# Splunk install for linux

By: Ryan Stewart

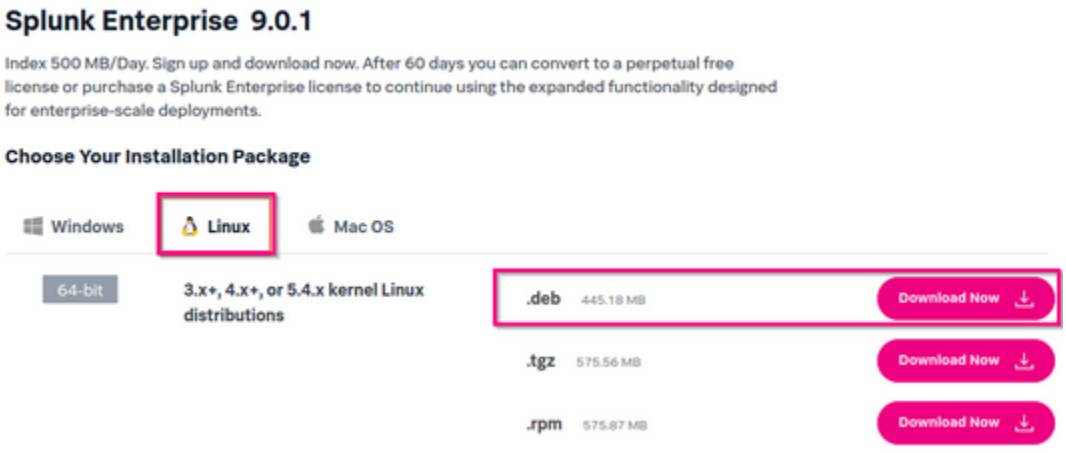
In this section, I'll guide you through installing Splunk on an Ubuntu 22.04 Desktop computer. While these instructions are tailored for **Ubuntu**, they can be adapted for other distributions and server environments.

## Installation via GUI:

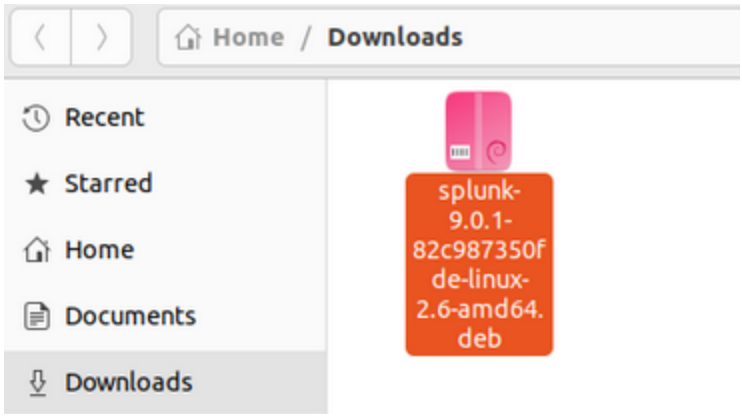
1. Go to the Splunk Site.

2. Create an account.

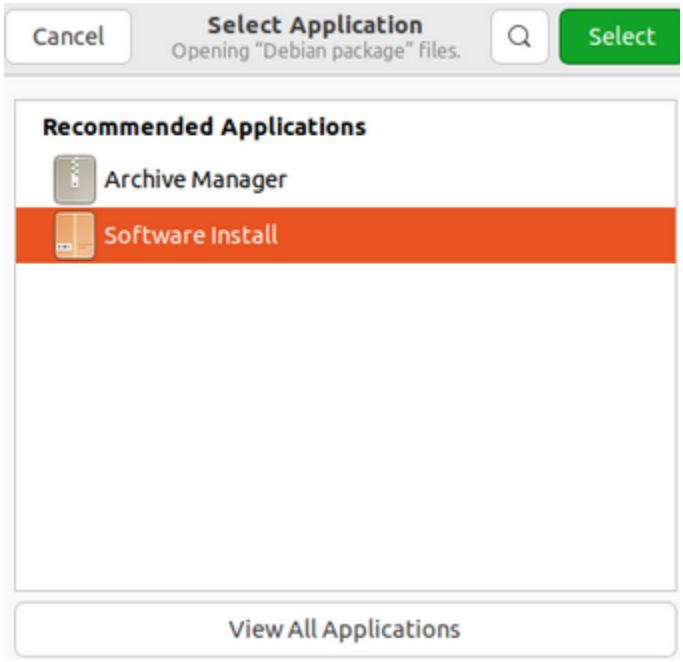
3. Download the .deb file.



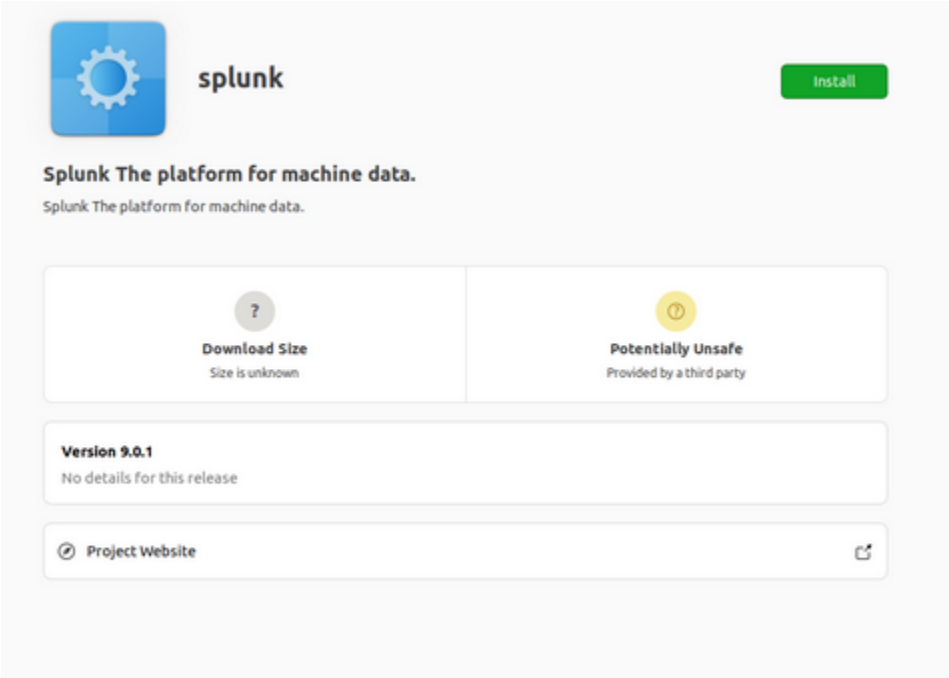

4. Navigate to your Downloads folder.




5. Right-click on the downloaded file > Open with Other Applications > Software Install.



6. Click on the "Install" button and wait for the installation to complete.



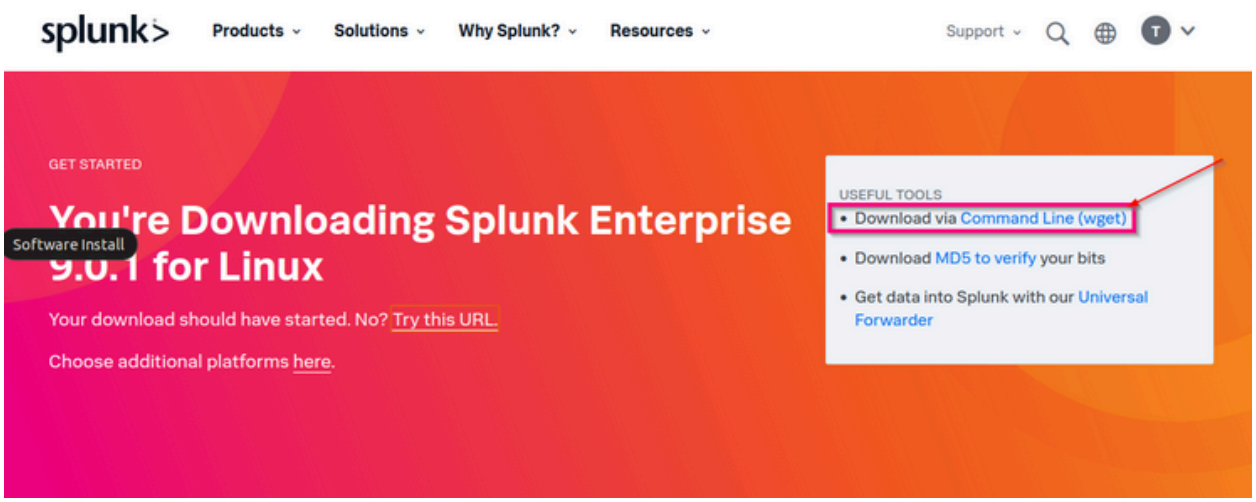

*Congratulations, Splunk has been successfully installed using the GUI.*

## Installation via CLI:

1. Go to the Splunk Site.

2. Create an account.

3. When downloading, check the upper right corner.




4. Click on "Command Linux Wget" to get the download command.

5. Use the terminal and navigate to your installation folder (e.g., /opt).


6. Paste the provided command; add "sudo" if required.

```
blueatom@blueatom-VirtualBox:/opt$ cd /opt/
blueatom@blueatom-VirtualBox:/opt$ wget -O splunk-9.0.1-82c987350fde-Linux-x86_64.tgz "https://download.splunk.com/produc
ts/splunk/releases/9.0.1/linux/splunk-9.0.1-82c987350fde-Linux-x86_64.tgz"
splunk-9.0.1-82c987350fde-Linux-x86_64.tgz: Permission denied
blueatom@blueatom-VirtualBox:/opt$ sudo wget -O splunk-9.0.1-82c987350fde-Linux-x86_64.tgz "https://download.splunk.com/p
roducts/splunk/releases/9.0.1/linux/splunk-9.0.1-82c987350fde-Linux-x86_64.tgz"
--2022-09-02 09:00:44--  https://download.splunk.com/products/splunk/releases/9.0.1/linux/splunk-9.0.1-82c987350fde-Linux
-x86_64.tgz
Resolving download.splunk.com (download.splunk.com)... 52.222.174.82, 52.222.174.65, 52.222.174.112, ...
Connecting to download.splunk.com (download.splunk.com)|52.222.174.82|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 603520037 (576M) [binary/octet-stream]
Saving to: 'splunk-9.0.1-82c987350fde-Linux-x86_64.tgz'

splunk-9.0.1-82c987350fde-Linu 100%[=================================================>] 575,56M  56,1MB/s    in 10s

2022-09-02 09:00:54 (55,8 MB/s) - 'splunk-9.0.1-82c987350fde-Linux-x86_64.tgz' saved [603520037/603520037]

blueatom@blueatom-VirtualBox:/opt$
```

7. Switch to the root user.

8. Extract the downloaded file:

```
tar xvzf splunk-9.0.1-82c987350fde-Linux-x86_64.tgz
```

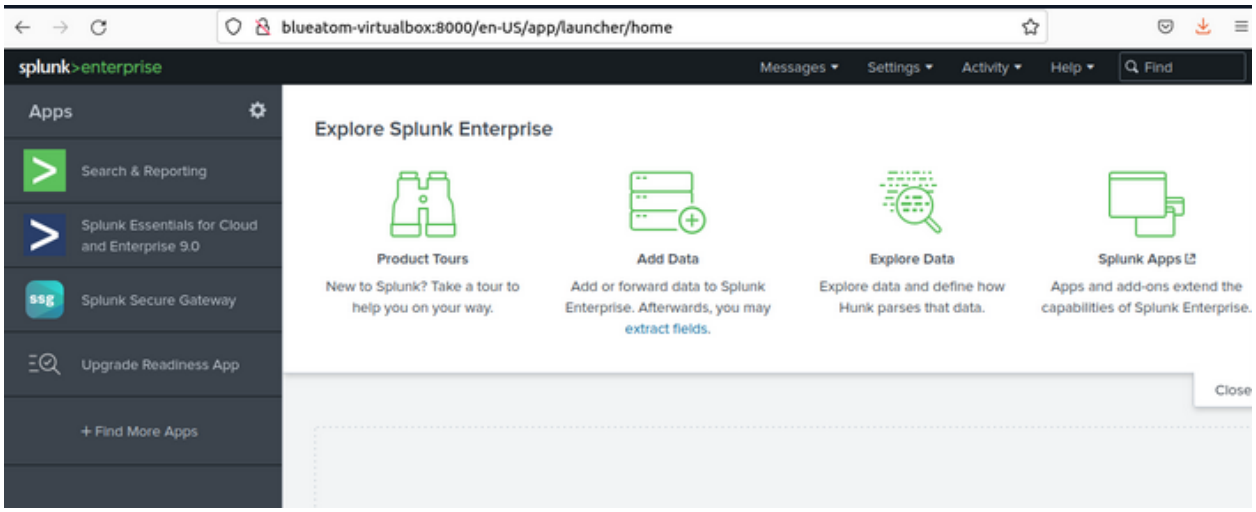
9. Launch Splunk:

/opt/splunk/bin/splunk start --accept-license

10. Answer any prompted questions.

11. Try connecting to the specified link.

```
The Splunk web interface is at http://blueatom-VirtualBox:8000
```



12. Check the Splunk installation.

*Note: By default, Splunk on Linux **does not** start at system startup. To enable automatic startup, run the following commands as root:*

```
/opt/splunk/bin/splunk enable boot-start
```

```
blueatom@blueatom-VirtualBox:~$ sudo su
[sudo] password for blueatom:
root@blueatom-VirtualBox:/home/blueatom# /opt/splunk/bin/splunk status
splunkd 20629 was not running.
Stopping splunk helpers...

Done.
Stopped helpers.
Removing stale pid file... done.
root@blueatom-VirtualBox:/home/blueatom# /opt/splunk/bin/splunk enable boot-start
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
root@blueatom-VirtualBox:/home/blueatom#
```

***Restart and check the status:***

```
/opt/splunk/bin/splunk status
```

```
blueatom@blueatom-VirtualBox:~$ sudo su
[sudo] password for blueatom:
root@blueatom-VirtualBox:/home/blueatom# /opt/splunk/bin/splunk status
splunkd is running (PID: 953).
splunk helpers are running (PIDs: 954 1988 2105 2189 2549 2634 2708 2712 2745).
root@blueatom-VirtualBox:/home/blueatom#
```

*If the output indicates that Splunk started successfully, the installation is complete.*