

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:

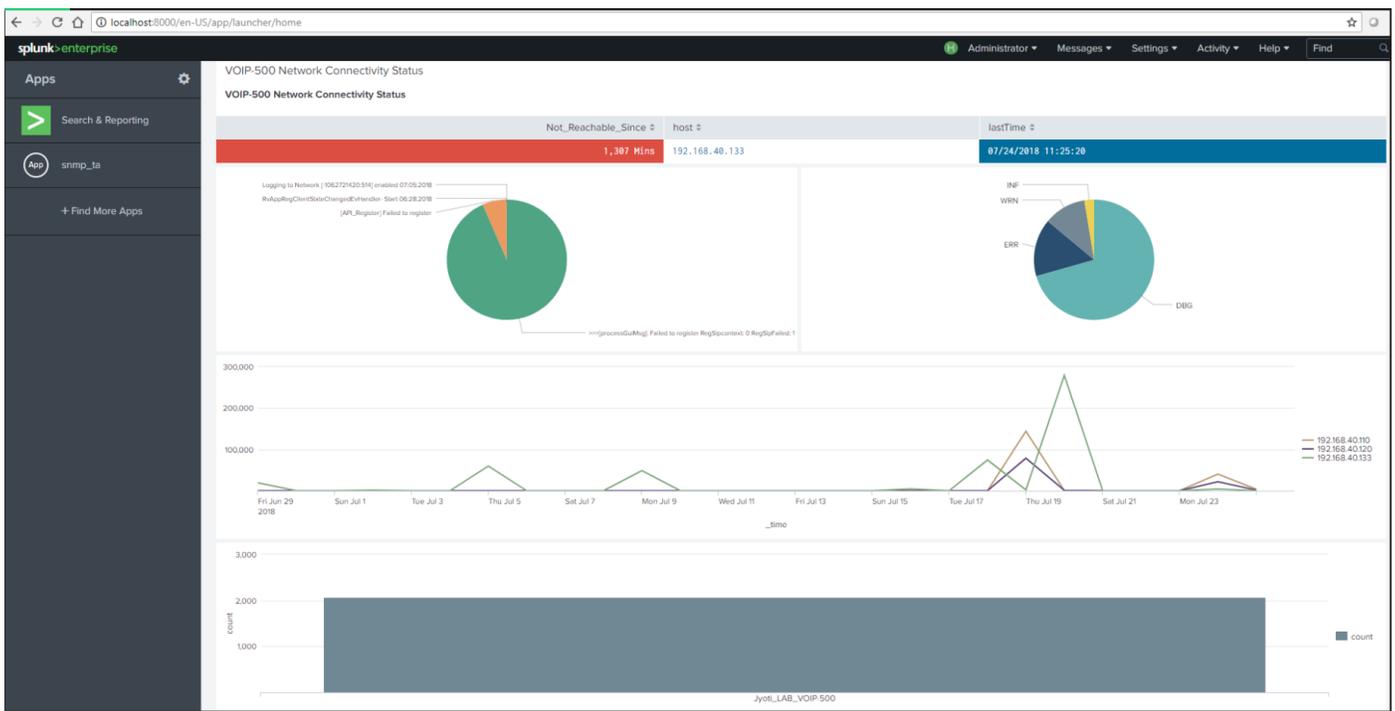


Figure 1. Example of a Splunk Enterprise dashboard.

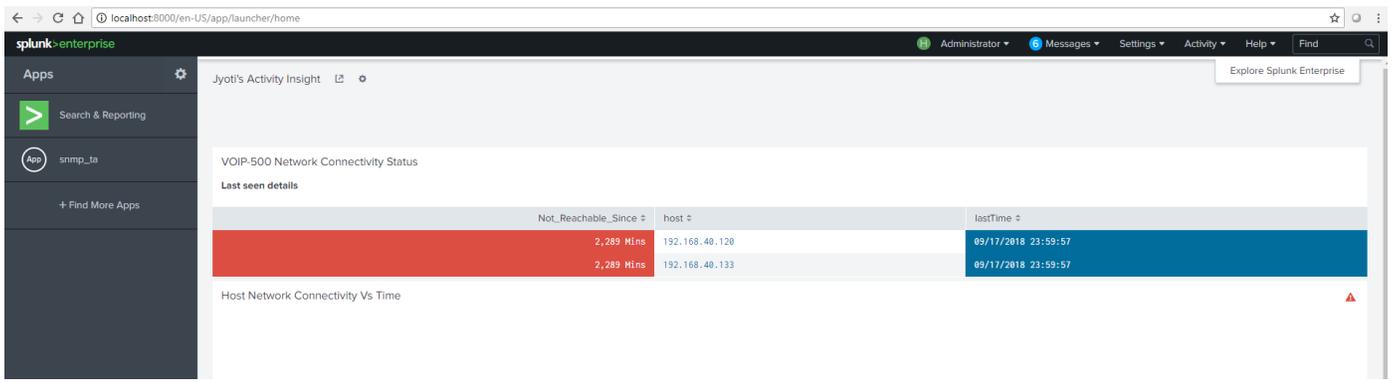


Figure 2. Example of a Splunk Enterprise dashboard.

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.

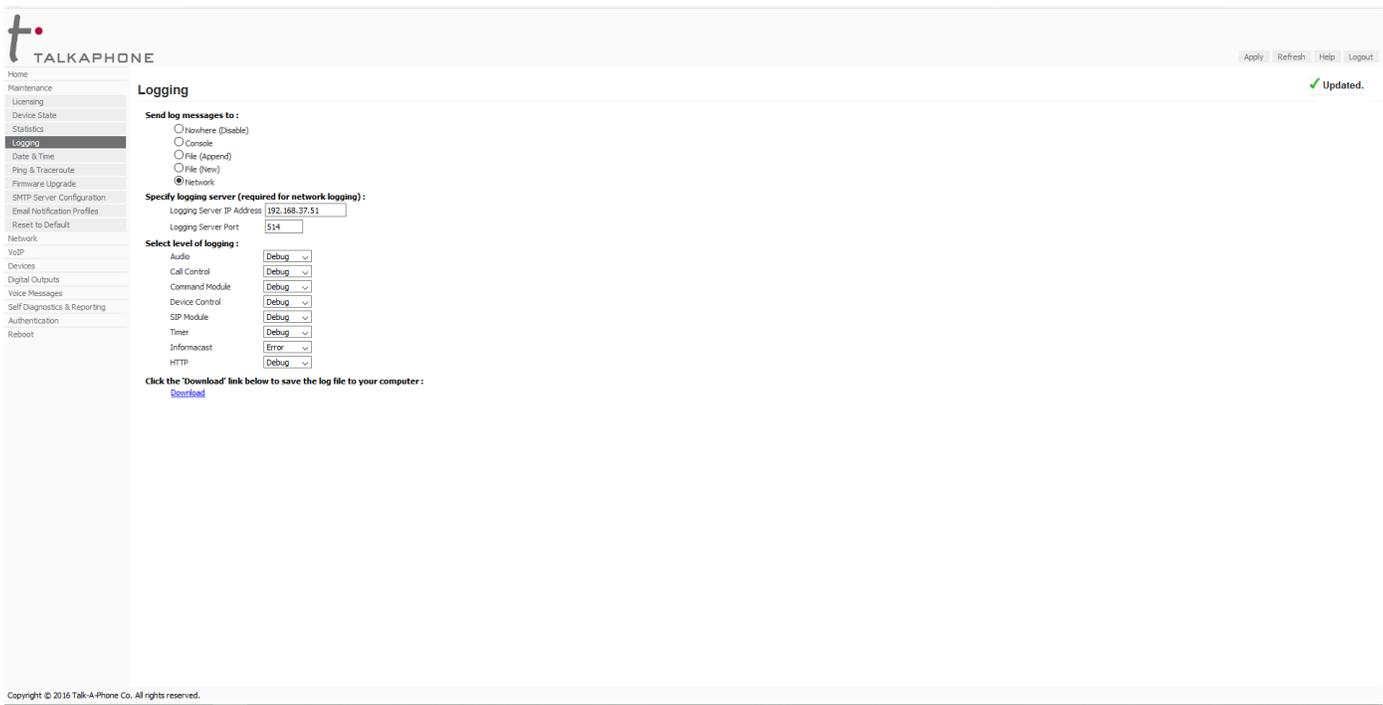


Figure 3. Configuration of VOIP-500/VOIP-600 for Syslog.

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.

New Index X

General Settings

Index Name
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type Events Metrics
The type of data to store (event-based or metrics).

Home Path
Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).

Cold Path
Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path
Thawed/resurrected db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check Enable Disable
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index GB ▾
Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket GB ▾
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path
Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App

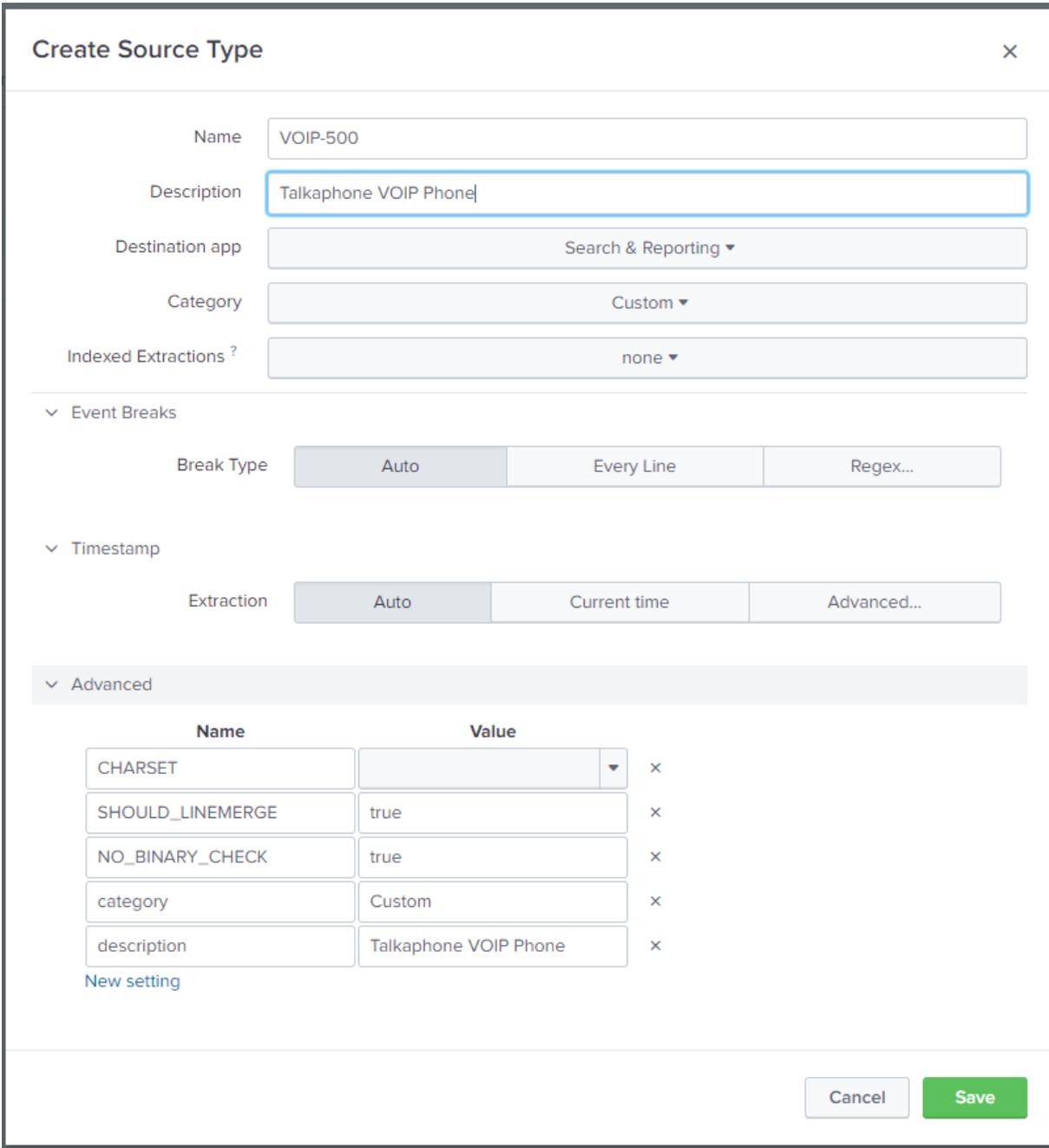
Storage Optimization

Tsidx Retention Policy Enable Reduction Disable Reduction
Warning: Do not enable reduction without understanding the full implications. It is extremely difficult to rebuild reduced buckets. [Learn More](#)

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.



Create Source Type [Close]

Name:

Description:

Destination app:

Category:

Indexed Extractions?:

Event Breaks

Break Type:

Timestamp

Extraction:

Advanced

Name	Value	
CHARSET	<input type="text"/>	×
SHOULD_LINEMERGE	true	×
NO_BINARY_CHECK	true	×
category	Custom	×
description	Talkaphone VOIP Phone	×

[New setting](#)

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**.

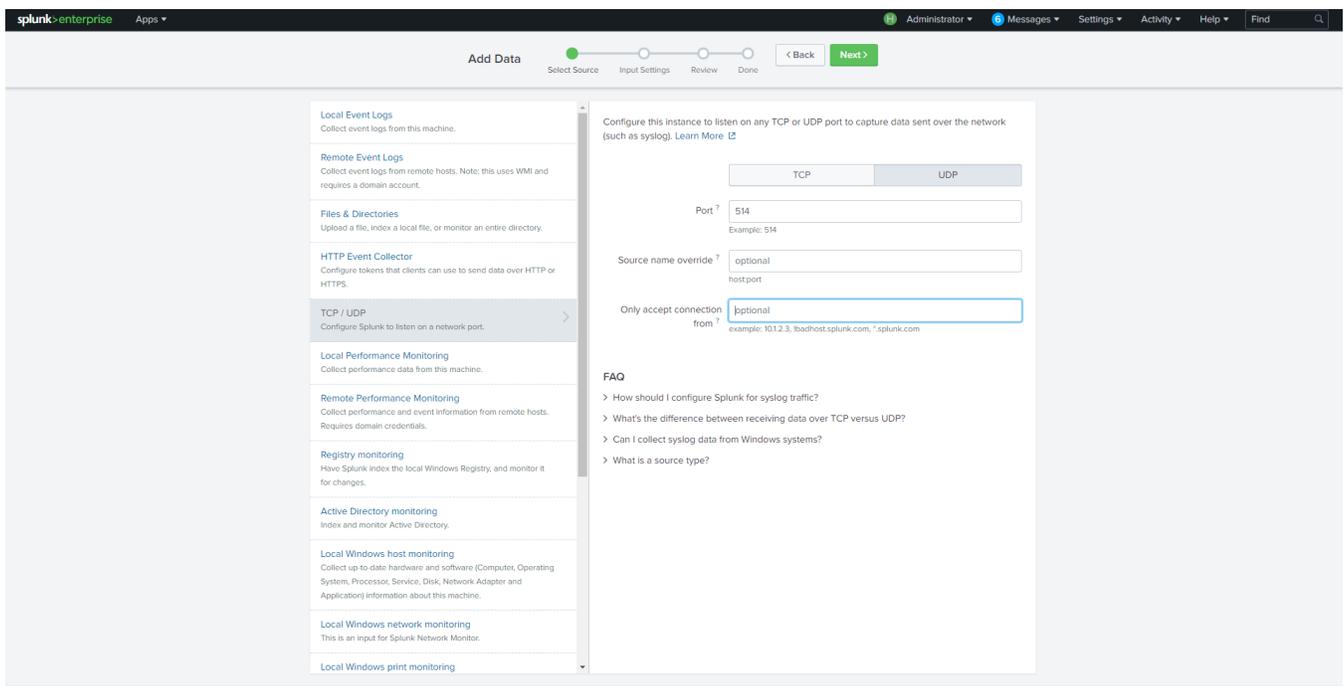


Figure 6. Configuring a data input -- Splunk Enterprise.

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

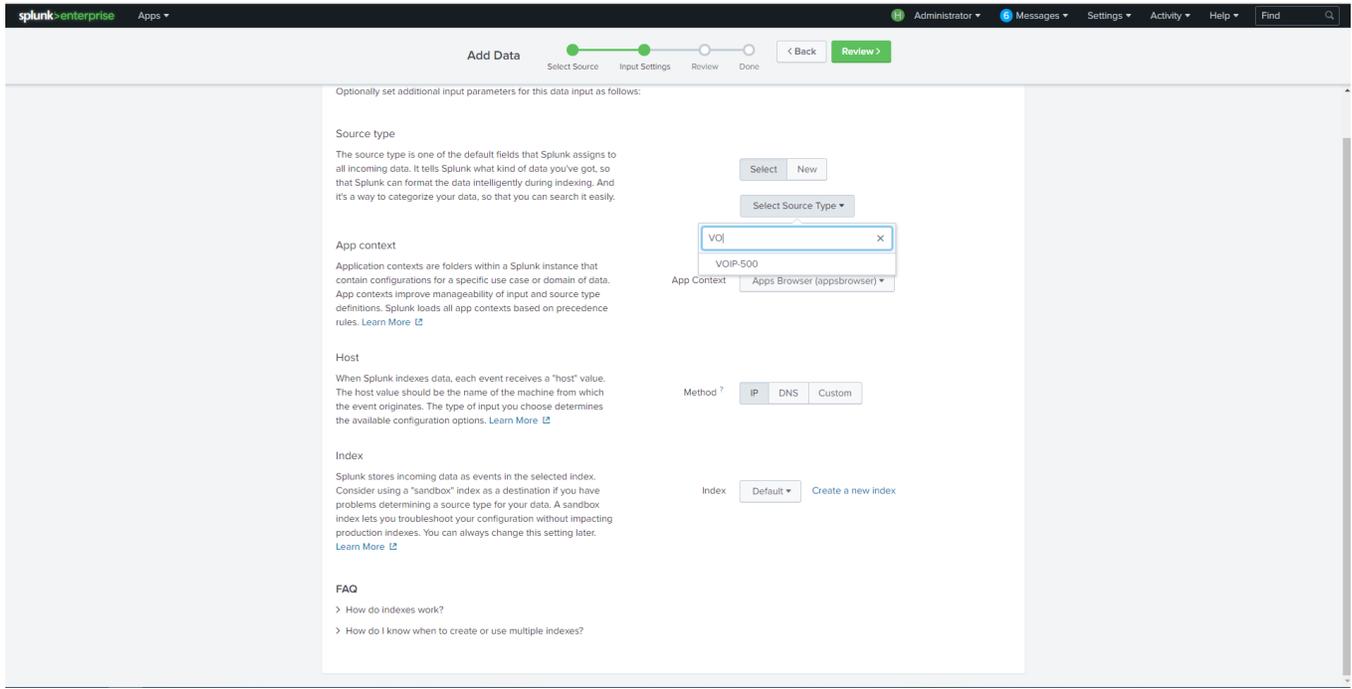


Figure 7. Specifying source type -- Splunk Enterprise.

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.

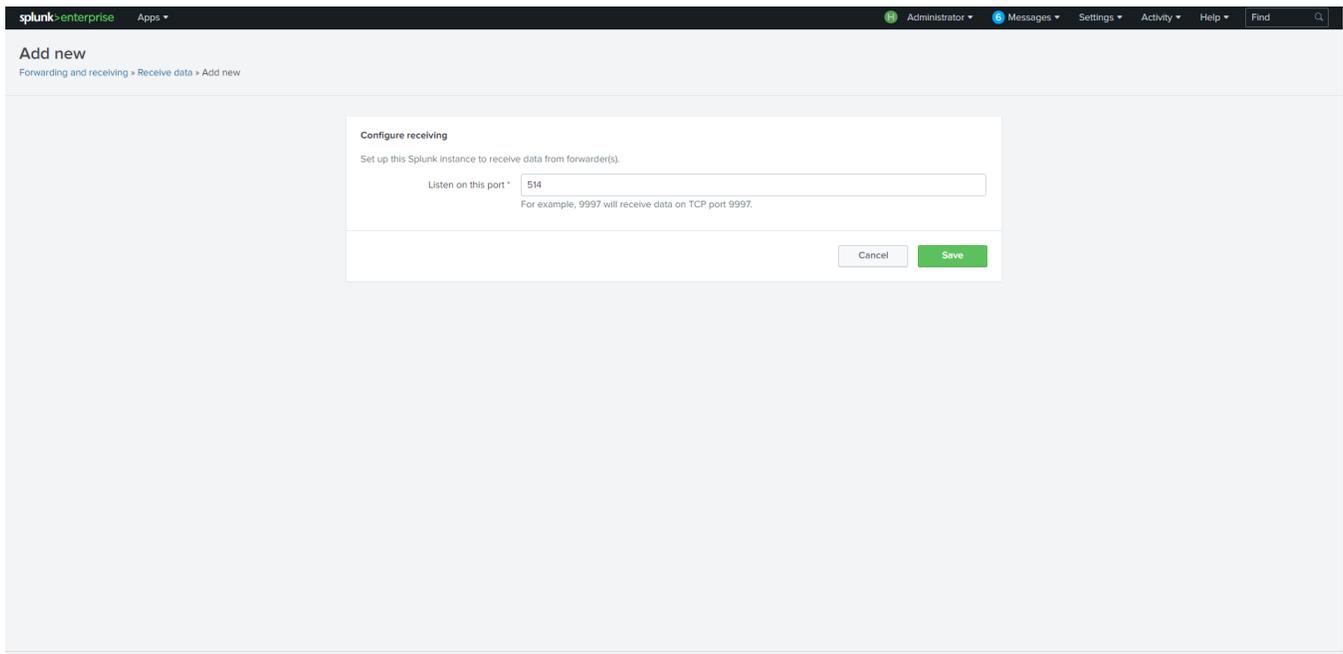


Figure 8. Adding a new receiving port -- Splunk Enterprise.

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

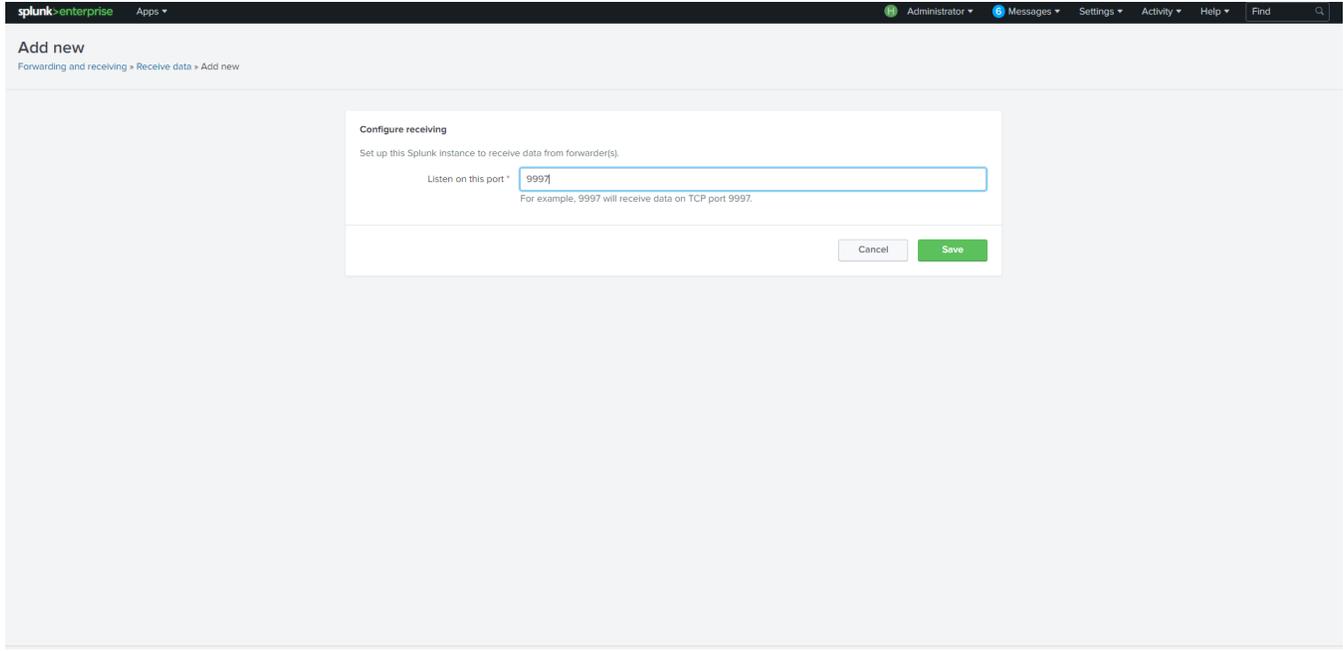


Figure 9. Adding a universal forwarder port -- Splunk Enterprise.

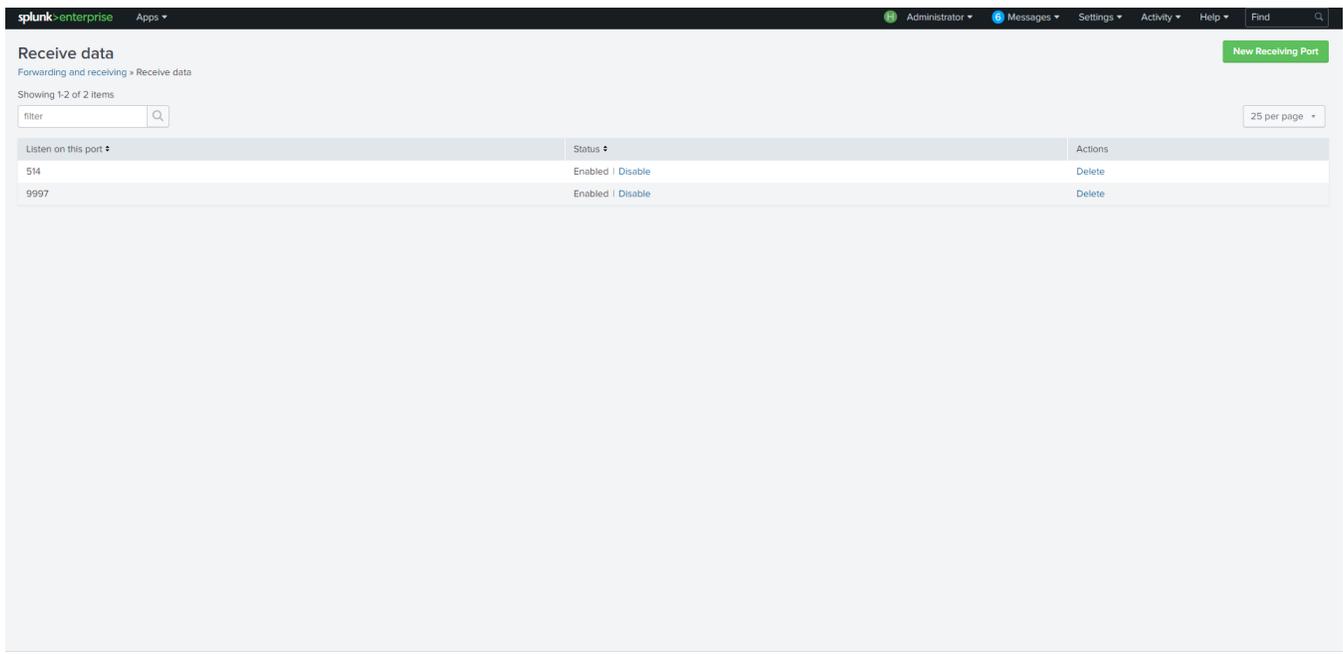


Figure 10. Receive data page showing configured ports -- Splunk Enterprise.

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>

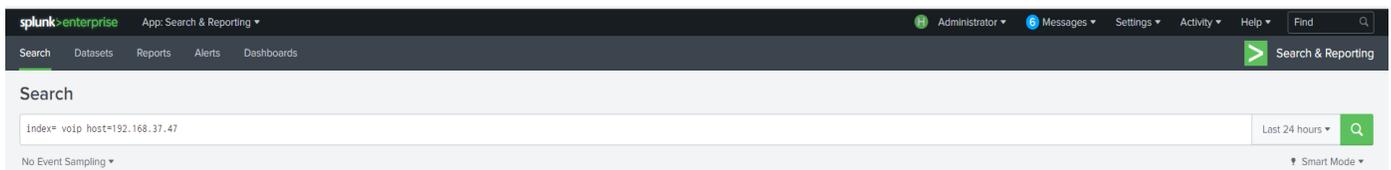
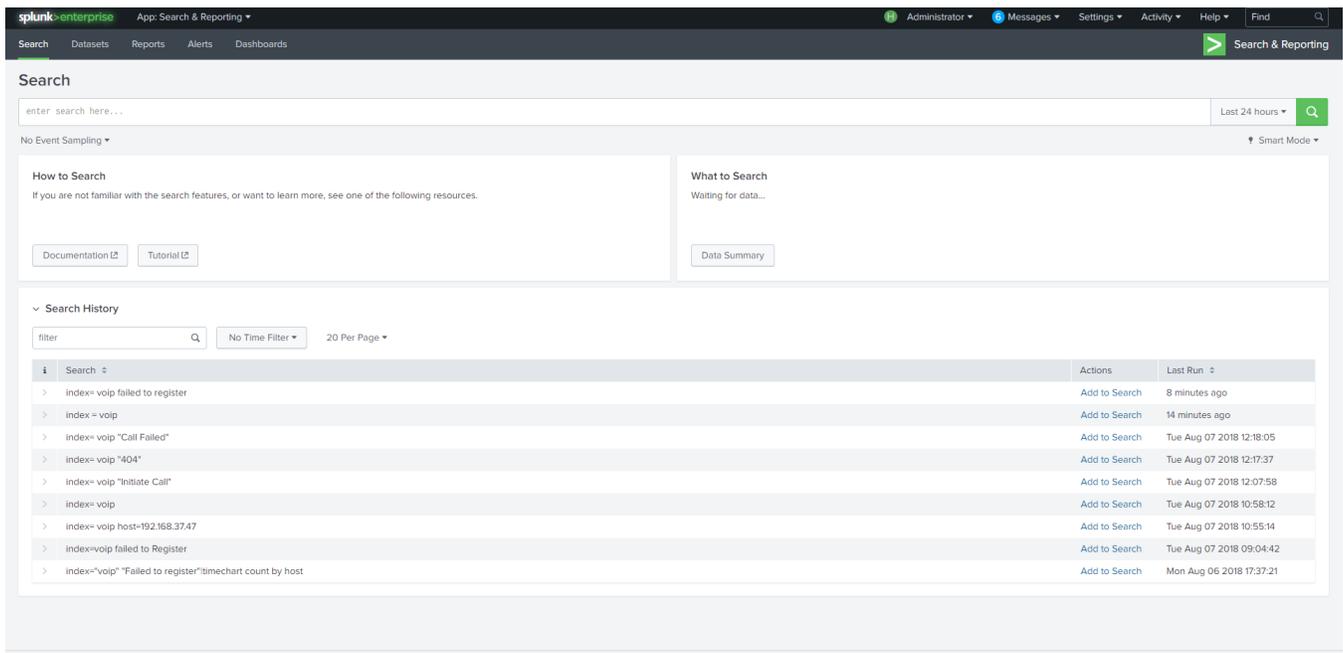


Figure 12. Searching by IP address of specific host -- Splunk Enterprise.

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.



The screenshot shows the Splunk Enterprise Search interface. At the top, there is a navigation bar with 'splunk enterprise' and 'App: Search & Reporting'. Below this, there are tabs for 'Search', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The main search area has a search bar with the placeholder 'enter search here...' and a 'Last 24 hours' filter. Below the search bar, there are sections for 'How to Search' and 'What to Search'. The 'Search History' section is expanded, showing a list of search queries and their results. The search history table has columns for 'Search', 'Actions', and 'Last Run'.

Search	Actions	Last Run
> index=voip failed to register	Add to Search	8 minutes ago
> index=voip	Add to Search	14 minutes ago
> index=voip "Call Failed"	Add to Search	Tue Aug 07 2018 12:18:05
> index=voip "404"	Add to Search	Tue Aug 07 2018 12:17:37
> index=voip "Initiate Call"	Add to Search	Tue Aug 07 2018 12:07:58
> index=voip	Add to Search	Tue Aug 07 2018 10:58:12
> index=voip host=192.168.37.47	Add to Search	Tue Aug 07 2018 10:55:14
> index=voip failed to Register	Add to Search	Tue Aug 07 2018 09:04:42
> index=voip "Failed to register" timechart count by host	Add to Search	Mon Aug 06 2018 17:37:21

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.

The screenshot shows the 'Email settings' page in Splunk Enterprise. The page is titled 'Email settings' and has a breadcrumb trail 'Server settings > Email settings'. The main content area is divided into three sections: 'Mail Server Settings', 'Email Format', and 'PDF Report Settings'.
Mail Server Settings:
- Mail host: smtp.gmail.com:465 (with a note: 'Set the host that sends mail for this Splunk instance.')
- Email security: Radio buttons for 'none', 'Enable SSL' (selected), and 'Enable TLS'. A note says: 'Check with SMTP server admin. When SSL is enabled, mail host should include the port, i.e. smtp.splunk.com:465'.
- Username: lyoti.ganani@gmail.com (with a note: 'Username to use when authenticating with the SMTP server. Leave empty for no authentication.')
- Password: masked with asterisks (with a note: 'Password to use when authenticating with the SMTP server.')
- Confirm password: empty field.
Email Format:
- Link hostname: empty field (with a note: 'Set a hostname for generating URLs in outgoing notifications. Enclose IPv6 addresses in square brackets (eg. [2001:db8:0]). Leave empty to autodetect.')
- Send emails as: Splunk Admin
- Email footer: A text area containing 'If you believe you've received this email in error, please see your Splunk administrator.' and 'splunk > the engine for machine data'.
PDF Report Settings:
- Report Paper Size: Letter (dropdown menu).

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.

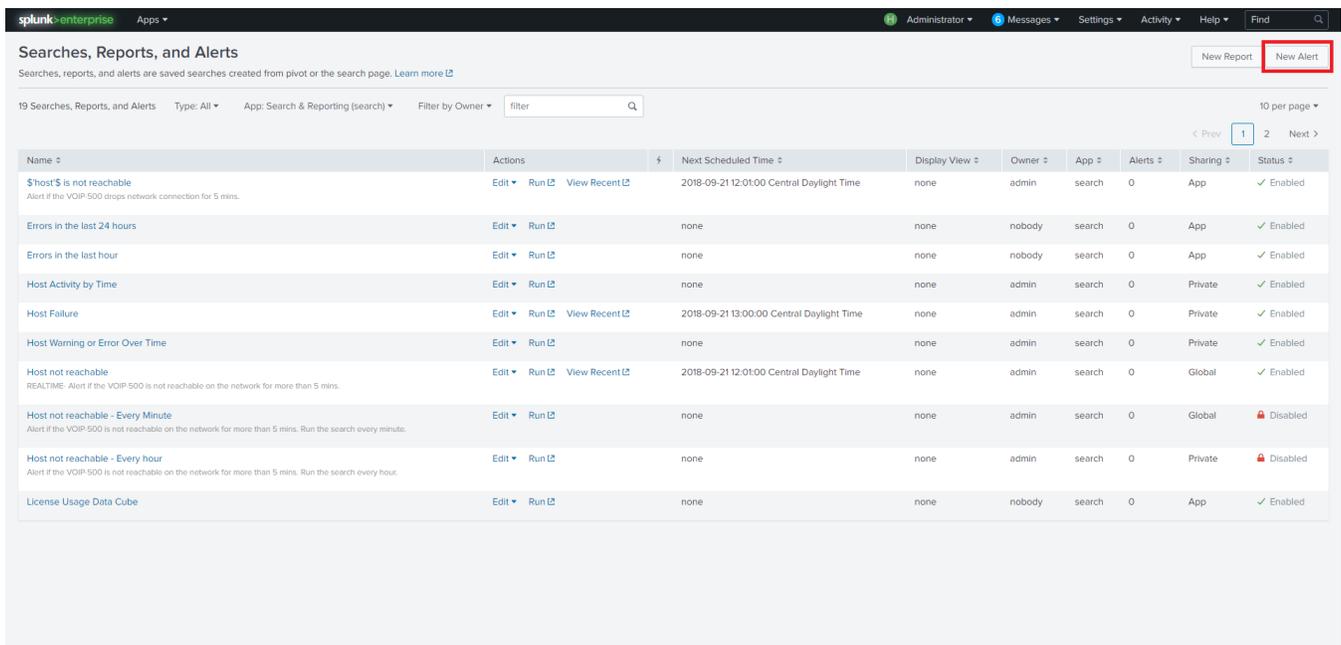


Figure 15. Creating an alert -- Splunk Enterprise.

c) Adding an alert for SIP registration failure.

Edit Alert
✕

Settings

Alert **Registration failures alert**

Description

Search

Alert type Scheduled Real-time

Run on Cron Schedule ▾

Time Range Last 7 days ▶

Cron Expression
e.g. 00 18 *** (every day at 6PM). [Learn More](#)

Trigger Conditions

Trigger alert when Number of Results ▾

is greater than ▾

Trigger Once For each result

Throttle ?

Trigger Actions

+ Add Actions ▾

When triggered ▼ 🔔 Add to Triqgered Alerts [Remove](#)

Cancel Save

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

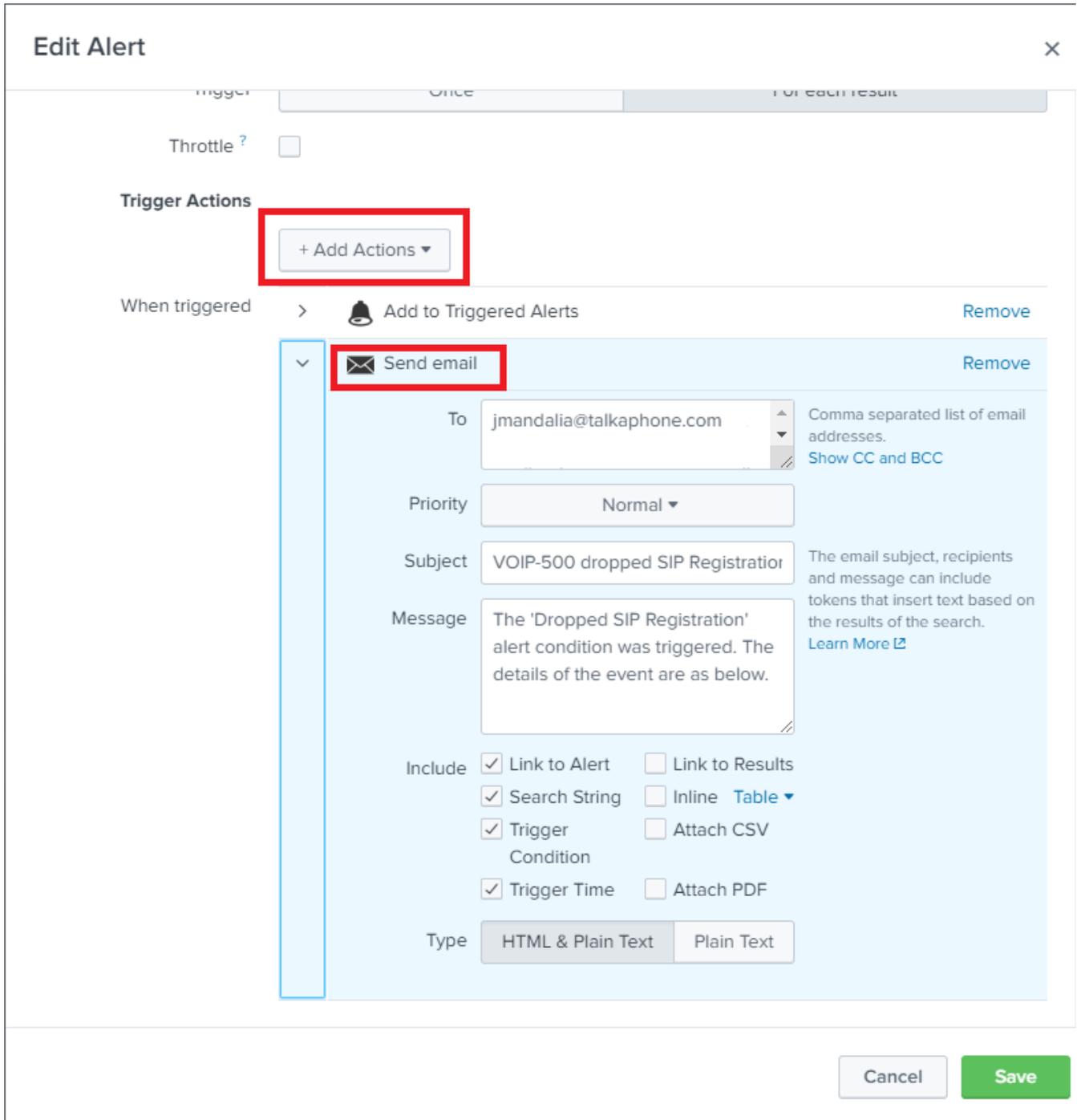
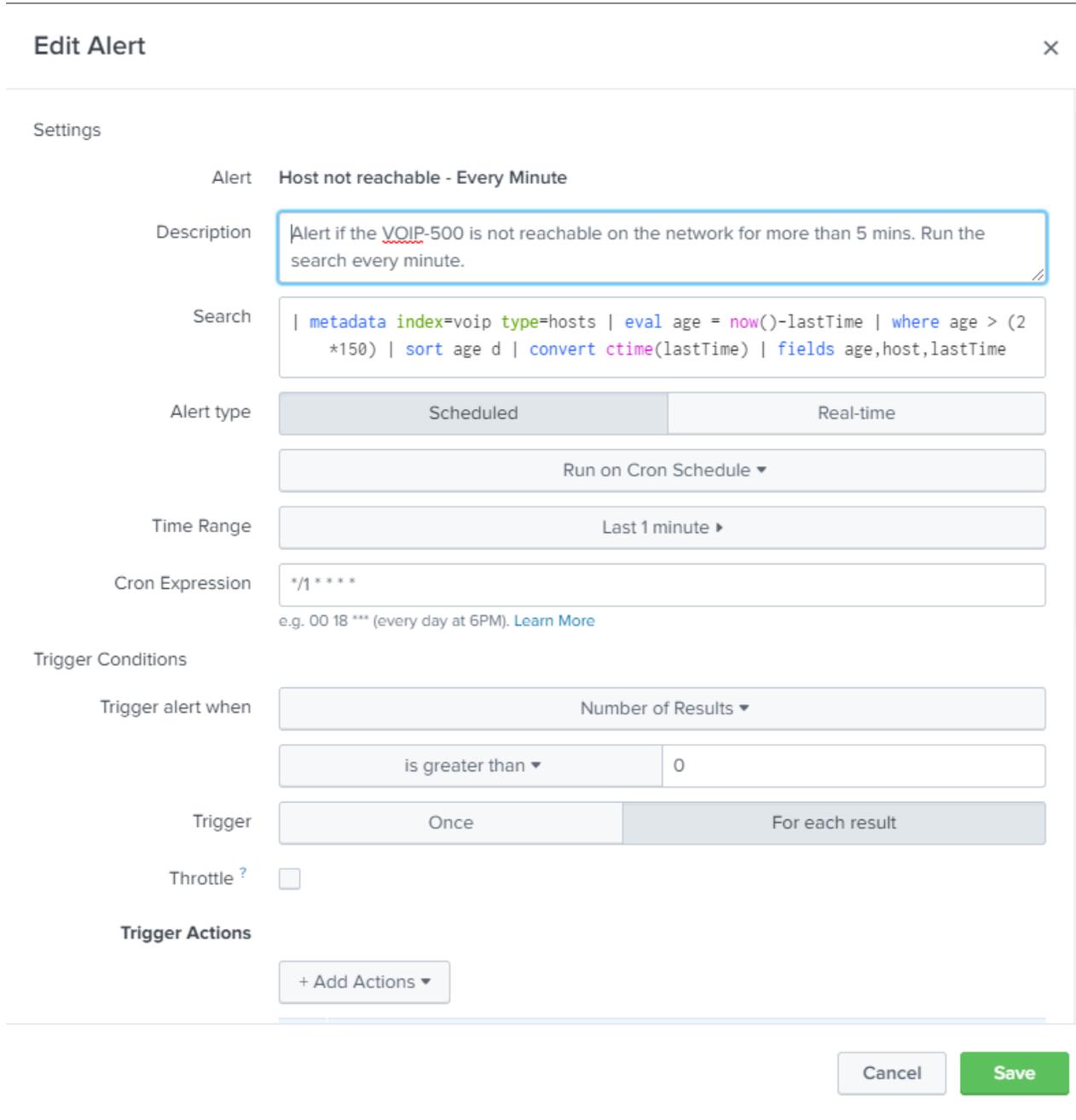


Figure 17. Adding a trigger action for SIP registration failure -- Splunk Enterprise.

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
```



The screenshot shows the 'Edit Alert' interface in Splunk Enterprise. The alert is named 'Host not reachable - Every Minute'. The description is 'Alert if the VOIP-500 is not reachable on the network for more than 5 mins. Run the search every minute.' The search query is: `| metadata index=voip type=hosts | eval age = now()-lastTime | where age > (2*150) | sort age d | convert ctime(lastTime) | fields age,host,lastTime`. The alert type is 'Scheduled' with a cron expression of `*/1****`. The trigger conditions are set to 'Number of Results' is greater than 0, triggered 'For each result'. There are 'Cancel' and 'Save' buttons at the bottom right.

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