YOUR KEY TO INTERNET SECURITY

Installation Guide

Check Point Analytics App by QOS

Version: 1.0.4

Date: 15 March 2016

How to use Check Point Analytics App by QOS

There are two methods by which Splunk acquires Check Point logs.

Method 1:[Preferred Method]

It is assumed that you have successfully installed LEA client on Splunk Enterprise. If not, then please download and install the LEA client first before proceeding further.

Here is the link to download the app from Splunk App marketplace.

https://splunkbase.splunk.com/app/1454/

If you are looking for step by step documentation to install LEA client please check the link below.

https://qostechnology.wordpress.com/2015/04/29/integration-of-splunk-with-checkpoint-managementlog-server/

Alternately you can find more information from official page of OPSEC LEA at below mentioned link.

http://docs.splunk.com/Documentation/OPSEC-LEA

Method 2:[If your Splunk Running on Windows]

Many customers could not use our Analytics app as the basic requirement for running our App was LEA client which runs mainly on Linux Operating Systems.

Our Check Point App won Splunk Revolution award as Splunk Conf 2015 @ Las Vegas. This motivated us to develop a new Add-on for Splunk. This Add-on will receive Check Point Tracker logs in syslog format and convert the same into LEA format so that our Analytics App can run smoothly on Windows as well. There is another advantages of using this Add-on, Sending syslog to Splunk is less complicated compared to configuring LEA client. As syslogs are in clear text format please make sure your Splunk Enterprise and Check Point Management/Log server are placed in secure zone.

Here is the link to download Check Point Add-On.

https://splunkbase.splunk.com/app/2996/

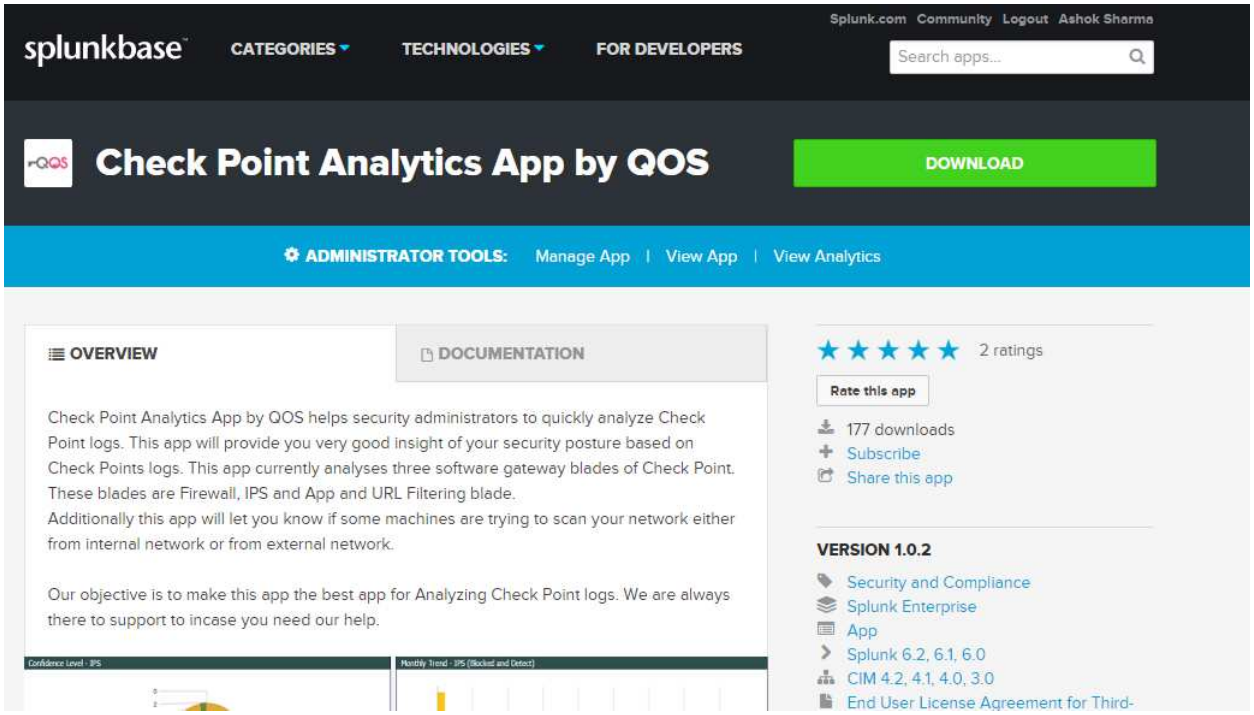
Check the link below to find step by step details to send Check Point logs through syslog.

https://qostechnology.wordpress.com/2015/12/28/how-to-send-check-point-tracker-logs-to-external-syslog-server/

Step-by-step guide to install and use Check Point Analytics App by QOS.

Here are the steps required to install Check Point Analytics App by QOS.

1. Down the App from https://splunkbase.splunk.com/app/2844/



splunkbase CATEGORIES ▾ TECHNOLOGIES ▾ FOR DEVELOPERS

Splunk.com Community Logout Ashok Sharma

Search apps...

Check Point Analytics App by QOS

DOWNLOAD

ADMINISTRATOR TOOLS: Manage App | View App | View Analytics

OVERVIEW DOCUMENTATION

Check Point Analytics App by QOS helps security administrators to quickly analyze Check Point logs. This app will provide you very good insight of your security posture based on Check Points logs. This app currently analyses three software gateway blades of Check Point. These blades are Firewall, IPS and App and URL Filtering blade.
Additionally this app will let you know if some machines are trying to scan your network either from internal network or from external network.

Our objective is to make this app the best app for Analyzing Check Point logs. We are always there to support to incase you need our help.

★★★★★ 2 ratings

Rate this app

177 downloads

Subscribe

Share this app

VERSION 1.0.2

Security and Compliance

Splunk Enterprise

App

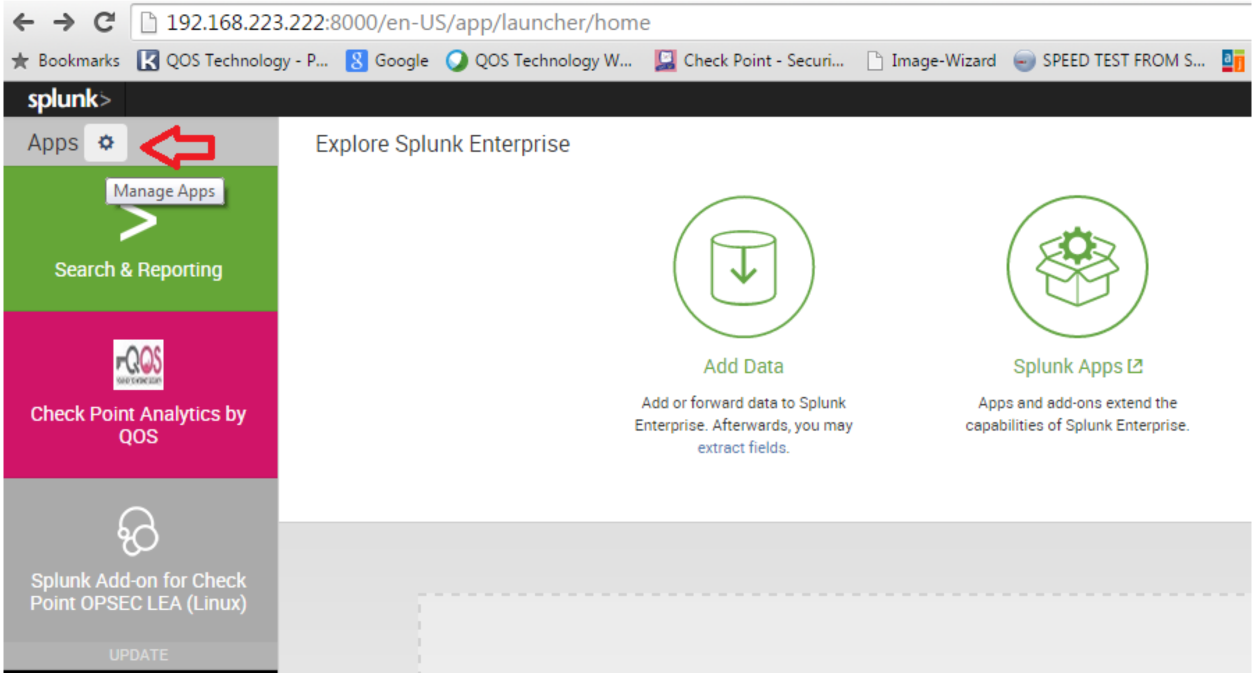
Splunk 6.2, 6.1, 6.0

CIM 4.2, 4.1, 4.0, 3.0

End User License Agreement for Third-

2. Now login to your Splunk Enterprise.

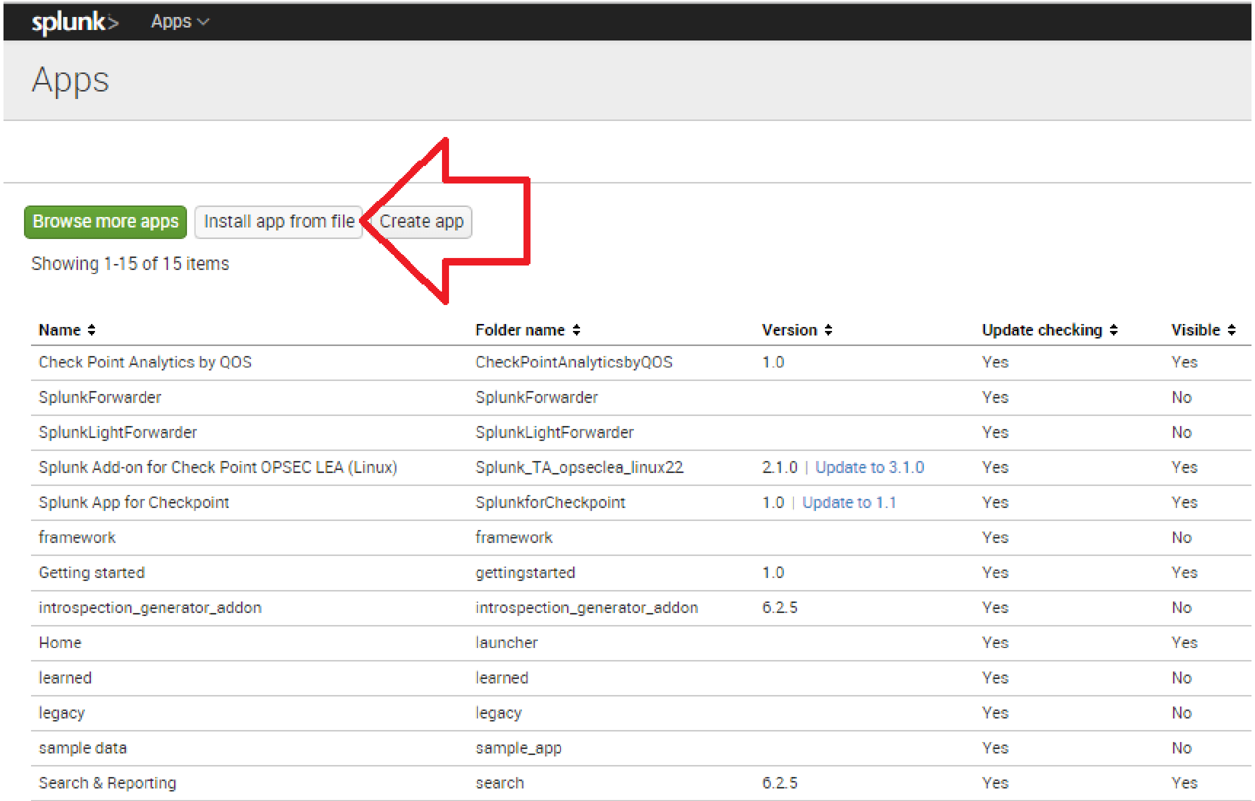
3. Click Manage App.



Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Apps and add-ons extend the capabilities of Splunk Enterprise.

4. Click "Install app from file".



Showing 1-15 of 15 items

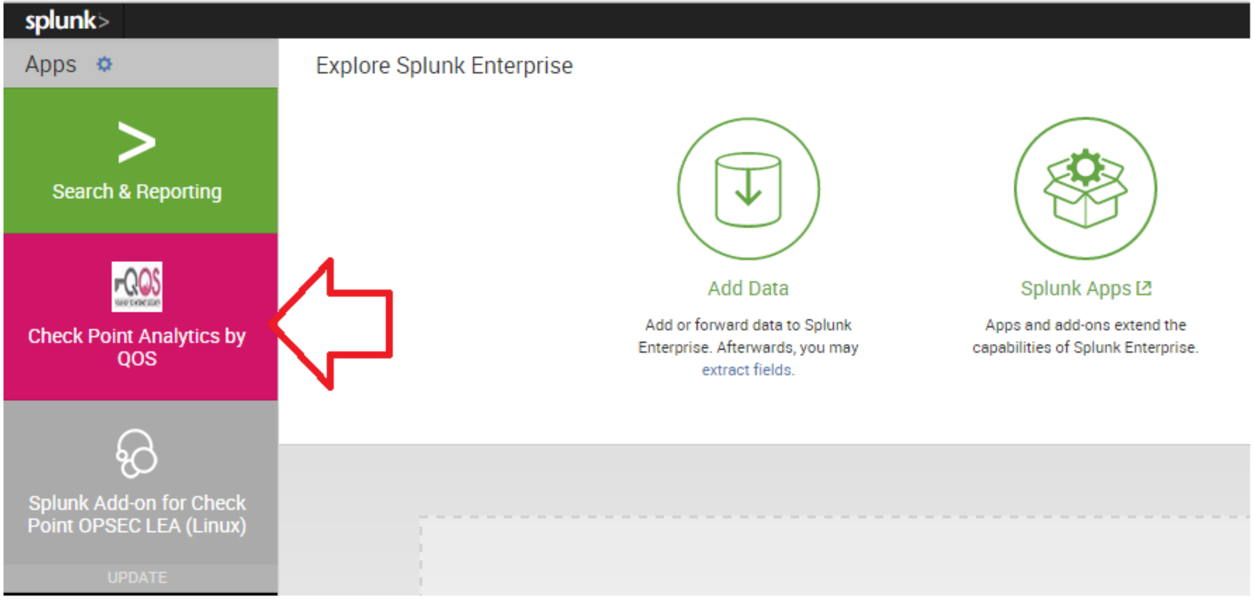
Name	Folder name	Version	Update checking	Visible
Check Point Analytics by QOS	CheckPointAnalyticsbyQOS	1.0	Yes	Yes
SplunkForwarder	SplunkForwarder		Yes	No
SplunkLightForwarder	SplunkLightForwarder		Yes	No
Splunk Add-on for Check Point OPSEC LEA (Linux)	Splunk_TA_opseclea_linux22	2.1.0 | Update to 3.1.0	Yes	Yes
Splunk App for Checkpoint	SplunkforCheckpoint	1.0 | Update to 1.1	Yes	Yes
framework	framework		Yes	No
Getting started	gettingstarted	1.0	Yes	Yes
introspection_generator_addon	introspection_generator_addon	6.2.5	Yes	No
Home	launcher		Yes	Yes
learned	learned		Yes	No
legacy	legacy		Yes	No
sample data	sample_app		Yes	No
Search & Reporting	search	6.2.5	Yes	Yes

5. Click on "Choose file" and select the Splunk app file which you have downloaded from https://splunkbase.splunk.com. File can be in tgz or spl format.
6. Now click upload.

7. You will be asked to restart the splunk. Click "Restart.

How to use Check Point Analytics App by QOS.

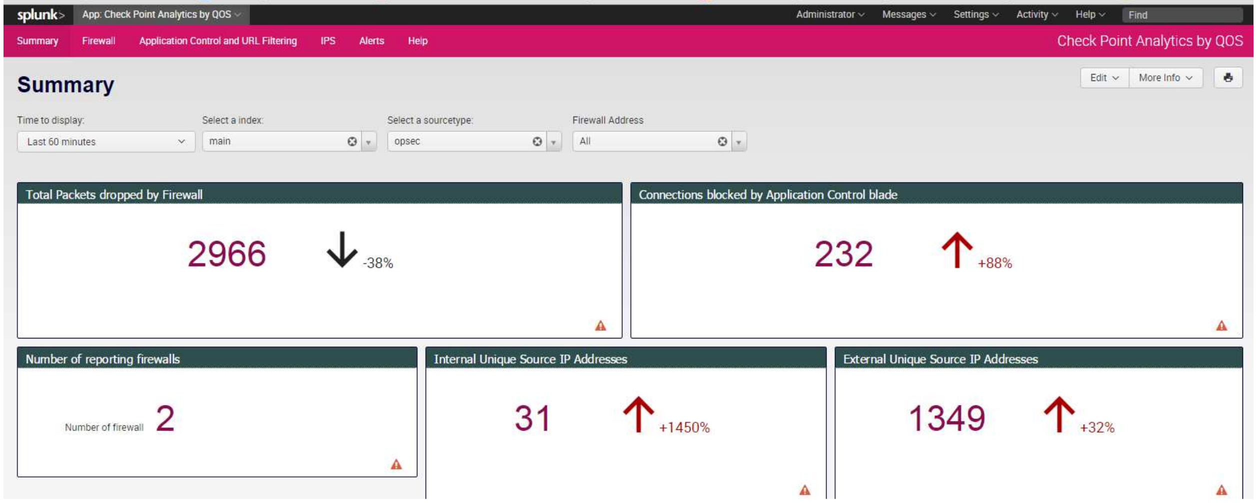
8. Click on Check Point Analytics App by QOS on left side of your Splunk server's home page.


splunk>
Apps
Search & Reporting
Check Point Analytics by QOS
Splunk Add-on for Check Point OPSEC LEA (Linux)
UPDATE
Explore Splunk Enterprise
Add Data
Splunk Apps

Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Apps and add-ons extend the capabilities of Splunk Enterprise.

9. Please note that this app assumes that you are using default settings for LEA. By default the index file used by LEA client is **main** and default sourcetype is **opsec.**


splunk>
App: Check Point Analytics by QOS
Administrator
Messages
Settings
Activity
Help
Find
Summary
Firewall
Application Control and URL Filtering
IPS
Alerts
Help
Check Point Analytics by QOS
Edit
More Info

Summary

Time to display: Last 60 minutes

Select a index: main

Select a sourcetype: opsec

Firewall Address: All

Total Packets dropped by Firewall: 2966 ↓ -38%

Connections blocked by Application Control blade: 232 ↑ +88%

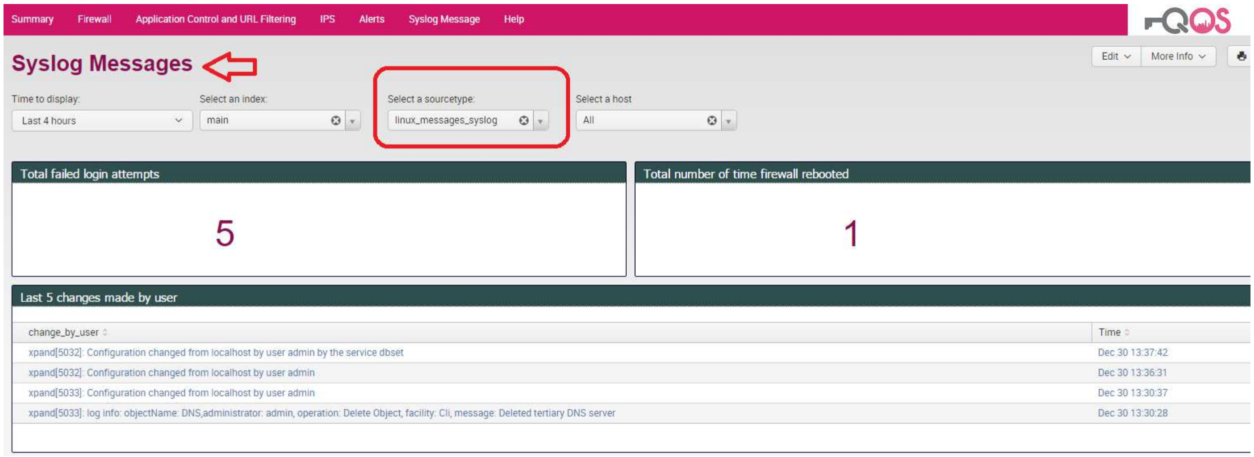
Number of reporting firewalls: Number of firewall 2

Internal Unique Source IP Addresses: 31 ↑ +1450%

External Unique Source IP Addresses: 1349 ↑ +32%

10. This version uses three Check Point blades. These are Firewall, IPS and App and URL Filtering blade.
11. As per your setup you can choose the appropriate index and sourcetype from drill down provided on top of this app. Remember your default setting says index = main, sourcetype = opsec.

12. With the new feature (Check Point Gaia syslog) which we have added in this release you need to modify the sourcetype under syslog section.



Syslog Messages

Time to display: Last 4 hours

Select an index: main

Select a sourcetype: linux_messages_syslog

Select a host: All

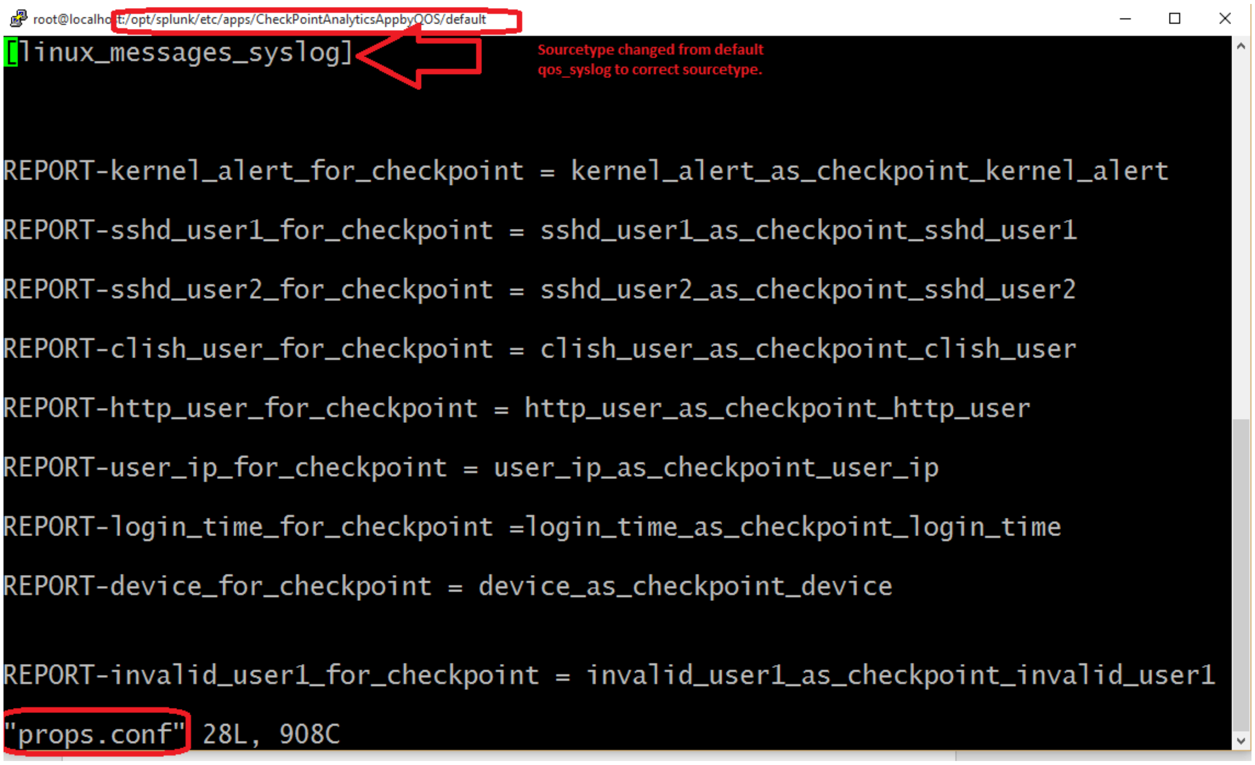
Total failed login attempts: 5

Total number of time firewall rebooted: 1

Last 5 changes made by user

change_by_user	Time
xpand[5032]: Configuration changed from localhost by user admin by the service dbset	Dec 30 13:37:42
xpand[5032]: Configuration changed from localhost by user admin	Dec 30 13:36:31
xpand[5033]: Configuration changed from localhost by user admin	Dec 30 13:30:37
xpand[5033]: log info: objectName: DNS,administrator: admin, operation: Delete Object, facility: Cli, message: Deleted tertiary DNS server	Dec 30 13:30:28

13. In order to analyze the syslog messages correctly you need to send syslog messages from Check Point management server and gateways (Gaia OS only) to Splunk on syslog UDP-514 port. In case you are already accepting syslog messages then you can skip step 14.
14. This can be achieved by creating a new data input. Click Settings-> Data Input -> Local inputs (UDP) -> Add new.
15. Now whatever sourcetype name you are going to create in step 13, you need to mention the same in /opt/splunk/etc/apps/CheckPointAnalyticsAppbyQOS/default/props.conf
16. By default we have given a temporary sourcetype = qos_syslog.
17. Change the temporary sourcetype once you have successfully installed this app. No need to restart Splunk after making changes to props.conf as suggested in step 13-14.


root@localhost:/opt/splunk/etc/apps/CheckPointAnalyticsAppbyQOS/default

Sourcetype changed from default qos_syslog to correct sourcetype.

```
[linux_messages_syslog]


REPORT-kernel_alert_for_checkpoint = kernel_alert_as_checkpoint_kernel_alert

REPORT-sshd_user1_for_checkpoint = sshd_user1_as_checkpoint_sshd_user1

REPORT-sshd_user2_for_checkpoint = sshd_user2_as_checkpoint_sshd_user2

REPORT-clish_user_for_checkpoint = clish_user_as_checkpoint_clish_user

REPORT-http_user_for_checkpoint = http_user_as_checkpoint_http_user

REPORT-user_ip_for_checkpoint = user_ip_as_checkpoint_user_ip

REPORT-login_time_for_checkpoint =login_time_as_checkpoint_login_time

REPORT-device_for_checkpoint = device_as_checkpoint_device


REPORT-invalid_user1_for_checkpoint = invalid_user1_as_checkpoint_invalid_user1

"props.conf" 28L, 908C
```

18. If you have any feedback and need support please do not hesitate to reach us **splunk@qos.co.in** and we promise to get back to you in less than 48 hrs.