**Splunk enterprise and forwarder installation**

<http://127.0.0.1:8000/en-US/account/login?return_to=%2Fen-US%2F>

Splunk Server configured in Port:**8000**

--First install the splunk enterprise for splunk server establishment and gave user name as admin and password different from splunk site registration

--Next install splunk forwarder with admin as user name and pswd different from site reg pswd and server password

use ipv4 ip addess from ipconfig in the cmd 192.168.176.158

--not working above go to CMD as administrator and go to the splunk enterprise bin directory then type the command

**splunk start**

which enable the splunk start working on port 8000

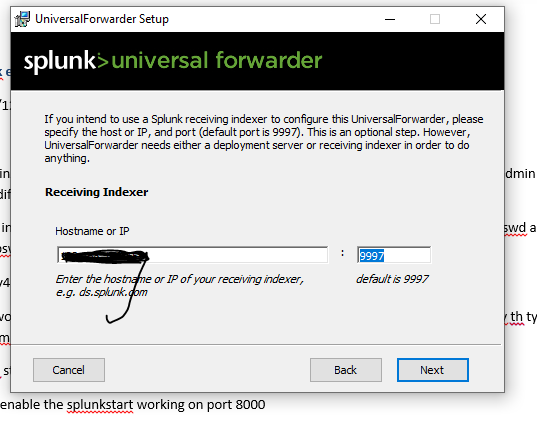
Go to Chrome**- http://127.0.0.1:8000/en-US/account/login?return\_to=%2Fen-US%2F**

-**For splunk forwarder**

**Note: Better to start forwarder with admin privilege to show log check box**

1- **Right-click** on the installer file (splunkuniversalforwarder-<version>-x64.msi)

2- Click **"Run as administrator"** from the menu.



**Note:** Remember that if you are configuring this in your local machine and you need to collect the log from local machine your splunk will be the deployment sever and you don’t need to configure the deployment server ip.

**Note:** Important to configure the receiving indexer with the ip of your system by using the cmd ipconfig and take the **IPV4 address** from there and paste it over here and default port should be 9997 that need to configure in the splunk enterprise before installation.

Steps – go to splunk enterprise with enterprise credentials, then follow these steps.

**Settings ->Forwarding and receiving -> Receiving data -> Set port 9997 enable**

**Check Forwarder Health**

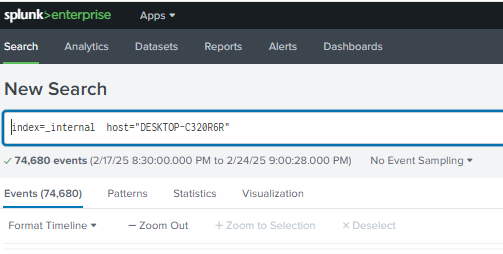
**Step-1**

* Go to the bin folder of the splunk using admin previlage **(CMD->run as administrator-> Enter Commant-> cd “C:\Program Files\SplunkUniversalForwarder\bin” – Press Enter)**
* Now you are in the bin directory-> enter the command **splunk list forward-server**
* Output will be like - **Active forwards:**

**10.0.0.1:9997**

**Check the logs are properly coming**

* Login on the Splunk console and go to the search bar and type



**index=\_internal host="DESKTOP-C320R6R**" if it showing events means your forwarder is properly collecting log

**Manual Creation of ‘inputs.conf’ if checkbox is not available**

**Right-click** on **Command Prompt** and select **"Run as administrator"**

* **Go to splunk forwarder local directory after viewing cmd prompt (cd “cd C:\Program Files\SplunkUniversalForwarder\etc\system\local”)**
* **Now you are in local and type following commands**

**Check if inputs.conf exists by running:**

**(cd “cd C:\ProgramFiles\SplunkUniversalForwarder\etc\system\local\ dir inputs.conf”)**

- Use this command in local directory of splunk forwarder: **dir inputs.conf**

**If inputs.conf is present, open it with Notepad: and check these files are added if not add those and save the file**

**(cd “cd C:\ProgramFiles\SplunkUniversalForwarder\etc\system\local\ notepad inputs.conf”)**

-Use this command in local directory of splunk forwarder: **notepad inputs.conf**

**---add following is not present and save the file---**

**[WinEventLog://Application]**

**disabled = 0**

**index = windows\_logs**

**[WinEventLog://Security]**

**disabled = 0**

**index = windows\_logs**

**[WinEventLog://System]**

**disabled = 0**

**index = windows\_logs**

**If inputs.conf is missing, follow these steps:**

1. In Command Prompt, create a new file using Notepad:

(**cd “cd C:\ProgramFiles\SplunkUniversalForwarder\etc\system\local\ notepad inputs.conf”)**

-Use this command in local directory of splunk forwarder: **notepad inputs.conf**

1. When Notepad opens, **copy and paste** the following configuration & Save the file

**[WinEventLog://Application]**

**disabled = 0**

**index = windows\_logs**

**[WinEventLog://Security]**

**disabled = 0**

**index = windows\_logs**

**[WinEventLog://System]**

**disabled = 0**

**index = windows\_logs**

Click **File → Save As**.

* In the **Save as type** dropdown, select **All Files**.
* Name the file as **inputs.conf**.
* Make sure it's saved in:

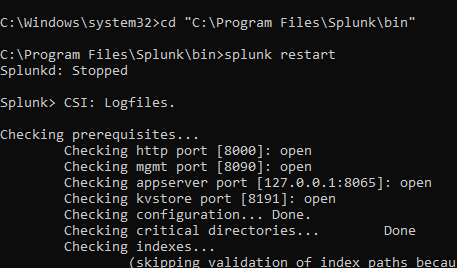
Manualy go and check the folder: C:\Program Files\SplunkUniversalForwarder\etc\system\local

## ****Step 5: Restart the Splunk Forwarder****

After updating inputs.conf, restart the Splunk Forwarder for changes to take effect.

Run the following command in bin directory of splunk.

**C:\Program Files\SplunkUniversalForwarder\bin\splunk restart**



## ****Step 6: Verify That Logs Are Being Sent****

1. **Check Forwarder Status**  
   Run this command to verify that logs are being monitored:

**C:\Program Files\SplunkUniversalForwarder\bin\splunk list inputstatus**

* + If it shows **WinEventLog://Application, Security**, and **System,** it's working.

**----All Setup Done---**