



# 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**

1.0 Introduction	4
1.1 About TalariaX Pte Ltd	4
1.2 About sendQuick	4
1.3 Purpose of Document	4
2.0 Send Email to sendQuick	5
2.1 Configure Email Filter in sendQuick	5
2.2 Configure Email Settings on Splunk.	8
2.3 Setting up An Alert	11
3.0 Sending SMS using Webhook Method	16



## Splunk - sendQuick Integration Guide

## **1.0 Introduction**

## 1.1 About TalariaX Pte Ltd

TalariaX<sup>™</sup> 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



### 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**.



Description	Splunk	
	Variables Usage	_
Mail To 🗹	splunk@entera64.sendquick.com	
		li.
Mail From		
		11.
Subject 🗌		
		1
Message 🗌		
		4
Match Mode		111.
Priority	5 -	

Figure 2: Configure email filter rule

Click on  $\ensuremath{\textit{View}}$  for the record that you have created :

er Rules	Email Filter							Searc	h:		
↓±	1		Rules								
No	Description	To	From 1	Subject 🕼	Message 🕼	Priority 1	Date Created	a N	latch	Alert	
1	Splunk	splunk@entera64.sendquick.com				5	14/11/2019	9	ANY	View 🖸	
Add Nev	w Record									Duplicate	Delet
howina 1	to 1 of total 1 recor	rds							Previ	ious 1	Nex
		_									

Figure 3: View more configuration of the filter rule



## 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 • entrie	5		Search:		
Show 5 entrie	15	Message Receiver	Search: Alert Template	Edit	
Show 5 entrie	15	Message Receiver No data available in table	Search: Alert Template	Edit	
Show 5 entrie	25	Message Receiver No data available in table	Search: Alert Template	Edit	Delete

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 E	mail Alert Voice	
Alert Template	xFRx:xSUBx:xMSGx		The default m • xFRx is • xSUBx • xSUBx • xDTM> • xCASE
Alast Mada	0		• xLEVE
Alert Mode	Once 💟		Once - system
	Disable Roster Management	-	Once & Repo
	Send Acknowledgement Not	O	Escalation - Escalation & Settings, then
	Send Acknowledgement Not	Ø	Dice & Repo Escalation - Escalation & settings, then Disable Rost Send acknow case has bee
ert Receiver	Claudie ruster management Not     Send Acknowledgement Not	O	Escalation - Escalation - Settings, then Disable Rost Send acknow case has bee
ert Receiver iblie Number to Receive A	Claudie Hoster Management Not     Send Acknowledgement Not	O tice ceive Alert Voice to I	Conce & Hepc Escalation - Escalation & settings, then Disable Rost Send acknow case has been

Figure 5: Configure receiver of alerts

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



Quicktip - To cheo in the sendQuick Domain.	ck yo dashl	our host and domai board under <b>Syste</b>	n name, you can find t em Overview under I	the value <b>lost</b> and
For e.g. our doma	in na	me is <b>entera64.se</b>	endquick.com	
Account: Standalon	e Mode	sendQuick®	<b>Entera</b> Server Admin	n
admin		Dashboard		
Dashboard				
≣ Server Setup	>	System Overview	System Usage Modem Status	
Messaging Setup	>			
🖨 Modem Setup	>	Host	entera64	
Phone Book & Roster	>	Domain	sendquick.com	
▼ Filter Rules	>	Gateway	192.168.1.1	
Notwork Monitor	\$	DNS Server	127.0.0.1	
	ŕ	System Version	Version: 20141225 (4.9.182)	
Security Setup	>		Patch No: 8 Last Patch File: SQEntera s20141	225-p8.enc
& Password Management	>		Last Patch Date: 16 Oct 2019 19:	18:46
		Figure 6: System Ov	erview	

## 2.2 Configure Email Settings on Splunk.

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

Settings >	Server	Settings >	Email	settings
------------	--------	------------	-------	----------

splunk>enterprise			Administrator •	Messages   Settings	Activity • Help • Find
Apps       Search & Reporting       + Find More Apps	Explore Splunk Enterprise Froduct Tours New to Splunk? Take a tour to help you on your way.	Add Data Add or forward data to Spi Enterprise. Afterwards, you extract fields.	Add Data Âţî Îŭ Monitoring Console	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 instrumentation Licensing Workload management	DATA Data Inputs Forwarding and receiving Indexes Report acceleration summaries Virtual indexes Source types DISTRIBUTED ENVIRONMENT Indexer clustering Forwarder management Data Fabric Distributed search USERS AND AUTHENTICATION Roles USERS Tokens Password Management Authentication Methods

Figure 7: To configure email settings on Splunk



splunk>enterprise Apps -	
Server settings Manage system settings including por	ts, host name, index path, email server, and system logging.
	General settings
	Login background
	Email settings
	Server logging
	Deployment client
	Search preferences
= 0	

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.

r settings » Email settings		
	Mail Server Settings	
	Mail bost	102362105
	Mail flost	Set the best that could will for this Salual instance
		Secure noscinar serios mair or cris spionik instance.
	Email security	none      Enable SSL     Enable TLS
		Check with SMTP server admin. When SSL is enabled, mail host should include the port. IE: smtp.splunk.com/465
	Username	
		Username to use when authenticating with the SMTP server, Leave empty for no authentication.
	Password	
		Password to use when authenticating with the SMTP server.

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.





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

Email Forma	at		
	Link hostname		
		Set a hostname for generating URLs in ou (eg. [2001:db8:0:1]). Leave empty to autoo	utgoing notification letect.
	Send emails as	splunk@talariax.com	
	Email footer *	end-of-message	

#### 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.

splunk>enterprise			
Apps	\$	Explore Splunk Enterprise	
Search & Repo	rting	<u>r</u>	
+ Find More A	ops	Product Tours	Add Data
	Figure	12: Search and reporting app	Add as fanuard data ta Cr

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\*

splunk>enterprise App: Search & Reporting •	🚯 Administrator 🕶	Messages 🕶	Settings   Activity	Help  Find  Q		
Search Analytics Datasets Reports Alerts Dashboards				Search & Reporting		
Search				$\sim$		
index=_internal " error " NOT debug source=*splunkd.log*				Last 24 hour 👻 Q		
No Event Sampling 👻				∮ Fast Mc.		
How to Search	What to Search			1		
If you are not familiar with the search features, or want to learn more, see one of the following resources.	109,864 Events	a month ago EARLIEST EVENT	18 days ago LATEST EVENT			
Figure 13: Search for error						

Click on the magnifying glass icon.

splunk>enterprise App: Search & Reporting • Administrator • Messages 🕶 Settings -Activity -> Search & Save As 🔻 New Table **New Search** Report index=\_internal " error " NOT debug source=\*splunkd.log\* 24 hours ✓ 43 events (11/20/19 4:00:00.000 PM to 11/21/19 4:50:20.000 PM) No Event Sampling ▼ ∮ Fa Events (43) Patterns Statistics Visualization 1 hc Format Timeline 🔻 - Zoom Out List 🔻 🖌 Format 50 Per Page 🔻 i Time Event < Hide Fields :≡ All Fields > 11/21/19 11-21-2019 15:55:06.881 +0800 ERROR HttpListener - Handler for /en-US/static/01681E21FAEA1CBDACB6F950E3072F90CC047009068F8874/ SELECTED FIELDS 3:55:06.881 PM D0A01/fonts/inconsolata-regular.woff sent a 0 byte response after earlier claiming a Content-Length of 32744!

Alert

Figure 14: Save Incident Scenario as

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

a host 1



Configure the alert according to your needs. For this example, we will use the sample alert provided by <u>splunk tutorial on Alert Samples</u>

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.

ave As Alert				
Settings				
Title	Errors reported (Real-time)			
Description	Optional			
				//
Permissions	Private		Shared in App	
Alert type	Scheduled		Real-time	
Expires	24		hour(s) 👻	
Trigger Conditions				
Trigger alert when	Nu	nber o	f Results 🔻	
	is greater than 💌		5	
in	1	minute(s		
Trigger	Once		For each result	
Throttle ?				

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

Trigger Conditions		
Trigger alert when	Numbe	er of Results 🔻
	is greater than ▼	5
in	1	minute(s) 🔻
Trigger	Once	For each result
Throttle ?		
Trigger Actions	+ Add Actions •	
		Cancel Save
	Figure 16:Add trigger	r 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**.

When triggered	~	🖂 Send emai	1	Remov
		То	splunk@entera64.sendquick.com	
			Comma separated list of email addresses.	
			Show CC and BCC	
		Priority	Normal 🕶	
		Subject	Splunk Alert: \$name\$	
			The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More 🗗	
		Message	The alert '\$name\$' was triggered.	
			ļi.	
		Include		
			□ Link to Alert     □ Link to Results       □ Search String     □ Inline	
			Trigger Attach CSV	

Figure 18: Enter details to send email when triggered

You should then have an alert like this.



splunk>enterprise	App: Search & Reportir	ıg ▼		0	Administrator 🔻	Messages 🔻	Setting
Search Analytics	Datasets Reports	Alerts	Dashboards				
Errors reported	d (Real-time)						
Enabled:	Disable ch ed in App. Owned by sen 21, 2019 5:26:01 PM -time. Edit	dquick. Edit		Trigger Condition: Number of Re Actions:	sults is > 5 in 1 minut Edit Iail	te. Edit	
i There are no fi	red events for this alert.						
	Figu	re 19: E	xample of Trigger A	ction configure in splunk			

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

splunk>	enterprise 4	Apps 🔻						Administrator •	Messages •	Settings •	Activity - H	elp 🔻	Find	ł
Jobs										Jobs		2		
Manage y	your jobs. <mark>Learn Mo</mark>	re 🖸								Trigg	ered Alerts			
1 Jobs	App: Search & Re	porting (search) 🔻	Filter by owne	er▼ S	tatus: All 🔻	filter	Q						50	) Per Pa
Edit Se	elected -													
i	Owner ‡	Application \$	Events \$	Size ≑	Created a	t •	Expires \$	R	untime 🗘 S	Status	Actions			
> [	sendquick	search	0	76 KB	Nov 21, 20	19 5:37:56 PM	Nov 21, 2019	5:48:19 PM 00	0:00:23 F	Running (real-time)	Job 🔻	п		• ±
l m	I metadata type≔sourcetypes I search totalCount > 0 [real-time]													
	Figure 20: To view any jobs running													

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

splunk>enterprise Apps -		(i) Administrator 🕶	Messages ▼ Settings ▼ Ac	tivity ▼ Help ▼	Find Q
Jobs Manage your jobs. Learn More E 2 Jobs App: Search & Reporting (search) * Edit Selected *	Owner: All • Status: All • filter	Q			50 Per Page 🔻
i 🗌 Owner 🗢 Application 🗢	Events	Expires 🗘 Runti	ime 🗘 Status	Actions	
> Sendquick search	0 64 KB Nov 21, 2019 5:53:07 PM	Nov 21, 2019 5:55:22 PM 00:00	0:15 Running (real-time)	Job 🔻 📕	• • ±
Errors reported (Real-time) [real-time]					
> Sendquick search	0 24 KB Nov 21, 2019 5:53:07 PM	Nov 22, 2019 5:53:13 PM 00:00	0:05 Done	Job 👻 🔢	- * ±
Errors reported (Real-time) [11/21/19 5:43:12	.000 PM to 11/21/19 5:53:12.000 PM]			-	

#### 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.

Account: Standalone Mode	sendQuick® Entera Server Admin 🔅 English 💽 OShutdown @Restart @Logout
admin	Usage Logs > Message Log
2 Dashboard	
≣ Server Setup	Queu Sent Inbox
D Messaging Setup	
🖨 Modem Setup	SMS MIM Sqoope
C Phone Book & Roster	Search From 21/11/2019 To 21/11/2019
▼ Filter Rules	Show 100 + entries Search:
Network Monitor	No. 18 Date & Time 10 Defining Date 10 Temporard Time 10 Decider 10 Mathematica 10 Mathematica 10
Security Setup	NO 12 LARIE LARIE LARIE LARIE UNITARIA LARIE AND ANNO MONTANA MENANDALI MENANDALI
A Password Management	1 21/11/2019 17:53:29 21/11/2019 17:53:29 00:09 splunk@talariax.com (Splunk) 93873088 Splunk Alert: Errors reported (Real-time)' was triggered.
♣ Password Management ♥ Backup & Diagnostic	1 21/11/2019 17:53:29 21/11/2019 17:53:29 00:09 splunk@talariax.com (Splunk) 93873088 Splunk Alert: Errors reported (Real-time)' was triggered.
Q. Password Management         Image: The second s	1       21/11/2019 17:53:29       21/11/2019 17:53:29       00:09       splunk@talariax.com (Splunk)       93873088       Splunk Alert: 'Errors reported (Real-time)' was triggered.         Save CSV       Save PDF       Refresh         Showing 1 to 1 of total 1 records       Previous       1       Next
<ul> <li>♀ Password Management</li> <li>♥ Backup &amp; Diagnostic</li> <li>Idit Usage Logs</li> <li>Message Log</li> </ul>	1       21/11/2019 17:53:29       21/11/2019 17:53:29       00:09       splunk@talariax.com (Splunk)       93873088       Splunk Alert: Errors reported (Real-time)' was triggered.         Save CSV       Save Excel       Save PDF       Reheath         Showing 1 to 1 of total 1 records       Previous       1       Next
<ul> <li>Q. Password Management</li> <li>♥ Backup &amp; Diagnostic</li> <li>Iait Usage Logs</li> <li>Message Log</li> <li>Conversation Summary</li> </ul>	1       21/11/2019 17:53:29       21/11/2019 17:53:29       00:09       splunk@talariax.com (Splunk)       93873088       Splunk Alert: Errors reported (Real-time)' was triggered.         Save CSV       Save PDF       Reheath       Previous       1       Next         Showing 1 to 1 of total 1 records       Previous       1       Next         Copyright © 2002-2019, TalariaX Pie Ltd, Singapore. All Rights Reserved. Thu, 21 Nov 2019 17:55

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**.

Wł	+ Add Actions ▼ Output the results of the search to a CSV lookup		Remov
	file		Keniov
ļ	Custom action to output results to telemetry endpoint	Medium •	
	Run a script     Invoke a custom script		Remov
C	S Webhook Generic HTTP POST to a specified URL		Cancel

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 :

/hon triggorod					
men uiggered	>	Remove			
	~	🔏 We	bhook		Remove
			URL	http://192.168.1.95/cmd/system/api/sendsr	
			-	Specified URL to send JSON payload via HTTP POST (ex., https://your.server.com /api/vl/webhook).	
				Learn More 12	

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.

Account: Standalone Mode	<b>sendQuick® Entera</b> Server Admin	🔋 English 💽 🖱 Shutdown 📿 Restart 👒 Logout
admin	Usage Logs > Message Log	
a Dashboard		
E Server Setup >	Queue Sent Jusent Inbox	
C Messaging Setup		
Modem Setup	SMS MIM Sqoope	
Sector A Phone Book & Roster	Search From 22/11/2019 To 22/11/2019	
▼ Filter Rules >	Show 100 - entries	Search:
Network Monitor		
A Security Setup >	No La Date & Time Delivery Date Turnaround Time Sender Mobile Number Message	
Arr Password Management     →	1 22/11/2019 15:21:33 22/11/2019 15:21:33 00:11 192.108.3.69 93873088 splunk	867377021459643 9
🏶 Backup & Diagnostic >	Save CSV Save Excel Save PDF Refresh	Empty Outbox Delete
	Showing 1 to 1 of total 1 moords	Previous 1 Next
Usage Logs	Showing I to To total Fredords	

Figure 25: Message log on sendQuick