

#### 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:





Page 1 of 16

Copyright 2018 Talk-A-Phone, LLC • 7530 North Natchez Avenue • Niles, Illinois 60714 • Phone 773.539.1100 • info@talkaphone.com • www.talkaphone.com.

All prices and specifications are subject to change without notice. Talk-A-Phone, Talkaphone, Scream Alert, WEBS, and WEBS Contact are registered trademarks of Talk-A-Phone, LLC. All rights reserved. All other trademarks mentioned in this document or website are the property of their respective owners and does not imply or indicate any approval, endorsement, sponsorship, or affiliation is expressly indicated.



## VOIP-500/VOIP-600 Series IP Call Stations

Integration with Splunk Enterprise – Syslog Monitoring

← → C ☆ ③ localhost:8000/en-U	S/app/launcher/home			☆ ○ :
splunk>enterprise		E Admi	nistrator 🔻 🜀 Messages 👻 Settings 🖲	Activity - Help - Find Q
Apps 🗘	Jyoti's Activity Insight 12 O			Explore Splunk Enterprise
Search & Reporting				
App snmp_ta	VOIP-500 Network Connectivity Status			
	Last seen details			
+ Find More Apps	Not_Reachable_Since \$	host ¢	lastTime \$	
	2,289 Mins	192.168.40.120	09/17/2018 23:59:57	
	2,289 Mins	192.168.40.133	09/17/2018 23:59:57	
	Host Network Connectivity Vs Time			<b>A</b>

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.

1.		
Г		
TALKAPHO	JNE	Apply Refresh Help Logout
Home		7.0.1.1
Maintenance	Logging	✓ Updated.
Licensing		
Device State	Send log messages to :	
Stausuus		
Date & Time		
Ping & Traceroute		
Firmware Upgrade	Network	
SMTP Server Configuration	Specify logging server (required for network logging) :	
Email Notification Profiles	Logging Server IP Address 192.168.37.51	
Reset to Default	Loging Server Part 514	
Network	Salet lavel of location -	
VoIP	Audio Debua v	
Devices	Cill Control Debin, y	
Digital Outputs		
Voice Messages		
Self Diagnostics & Reporting	Envice Control Debug V	
Authentication	SIP MODE DECKY V	
Reboot	imer Ueoug V	
	HTTP Debug v	
	Click the 'Download' link below to save the log file to your computer :	
	Download	
Copyright @ 2016 Talk-A-Phone (	Co. Al rights reserved.	
oupping it a colo fait without t		

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

Page 2 of 16



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.



Integration with Splunk Enterprise – Syslog Monitoring

New Index				×		
General Settings						
Index Name	Talkaphone_VOIP			٦		
	Set index name (e.g., INDEX_NAME). Search using ind	dex=INDEX_NAME.				
Index Data Type	🗄 Events	Ø	Metrics			
	The type of data to store (event-based or metrics).					
Home Path	optional					
	Hot/warm db path. Leave blank for default (\$SPLUNK,	_DB/INDEX_NAME/db).				
Cold Path	optional					
	Cold db path. Leave blank for default (\$SPLUNK_DB/	NDEX_NAME/colddb).				
Thawed Path	optional	optional				
	Thawed/resurrected db path. Leave blank for default	(\$SPLUNK_DB/INDEX_I	NAME/thaweddb).			
Data Integrity Check	Enable	0	Disable			
	Enable this if you want Splunk to compute hashes on integrity.	every slice of your data	for the purpose of data			
Max Size of Entire Index	500		GB 🔻			
	Maximum target size of entire index.					
Max Size of	auto		GB 🔻			
Hot/Warm/Cold Bucket	Maximum target size of buckets. Enter 'auto_high_vo	lume' for high-volume in	idexes.			
Frozen Path	optional					
	Frozen bucket archive path. Set this if you want Splur	nk to automatically archiv	ve frozen buckets.			
Арр	Search &	Reporting 🔻				
Storage Optimization						
Tsidx Retention Policv	Enable Reduction	Disabl	e Reduction			
)	Warning: Do not enable reduction without understand rebuild reduced buckets. Learn More 12	ding the full implications	. It is extremely difficult to			
			Cancel Save	9		

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

Page 4 of 16

Copyright 2018 Talk-A-Phone, LLC • 7530 North Natchez Avenue • Niles, Illinois 60714 • Phone 773.539.1100 • info@talkaphone.com. • www.talkaphone.com.

All prices and specifications are subject to change without notice. Talk-A-Phone, Talkaphone, Scream Alert, WEBS, and WEBS Contact are registered trademarks of Talk-A-Phone, LLC. All rights reserved. All other trademarks mentioned in this document or website are the property of their respective owners and does not imply or indicate any approval, endorsement, sponsorship, or affiliation with such owners unless such approval, endorsement, sponsorship, or affiliation is expressly indicated.



# 3. Add Source Type.

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

Create Source Type						×	
Name	Name VOIP-500						
Description	Talkapho	ne VOIP Phone					
Destination app			Search	& Reporting			
Category			(	Custom 💌			
Indexed Extractions ?				none 🔻			
✓ Event Breaks							
Break Type	e	Auto	Eve	ery Line	Regex		
✓ Timestamp							
Extraction	1	Auto	Currei	nt time	Advanced		
✓ Advanced							
Name		Valu	ue				
CHARSET			-	×			
SHOULD_LINEMERG	θE	true		×			
NO_BINARY_CHECH	<	true		×			
category		Custom		×			
description		Talkaphone VOI	P Phone	×			
New setting							
					Cancel	ave	

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

Page 5 of 16

Copyright 2018 Talk-A-Phone, LLC • 7530 North Natchez Avenue • Niles, Illinois 60714 • Phone 773.539.1100 • info@talkaphone.com • www.talkaphone.com

All prices and specifications are subject to change without notice. Talk-A-Phone, Talkaphone, Scream Alert, WEBS, and WEBS Contact are registered trademarks of Talk-A-Phone, LLC. All rights reserved. All other trademarks mentioned in this document or website are the property of their respective owners and does not imply or indicate any approval, endorsement, sponsorship, or affiliation is expressly indicated.



#### 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.

splunk>enterprise Apps -				📵 Administrator 🕶	🌀 Messages 🔻	Settings 🕶	Activity -	Help 🔻	Find	۹
	Add Data Select So	urce Input Settings Review	O C Back Next>	l						
	Local Event Logs Collect event logs from this machine.	Configure this instance to lis (such as syslog). Learn More	ten on any TCP or UDP port to capt 亿	ure data sent over the ne	work					
	Remote Event Logs Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.		ТСР	UDP						
	Files & Directories Upload a file, index a local file, or monitor an entire directory.	Port ?	514 Example: 514							
	HTTP Event Collector Configure tokens that clients can use to send data over HTTP or HTTPS.	Source name override ?	optional host.port							
	TCP / UDP >	Only accept connection from ?	optional example: 10.1.2.3, lbadhost.splunk.com,	.splunk.com						
	Local Performance Monitoring Collect performance data from this machine.	FAQ								
	Remote Performance Monitoring Collect performance and event information from remote hosts. Requires domain credentials.	How should I configure Sp     What's the difference betw     Can L collect surface data fi	lunk for syslog traffic? veen receiving data over TCP versu	s UDP?						
	Registry monitoring Have Splunk index the local Windows Registry, and monitor it for changes.	> What is a source type?	on millows systems.							
	Active Directory monitoring Index and monitor Active Directory.									
	Local Windows host monitoring Collect up to date hardware and software (Computer, Operating System, Processor, Service, Disk, Network Adapter and Application) information about this machine.									
	Local Windows network monitoring This is an input for Splunk Network Monitor.									
	Local Windows print monitoring	*								

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



# VOIP-500/VOIP-600 Series IP Call Stations Integration with Splunk Enterprise – Syslog Monitoring

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

splunk>enterprise Apps -		🔒 Administrator 🕶	🌀 Messages ▾	Settings -	Activity -	Help 🔻	Find	٩
	Add Data O O C Back Review Done							
	Optionally set additional input parameters for this data input as follows:							ľ
	Source type The source type is one of the default fields that Splank assigns to all incoming data. It tells Splank what kind of data you've got, so that Splank can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily. App context Application contexts are folders within a Splank instance that contain configurations for a specific use case or domain of data. App context App context App context is prove manageability of input and source type defaultions: Source type	•						
	rules. Learn More 12 Host When Splunk indexes data, each event receives a "host" value. The host values should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More 12							
	Index Splunk stores incoming data as events in the selected index. Consider using a "sandbor" index as a destination if you have problems determining a source type for your data. A sandbox index lets your oblehends your configuration without impacting production indexes. You can always change this setting later. Learn More 12	dex						
	FAQ > How do Indexes work? > How do I know when to create or use multiple indexes?							

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.

splunk>enterprise Apps •		🛞 Administrator 🕶	5) Messages ▼ Settings ▼	Activity • Help •	Find Q
Add new Forwarding and receiving » Receive data » Add new					
	Configure receiving Set up this Splunk instance to receive data from forwarder(s).				
	Listen on this port * 514 For example, 9997 will receive data on TCP port 9997.				
		Cancel Save			

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



# **VOIP-500/VOIP-600 Series IP Call Stations**

Integration with Splunk Enterprise – Syslog Monitoring

c) Add a universal forwarder port of 9997.

splunk>enterprise Apps +			🔠 Administrator 🕶	🌀 Messages ▾ Settings ▾ Ac	ivity 🕶 Help 🕶 🛛 Find 🔍
Add new Forwarding and receiving > Receive data > Add new					
	Configure receiving				
	Set up this Splunk instance to receive	e data from forwarder(s).			
	Listen on this port "	9997			
		For example, 9997 will receive data on TCP port 9997.			
			Cancel Save		

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

splunk>enterprise Apps +		📵 Administrator 🕶	🌀 Messages 🔻	Settings 🔻	Activity -	Help 🕶 🛛 Find 🔍
Receive data Forwarding and receiving + Receive data						New Receiving Port
Showing 1-2 of 2 items filter Q						25 per page 🔻
Listen on this port \$	Status •			Actions		
514	Enabled   Disable			Delete		
9997	Enabled   Disable			Delete		



Page 9 of 16



## 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

splunk>enterprise App: Search & Reporting +	🔒 Administrator 🕶	🌀 Messages 🕶	Settings 🕶	Activity -	Help 🔻	Find	٩
Search Datasets Reports Alerts Dashboards					<b>&gt;</b> s	earch & R	eporting
New Search					Sa	ve As 🔻	Close
index = Talkaphone_VOIP						All time 🔻	Q

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:

ndex = Talkaphone	_VOIP host= <ip< th=""><th>_Address_o</th><th>of_Talkaphone_</th><th>_VOIP_device&gt;</th></ip<>	_Address_o	of_Talkaphone_	_VOIP_device>
-------------------	--	------------	----------------	---------------

splunk>enterprise App: Search & Reporting +	🔒 Administrator 🕶	🌀 Messages 🔻	Settings 🔻	Activity -	Help  Find  Q
Search Datasets Reports Alerts Dashboards					Search & Reporting
Search					
index= voip host=192.168.37.47					Last 24 hours 🔻 🔍
No Event Sampling 🕶					Smart Mode ▼

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.

splunk>enterprise App: Search & Reporting -		🔒 Administrator 🕶	🌀 Messages 🔻	Settings -	Activity -	Help 🔻	Find Q
Search Datasets Reports Alerts Dashboards						<b>&gt;</b> s	earch & Reporting
Search							
enter search here						Last	24 hours • Q
No Event Sampling 🕶							🕈 Smart Mode 🔻
How to Search If you are not familiar with the search features, or want to learn more, see one of the following resources.	What to Search Waiting for data						
Documentation 12 Tutorial 12	Data Summary						
<ul> <li>✓ Search History</li> <li>filter</li> <li>Q) No Time Filter ▼ 20 Per Page ▼</li> </ul>							
i Search 0				Actions	Last R	un ¢	
> index= voip failed to register				Add to Search	h 8 minu	ites ago	
> index = voip				Add to Search	h 14 min	utes ago	
> index= voip "Call Failed"				Add to Search	h Tue Ai	ug 07 2018	12:18:05
> index= voip "404"				Add to Search	h Tue Ai	ug 07 2018	12:17:37
> index= voip "Initiate Call"				Add to Search	h Tue Ai	ug 07 2018	12:07:58
> index= voip				Add to Search	h Tue Ar	ug 07 2018	10:58:12
> Index= volp host=192.168.37.47				Add to Search	h Tue Ai	ug 07 2018	10:55:14
> index=voip failed to Register				Add to Search	h Tue Ai	ug 07 2018	09:04:42
> Index="volp" "Failed to register"/timechart count by host				Add to Search	h Mon A	ug 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.

Email settings Server settings + Email settings Mall Server Settings Mall Server Settings Mall Server Settings Mall Nettings Mall Netti
Mail Server Settings         Mail host:       smtp.gmail.com.465         Set the host that sends mail for this Splunk instance.         Email security       one       Enable SSL       Enable TLS         Check with SMTP server admin. When SSL is enabled, mail host should include the port. IE:       Check with SMTP server. Leave empty for no authentication.         Username to use when authenticating with the SMTP server. Leave empty for no authentication.       The SMTP server. Leave empty for no authentication.
Mail Server Settings Mail Settings Ma
Mail host     smtg.gmail.com:465       Set the host that sends mail for this Splunk instance.       Email security     one       Emails security     Enable SSL       Check vith SMTP server admix. When SSL is enabled, mail host should include the port. IE:       Check vith SMTP server admix. When SSL is enabled, mail host should include the port. IE:       Username     [yoti.giananit@gmail.com]       Username to use when authenticating with the SMTP server. Leave empty for no authentication.
Set the host that sends mail for this Splunk instance.         Email security       one       Enable SSL       Enable TLS         Check with SMTP server admix. When SSL is enabled, mail host should include the port. IE:       State Sta
Email security O none Enable SSL O Enable TLS Check with SMTP server admix. When SSL is enabled, mail host should include the port. IE: strappaties.com 465 Username To use when authenticating with the SMTP server. Leave empty for no authentication.
Check vith SMTP server admix. When SSL is enabled, mail host should include the port. IE: smtp.spublick.com/465 Username to use when authenticating with the SMTP server. Leave empty for no authentication.
Username (yoti gianani@gmail.com) Username to use when authenticating with the SMTP server. Leave empty for no authentication.
Username to use when authenticating with the SMTP server. Leave empty for no authentication.
Password ******
Password to use when authenticating with the SMTP serves.
Confirm password
Email Format
Link hostname
Set a hostname for generating URLs in outgoing notifications. Enclose IPv6 addresses in square brackets (eg. (2001/db8:01), Leave empty to autodetect.
Send emails as Splunk Admin
Emailfooter' If you believe you've received this email in error, please see your Spluwk administrator.
splumk > the engine for machine data
rwr report setungs
Report Paper Sze Letter r

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.

splunk≻enterprise Apps -			📵 Administrator 🕶	🧿 Messages ▾	Settings •	Activity -	Help 🔻	Find Q
Searches, Reports, and Alerts Searches, reports, and alerts are saved searches created from pivot or the search page. Learn more 12							New Repor	New Alert
19 Searches, Reports, and Alerts Type: All  App: Search & Reporting (search)  Filter by Owner	r • filter Q						< Prev 1	10 per page ♥ 2 Next >
Name ¢	Actions 5	Next Scheduled Time ¢	Display View \$	Owner ¢	App ¢	Alerts ¢	Sharing ¢	Status ¢
\$host\$ is not reachable Alert if the VOIP-500 drops network connection for 5 mins.	Edit • Run 12 View Recent 12	2018-09-21 12:01:00 Central Daylight Time	none	admin	search	0	Арр	✓ Enabled
Errors in the last 24 hours	Edit 💌 Run 🖾	none	none	nobody	search	0	Арр	✓ Enabled
Errors in the last hour	Edit 🝷 Run 🖾	none	none	nobody	search	0	App	✓ Enabled
Host Activity by Time	Edit 🔻 Run 🗠	none	none	admin	search	0	Private	✓ Enabled
Host Failure	Edit 💌 Run 🖾 View Recent 🖾	2018-09-21 13:00:00 Central Daylight Time	none	admin	search	0	Private	✓ Enabled
Host Warning or Error Over Time	Edit ▼ Run 🖄	none	none	admin	search	0	Private	✓ Enabled
Host not reachable REALTIME- Alert if the VOIP 500 is not reachable on the network for more than 5 mins.	Edit 👻 Run 🖾 View Recent 🖄	2018-09-21 12:01:00 Central Daylight Time	none	admin	search	0	Global	✓ Enabled
Host not reachable - Every Minute Alert if the VOIP-500 is not reachable on the network for more than 5 mins. Run the search every minute.	Edit 🝷 Run 🖾	none	none	admin	search	0	Global	Disabled
Host not reachable - Every hour Alert if the VOIP-500 is not reachable on the network for more than 5 mins. Run the search every hour.	Edit 👻 Run 🖄	none	none	admin	search	0	Private	Disabled
License Usage Data Cube	Edit ▼ Run 12	none	none	nobody	search	0	App	✓ Enabled

Figure 15. Creating an alert -- Splunk Enterprise.



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

Edit Alert				×
Settings				<b>^</b>
Alert	Registration failures alert			- 1
Description	Alert if the <u>VOIP</u> -500 has lost SIP Registre	tion for	more than 1 minute.	
Search	index=voip failed to Register			
Alert type	Scheduled		Real-time	
	Run on (	Cron Sch	edule 🔻	
Time Range	La	st 7 days	•	
Cron Expression	*/1 * * * *			
	e.g. 00 18 *** (every day at 6PM). Learn More			
Trigger Conditions				_
Trigger alert when	Numb	er of Res	ults 🔻	
	is greater than 🔻	0		
Trigger	Once		For each result	
Throttle ?				
Trigger Actions				
	+ Add Actions 💌			
When triggered	<ul> <li>Add to Triggered Alerts</li> </ul>		Ren	nove 🝷
			Cancel	Save

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

Page 14 of 16



# **VOIP-500/VOIP-600 Series IP Call Stations**

Integration with Splunk Enterprise – Syslog Monitoring

mgger		Once		I OF Educities unit
Throttle ?				
Trigger Actions				
	+ 4	Add Actions 🔻		
When triggered	>	👃 Add to Trig	gered Alerts	Remov
	~	🔀 Send emai		Remove
		То	jmandalia@talkaphone.com	Comma separated list of emai addresses. Show CC and BCC
		Priority	Normal 🔻	
		Subject	VOIP-500 dropped SIP Registratio	The email subject, recipients and message can include
		Message	The 'Dropped SIP Registration' alert condition was triggered. The details of the event are as below.	tokens that insert text based of the results of the search. Learn More 🖸
		Include	<ul> <li>Link to Alert</li> <li>Link to Result</li> <li>Search String</li> <li>Inline Table</li> <li>Trigger</li> <li>Attach CSV</li> <li>Condition</li> </ul>	ilts e ▼
			Trigger Time Attach PDF	
		Туре	HTML & Plain Text Plain Text	





### 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

Edit Alert		
Settings		
Alert	Host not reachable - Every Minute	
Description	Alert if the VOIP-500 is not reachable on the search every minute.	ne network for more than 5 mins. Run the
Search	metadata index=voip type=hosts   ev *150)   sort age d   convert ctim	al age = now()-lastTime   where age > (2 e(lastTime)   fields age,host,lastTime
Alert type	Scheduled	Real-time
	Run on Cr	on Schedule 🔻
Time Range	Last	minute •
Cron Expression	*/1 * * * *	
Trigger Conditions	e.g. 00 18 *** (every day at 6PM). Learn More	
Trigger alert when	Number	of Results 🔻
	is greater than 💌	0
Trigger	Once	For each result
Throttle ?		
Trigger Actions		
	+ Add Actions 🔻	
		Cancel Save

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

Page 16 of 16

Copyright 2018 Talk-A-Phone, LLC • 7530 North Natchez Avenue • Niles, Illinois 60714 • Phone 773.539.1100 • info@talkaphone.com • www.talkaphone.com.

All prices and specifications are subject to change without notice. Talk-A-Phone, Talkaphone, Scream Alert, WEBS, and WEBS Contact are registered trademarks of Talk-A-Phone, LLC. All rights reserved. All other trademarks mentioned in this document or website are the property of their respective owners and does not imply or indicate any approval, endorsement, sponsorship, or affiliation with such owners unless such approval, endorsement, sponsorship, or affiliation is expressly indicated.