Installation Guide

Check Point Analytics App by QOS

Version: 1.0

Date: 20 Aug 2015

http://qostechnology.in
splunk@qos.co.in

How to use Check Point Analytics App by QOS

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.

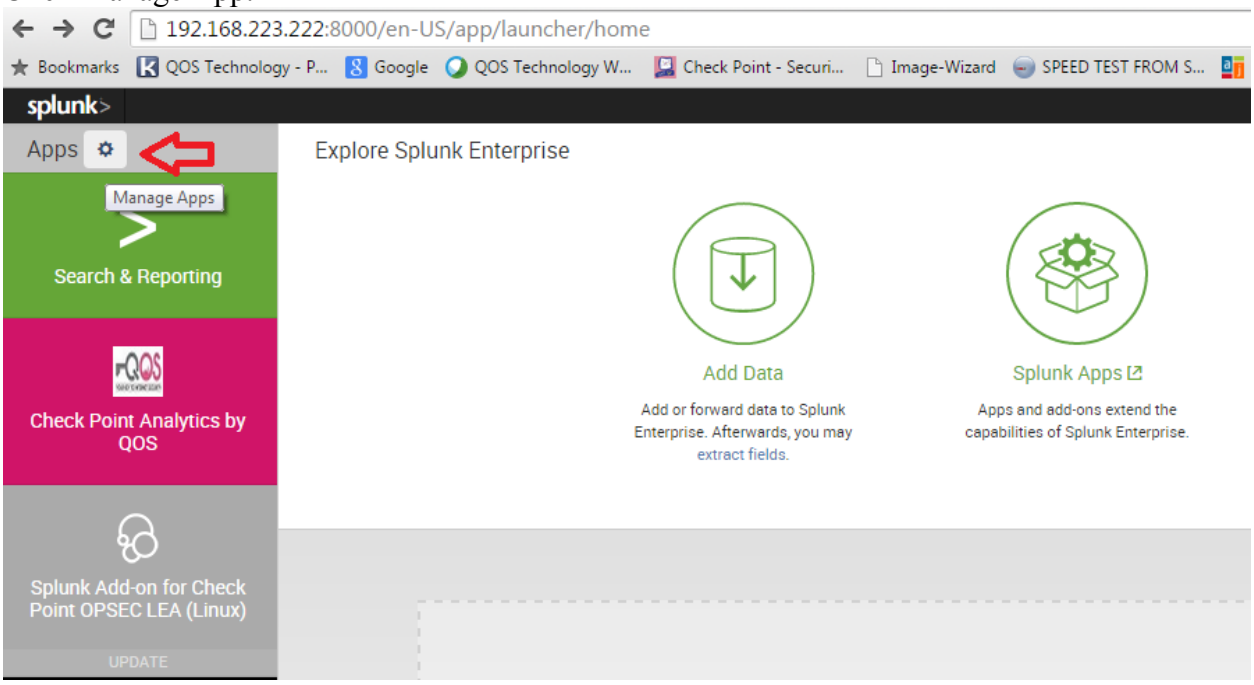
http://docs.splunk.com/Documentation/OPSEC-LEA

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

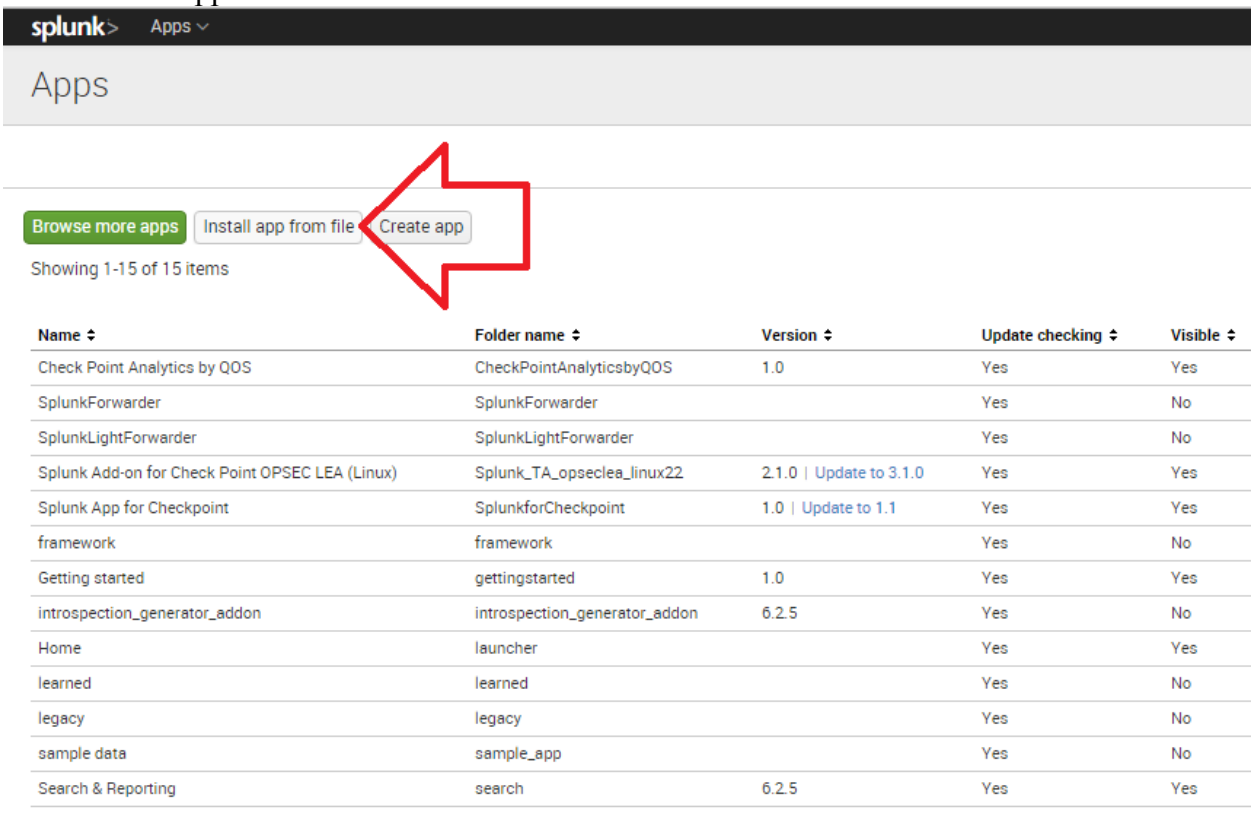
Here are the steps required to install Check Point Analytics App by QOS.

1. Down the App from https://splunkbase.splunk.com
2. Now login to your Splunk Enterprise.

3. Click Manage App.



4. Click "Install app from file".



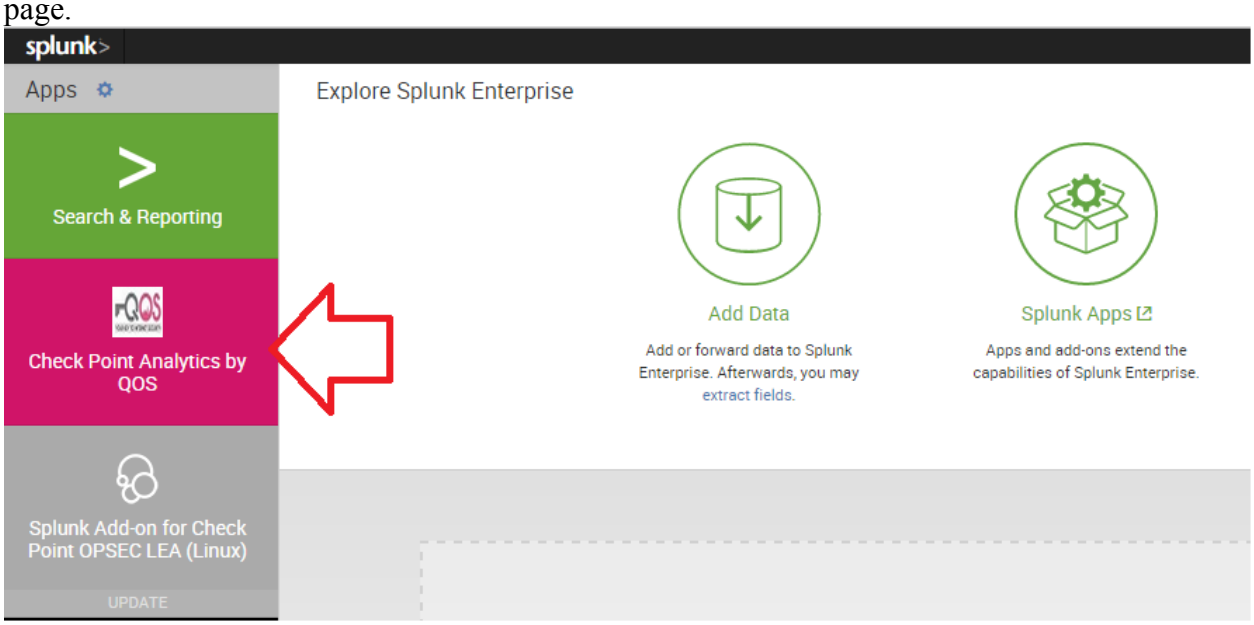
Name	Folder name	Version	Update checking	Visible
Check Point Analytics by QOS	CheckPointAnalyticsbyQOS	1.0	Yes	Yes
SplunkForwarder	SplunkForwarder		Yes	No
SplunkLightForwarder	SplunkLightForwarder		Yes	No
Splunk Add-on for Check Point OPSEC LEA (Linux)	Splunk_TA_opseclea_linux22	2.1.0 | Update to 3.1.0	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.

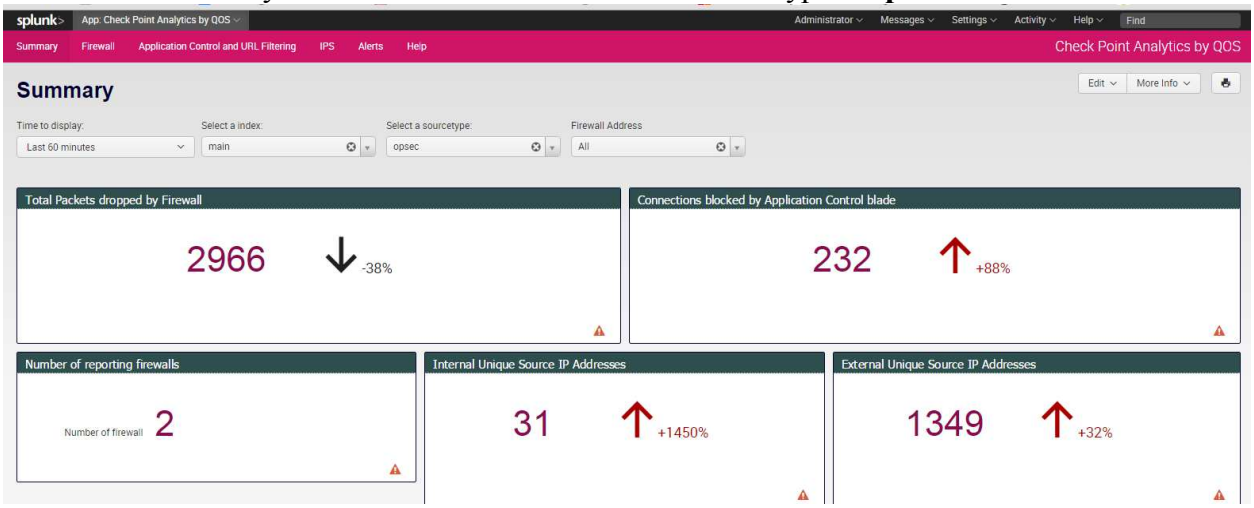
7. You will be asked to restart the splunk. Click "Restart.

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.



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.**



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 places on top of this app.
12. 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.