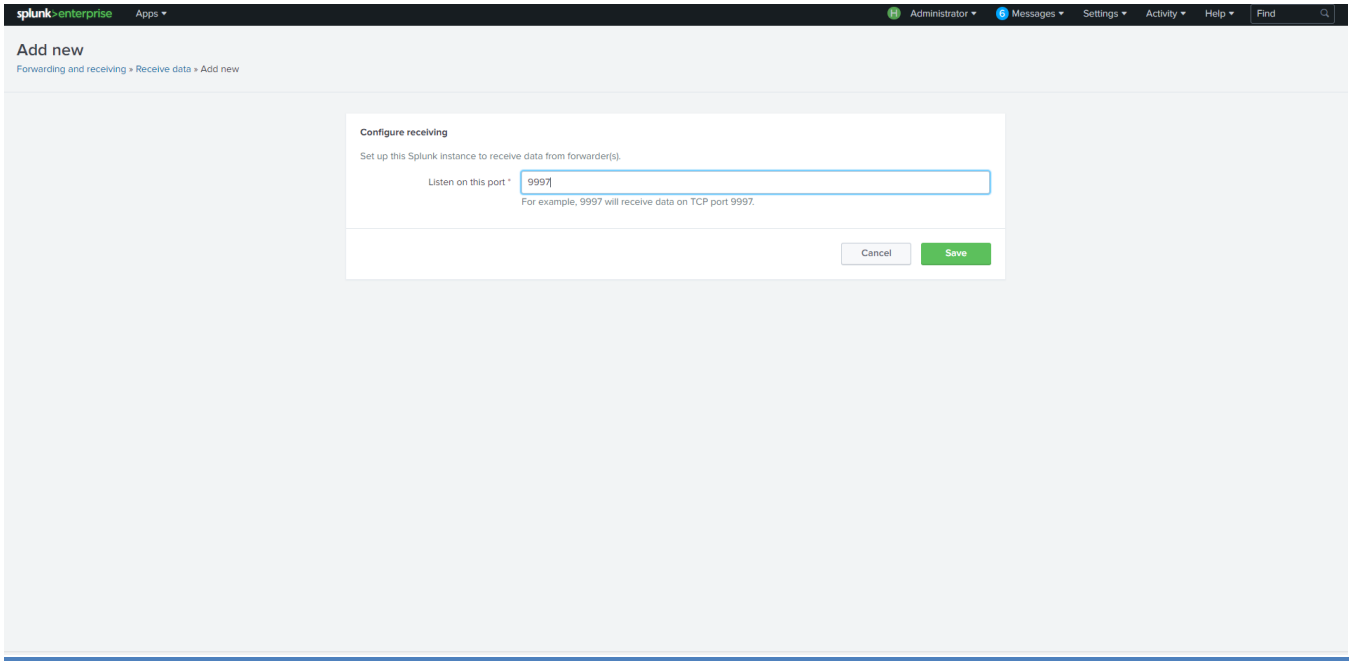


**Figure 9. Adding a universal forwarder port -- Splunk Enterprise.**

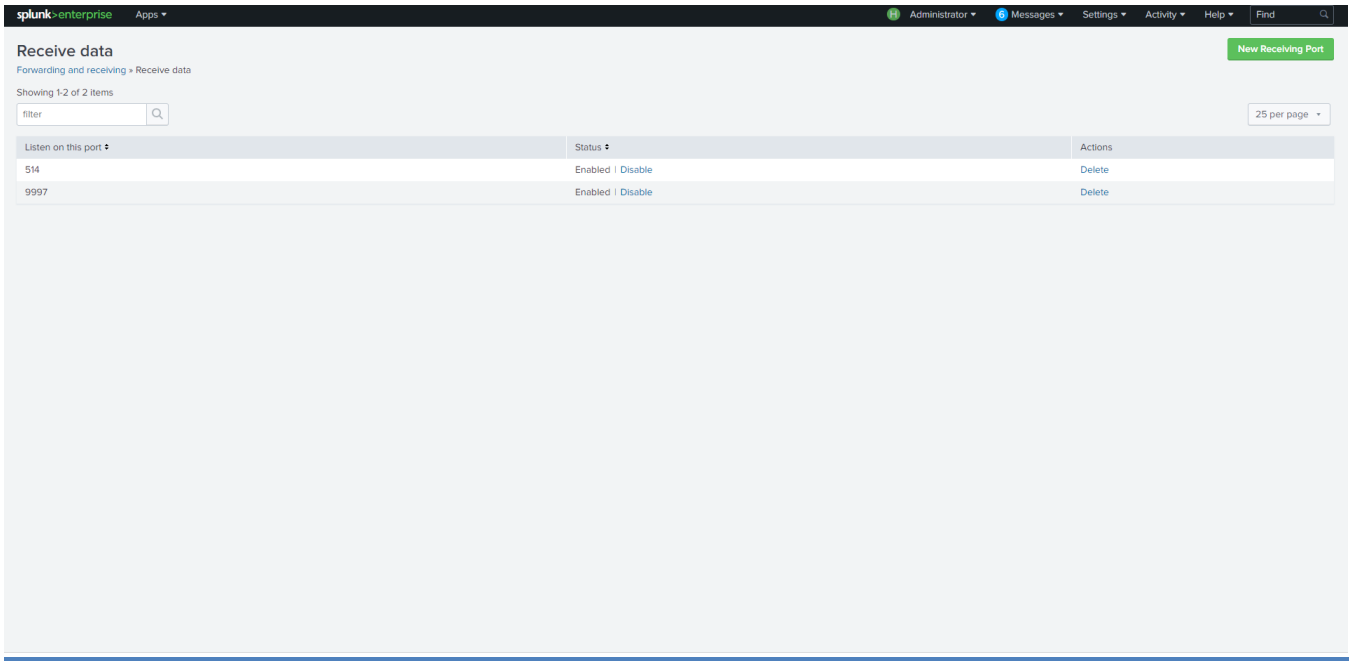


**Figure 10. Receive data page showing configured ports -- Splunk Enterprise.**

## 4. Creating Alerts

1. **Parsing VOIP-500/VOIP-600 Log Data.** With the previous steps carried out, the data from the VOIP-500/VOIP-600 is transmitted to the Splunk Enterprise server.

   To parse the logs and identify the incoming data from the VOIP-500/VOIP-600 call stations, use the following search under **Search and Reporting**.

   a) In the search bar, enter **index = <index_created_in_Step_3.2.c>**

   In the example provided in **Step 3.2(c)**, the index would be **Talkaphone_VOIP**

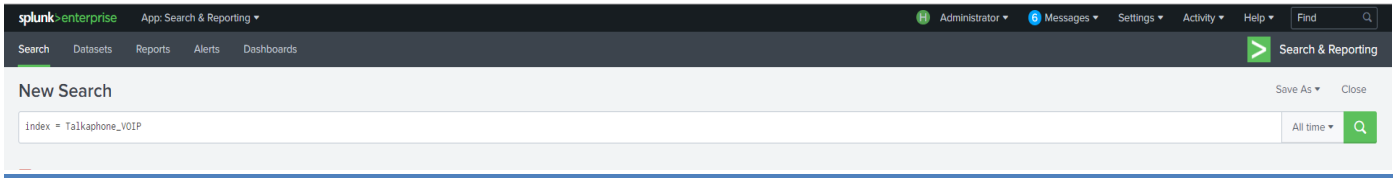


**Figure 11. Searching on an index -- Splunk Enterprise.**

   b) Moreover, logs can be filtered from a specific host by IP address (i.e. a specific VOIP-500/VOIP-600 unit).

   Returning to the example of **Step 3.2(c)**, the search would be specified as:

   **index = Talkaphone_VOIP host=<IP_Address_of_Talkaphone_VOIP_device>**

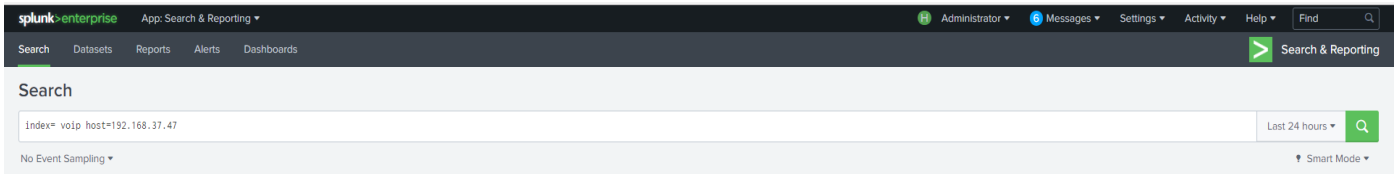


**Figure 12. Searching by IP address of specific host -- Splunk Enterprise.**

## 2. Search Strings for Parsing Various Error Conditions for the VOIP-500/VOIP-600 Series IP Call Station.

| VOIP-500/VOIP-600 Event to be Monitored | Search String (Error Code) for Search Bar Input |
|---|---|
| Power Cycle | Successful System Startup |
| Failed SIP Registration | Failed to Register |
| Button Pressed | Button Pressed: Auto Dial |
| Call Placed | Initiate Call |
| Failed Call | Call Failed |
| Unsuccessful Call Due to Invalid Number | Call Failed -Request Time-out failure_reason = 404 |

## 3. Example Searches.

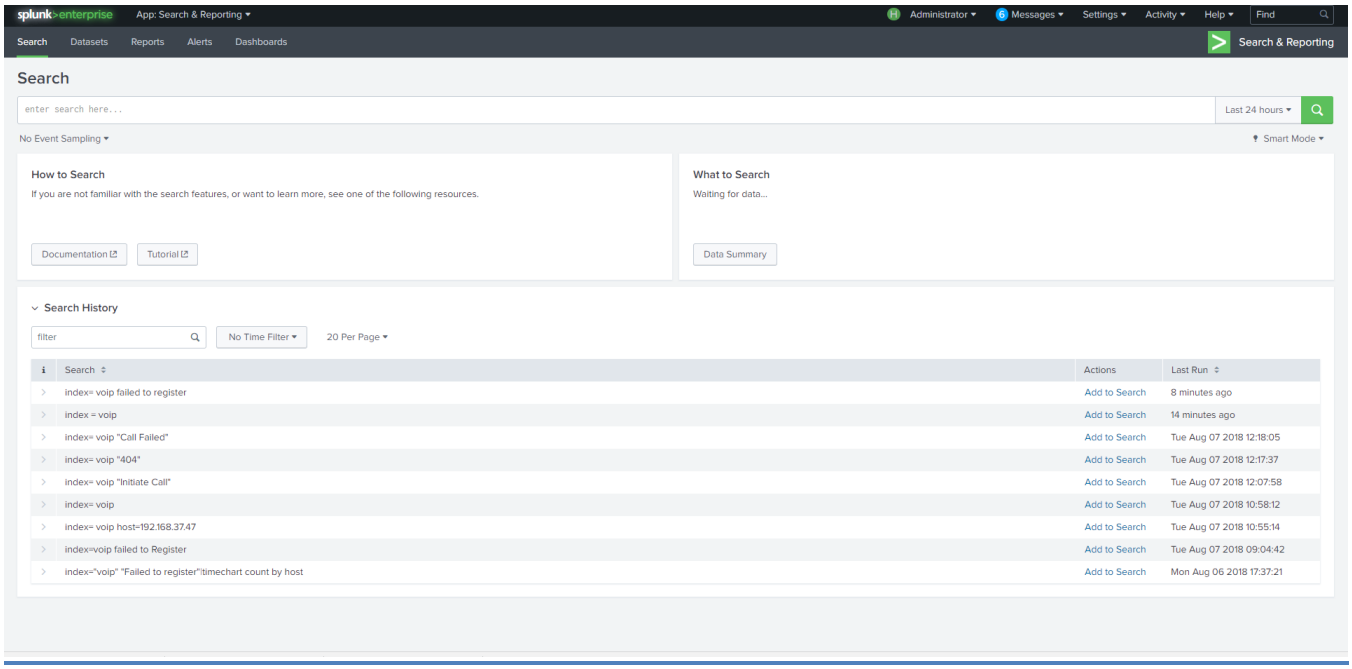


**Figure 13. Example searches -- Splunk Enterprise.**

## 4. Creating Alerts from Search Results.

### a) Configuring SMTP email settings to receive email messages when an alert is activated.

1. Go to **Settings > Server Settings > Email Settings**.

2. Configure the SMTP settings.

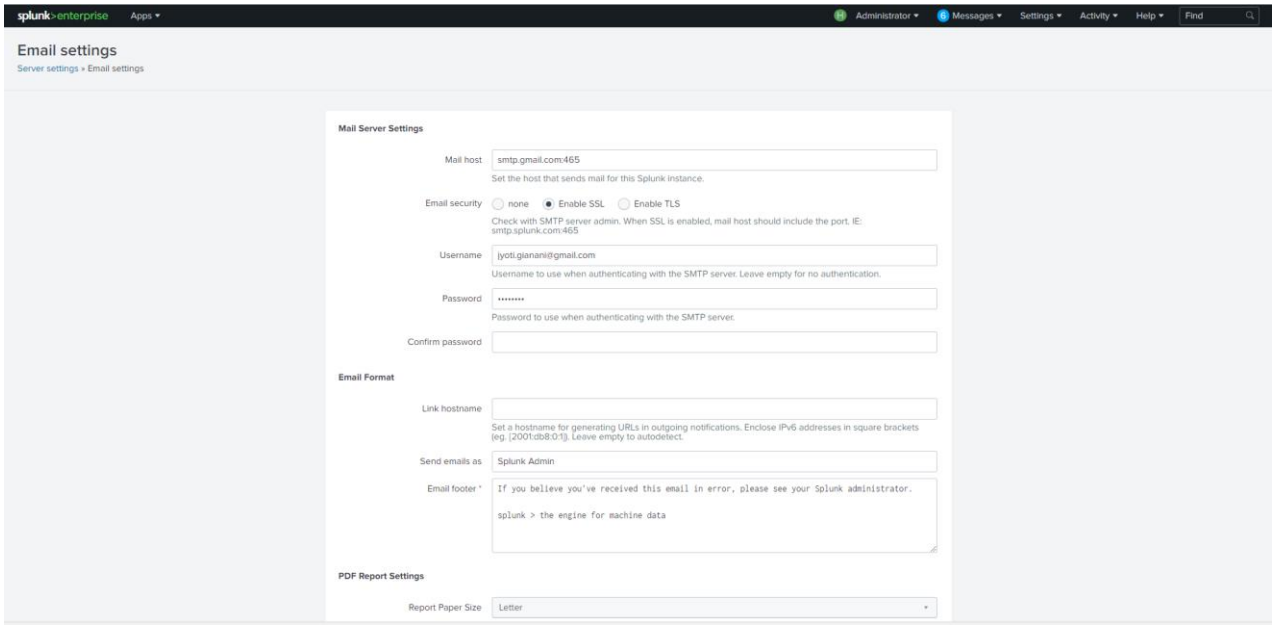


**Figure 14. SMTP settings -- Splunk Enterprise.**

### b) Adding an Alert.

1. Go to **Settings > Searches, Reports, and Alerts**.
2. Click **New Alert** as shown in the highlight below.

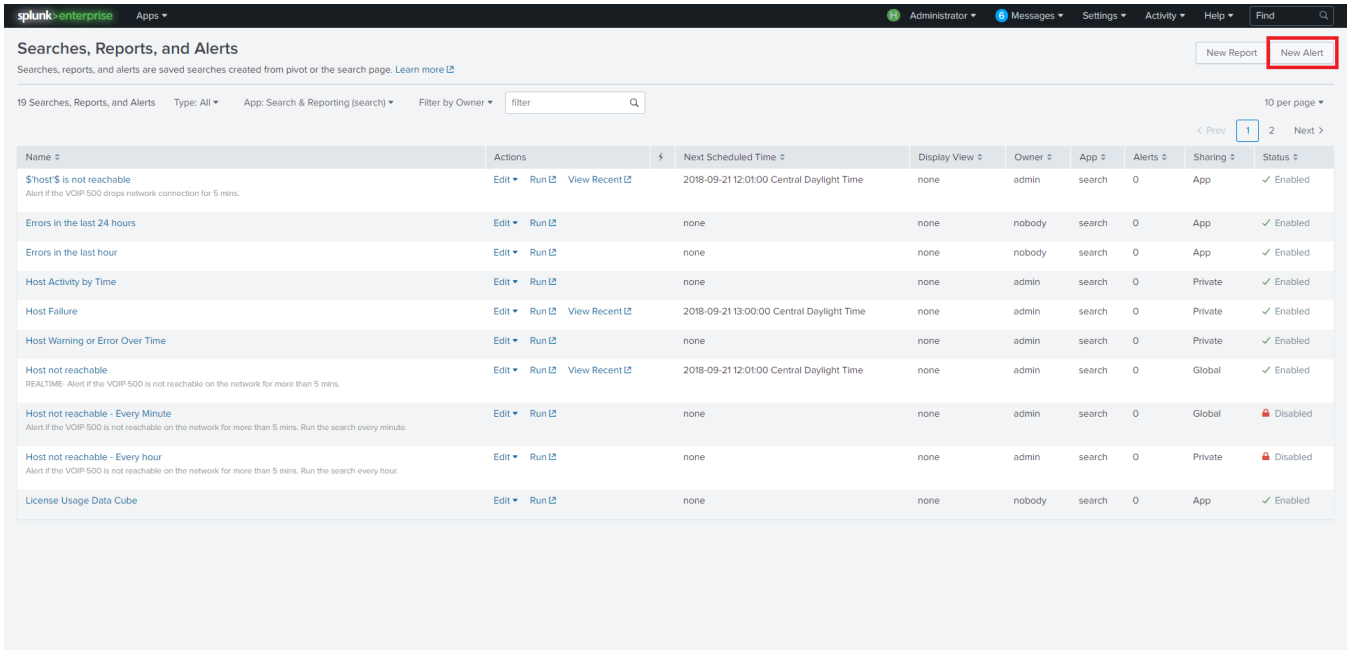


**Figure 15. Creating an alert -- Splunk Enterprise.**

### c) Adding an alert for SIP registration failure.

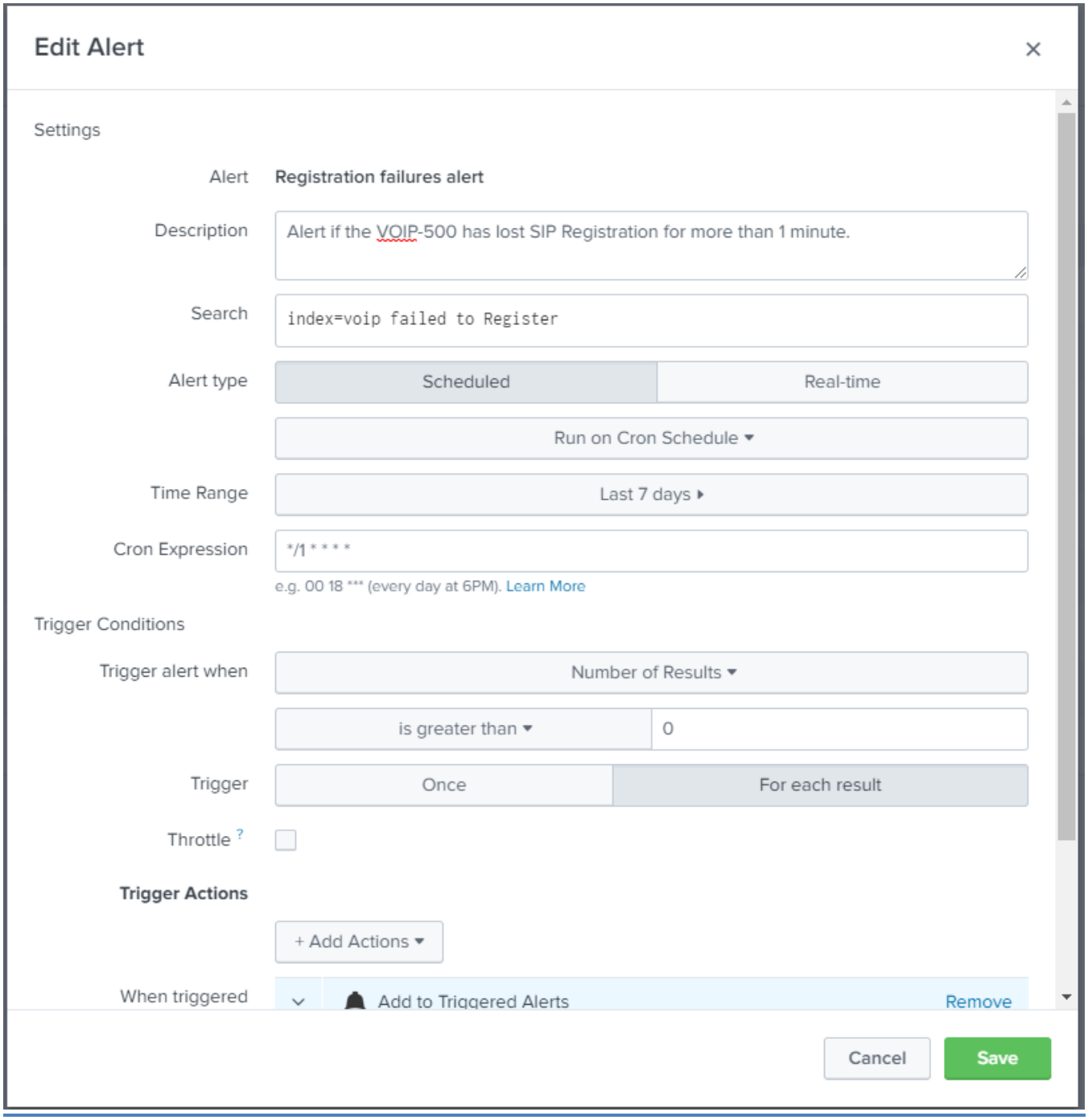


**Figure 16. Example of an alert for SIP registration failure -- Splunk Enterprise.**

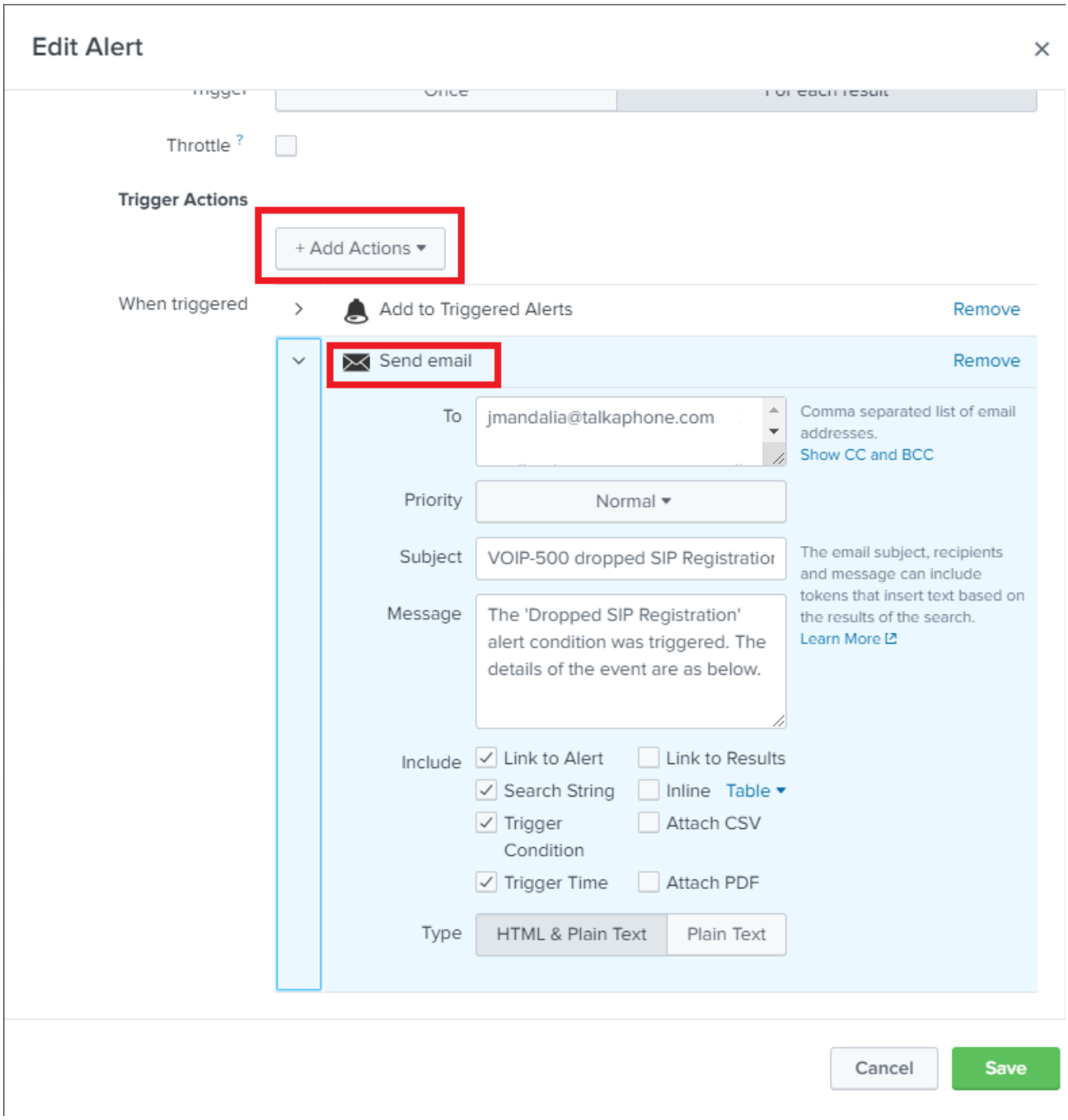


**Figure 17. Adding a trigger action for SIP registration failure -- Splunk Enterprise.**

### d) Adding an alert for "Host Unreachable on the Network".

1. The following string expression should be entered in to the **Search** field:

   | metadata index=voip type=hosts | eval age = now()-lastTime | where age > (2*150) | sort age d | convert time(lastTime) | fields age,host,lastTime

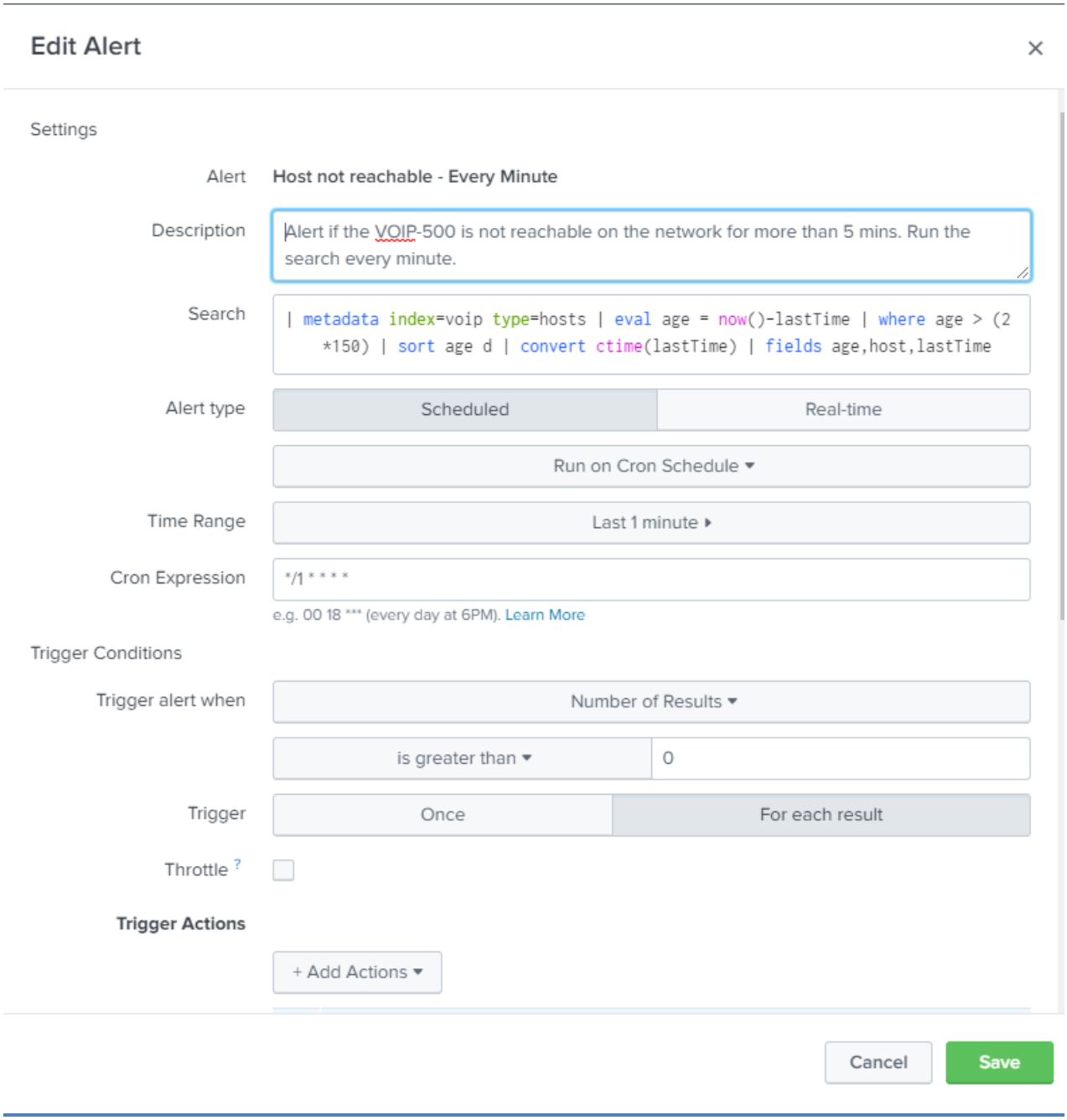


**Figure 18. Adding an alert for "Host Unreachable on the Network" -- Splunk Enterprise.**