**Installation Steps for Splunk**

Below are the steps connection between SplunkIndexer and Splunk forwarder

* I am using Splunk Indexer and Splunk Searchehad as same componenet in
* Download the latest Enterprise tar file which will act as Splunk indexer and searchhead.
* Execute the command below to extract the tar file

[root@d3d855989802 splunk]# tar xvzf splunk-7.1.3-51d9cac7b837-Linux-x86\_64.tgz -C /opt/splunk

* To start splunk in your terminal

splunk/bin/splunk start --accept-license

* To enable splunk at boot time

[root@d3d855989802 splunk]# splunk/bin/splunk enable boot-start

* check the splunk is enable or not

[root@d3d855989802 splunk]# ls -lrt /etc/init.d/splunk

-rwx------. 1 root root 995 Oct 27 00:21 /etc/init.d/splunk

**Installation of Universal forwarder**

* Download the executable for splunk forwarder from splunk site (**Note:** *splunk Enterprise is used for indexer , searchhead, Deployment server, ect. there is different executable for splunk forwarder*)
* Execute the below command in other box for universal forwarder

tar xvzf splunkforwarder-7.2.0-8c86330ac18-Linux-x86\_64.tgz -C /opt/splunk

[root@39aa82e63c03 splunkforwarder]# ls -lrt

total 128

-r--r--r--. 1 10777 10777 63711 Sep 28 17:04 license-eula.txt

-r--r--r--. 1 10777 10777 57 Sep 28 17:04 copyright.txt

-r--r--r--. 1 10777 10777 846 Sep 28 17:07 README-splunk.txt

drwxr-xr-x. 3 10777 10777 41 Sep 28 17:30 share

drwxr-xr-x. 3 10777 10777 58 Sep 28 17:30 openssl

drwxr-xr-x. 2 10777 10777 27 Sep 28 17:30 include

-rw-r--r--. 1 10777 10777 0 Sep 28 17:30 ftr

drwxr-xr-x. 13 10777 10777 4096 Sep 28 17:30 etc

drwxr-xr-x. 5 10777 10777 4096 Sep 28 18:00 lib

drwxr-xr-x. 3 10777 10777 4096 Sep 28 18:00 bin

-r--r--r--. 1 10777 10777 40974 Sep 28 18:00 splunkforwarder-7.2.0-8c86330ac18-linux-2.6-x86\_64-manifest

[root@39aa82e63c03 splunkforwarder]# pwd

/opt/splunk/splunkforwarder

* Accept the lience while starting the splunk forwarder

[root@39aa82e63c03 splunkforwarder]# bin/splunk start --accept-license

* Create a new app . Create the below directory under
* SPLUNK\_HOME/etc/app/
* <testapp>/local/input.conf (This file contains possible settings you can use to configure inputs,distributed inputs such as forwarders, and file system monitoring in inputs.conf.)

Add the stanza in the input.conf file

[monitor:///opt/IBM/middleware/user\_projects/domains/Test/servers/ITM\_server\*/logs/\*(.out|.log)\*]

index=app

sourcetype=IBM:AUT:TAM

blacklist = (\.(tar|gz|bz2|tar.gz|tgz|tbz|tbz2|zip|z)$)

* Configure the universal forwarder to connect to a receiving indexer by the below command. BY default it listen to 9777 port. So we can configure with 9777 on it

[root@39aa82e63c03 bin]# ./splunk add forward-server 172.17.0.2:9997

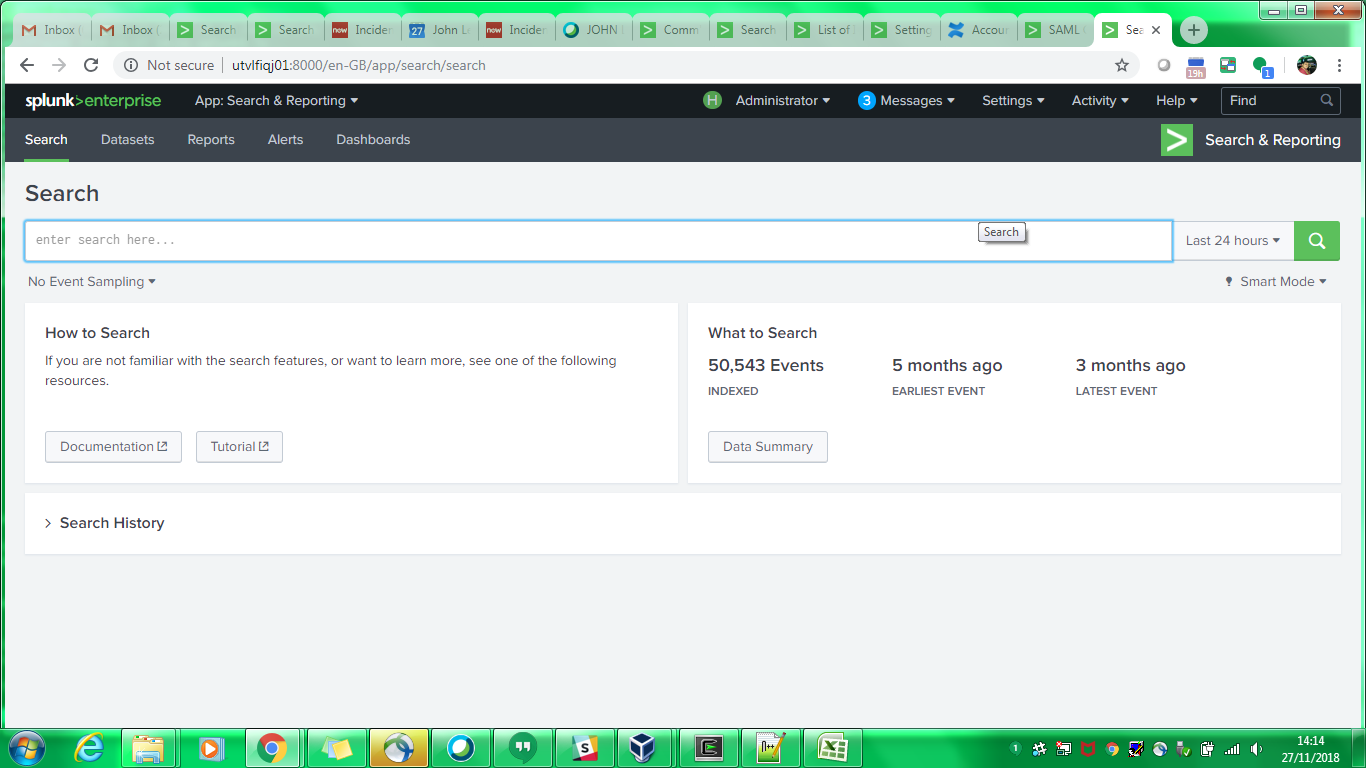
Splunk username: <splunkforwarder\_username>

Password:

Added forwarding to: 172.17.0.2:9997.

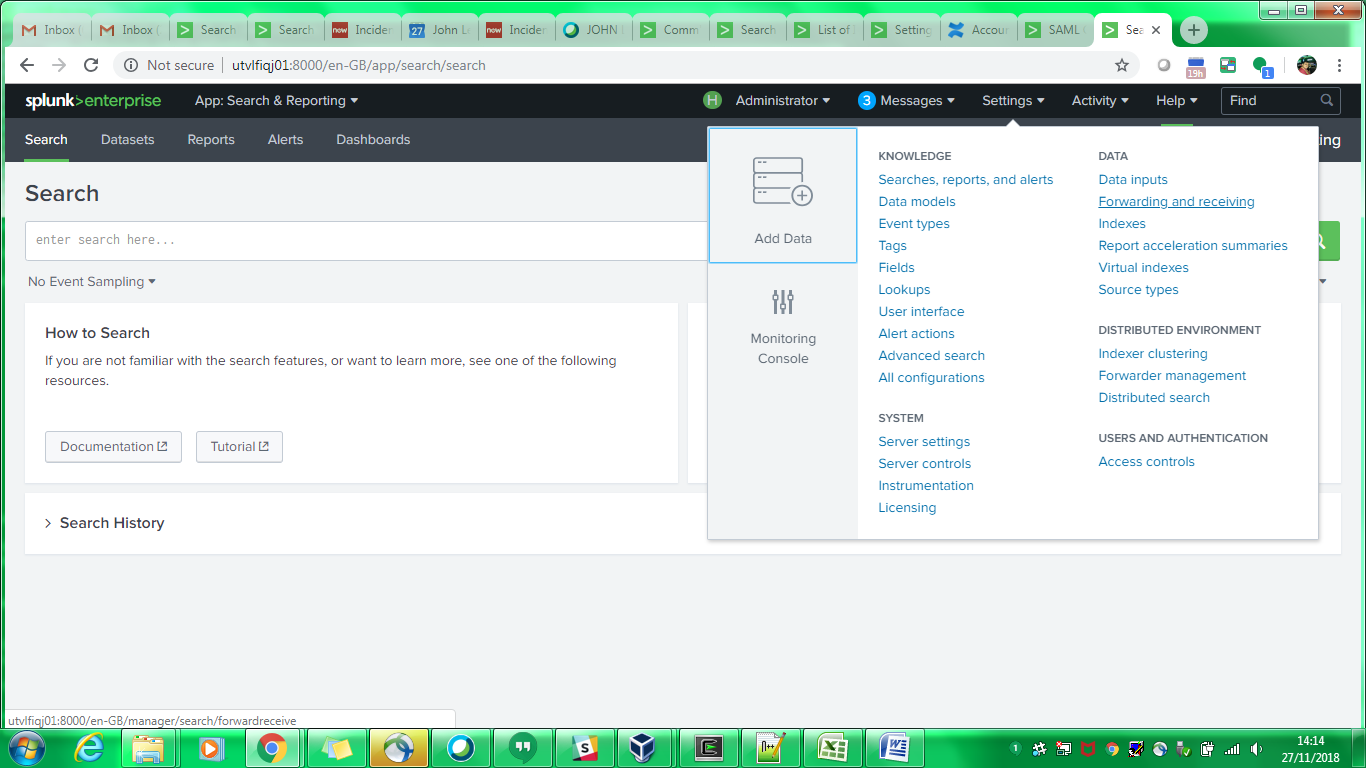
**Configure the port at the Indexer side**

* Configure the port at Splunk Enterprise at Indexer from GUI. Below are the steps
* Open the Splunk Enterprise Dashboard.



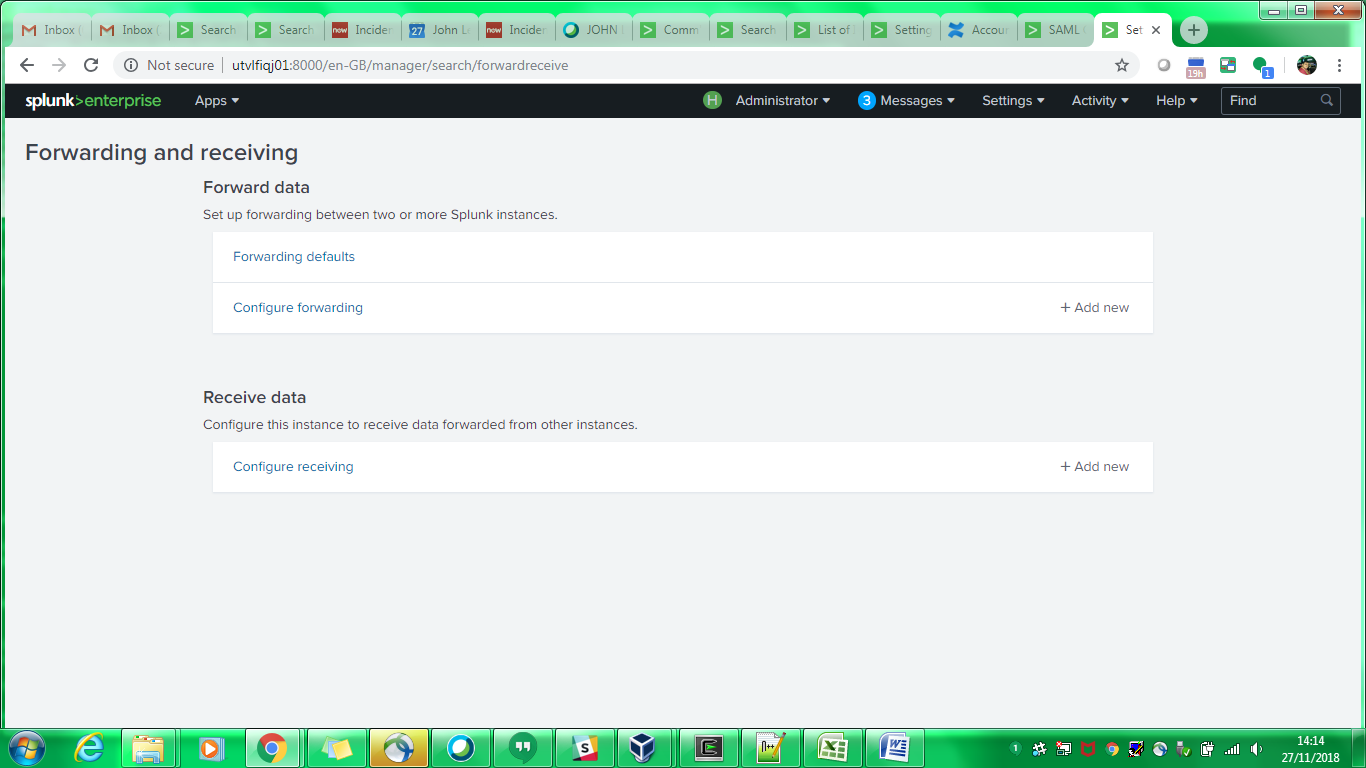
*Fig. 1*

* Click on the “**Setting** > **Forwarding and receiving**” as shown in below Fig.2



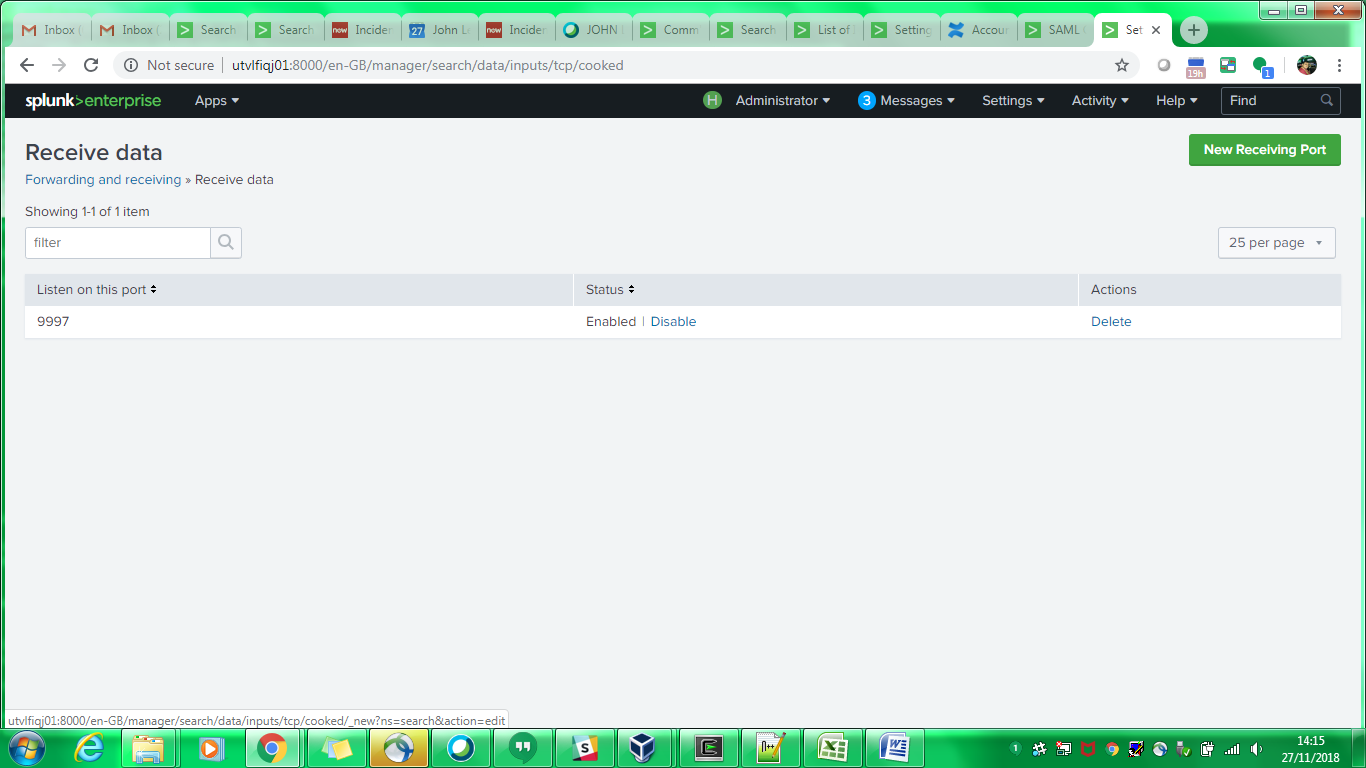
*Fig. 2*

* You will be reverted to Forwarding and receiving page and you have to Click the “**Configure receiving**”

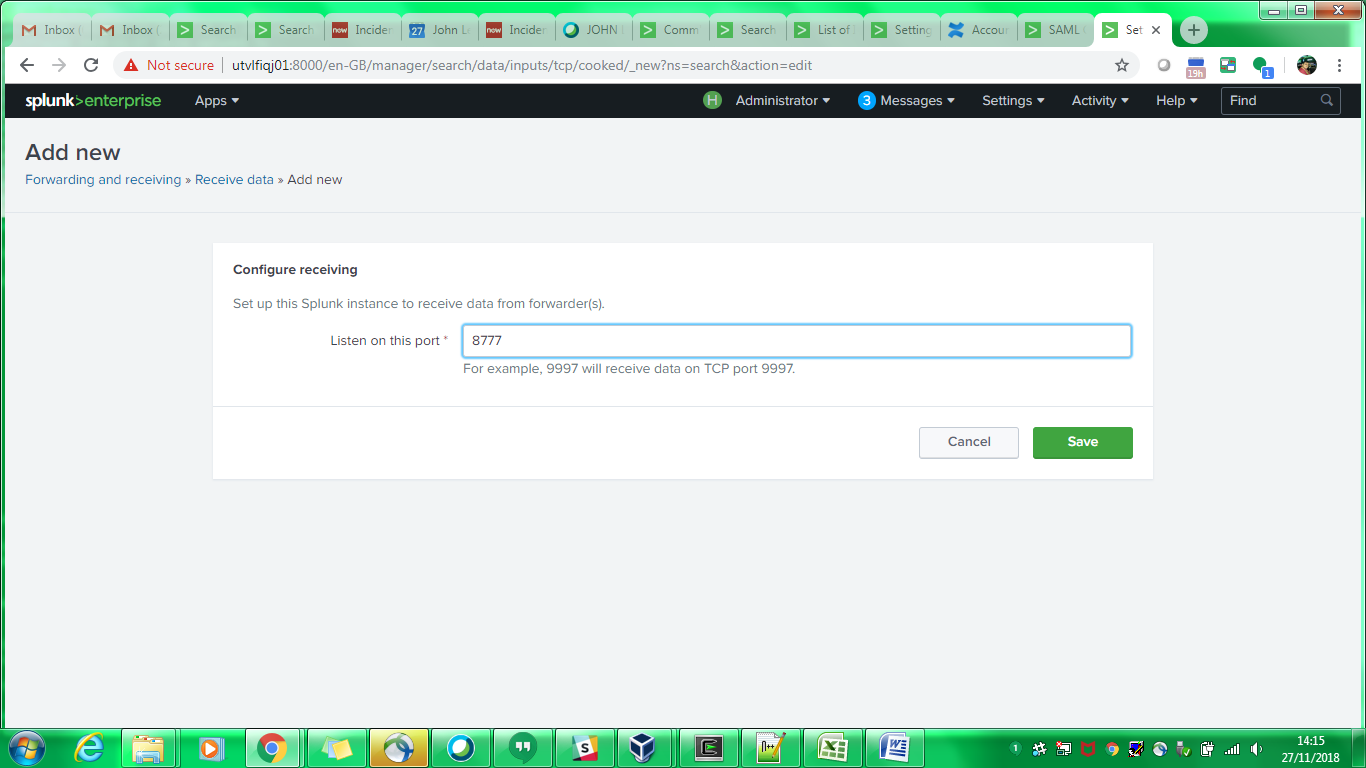


*Fig. 3*

* After Clicking the option you will be landed to below page and Click “**New Receiving Port**” to configure with port that will communicate with Splunk forwarder. Below are Figs that show how to configure the port. (By default 9997 can be configure)



*Fig. 4*



*Fig. 5*