

Registration for .conf25 is open! Join us in Boston September 8–11. | Register now >

splunk>
a CISCO company

Platform ▾Security ▾Observability ▾Industries ▾Resources ▾

QSupport ▾GLog In


Trials & Downloads

Free trials and downloads

Splunk Cloud Platform

See the power of the Splunk Platform in a Splunk-hosted cloud environment and get fast insights. Try up to 5GB of data/day for 14 days, no credit card required.

Get My Free TrialView Product



Start your cloud platform trial

Already have a Splunk account? [Log In >](#)

Business Email

Password

First Name

Last Name

- login with account
- go to products and select free trial

Choose Your Installation Package

Windows **Linux** Mac OS

64-bit

3.x+, 4.x+, or 5.4.x kernel Linux distributions

Package Format	Size	Action
.tgz	577.34 MB	Download Now
.deb	448.87 MB	Download Now
.rpm	577.46 MB	Download Now

[Release Notes](#) | [System Requirements](#) | [Previous Releases](#) | [All Other Downloads](#)

When download will complete go to the terminal in ubuntu.

- ❖ Shift it super user

To run a command as administrator (user "root"), use "sudo <command>". See "man sudo_root" for details.

```
admin@osboxes:~$ sudo su
[sudo] password for admin:
root@osboxes:/home/admin#
```

- ❖ Go to Download folders using the command
`cd /home/<your username>/Downloads`
- ❖ Then use command to see which files and folders have in that folder

Ls

```
root@osboxes: /home/admin/Downloads
root@osboxes:/home/admin# cd /home/admin/Downloads/
root@osboxes:/home/admin/Downloads# ls
splunk-9.0.5-e9494146ae5c-Linux-x86_64.tgz
root@osboxes:/home/admin/Downloads#
```

- ❖ So now unzip the file using the following command

`tar -xvzf <download file name>`

```
root@osboxes:/home/admin/Downloads# ls
splunk-9.0.5-e9494146ae5c-Linux-x86_64.tgz
root@osboxes:/home/admin/Downloads# tar -xvzf splunk-9.0.5-e9494146ae5c-Linux-x86_64.tgz
```

When it unzip you see other folder their name splunk, do the following steps

- ❖ Go to that folder

`cd splunk`

- ❖ See what have in that folder

`ls`

- ❖ Go to bin folder

`cd bin`

- ❖ See what have in bin folder with ls command

```
root@osboxes:/home/admin/Downloads/splunk/bin
root@osboxes:/home/admin/Downloads# ls
splunk splunk-9.0.5-e9494146ae5c-Linux-x86_64.tgz
root@osboxes:/home/admin/Downloads# cd splunk
root@osboxes:/home/admin/Downloads/splunk# ls
bin          openssl
copyright.txt  quarantined_files
etc          README-splunk.txt
ftr         share
include     splunk-9.0.5-e9494146ae5c-linux-2.6-x86_64-manifest
lib         swidtag
license-eula.txt
root@osboxes:/home/admin/Downloads/splunk# cd bin/
root@osboxes:/home/admin/Downloads/splunk/bin#
```

- ❖ Run the following commands to start the installation

`./splunk start`

```
root@osboxes: /home/admin/Downloads/splunk/bin
root@osboxes: /home/admin/Downloads/splunk/bin# ./splunk start
```

- ❖ Use space bar key to read out the lisencc that show after it
- ❖ At end write **y** to accept the lisencc

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

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise,
you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.
```

- ❖ Then login using username and password

```
Splunk software must create an administrator account during startup. Otherwise,
you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: admin
Password must contain at least:
  * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Copying '/home/admin/Downloads/splunk/etc/openldap/ldap.conf.default' to '/home/
```

- ❖ At end it will show link go to that link and login graphically
- ❖ Else write your machine ip address and port number like 8000 in browser and then splunk open graphically

```
Splunk software must create an administrator account during startup. Otherwise,
you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: admin
Password must contain at least:
  * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Copying '/home/admin/Downloads/splunk/etc/openldap/ldap.conf.default' to '/home/
```

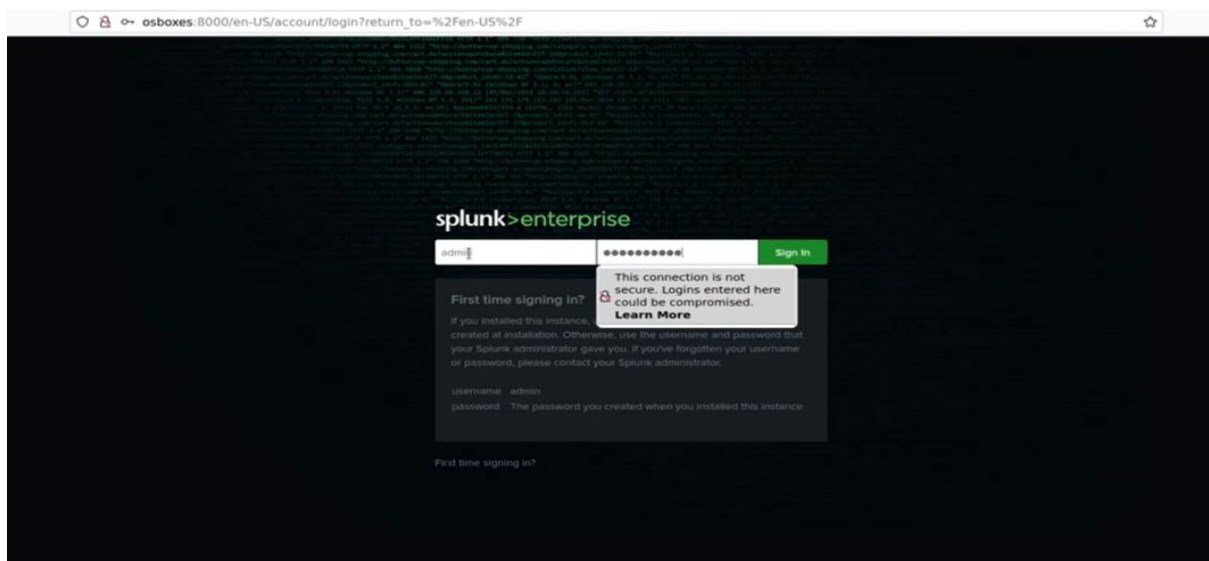
```
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done

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

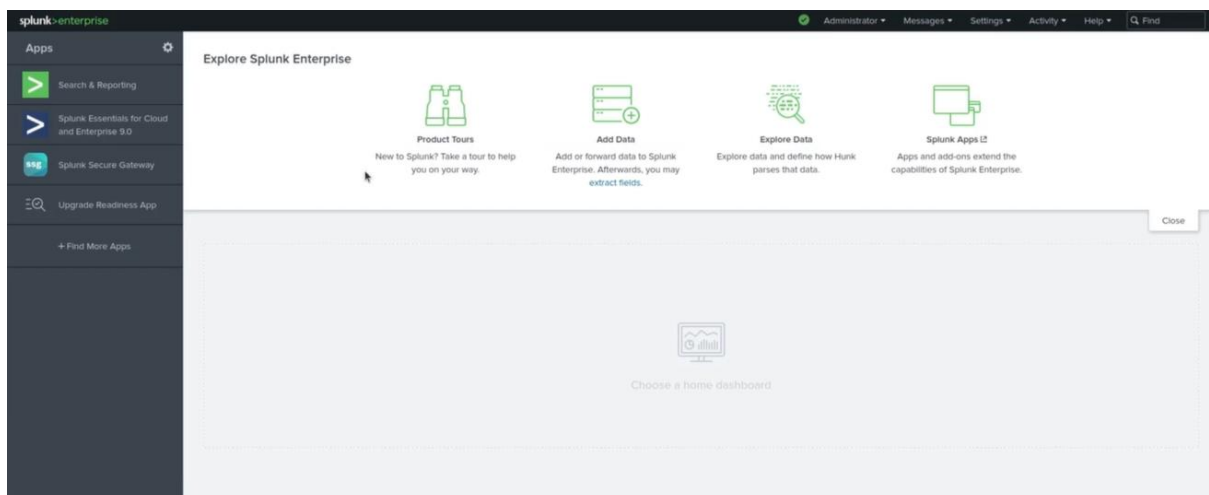
If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com/

The Splunk web interface is at http://osboxes:8000
```

❖ login



Splunk interface



Note: when you shutdown the machine splunk also shutdown. You can repeat the process to open it. Go to `/bin` directory of splunk and run command `./splunk start`. then login.