



Splunk - sendQuick Integration Guide

Prepared by

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

Version Number	Date Issued	Update Information
V1.0	22.11.2019	First published version

Table of Contents

1.0 Introduction	2
2.0 Send Email to sendQuick	2
2.1 Configure Email Filter in sendQuick	2
2.2 Configure Email Settings on Splunk.	7
2.3 Setting up An Alert	9
3.0 Sending SMS using Webhook Method	15

Splunk - sendQuick Integration Guide

1.0 Introduction

This document is a guide on how to integrate sendQuick with Splunk 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.

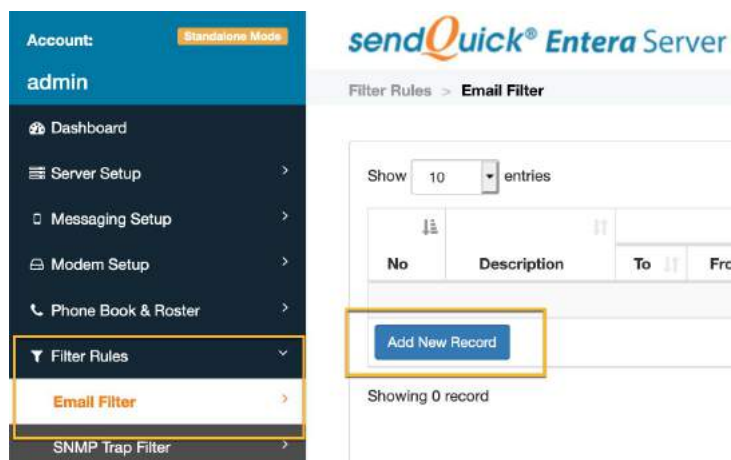
2.0 Send Email to sendQuick

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



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**.

The screenshot shows a dialog box titled "Add Mail Filter Rule". It contains several input fields: "Description" with the value "Splunk", "Mail To" (checked) with the value "splunk@entera64.sendquick.com", "Mail From", "Subject", and "Message" (all unchecked). At the bottom, there is a "Match Mode" section with radio buttons for "ALL" and "ANY" (selected), and a "Priority" dropdown set to "5". "Save" and "Cancel" buttons are at the bottom right.

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

The screenshot shows the "sendQuick Entera Server Admin" interface. The breadcrumb is "Filter Rules > Email Filter". There is a search bar and a "Show 10 entries" dropdown. A table lists filter rules with columns: No, Description, To, From, Subject, Message, Priority, Date Created, Match, and Alert. One record is shown with "Splunk" as the description and "splunk@entera64.sendquick.com" as the "To" address. The "Match" column shows "ANY" and the "Alert" column has a "View" link circled in red. Below the table are "Add New Record", "Duplicate", and "Delete" buttons. At the bottom, there are "Email Forwarding" and "Message Time Buffer" buttons.

No	Description	To	From	Subject	Message	Priority	Date Created	Match	Alert
1	Splunk	splunk@entera64.sendquick.com				5	14/11/2019	ANY	View

Then click on **Add New Record**

Email Filter Rules	
Description	Splunk
Mail To	splunk@entera64.sendquick.com
Mail From	
Subject	
Message	
Match Mode	ANY

Expand

Show 5 entries Search:

No	Message Receiver	Alert Template	Edit
No data available in table			

Add New Record Delete

Showing 0 record Previous Next

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

Email Filter Rules	
Description	Splunk
Mail To	splunk@entera64.sendquick.com
Mail From	
Subject	
Message	
Match Mode	ANY

Alert Message Alert Email Alert Voice

Alert Template

xFRcxSUBcxMSGx

The default me

- xFRcx is
- xSUBcx
- xMSGcx
- xDTMx
- xCASEI
- xLEVEL

Alert Mode

Once

Disable Roster Management

Send Acknowledgement Notice

Once - system
Once & Repor
Escalation - s
Escalation & I
settings, then i

Disable Roste
Send acknow
case has been

Alert Receiver

Mobile Number to Receive Alert

99873088

Email to Receive Alert

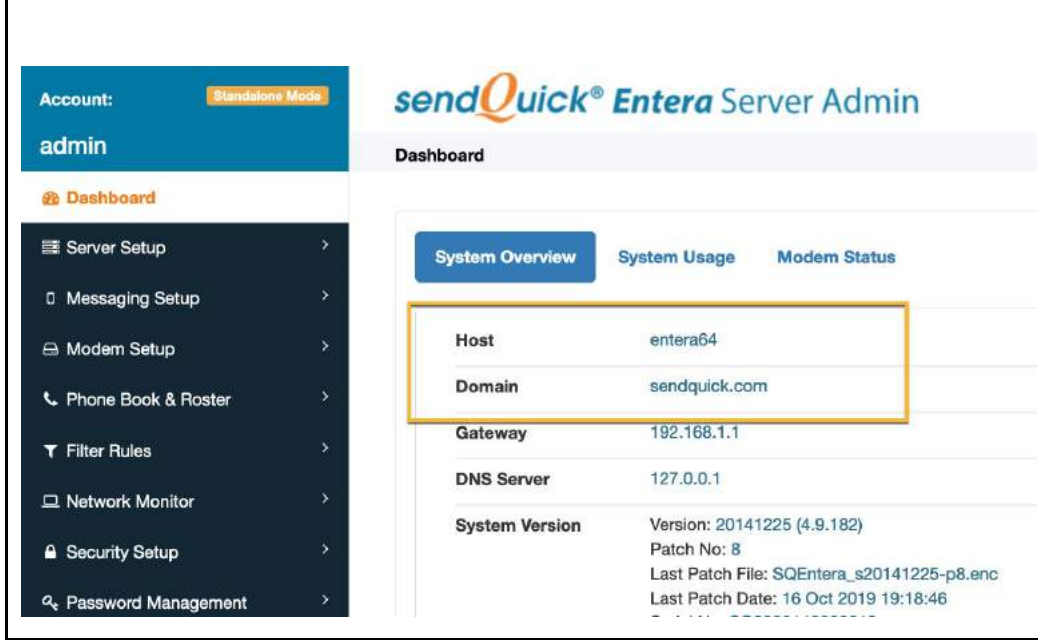
andyhun@talarix.com

Voice to Receive Alert

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*



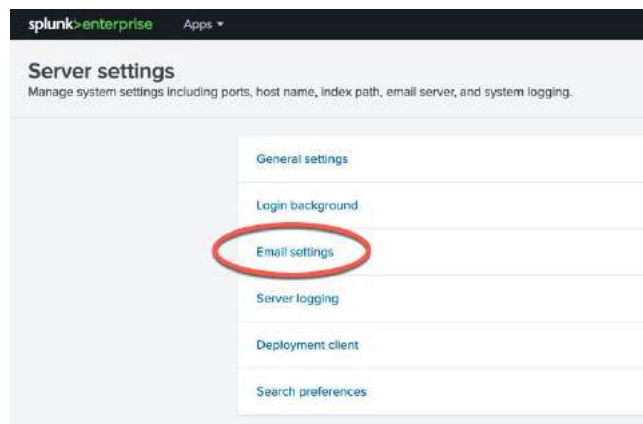
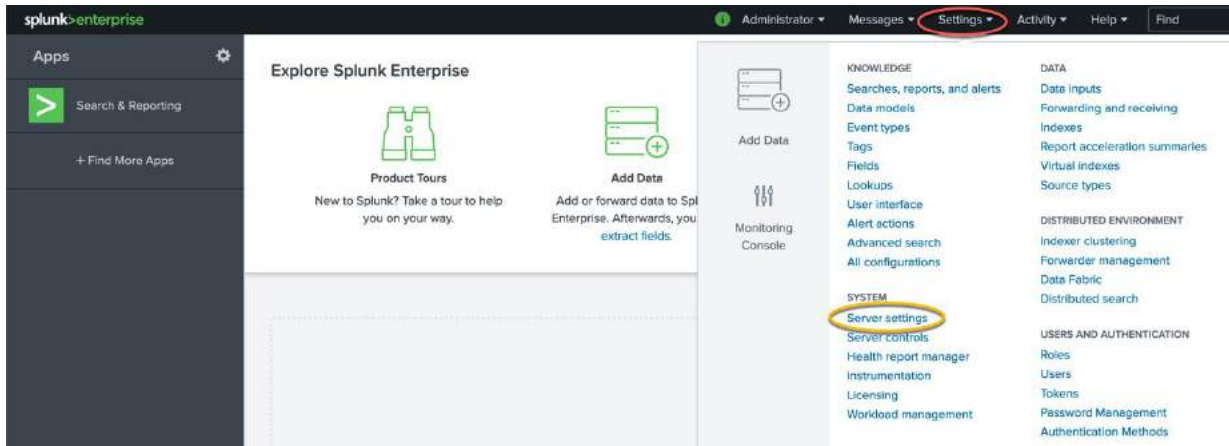
The screenshot displays the 'sendQuick® Entera Server Admin' dashboard. On the left is a navigation menu with options like 'Server Setup', 'Messaging Setup', 'Modem Setup', 'Phone Book & Roster', 'Filter Rules', 'Network Monitor', 'Security Setup', and 'Password Management'. The main content area shows the 'System Overview' tab selected, with a table listing system details. A yellow box highlights the 'Host' and 'Domain' rows.

System Overview	
Host	entera64
Domain	sendquick.com
Gateway	192.168.1.1
DNS Server	127.0.0.1
System Version	Version: 20141225 (4.9.182) Patch No: 8 Last Patch File: SQEntera_s20141225-p8.enc Last Patch Date: 16 Oct 2019 19:18:46

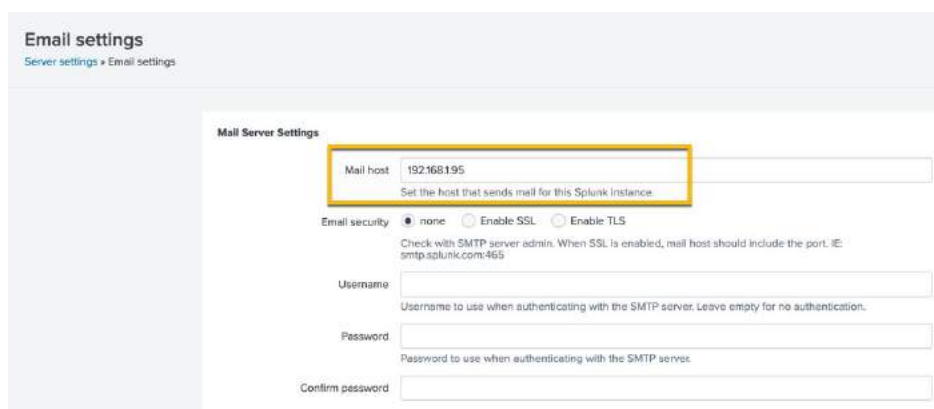
2.2 Configure Email Settings on Splunk.

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

Settings > Server Settings > 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.



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

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

Email Format

Link hostname

Set a hostname for generating URLs in outgoing notification (eg. [2001:db8:0:1]). Leave empty to autodetect.

Send emails as

Email footer *

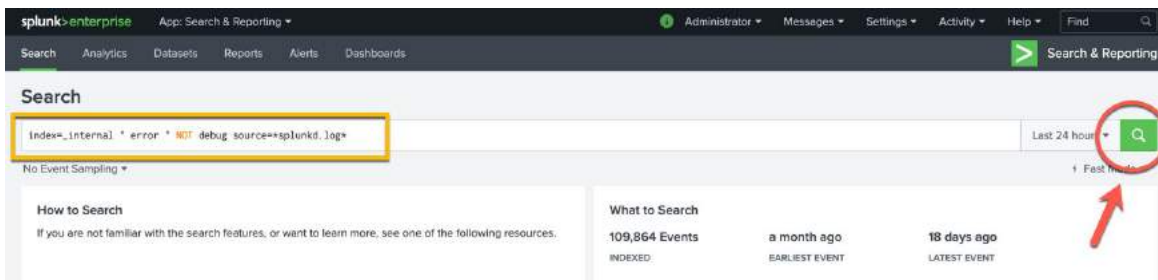
2.3 Setting up An Alert

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.



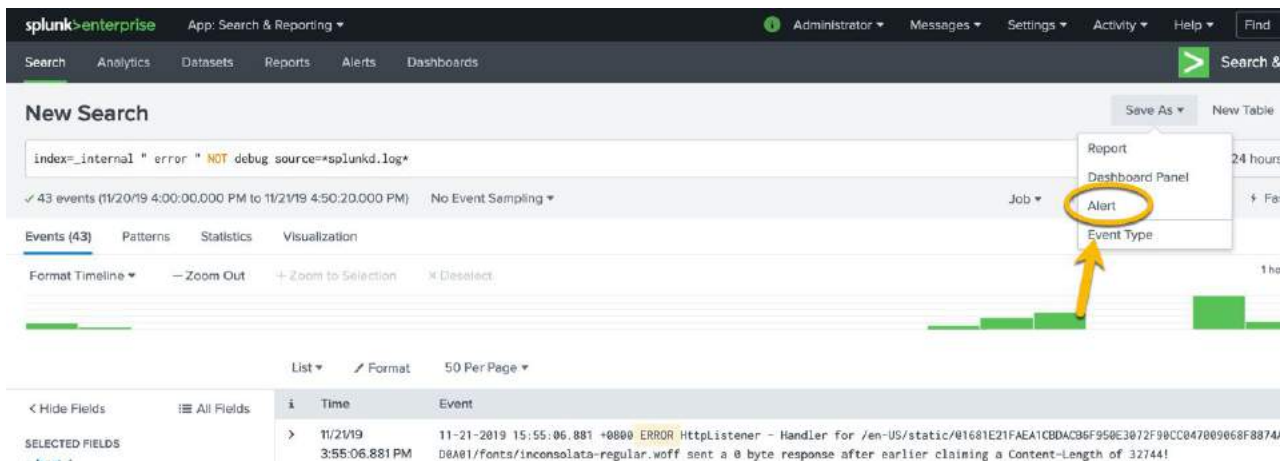
On the search bar, key in the following to create a new search to look for errors (*for more on splunk searches, please refer to documentation from splunk*)

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



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**



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 :

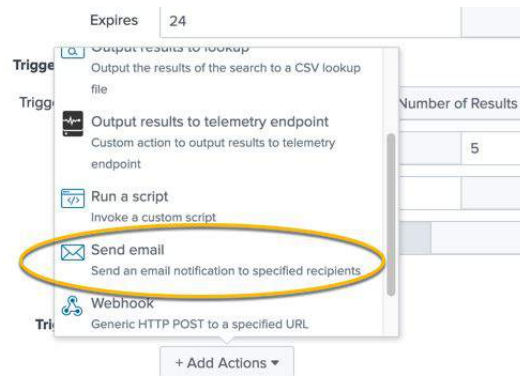
- **Title:** Errors reported (Real-time)
- **Alert type:** Real-time
- **Trigger condition:** Number of Results
- **Trigger if number of results:** is greater than 5 in 1 minute.

The screenshot shows the 'Save As Alert' configuration window. The 'Title' field is highlighted with a yellow box and contains the text 'Errors reported (Real-time)'. The 'Alert type' is set to 'Real-time', also highlighted with a yellow box. The 'Trigger Conditions' are set to 'Number of Results' is greater than 5 in 1 minute(s). The 'Trigger' is set to 'Once'. The 'Throttle' checkbox is unchecked.

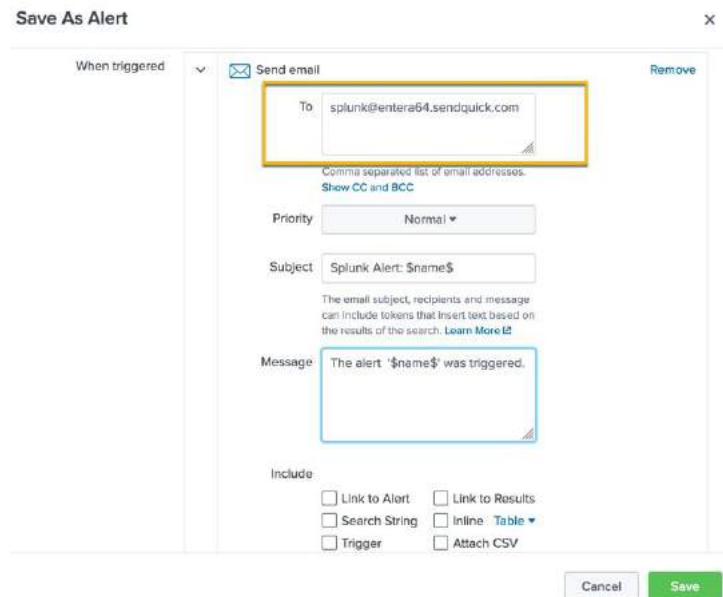
Before you click **Save**, scroll down until you see **Trigger Action**. Click on the **Add Actions** button.

The screenshot shows the 'Trigger Conditions' section of the 'Save As Alert' configuration window. The 'Trigger Actions' section is visible, showing a '+ Add Actions' button highlighted with a yellow oval and an arrow pointing to it. The 'Cancel' and 'Save' buttons are visible at the bottom right.

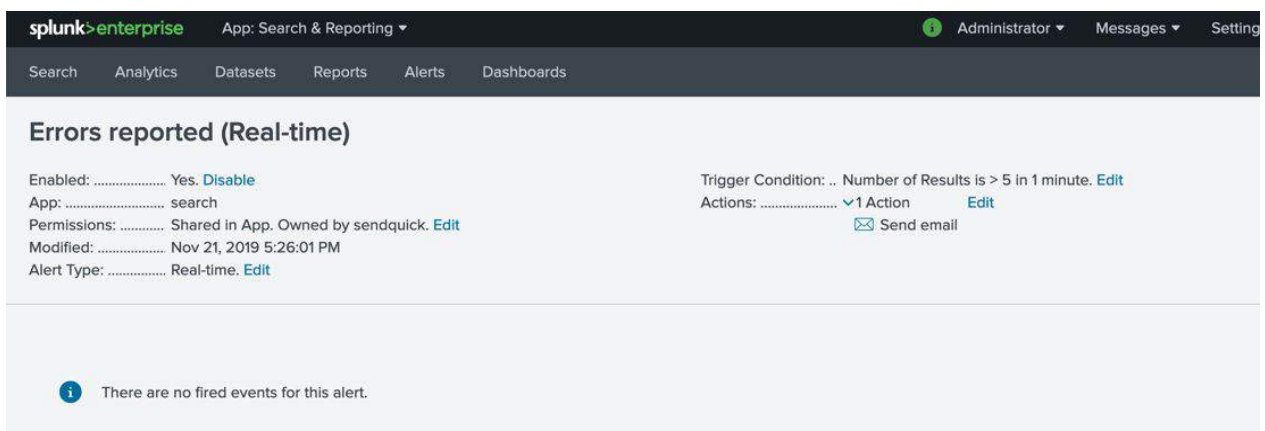
Select **Send email** from the options provided.



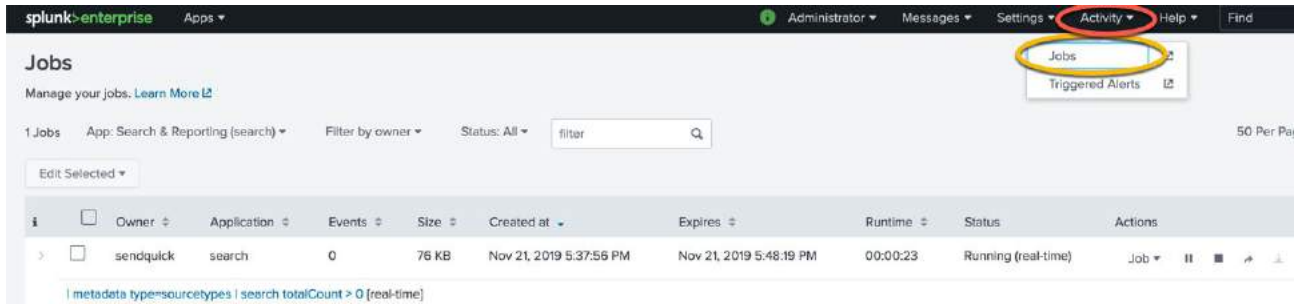
Enter the same email address configured in sendQuick email filter in the **To** field. Select **Plain Text** for **Type** and click **Save**.



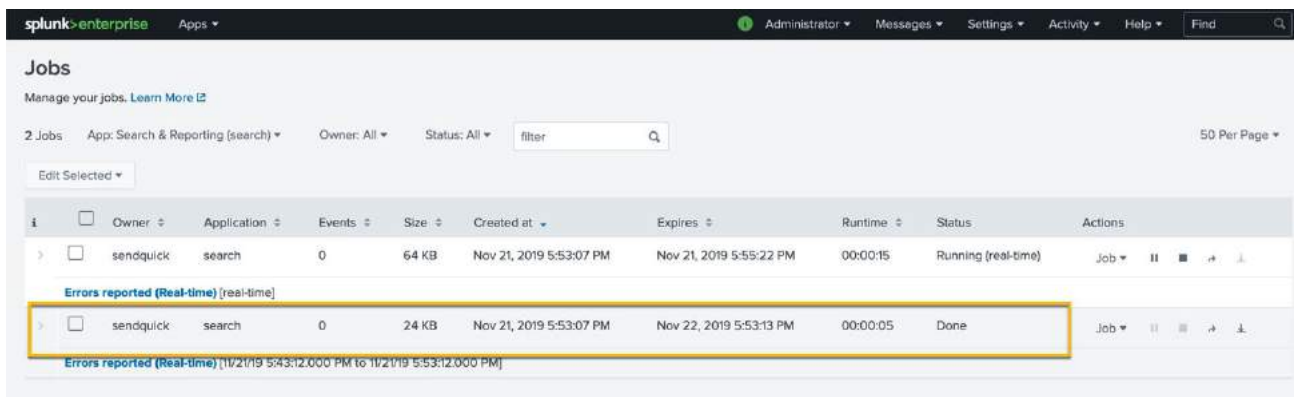
You should then have an alert like this.



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



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



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.

The screenshot displays the 'sendQuick Entera Server Admin' dashboard. On the left is a navigation menu with 'Message Log' highlighted. The main content area shows the 'Message Log' page with tabs for 'Queue', 'Sent', 'Unsent', and 'Inbox'. The 'Sent' tab is active, and the 'SMS' sub-tab is selected. Search filters are set for 'From: 21/11/2019' and 'To: 21/11/2019'. A table lists message records, with one record highlighted:

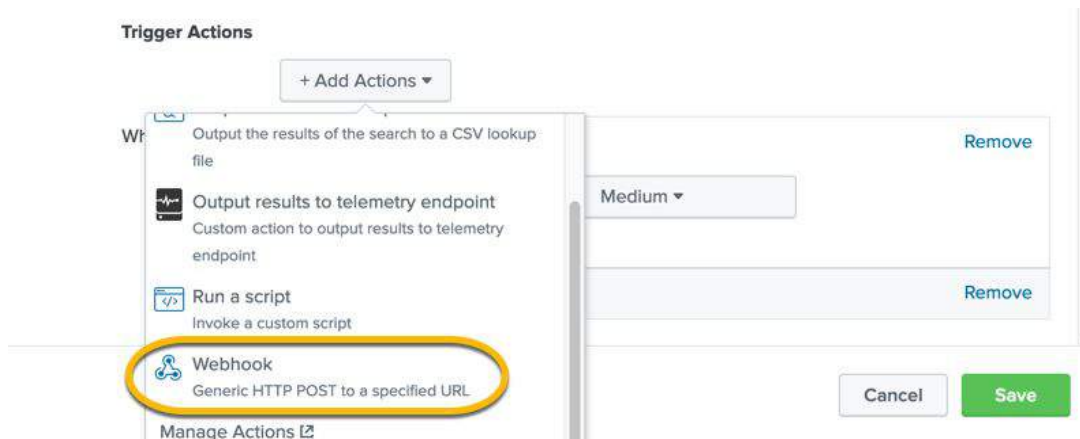
No.	Date & Time	Delivery Date	Turnaround Time	Sender	Mobile Number	Message
1	21/11/2019 17:53:29	21/11/2019 17:53:29	00:00	splunk@talarix.com (Splunk)	93873088	Splunk Alert: 'Errors reported (Real-time)' was triggered.

Below the table are buttons for 'Save CSV', 'Save Excel', 'Save PDF', and 'Refresh'. The page indicates 'Showing 1 to 1 of total 1 records'.

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.

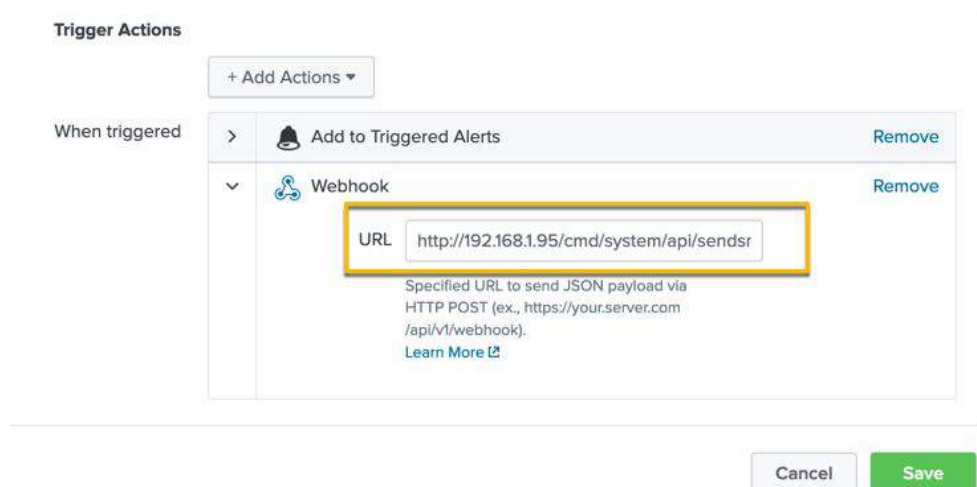
When setting up the Alert in Splunk (see section 2.3), under the **Trigger Actions**, select **Webhook - Generic HTTP POST to a specified URL**.



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 :

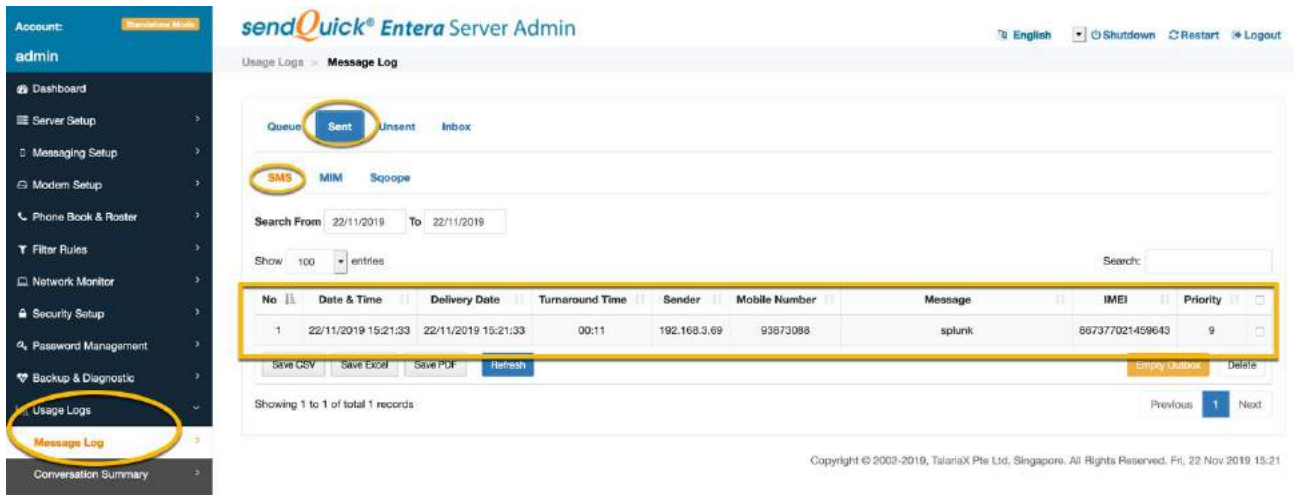


For more options on what parameters to use for the webhook, please refer to Splunk manuals.

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.



The screenshot shows the 'sendQuick Entera Server Admin' interface. On the left is a navigation menu with 'Message Log' highlighted. The main content area is titled 'Usage Logs > Message Log' and features tabs for 'Queue', 'Sent', 'Unsent', and 'Inbox'. The 'Sent' tab is active, and within it, the 'SMS' filter is selected. Search filters are set for 'From: 22/11/2019' and 'To: 22/11/2019'. A table below shows one record:

No	Date & Time	Delivery Date	Turnaround Time	Sender	Mobile Number	Message	IMEI	Priority
1	22/11/2019 15:21:33	22/11/2019 15:21:33	00:11	192.168.3.69	93873088	splunk	867377021459643	9

Below the table are buttons for 'Save CSV', 'Save Excel', 'Save PDF', 'Refresh', 'Empty checkbox', and 'Delete'. The status 'Showing 1 to 1 of total 1 records' is displayed at the bottom of the table area. A footer note reads: 'Copyright © 2002-2019, TalariaX Pte Ltd, Singapore. All Rights Reserved. Fri, 22 Nov 2019 15:21'.