Splunk – sendQuick Integration Guide

Version 1.1

TalariaX Pte Ltd

76 Playfair Road

#08-01 LHK2 Building

Singapore 367996

Tel : +65 6280 2881 Fax : +65 6280 6882

Email : info@talariax.com

www.TalariaX.com

REVISION SHEET

Release No.	Date	Description
1.0	22/11/2019	First published version
1.1	27/01/2021	Revised with new format

Table of Contents

Splunk - sendQuick Integration Guide

1.0 Introduction

1.1 About TalariaX Pte Ltd

TalariaX™ develops and offers **enterprise mobile messaging solutions** to facilitate and improve business workflow and communication, and is widely used in areas such as IT alerts & notifications, secure remote access via 2-Factor Authentication, emergency & broadcast messaging, business process automation and system availability monitoring.

In addition to functionality, TalariaX's messaging solutions have also been developed with other key features in mind. These include **security** and **confidentiality** of company information, and **ease in mitigating disruption** during unplanned system downtime such as that arising from cyberattacks.

1.2 About sendQuick

sendQuick is a comprehensive Short Messaging Service (SMS) and Mobile Instant Messaging (MIM) gateway that is available in the form of an **appliance** or as a **cloud-based** solution. ***sendQuick*** is used by more than 1,500 businesses, including many Fortune Global 500 companies, in 40 countries and across industries such as banking, finance, insurance, manufacturing, retail, government, education, and healthcare.

1.3 Purpose of Document

This document is a guide on how to integrate sendQuick with Spunk to send SMS alerts. In this guide, we will be using sendQuick Entera for the integration. We will illustrate two methods in this guide:

- Email method
- Webhook http method

The common method is the email method. This method allows users to make full use of sendQuick notification management features such as roster and escalation management. Besides SMS, sendQuick can also notify alerts through other communication channels such as social messenger applications, multiple emails and automated Voice calls.

2.0 Send Email to sendQuick

When any device is down or there is a need to send a notification alert, Splunk can trigger an email to sendQuick. sendQuick will then convert the email message to SMS.

2.1 Configure Email Filter in sendQuick

sendQuick allows you to configure alerts to be sent to multiple phone numbers, groups or even combination of emails and sms. To explore this feature, navigate on the sendQuick dashboard to :

Filter Rules > Email Filter

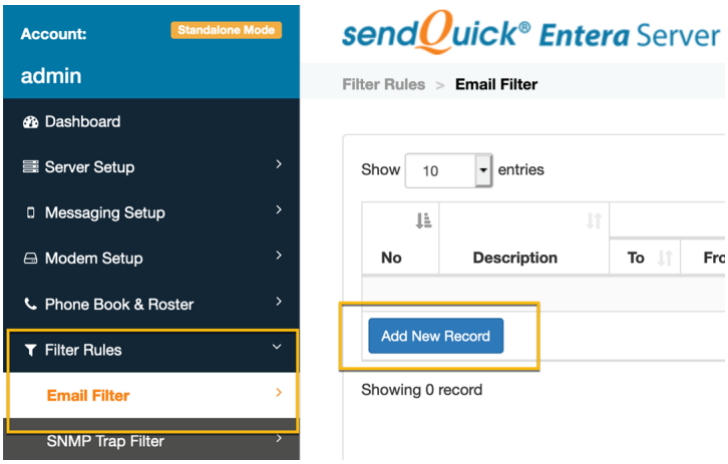

Figure 1: Select Email Filter

Click on **Add New Record.**

You can then create a new record to define the email address Splunk should send to. In our example, we will use ***splunk@entera64.sendquick.com***

The user email can be anything meaningful that you choose but the domain name of the email address must correspond to your domain name of your sendQuick system.

Fill in the **Description, Mail To** and for **Match Mode**, check on **ANY**. Once done, click **Save**.

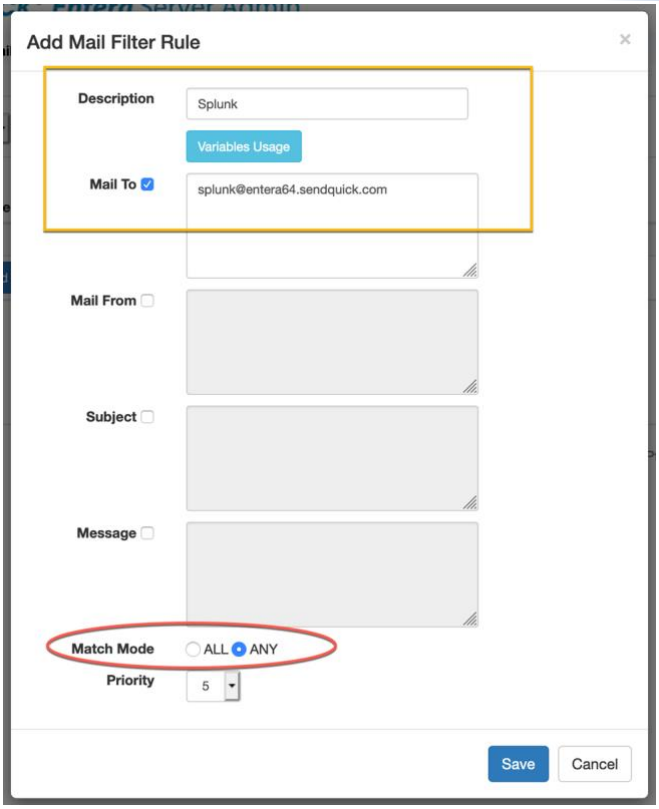

Figure 2: Configure email filter rule

Click on **View** for the record that you have created :

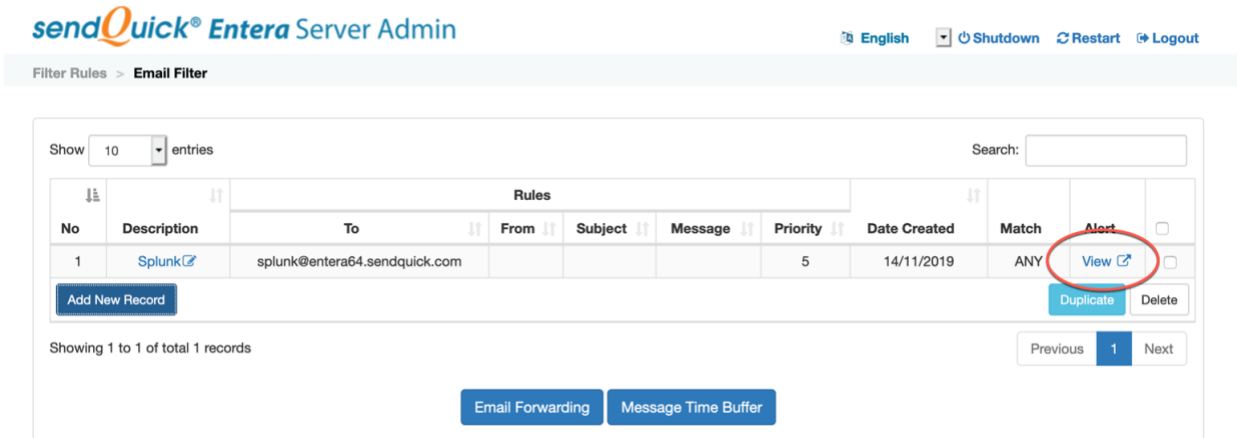

Figure 3: View more configuration of the filter rule

Then click on **Add New Record**

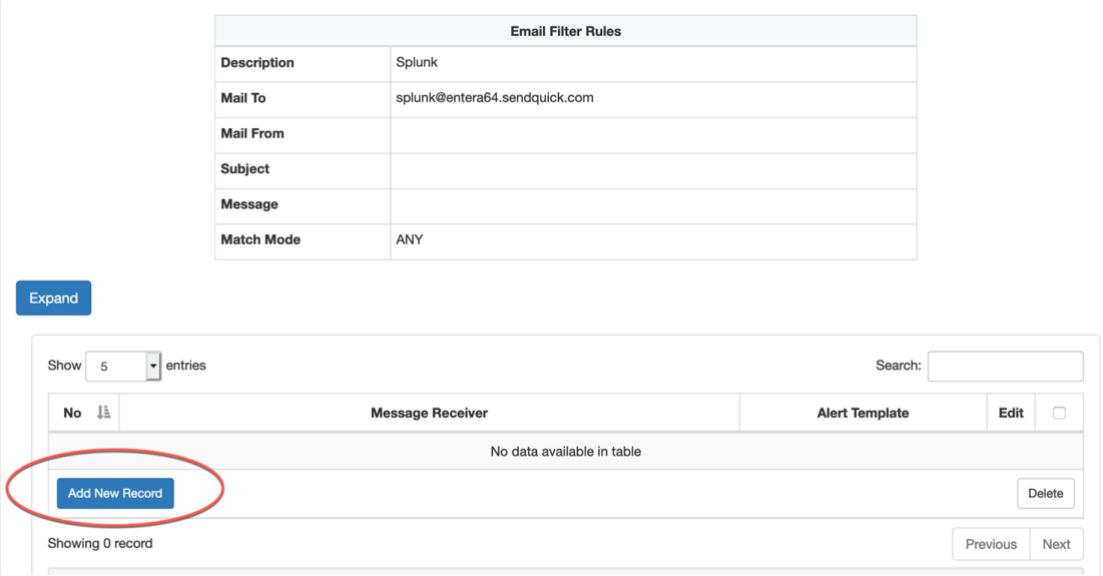

Figure 4: Add New Record to configure recipients of alert notifications

You can then add multiple numbers, emails, or even pre-defined groups to receive the notification alerts.

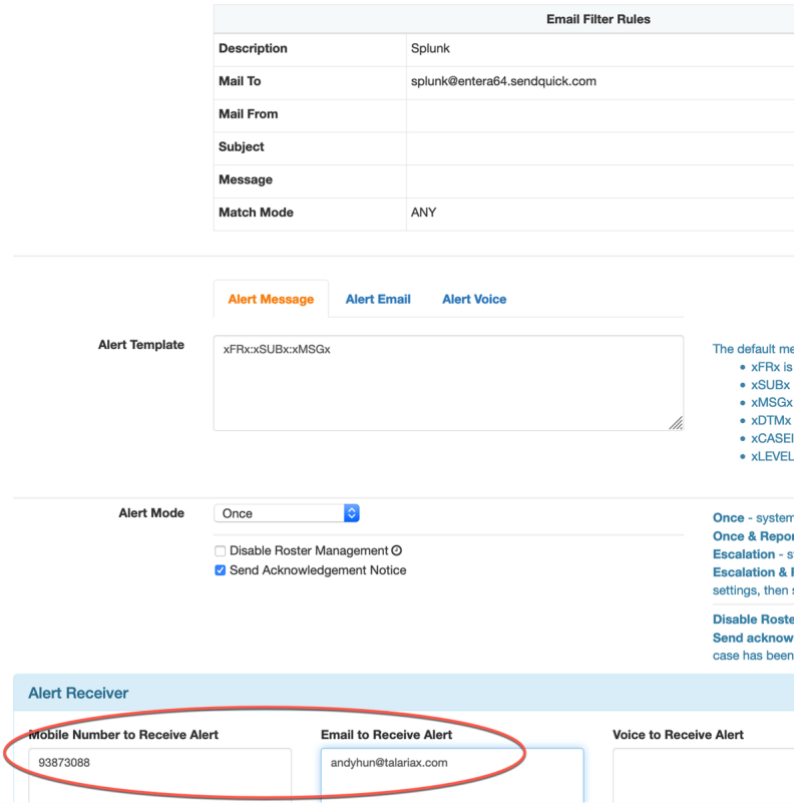

Figure 5: Configure receiver of alerts

After you have keyed in the information, click on **Save** to continue.

Quicktip - To check your host and domain name, you can find the value in the sendQuick dashboard under **System Overview** under **Host** and **Domain.**

For e.g. our domain name is ***entera64.sendquick.com***

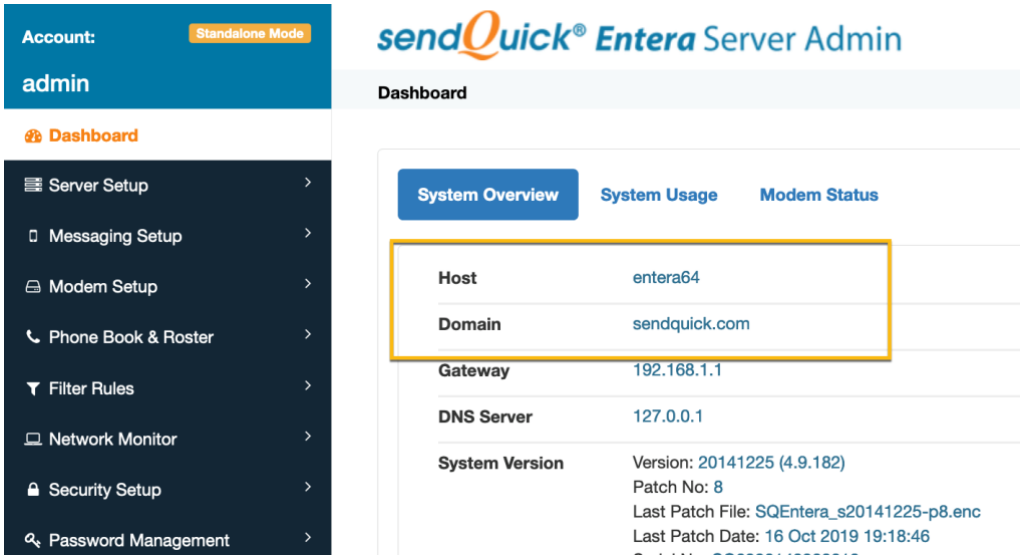

Figure 6: System Overview

2.2 Configure Email Settings on Splunk.

On the dashboard of Splunk, navigate to the following item :

Settings > Server Settings > Email settings

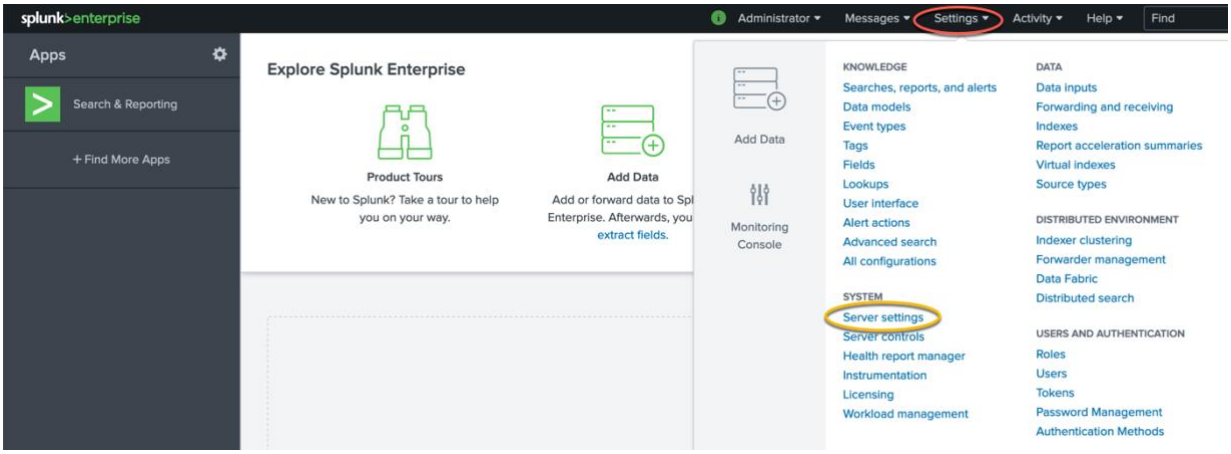

Figure 7: To configure email settings on Splunk

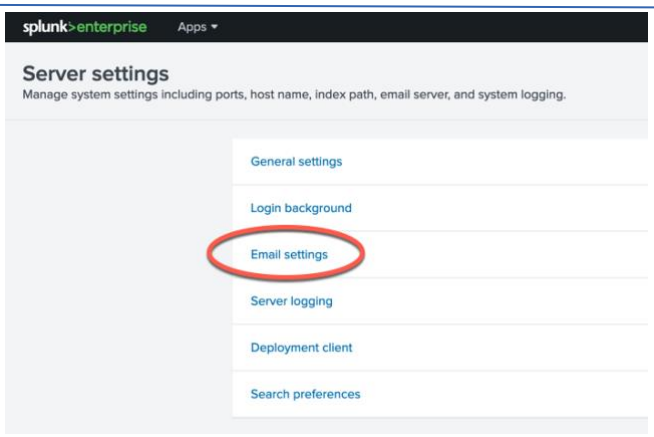

Figure 8: Select Email settings

In the **Mail Server Settings** section, key in your sendQuick IP address in the **Mail Host** field as shown in the screenshot below.

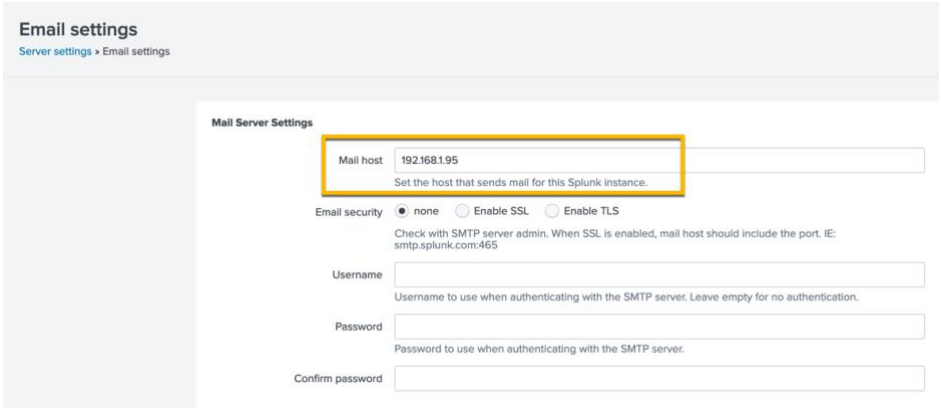

Figure 9: Configure Email server settings

For **Email Security**, leave it as “none” unless you have configured SSL or TLS in sendQuick.

Please note that you will also need to have the same security certificate on Splunk for this to work. Please refer to Splunk manuals on how to configure this. If no security has been configured, leave the **Username** and **Password** fields blank.

Quicktip - To check what security was installed on sendQuick, navigate to the following item on the sendQuick dashboard :

Security Setup > SSL Setup > SSL Protocol

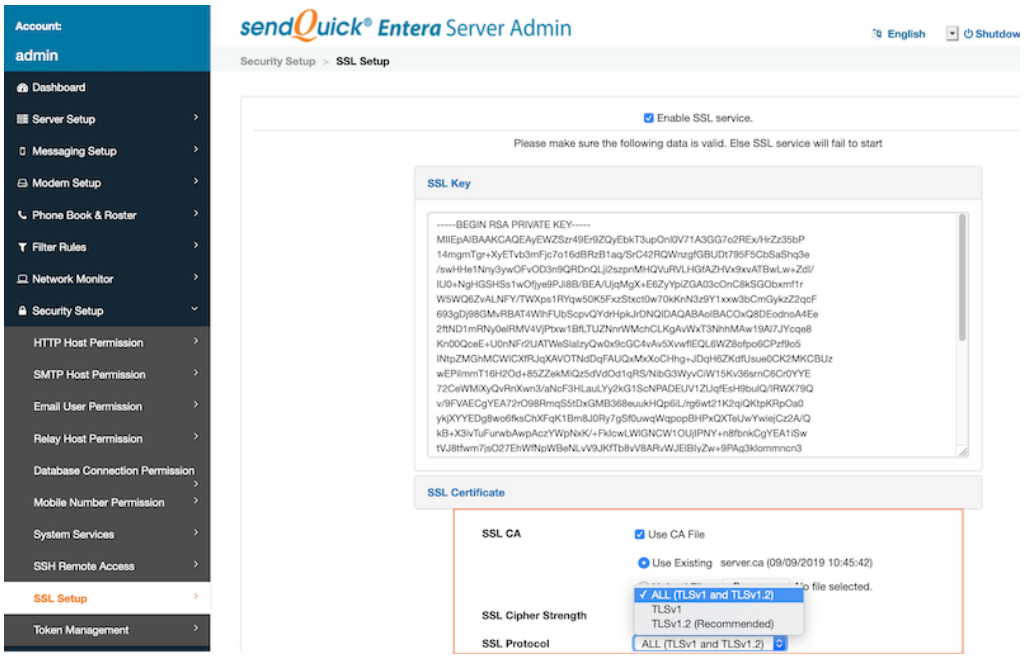

Figure 10: SSL Setup on sendQuick

You can key in the email address of your choice in the **Send emails as** field and **Email footer**. Click on **Save.**

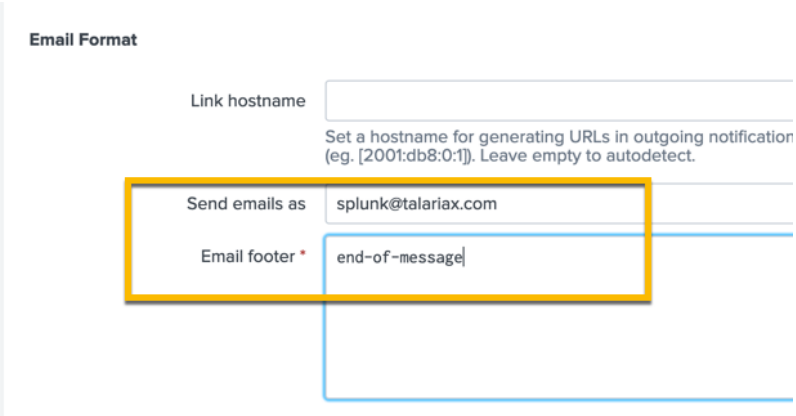

Figure 11: Configure sender email address on Splunk

2.3 Setting up An Alert

To create an alert in Splunk, you can save an alert from a search. In this example we will create a sample real-time alert. On the splunk>enterprise dashboard, click on the **Search & Reporting** app.

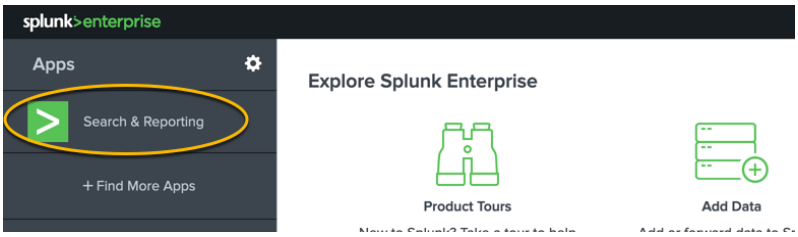

Figure 12: Search and reporting app

On the search bar, key in the following to create a new search to look for errors (*for more on splunk searches, please refer to documentation from Splunk*)

index=_internal " error " NOT debug source=*splunkd.log*

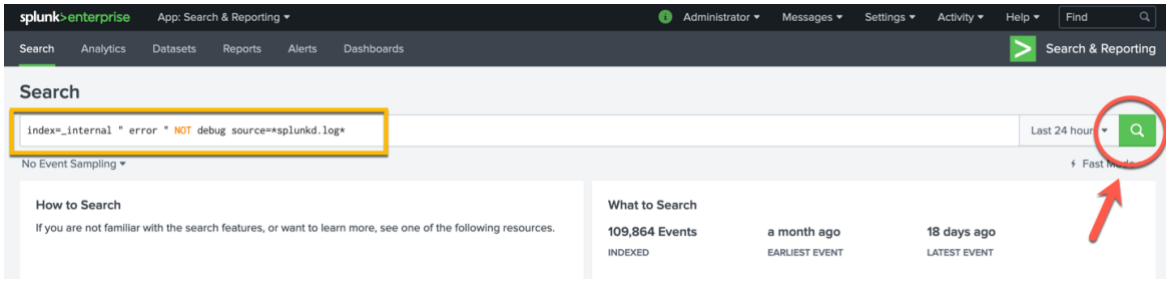

Figure 13: Search for error

Click on the magnifying glass icon.

After the search results has appeared, you can then save it as an alert by selecting **Save As > Alert**

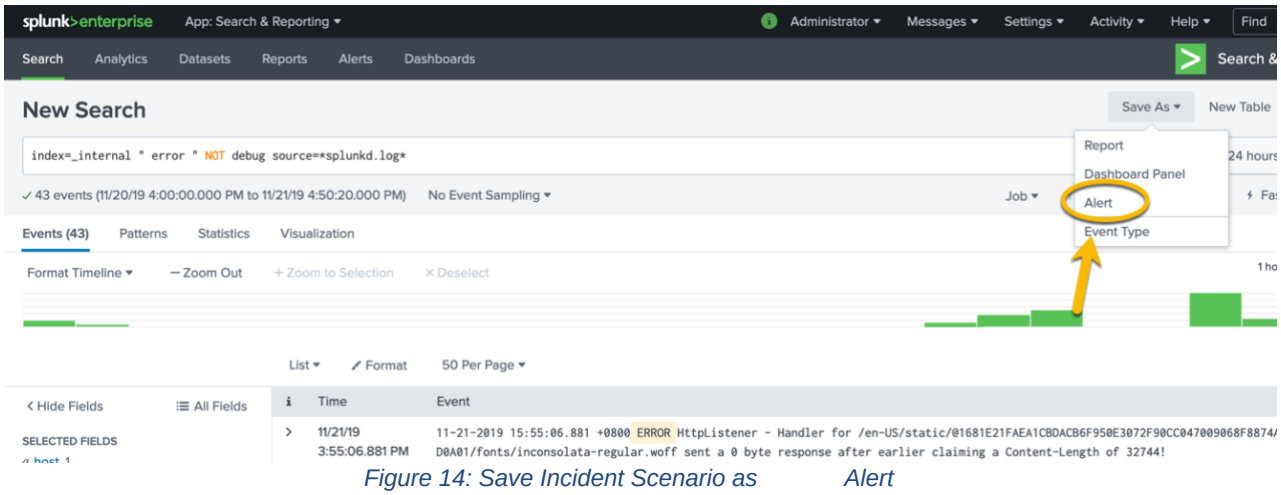

Figure 14: Save Incident Scenario as Alert

Configure the alert according to your needs. For this example, we will use the sample alert provided by [splunk tutorial on Alert Samples]

Fill in the following :

- **Title**: Errors reported (Real-time)
- **Alert type**: Real-time
- **Trigger condition**: Number of Results
- **Trigger if number of results**: is greater than 5 in 1 minute.

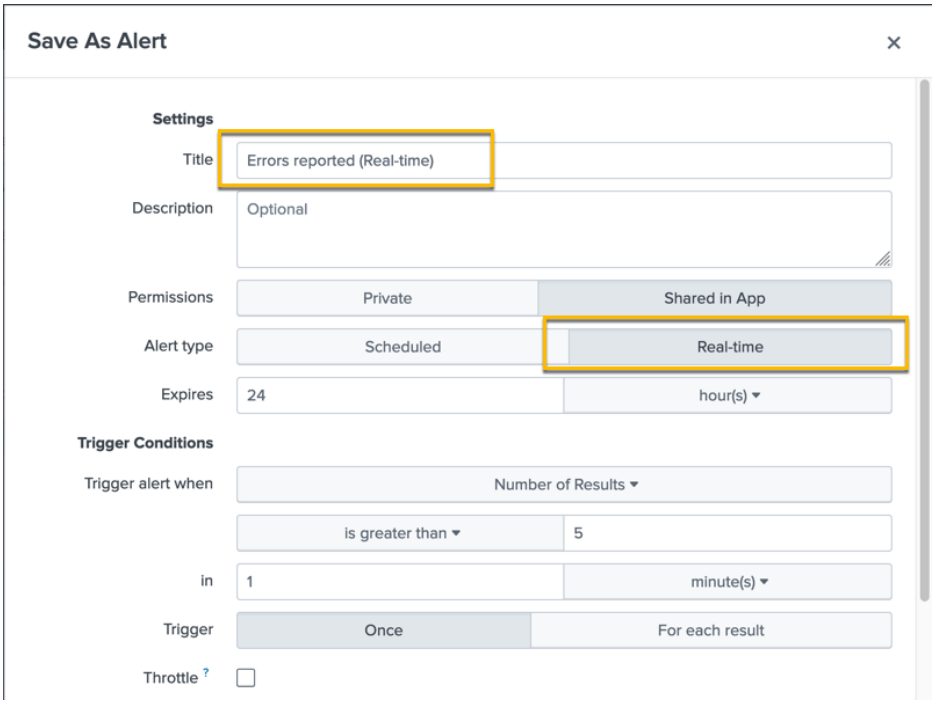

Figure 15: Configuring alert on Splunk

Before you click **Save,** scroll down until you see **Trigger Action**. Click on the **Add Actions** button.

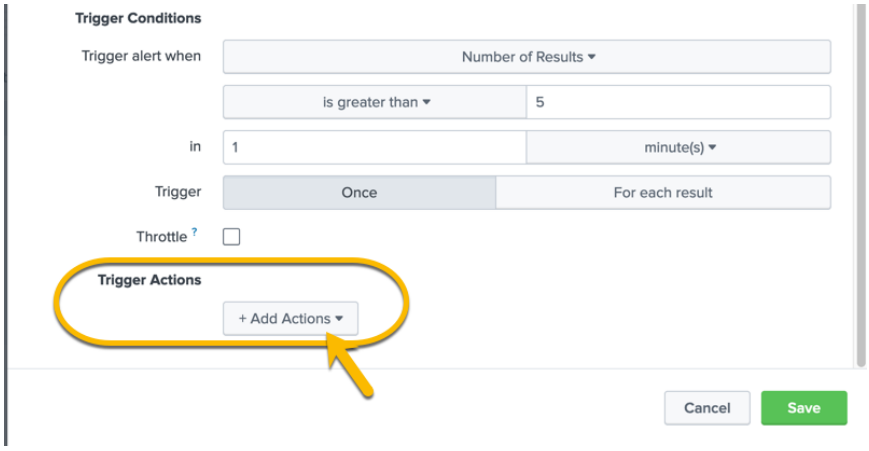

Figure 16:Add trigger actions

Select **Send email** from the options provided.

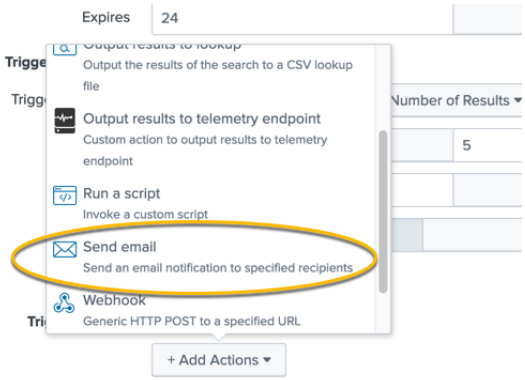

Figure 17: Select "Send email" as trigger action

Enter the same email address configured in sendQuick email filter in the **To** field. Select **Plain Text** for **Type** and click **Save**.

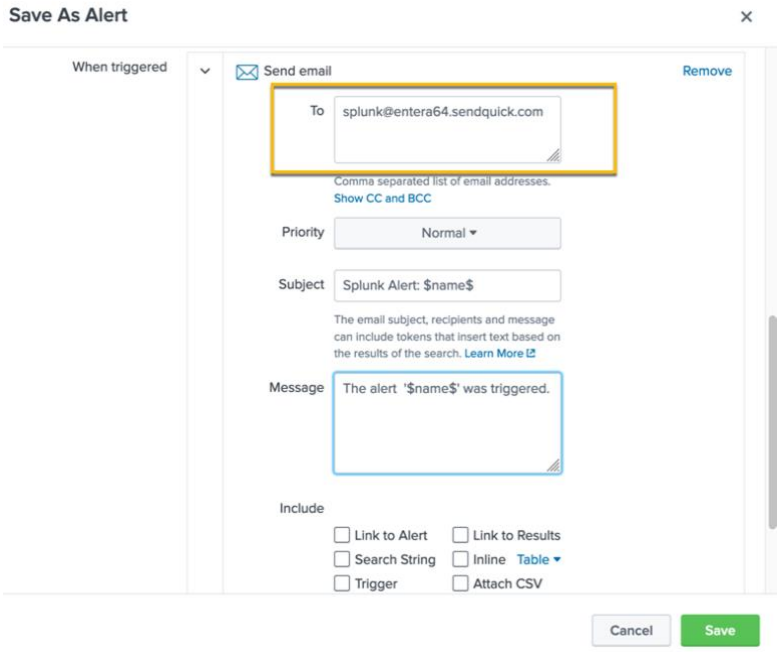

Figure 18: Enter details to send email when triggered

You should then have an alert like this.

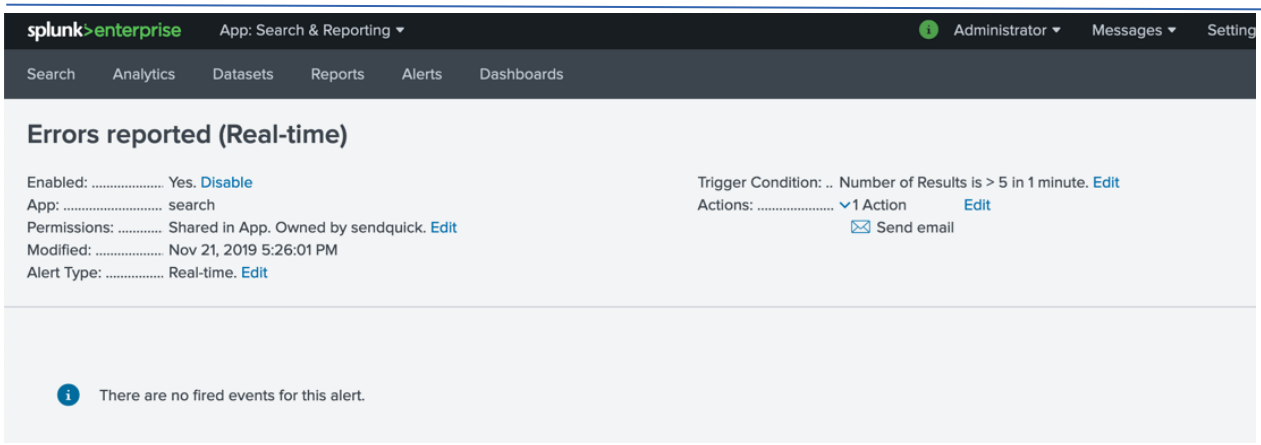

Figure 19: Example of Trigger Action configure in splunk

To check if the Job is running, from the dashboard menu, select **Activity > Jobs**

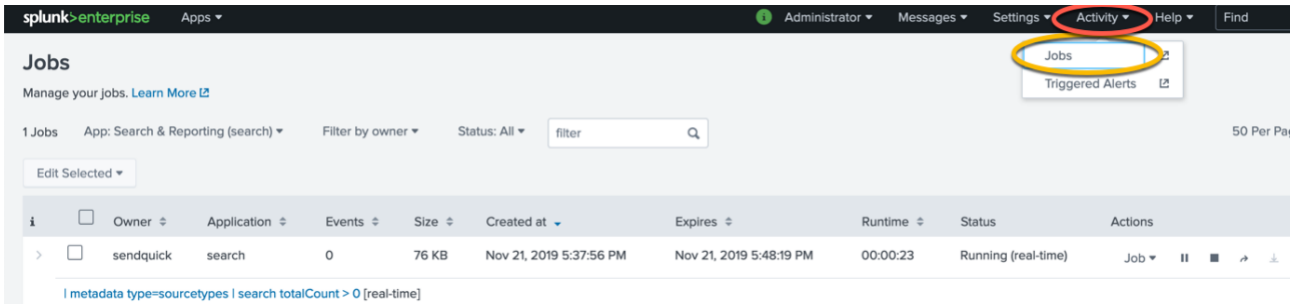

Figure 20: To view any jobs running

If the condition is triggered, the **Status** will be changed to **Done**.

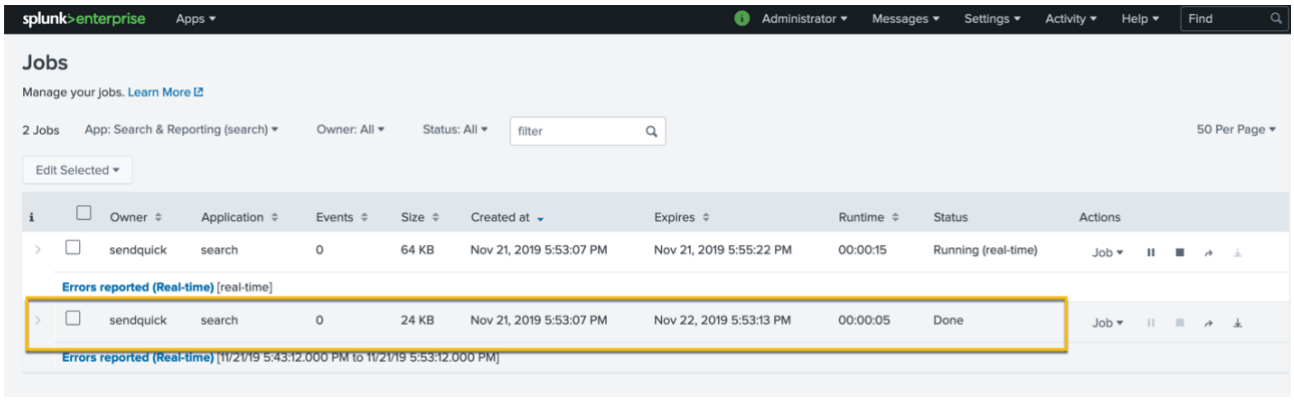

Figure 21: Status of trigger actions

To confirm that sendQuick has subsequently received the email and sent out as SMS, go to sendQuick dashboard. Navigate to :

Usage Logs > Message Logs

Click on the **Sent** tab and **SMS** tab. If there is a corresponding entry in the logs, that means the SMS text was sent successfully.

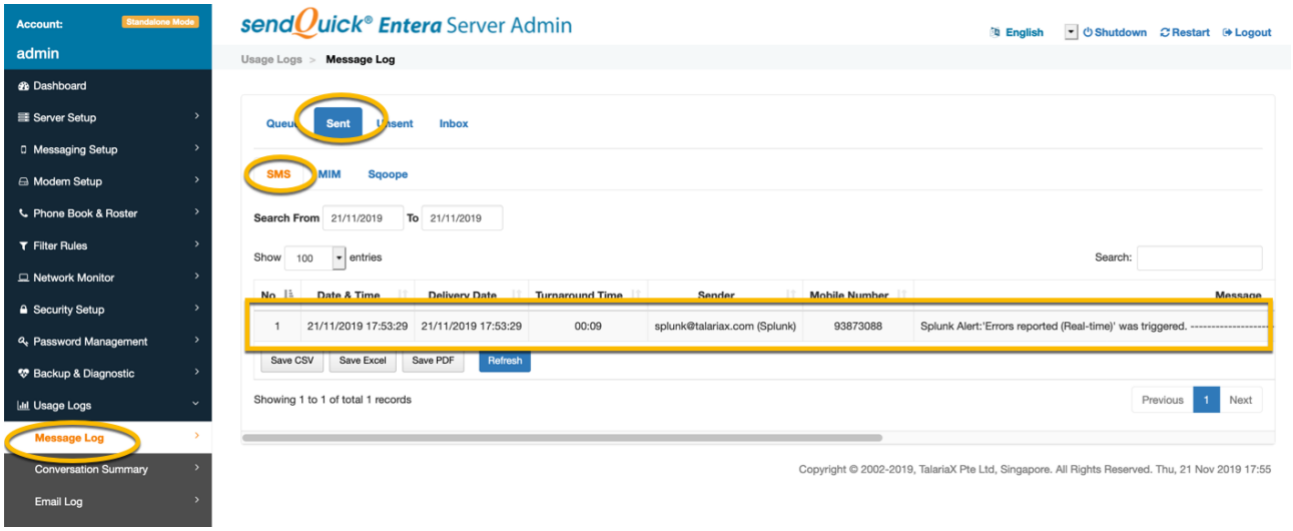

Figure 22: Message log on sendQuick

3.0 Sending SMS using Webhook Method

Similarly, notification alerts can be sent to sendQuick from Splunk via Webhook (http) method. You do not need to do any configuration in sendQuick.

When setting up the Alert in Splunk (see section 2.3), under the **Trigger Actions**, select **Webhook - Generic HTTP POST to a specified URL**.

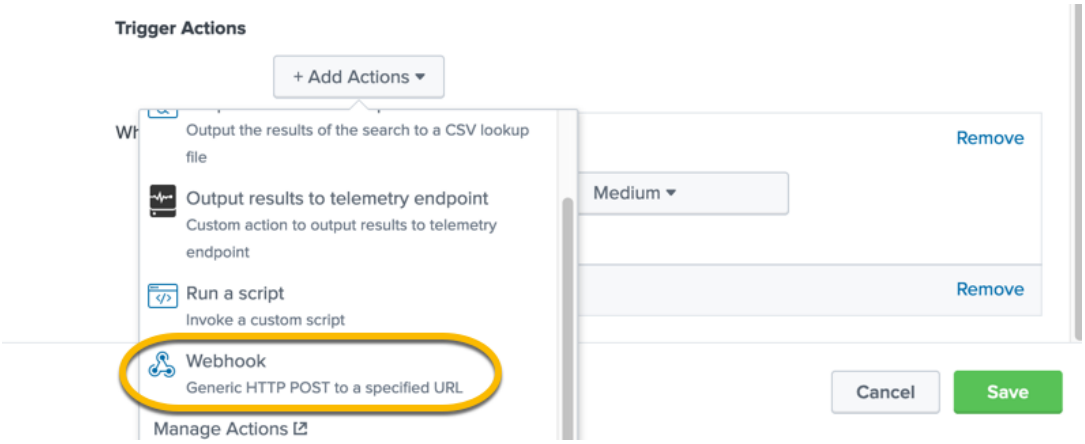

Figure 23: Trigger action using Webhook

For the URL, the syntax that sendQuick will accept is as follows:

http://<*sendQuickIP*>/cmd/system/api/sendsms.cgi?tar_num=%SMSNUMBER&tar_msg=%SMSTEXT

Replace <*sendQuickIP*> with the IP address of your sendQuick appliance. See the example :

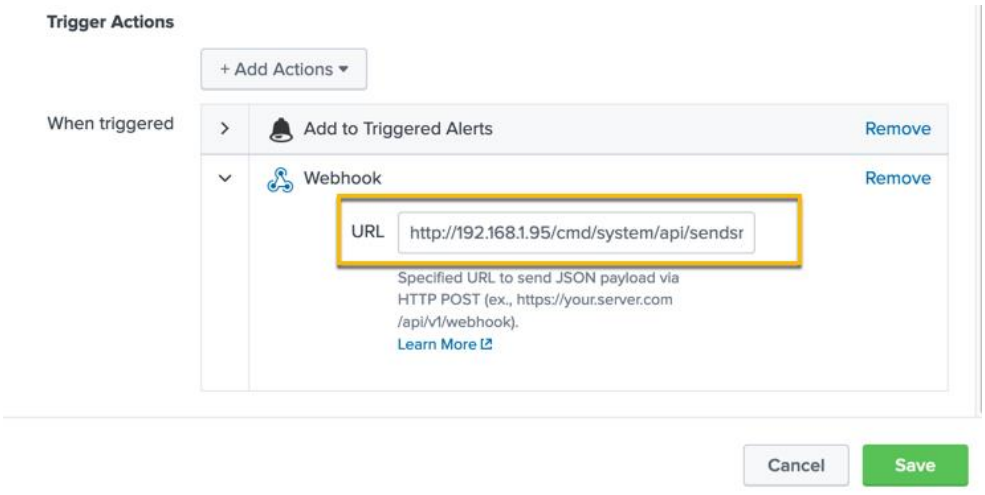

Figure 24: Adding URL for the webhook

For more options on what parameters to use for the webhook, please refer to Splunk manuals.

To confirm that sendQuick has subsequently received the email and sent out as SMS, go to sendQuick dashboard. Navigate to :

Usage Logs > Message Logs

Click on the **Sent** tab and **SMS** tab. If there is a corresponding entry in the logs, that means the SMS text was sent successfully.

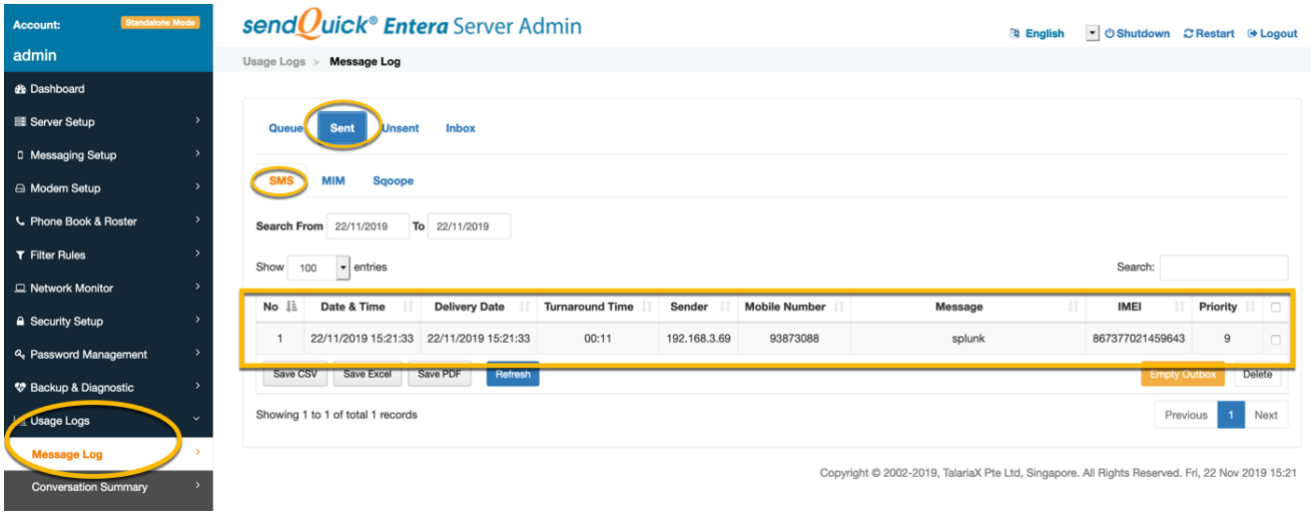

Figure 25: Message log on sendQuick