

# How to install SplunkForwarder(Linux or Ubuntu)

## 1. Download Splunk Universal Forwarder

- Visit: [https://www.splunk.com/en\\_us/download/](https://www.splunk.com/en_us/download/)
- Click: **Universal forwarder**
- Create an account to proceed
- Under **Choose your installation package**, select **Linux**
- Choose **“.deb”** package and it downloads it

## 2. Navigate to the Downloads Directory:

- Open a terminal on your system and run the following commands:
  - `cd Downloads`
  - `ls`

You should see a file like **splunkforwarder-<version>.deb**

## 4. Install the Splunk Universal Forwarder

Install the downloaded package using **dpkg**

- `sudo dpkg -i splunkforwarder-<version>.deb`

## 5. Navigate to Splunk Forwarder Directory

After the installation is complete, go to the Splunk Forwarder's installation directory:

- `Cd /opt/splunkforwarder/bin`

## 6. Start Splunk Forwarder and Accept the License

- `sudo ./splunk start --accept-license`

## 7. Enable Splunk Forwarder to Start on Boot

- `sudo ./splunk enable boot-start`

## 8. Add Forward-Server and Configure Inputs

- `sudo ./splunk add forward-server <indexer_host>:<port>`

## 9. Add Monitored Logs or Files

- `sudo ./splunk add monitor /var/log`

## 10. Restart the Splunk Forwarder

- `sudo ./splunk restart`

## 11. Check Splunk Forwarder Status

- `sudo ./splunk status`

## Warning Error

```
mohamed@mohamed-VirtualBox:~/Downloads$ sudo /opt/splunkforwarder/bin/splunk add
forward-server 192.168.50.47:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Your session is invalid. Please login.
Splunk username: Mohamed
Password:
192.168.50.47:9997 forwarded-server already present
mohamed@mohamed-VirtualBox:~/Downloads$ sudo /opt/splunkforwarder/bin/splunk add
monitor /var/log/syslog
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added monitor of '/var/log/syslog'.
```

The error in the screenshot shows that the Splunk session is invalid, and it asks to log in again. Here are the steps to resolve the issue:

### 1. Re-login to Splunk Forwarder

- Ensure you have the proper credentials for Splunk.

Run the command to log in again: bash

```
sudo /opt/splunkforwarder/bin/splunk login
```

- Enter your username and password when prompted.

### 2. Check SPLUNK\_HOME Permissions

The warning indicates an ownership issue with the SPLUNK\_HOME directory. Ensure that the Splunk user owns the directory: bash

```
sudo chown -R splunkfwd:splunkfwd /opt/splunkforwarder
```

- If your Splunk user is named differently, replace `splunkfwd` with the correct username.

### 3. Restart the Splunk Forwarder

Restart the Splunk service to apply any changes: bash

```
sudo /opt/splunkforwarder/bin/splunk restart
```

### 4. Verify the Forwarder Connection

Ensure that the forward-server is correctly set up: bash

```
sudo /opt/splunkforwarder/bin/splunk list forward-server
```

- Confirm the IP (`192.168.50.47:9997` in this case) is listed.

### 5. Monitor Configuration

Verify that the monitored path (`/var/log/syslog`) is properly added: bash  
`sudo /opt/splunkforwarder/bin/splunk list monitor`

## 6. Review Splunk Logs

If issues persist, check Splunk logs for detailed errors: bash  
`cat /opt/splunkforwarder/var/log/splunk/splunkd.log`

## 7. Firewall/Network Check

Ensure the Splunk forwarder can communicate with the Splunk indexer on port `9997`. bash  
`telnet 192.168.50.47 9997`

- If the connection fails, check your firewall rules or network configuration.

Once you've re-logged in, fixed the permissions, and verified the forwarder configuration, the issue should be resolved. Let me know if you encounter further issues!