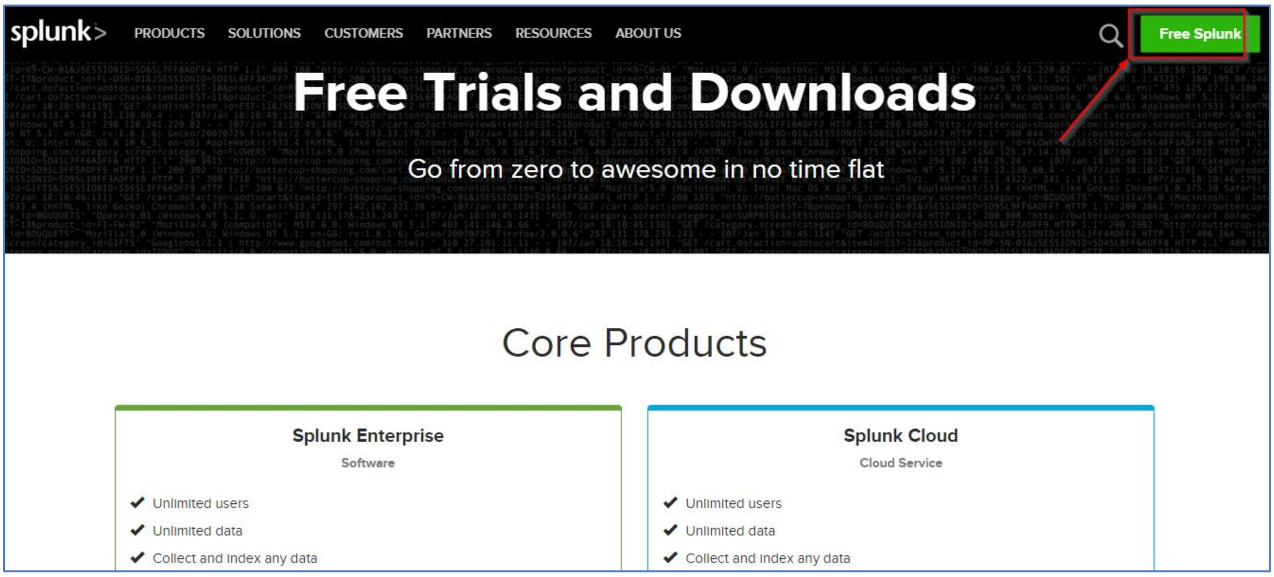
Splunk Installation Guide for LINUX

Installation Guide

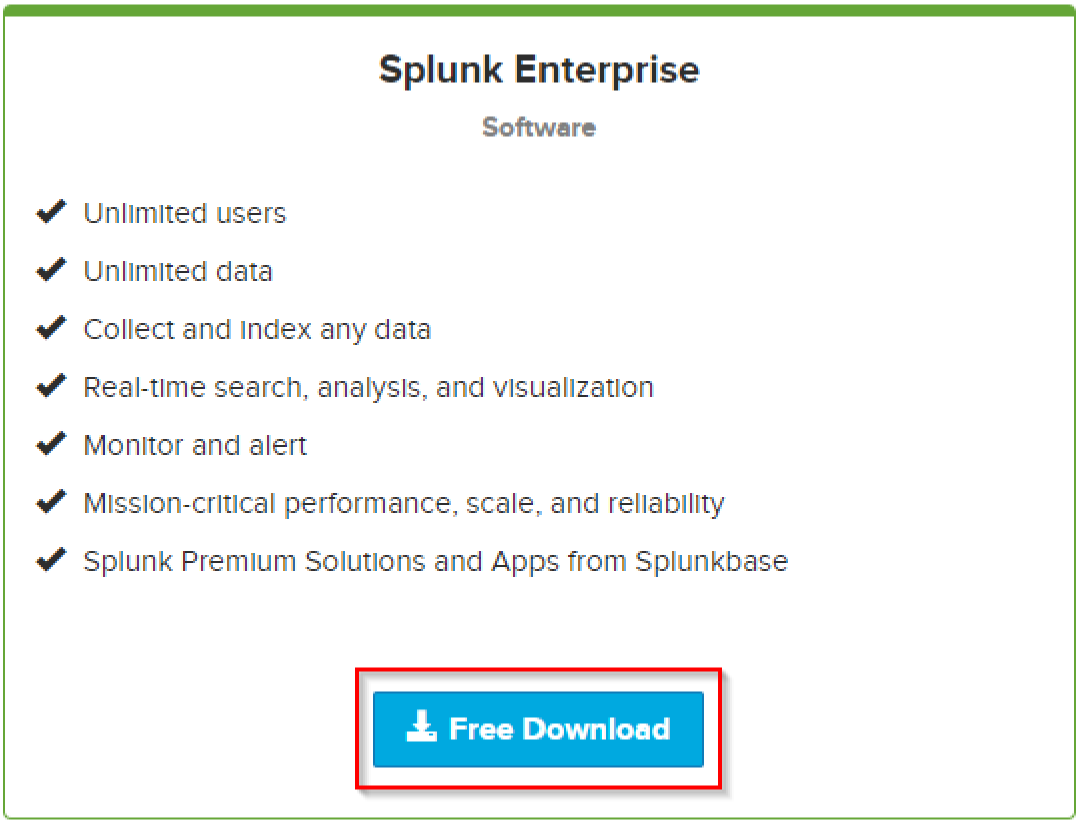
edureka!

Splunk Installation Guide for LINUX

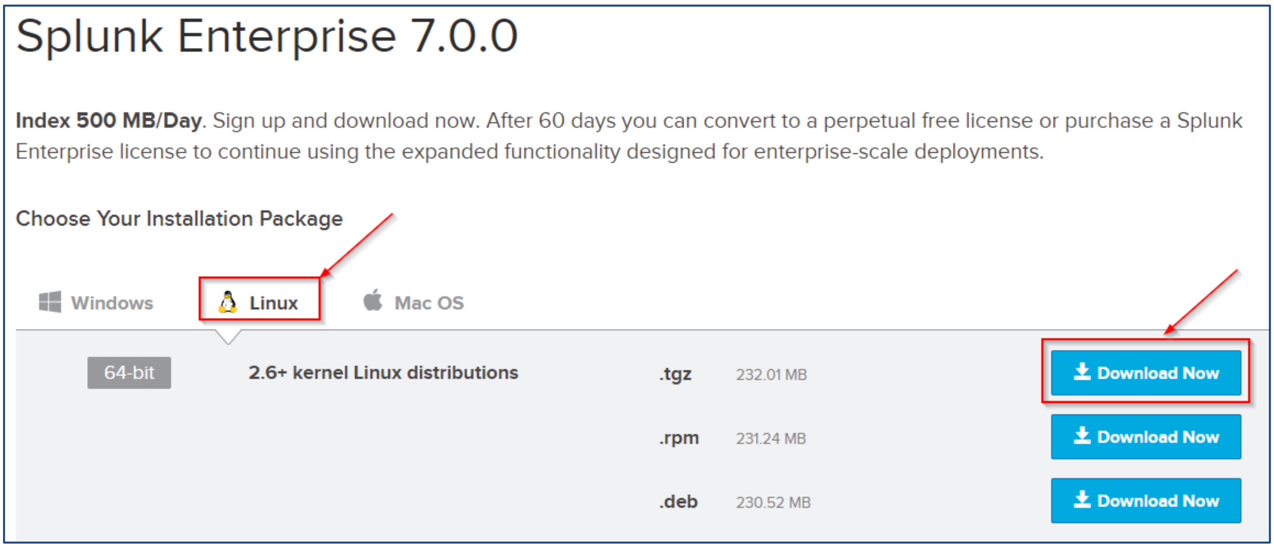
Step 1: Go to this link and create the Splunk account: https://www.splunk.com/en_us/download.html



Step 2: Click on "Free Download"


Splunk Enterprise
Software
✓ Unlimited users
✓ Unlimited data
✓ Collect and index any data
✓ Real-time search, analysis, and visualization
✓ Monitor and alert
✓ Mission-critical performance, scale, and reliability
✓ Splunk Premium Solutions and Apps from Splunkbase
Free Download

Step 3: Select "Linux" and click "Download now" for .tgz, which is a Tar file.



Splunk Enterprise 7.0.0

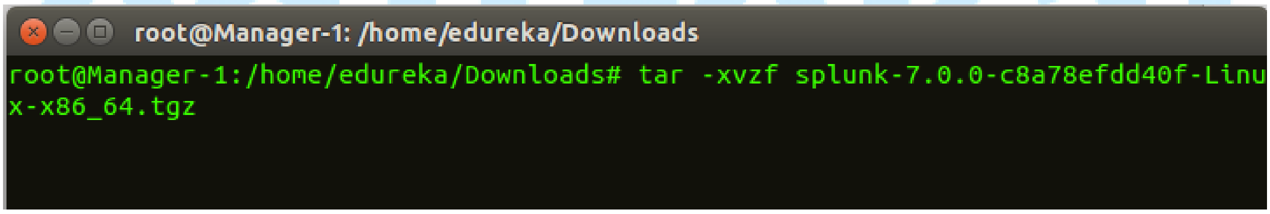
Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package

64-bit	2.6+ kernel Linux distributions	.tgz	232.01 MB	Download Now
		.rpm	231.24 MB	Download Now
		.deb	230.52 MB	Download Now

Step 4: Now from the terminal, run the following command to extract the Tar file:-

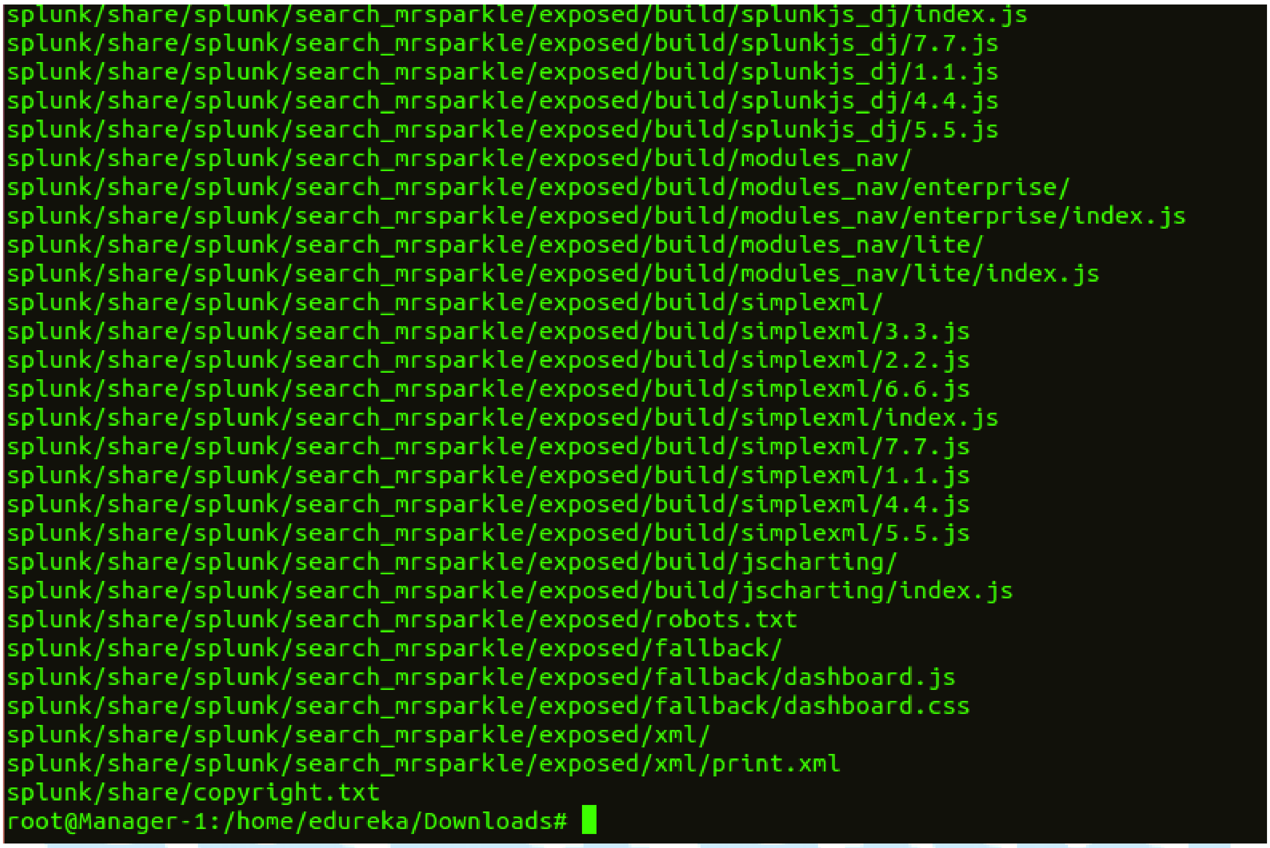
tar -xvzf 'filename.tgz'



root@Manager-1: /home/edureka/Downloads

```
root@Manager-1:/home/edureka/Downloads# tar -xvzf splunk-7.0.0-c8a78efdd40f-Linu
x-x86_64.tgz
```

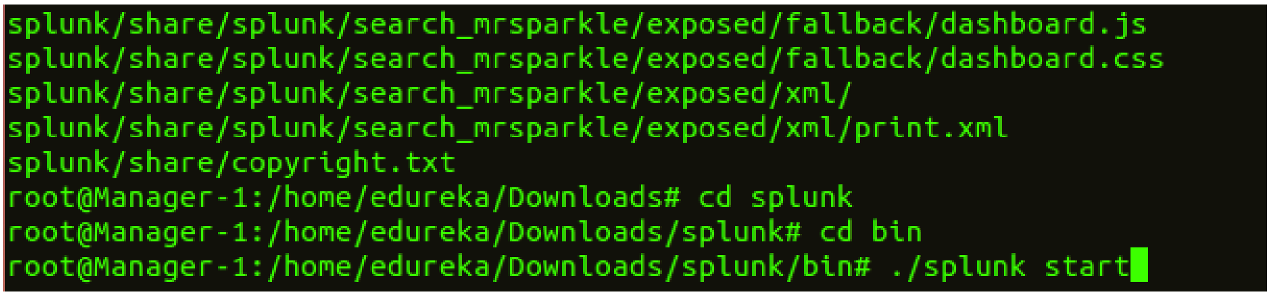
Step 5: The following contents will be extracted:



```
splunk/share/splunk/search_mrsparkle/exposed/build/splunkjs_dj/index.js
splunk/share/splunk/search_mrsparkle/exposed/build/splunkjs_dj/7.7.js
splunk/share/splunk/search_mrsparkle/exposed/build/splunkjs_dj/1.1.js
splunk/share/splunk/search_mrsparkle/exposed/build/splunkjs_dj/4.4.js
splunk/share/splunk/search_mrsparkle/exposed/build/splunkjs_dj/5.5.js
splunk/share/splunk/search_mrsparkle/exposed/build/modules_nav/
splunk/share/splunk/search_mrsparkle/exposed/build/modules_nav/enterprise/
splunk/share/splunk/search_mrsparkle/exposed/build/modules_nav/enterprise/index.js
splunk/share/splunk/search_mrsparkle/exposed/build/modules_nav/lite/
splunk/share/splunk/search_mrsparkle/exposed/build/modules_nav/lite/index.js
splunk/share/splunk/search_mrsparkle/exposed/build/simplexml/
splunk/share/splunk/search_mrsparkle/exposed/build/simplexml/3.3.js
splunk/share/splunk/search_mrsparkle/exposed/build/simplexml/2.2.js
splunk/share/splunk/search_mrsparkle/exposed/build/simplexml/6.6.js
splunk/share/splunk/search_mrsparkle/exposed/build/simplexml/index.js
splunk/share/splunk/search_mrsparkle/exposed/build/simplexml/7.7.js
splunk/share/splunk/search_mrsparkle/exposed/build/simplexml/1.1.js
splunk/share/splunk/search_mrsparkle/exposed/build/simplexml/4.4.js
splunk/share/splunk/search_mrsparkle/exposed/build/simplexml/5.5.js
splunk/share/splunk/search_mrsparkle/exposed/build/jscharting/
splunk/share/splunk/search_mrsparkle/exposed/build/jscharting/index.js
splunk/share/splunk/search_mrsparkle/exposed/robots.txt
splunk/share/splunk/search_mrsparkle/exposed/fallback/
splunk/share/splunk/search_mrsparkle/exposed/fallback/dashboard.js
splunk/share/splunk/search_mrsparkle/exposed/fallback/dashboard.css
splunk/share/splunk/search_mrsparkle/exposed/xml/
splunk/share/splunk/search_mrsparkle/exposed/xml/print.xml
splunk/share/copyright.txt
root@Manager-1:/home/edureka/Downloads# 
```

Step 6: The files would have been extracted under a new Directory called splunk. We should use the command ***cd splunk*** to enter that directory and then again use ***cd bin*** to enter the bin directory.

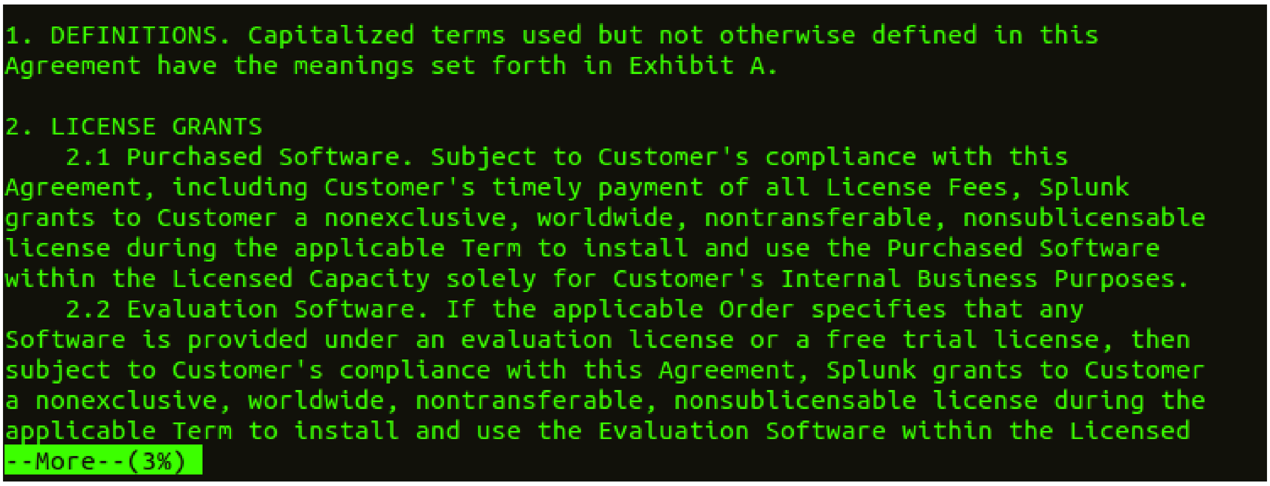
We can start the Splunk service now by giving the command ***./splunk start***



```
splunk/share/splunk/search_mrsparkle/exposed/fallback/dashboard.js
splunk/share/splunk/search_mrsparkle/exposed/fallback/dashboard.css
splunk/share/splunk/search_mrsparkle/exposed/xml/
splunk/share/splunk/search_mrsparkle/exposed/xml/print.xml
splunk/share/copyright.txt
root@Manager-1:/home/edureka/Downloads# cd splunk
root@Manager-1:/home/edureka/Downloads/splunk# cd bin
root@Manager-1:/home/edureka/Downloads/splunk/bin# ./splunk start
```

It will then ask to agree to the software license agreement as shown:

Click on enter.

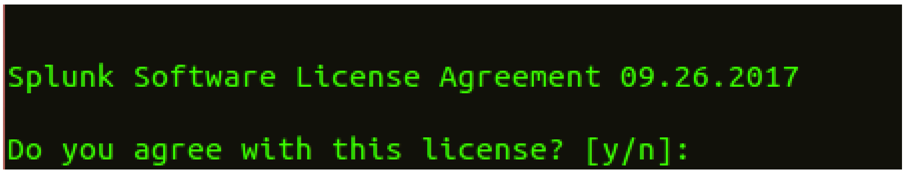


```
1. DEFINITIONS. Capitalized terms used but not otherwise defined in this
Agreement have the meanings set forth in Exhibit A.

2. LICENSE GRANTS
    2.1 Purchased Software. Subject to Customer's compliance with this
Agreement, including Customer's timely payment of all License Fees, Splunk
grants to Customer a nonexclusive, worldwide, nontransferable, nonsublicensable
license during the applicable Term to install and use the Purchased Software
within the Licensed Capacity solely for Customer's Internal Business Purposes.
    2.2 Evaluation Software. If the applicable Order specifies that any
Software is provided under an evaluation license or a free trial license, then
subject to Customer's compliance with this Agreement, Splunk grants to Customer
a nonexclusive, worldwide, nontransferable, nonsublicensable license during the
applicable Term to install and use the Evaluation Software within the Licensed
--More--(3%)
```

Click on Enter.

Step 7: Next, Click on ‘y’ for agreeing to the terms.

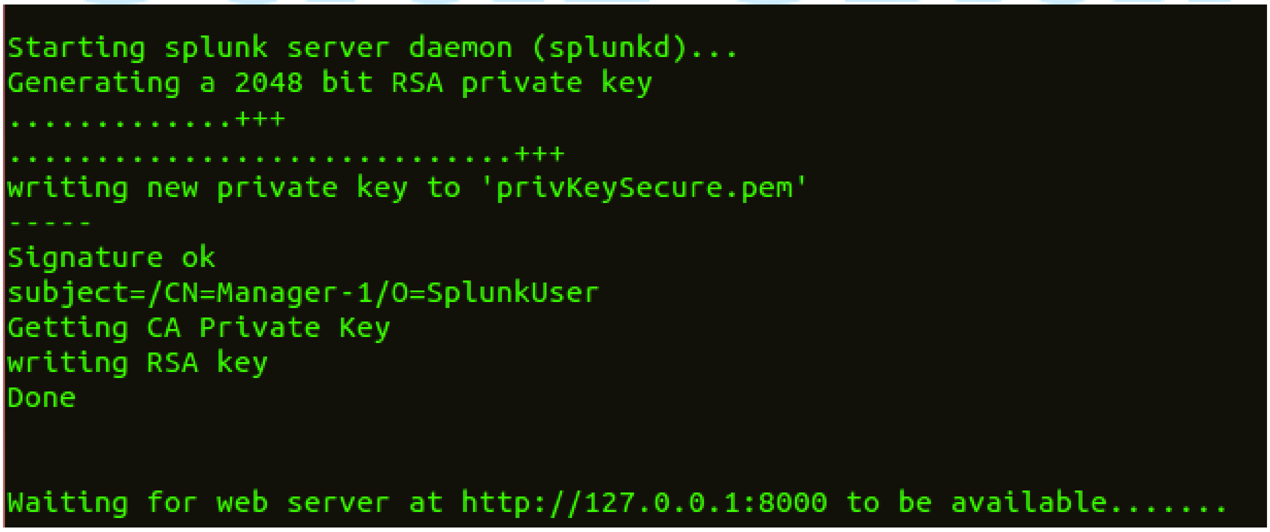


```

Splunk Software License Agreement 09.26.2017

Do you agree with this license? [y/n]:
```

Splunk will be installed successfully as shown below:

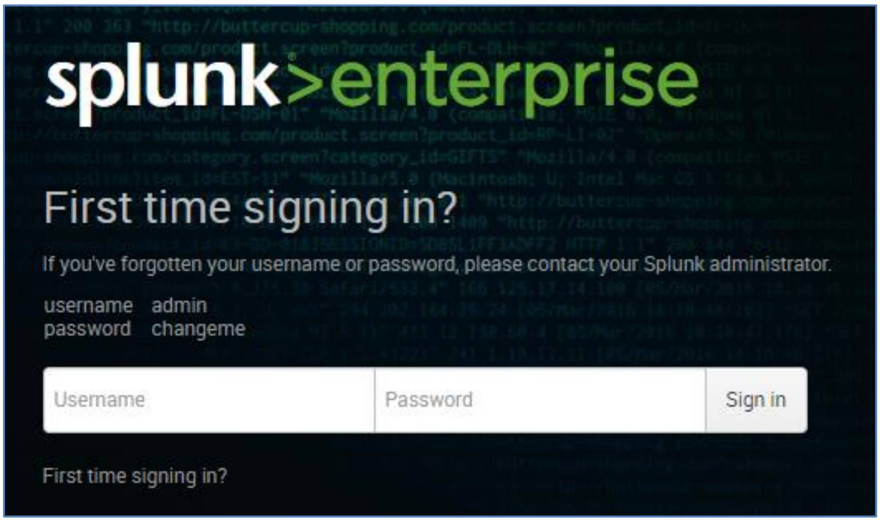


```
Starting splunk server daemon (splunkd)...
Generating a 2048 bit RSA private key
.............+++
...............................+++
writing new private key to 'privKeySecure.pem'
-----
Signature ok
subject=/CN=Manager-1/O=SplunkUser
Getting CA Private Key
writing RSA key
Done


Waiting for web server at http://127.0.0.1:8000 to be available.......
```

The Splunk web interface is at http://localhost:8000. This is the port number, when this is displayed it is indication that connection is established. You will then automatically get connected to the Default Web.

Step 8: Enter the user name as “admin” and password as “changeme” and click on “Sign in”

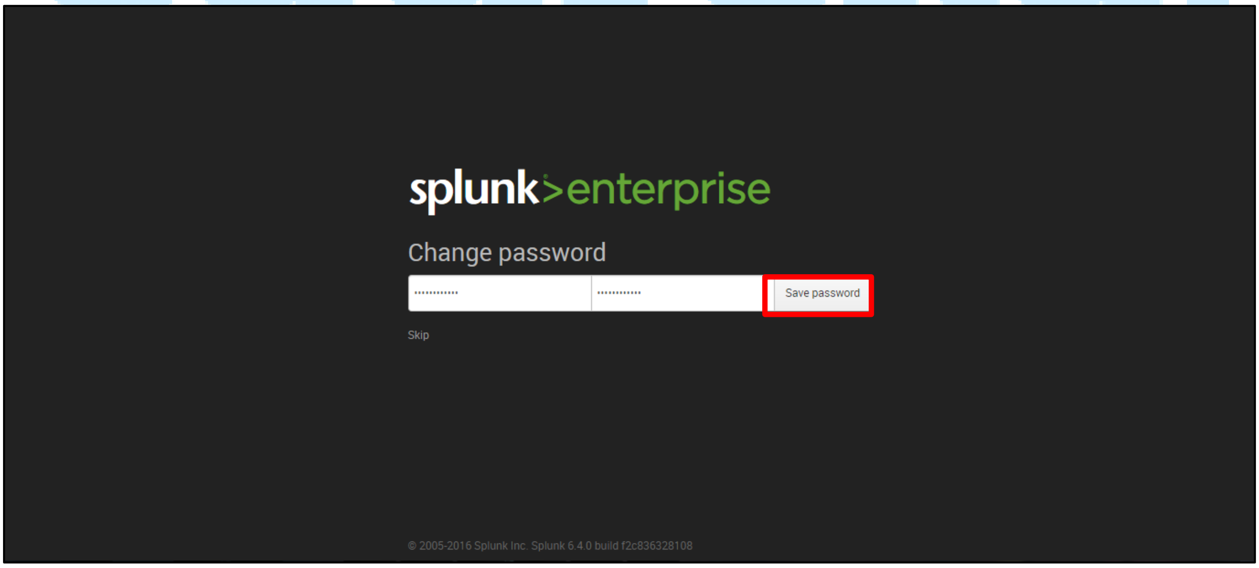


First time signing in?

If you've forgotten your username or password, please contact your Splunk administrator.

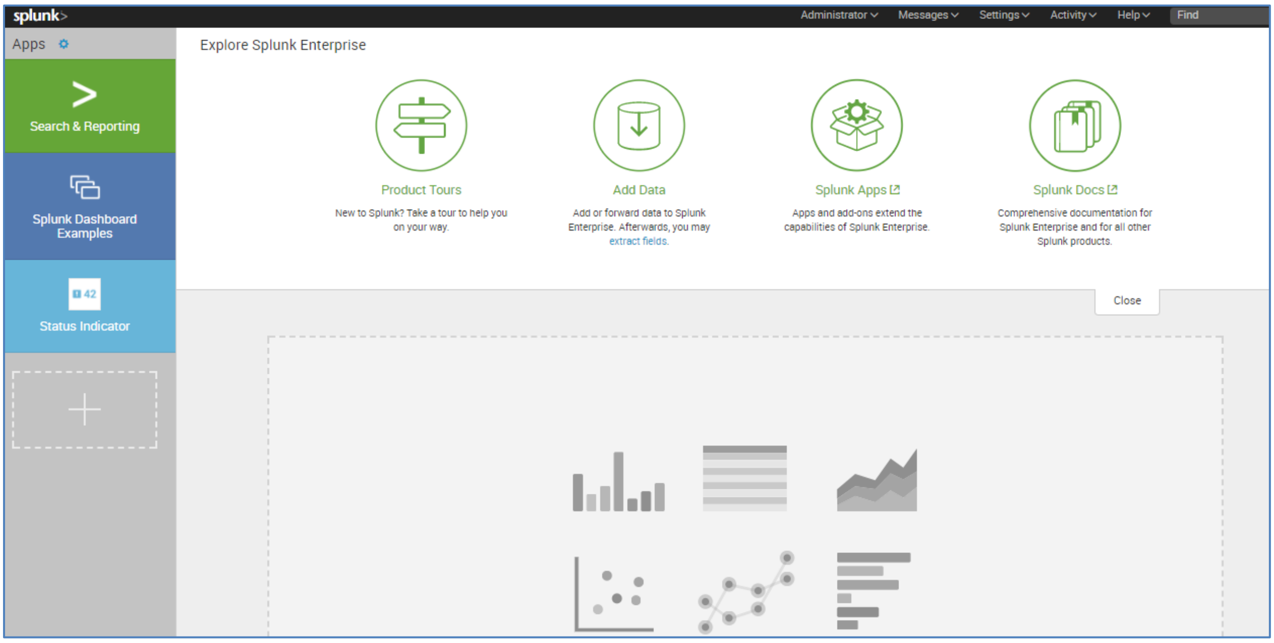
username admin
password changeme

Step 9: Now change your password and click on “Save password”



© 2005-2016 Splunk Inc. Splunk 6.4.0 build f2c836328108

Step 10: Now your Splunk tool is ready to use.



New to Splunk? Take a tour to help you on your way.

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

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

Comprehensive documentation for Splunk Enterprise and for all other Splunk products.

CONGRATULATIONS! *Your Splunk is installed.*