INSTALLING SPLUNK FORWARDER (Windows)

By: SAMEER HASSAN

GitHub-link: GitHub - sameerhassancode/Wazuh-labs

LinkedIn: https://www.linkedin.com/in/sameer-hassan-15a428255/

Need training on Splunk?

Contact number: +923355345678

Email: sameerishassan@gmail.com

LinkedIn: https://pk.linkedin.com/in/sameer-hassan-15a428255

Other SIEM

1. Wazuh

2. IBM Qradar

What is Splunk?

Splunk is a powerful log management and SIEM tool used for:

Collecting machine data from servers, apps, network devices

Indexing, searching, and analyzing logs in real time

Creating dashboards, alerts, and reports for monitoring and security

Splunk is very flexible, user-friendly, and is often used by:

- SOC teams
- IT operations
- DevOps and SREs
- Security analysts

Splunk Forwarder:

Splunk Forwarder is a lightweight agent used to collect and send logs from remote systems to the main Splunk server (called the indexer). It ensures real-time data collection from endpoints like Windows, Linux, and network devices.

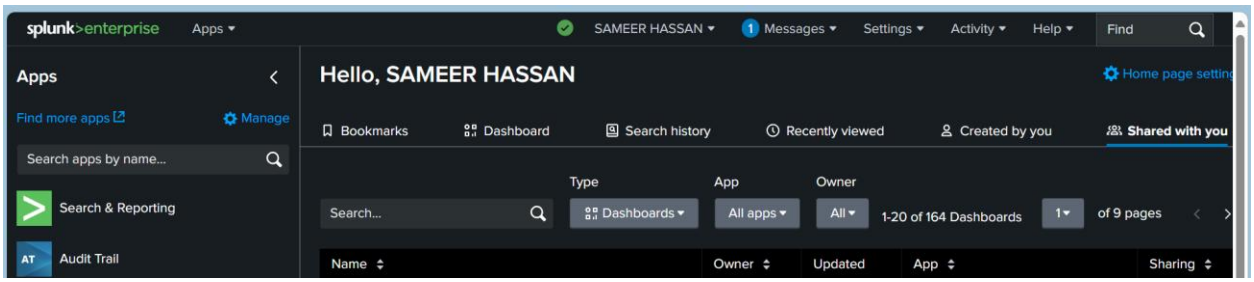
Types of Splunk Forwarders

1. Universal Forwarder (UF) – Most common, lightweight, for log forwarding only.
2. Heavy Forwarder (HF) – Full Splunk instance; can parse and filter data before sending.

Use Case Example:

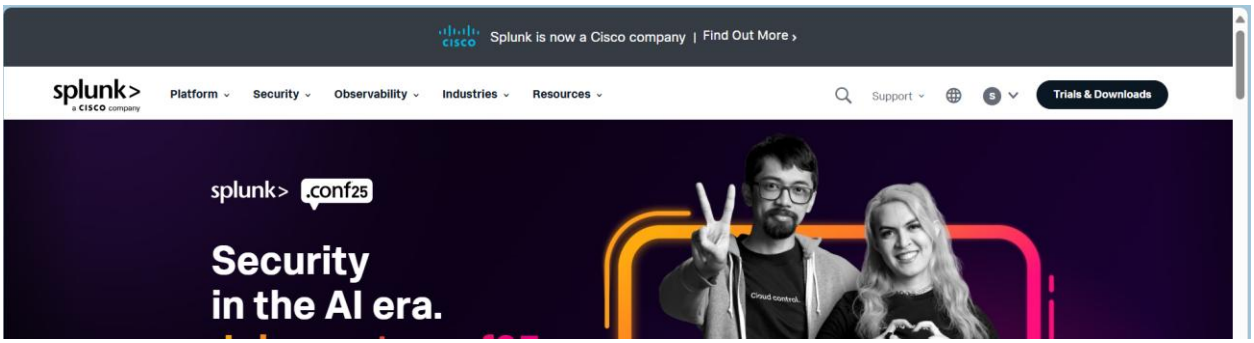
Install Splunk Universal Forwarder on a Windows server Configure it to monitor event logs Forward those logs to your central Splunk server for search, alerting, and dashboards.

Splunk:

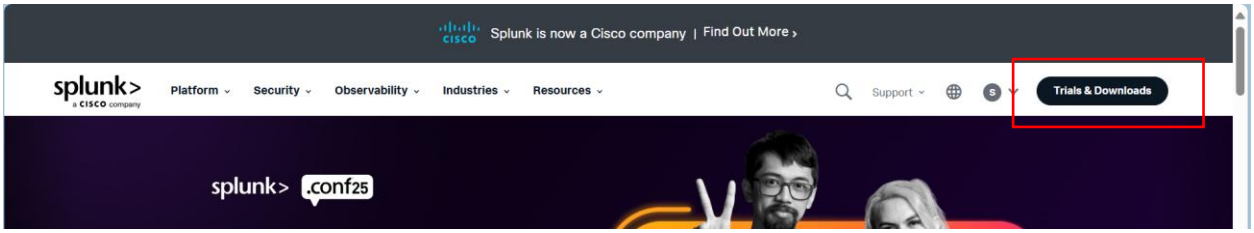


1: **Install Splunk Universal Forwarder on Windows**

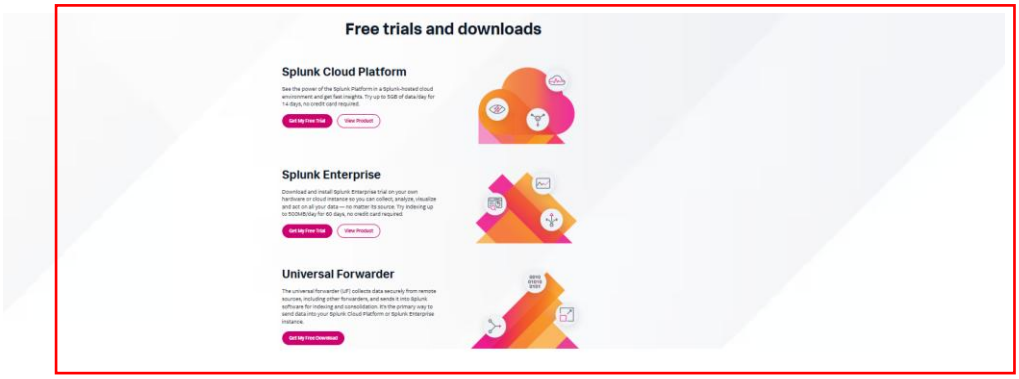
Open Splunk official website.



Click on Trails & Download button

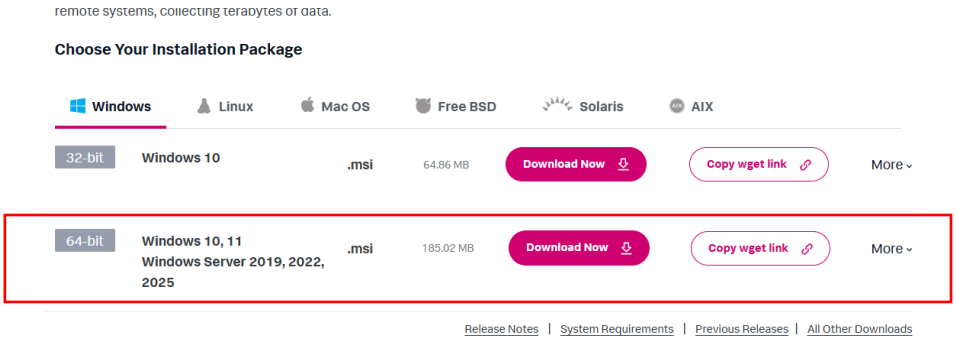


It will redirect you to download page. (if not login it will ask for login)

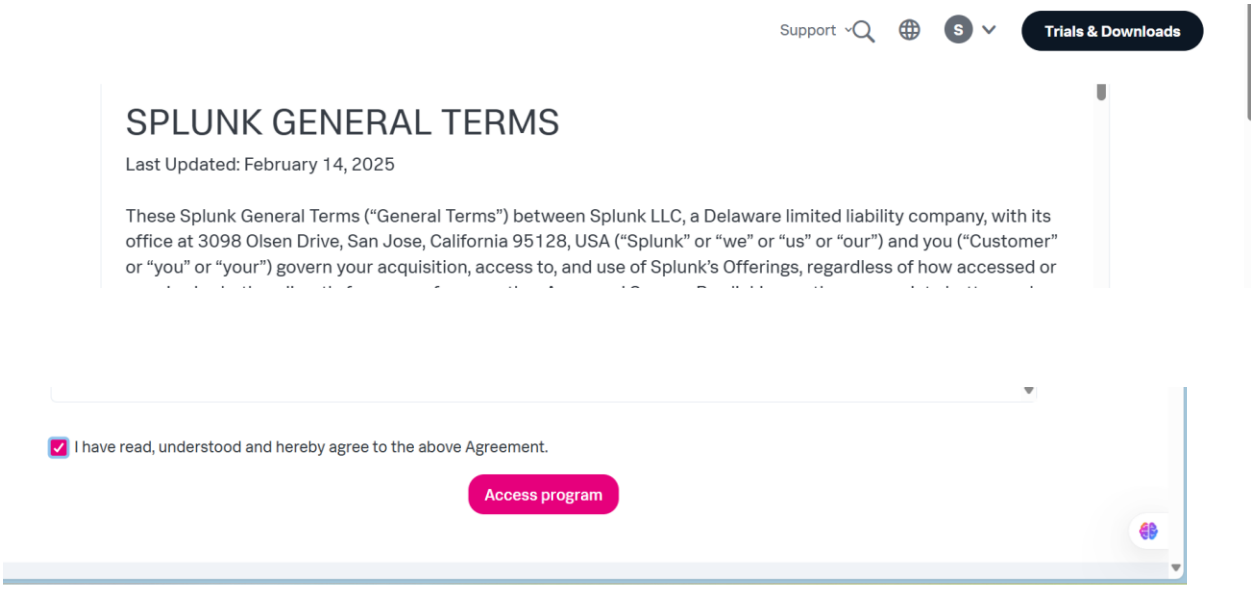


Now click on Get my Free Download Under Universal Forwarder section:

Now after clicking the download button it will redirect to main download page here select suitable version of windows universal forwarder and click download

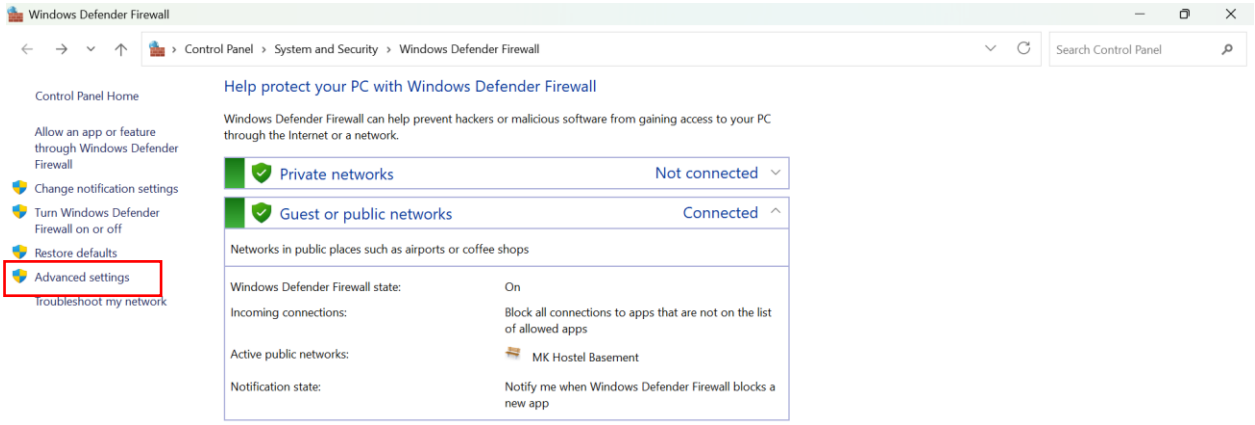


After clicking download you will redirect to license and agreement page accept and download

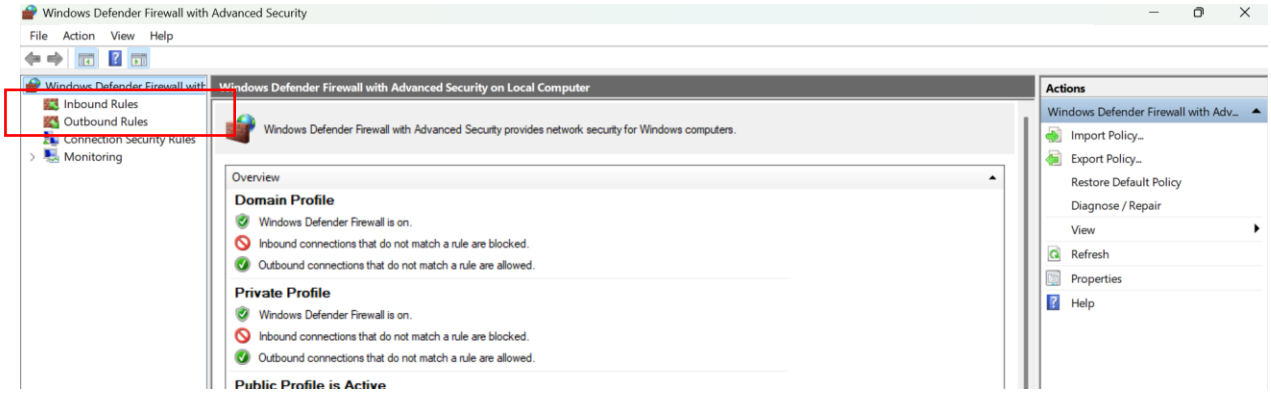


Now open windows firewall to allow 9997 and 8089 port for Splunk

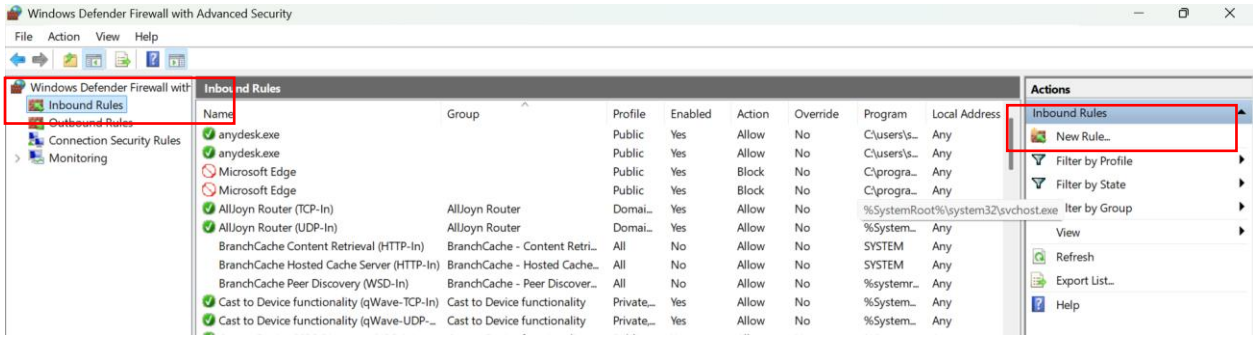
Open- Windows Firewall then click on Advance settings



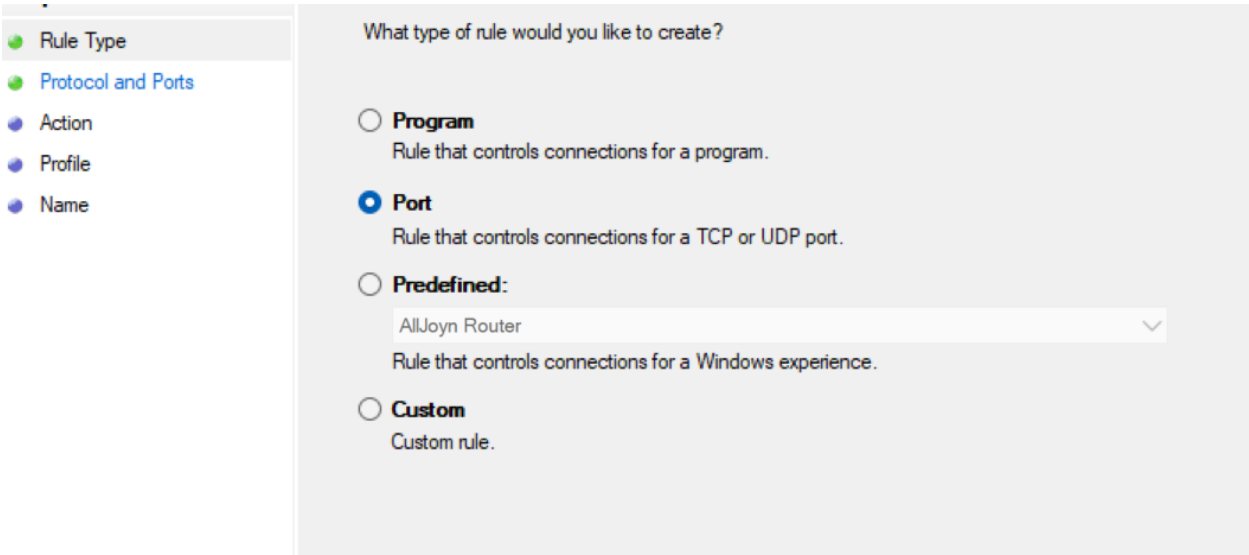
In advance setting you can see the inbound and outbound rules to allow or block any port or app.



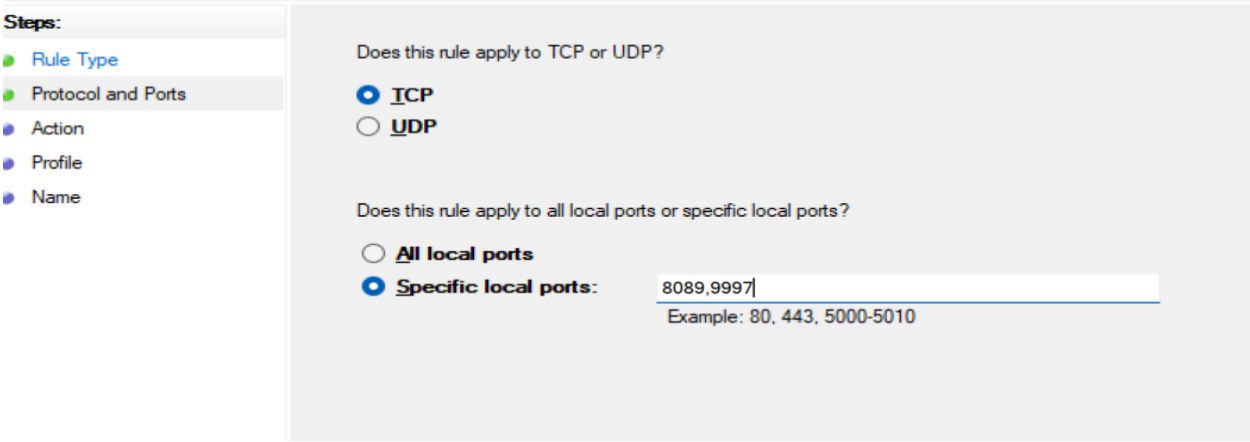
Now click on inbound rules and then **New Rules**



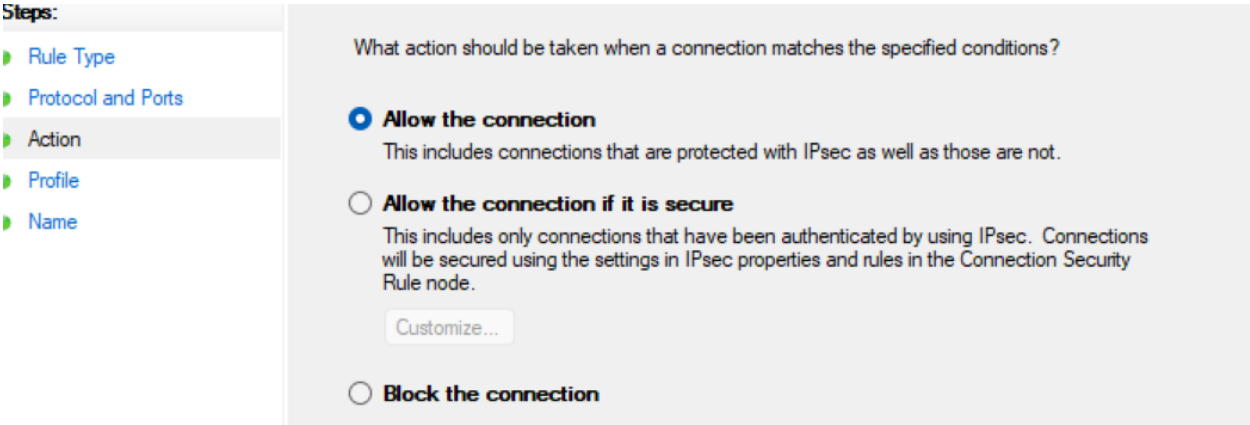
After clicking new rule it will show a popup select port



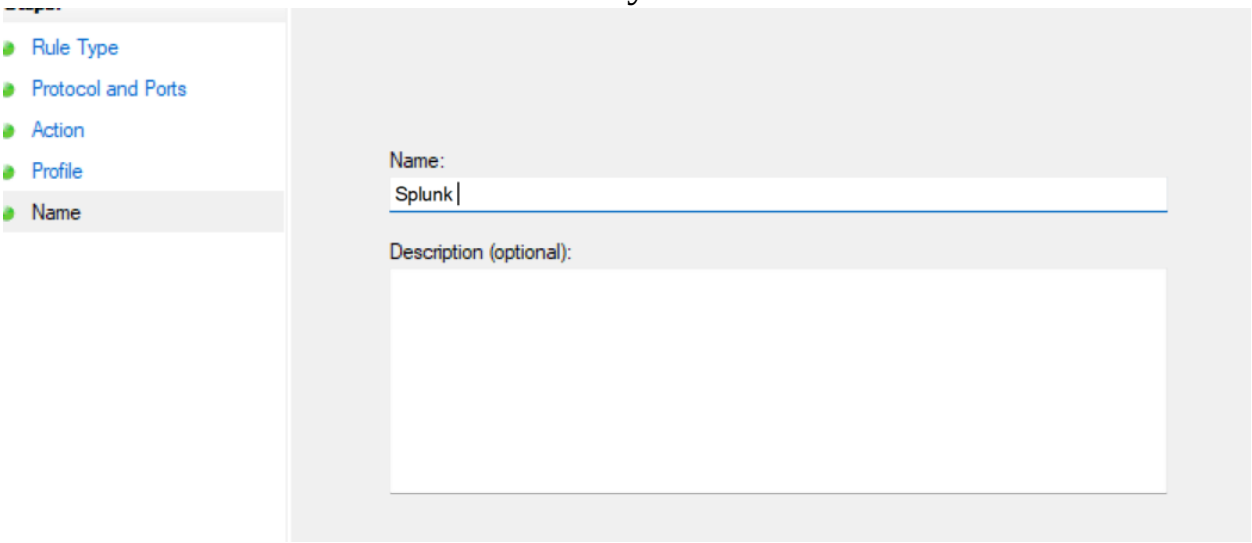
Click next and then type the ports you want to allow. i.e 9997 and 8089



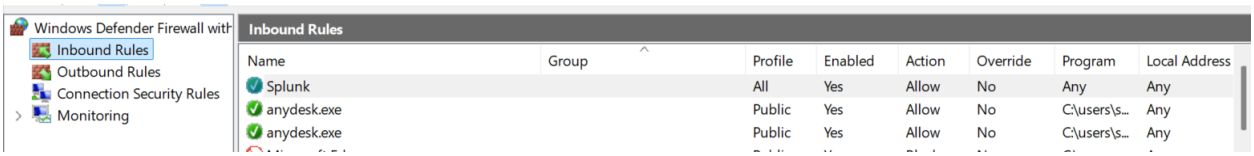
Now select Allow the connection



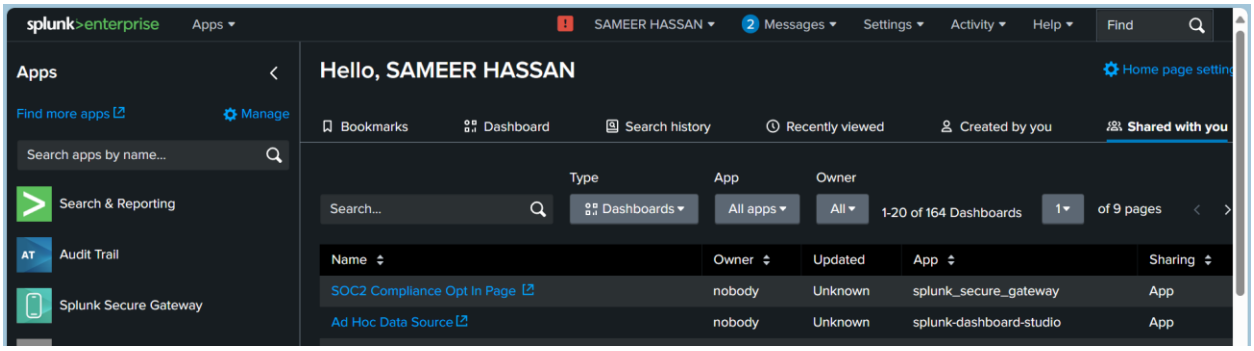
Now write the rule name and hit okay!



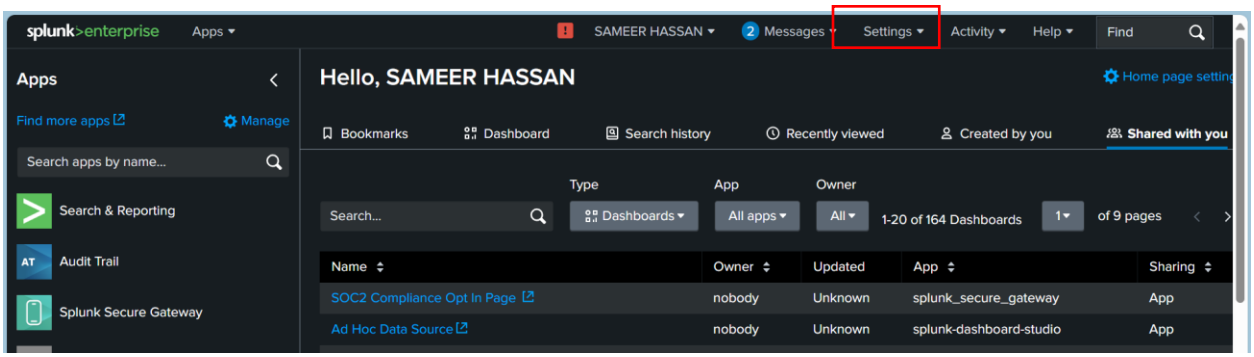
Rule is created:



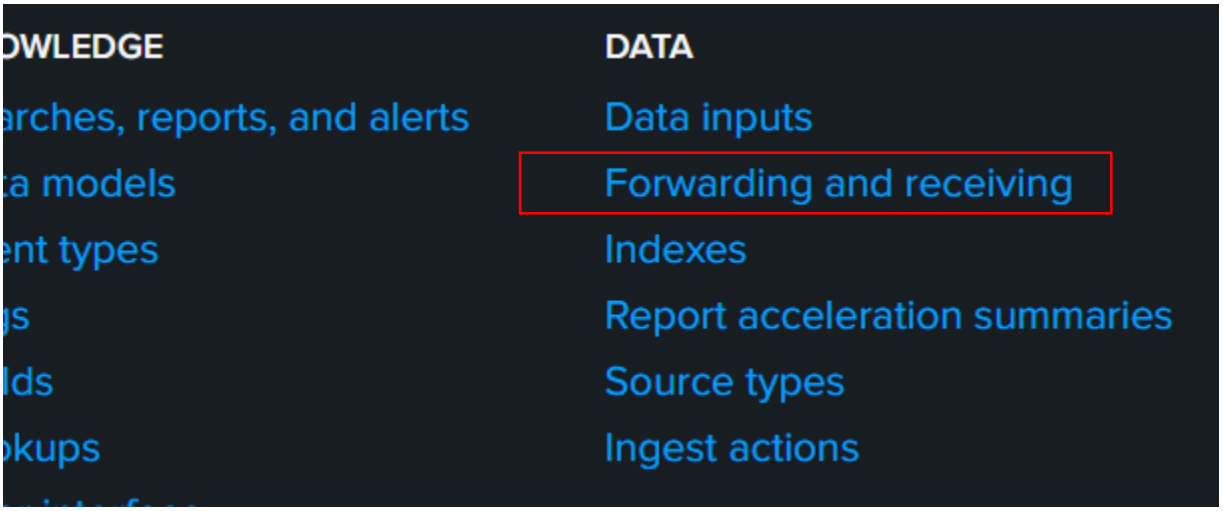
Now open Splunk dashboard



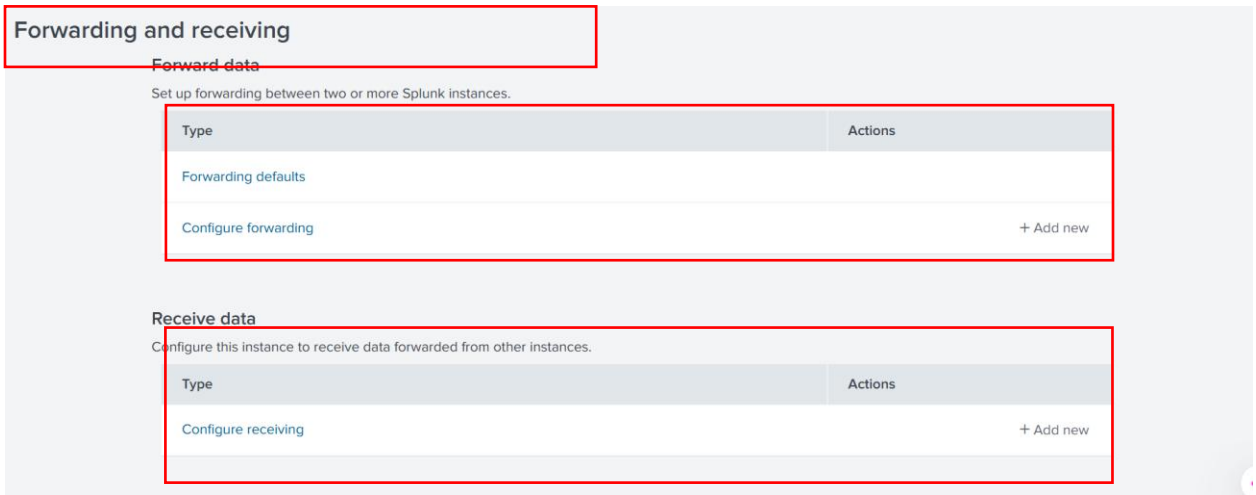
Click on setting



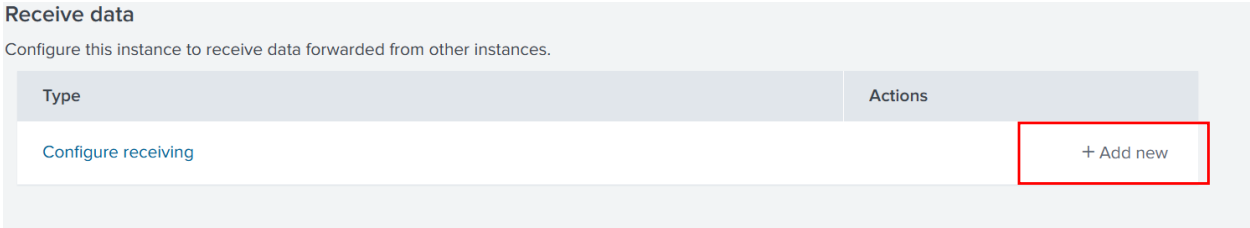
Click the setting will show Menu in different sections find the data section and click on forwarding and receiving



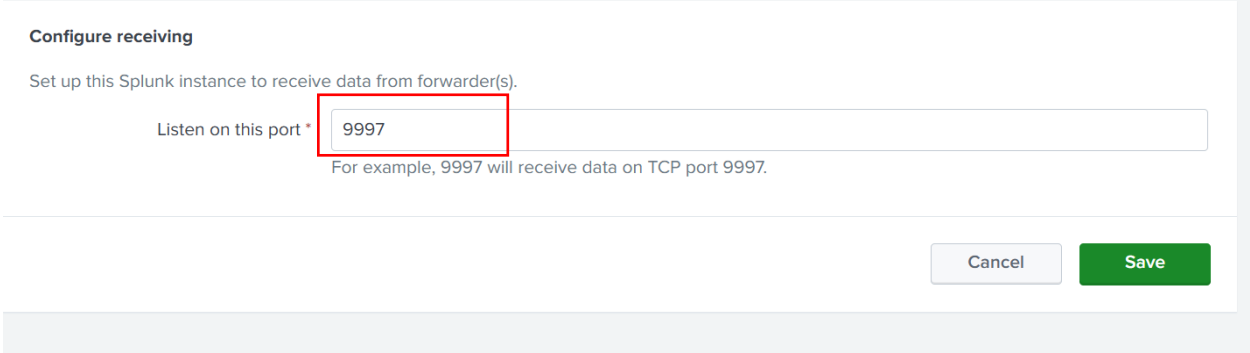
After opening forwarding and receiving page you will see two type **forwarding data and receiving data**



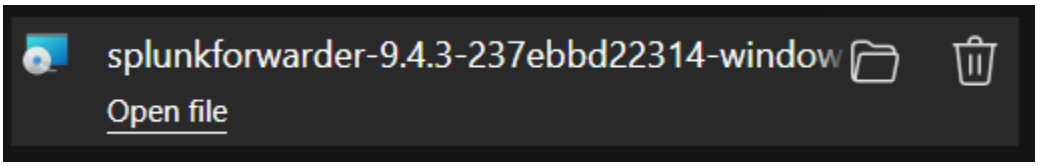
Click on add new in receive data section:



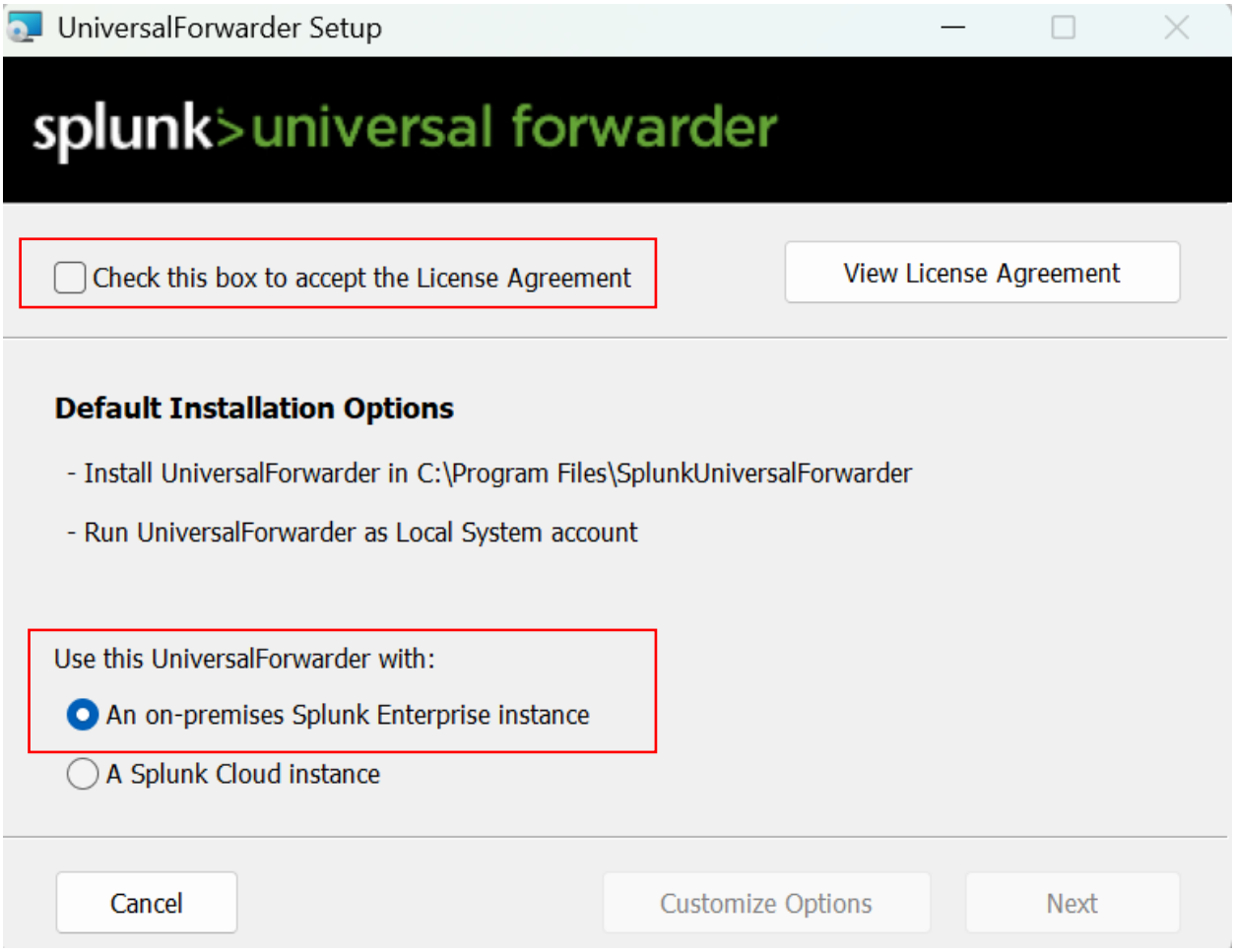
Type the port 9997 and click save



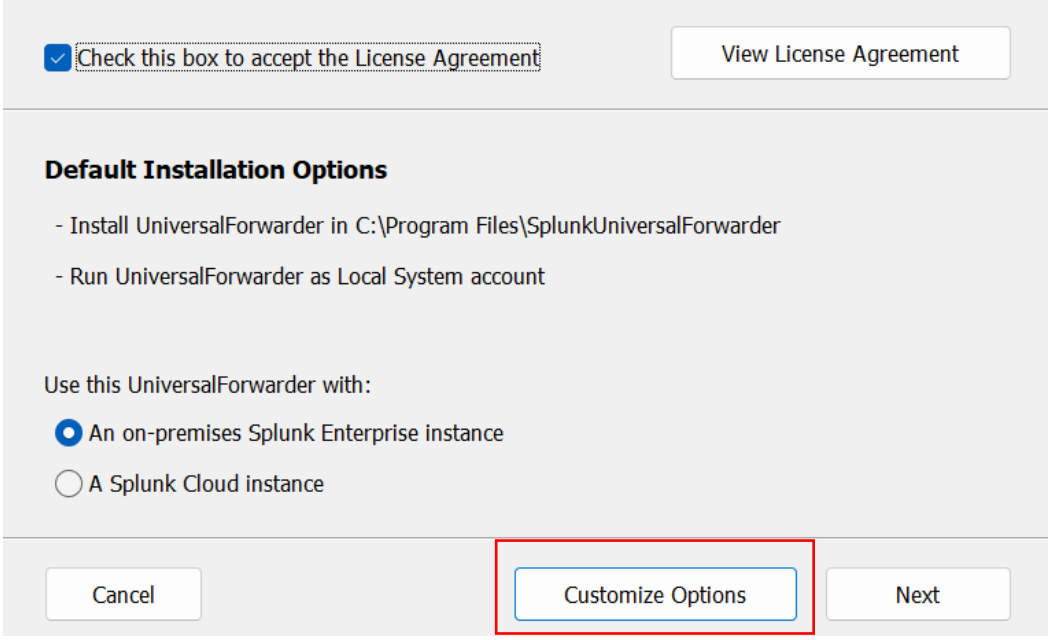
After Successful download start the forwarder



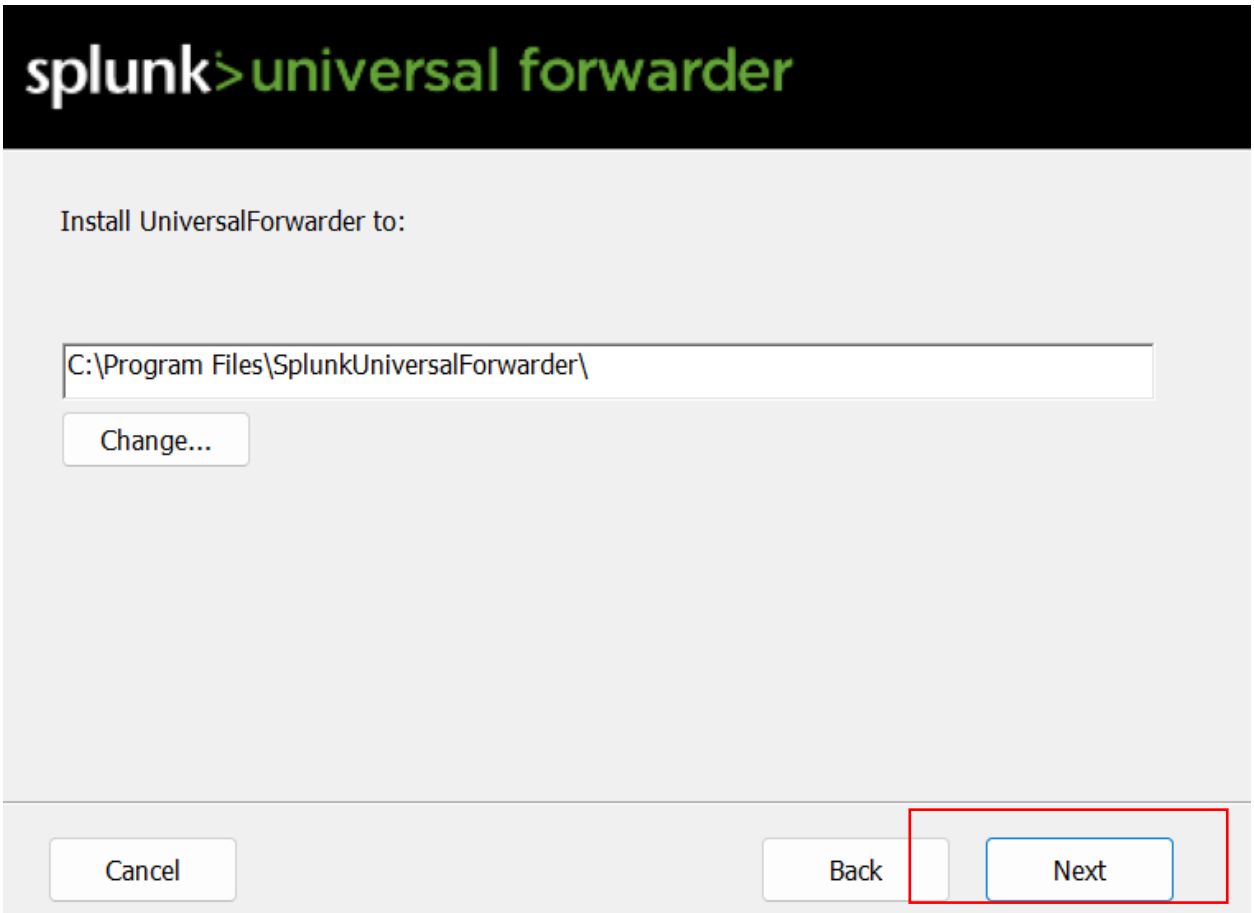
While installing it will ask you to accept the term check box. And another option of Splunk enterprise or cloud instance so I go with enterprise.



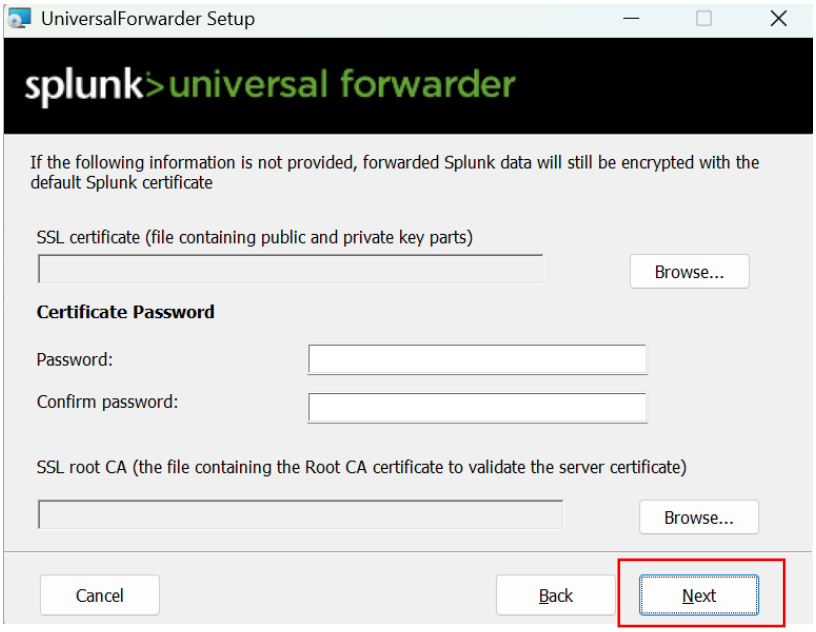
After checking the License box click on customize options



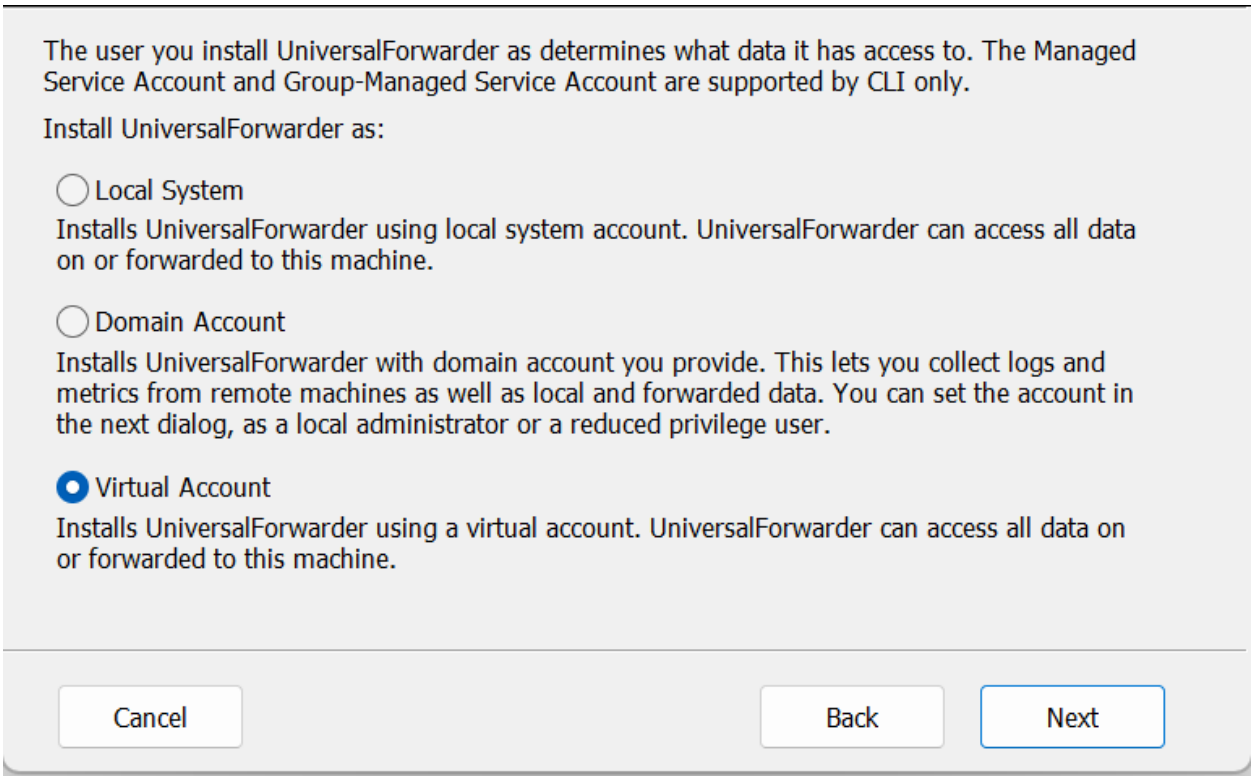
Click next:

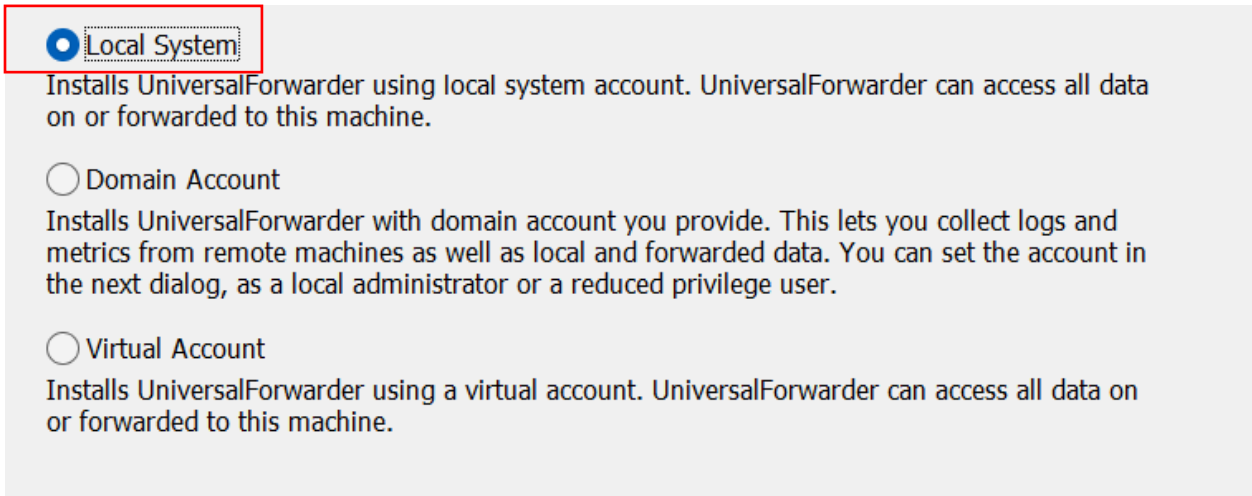


Next

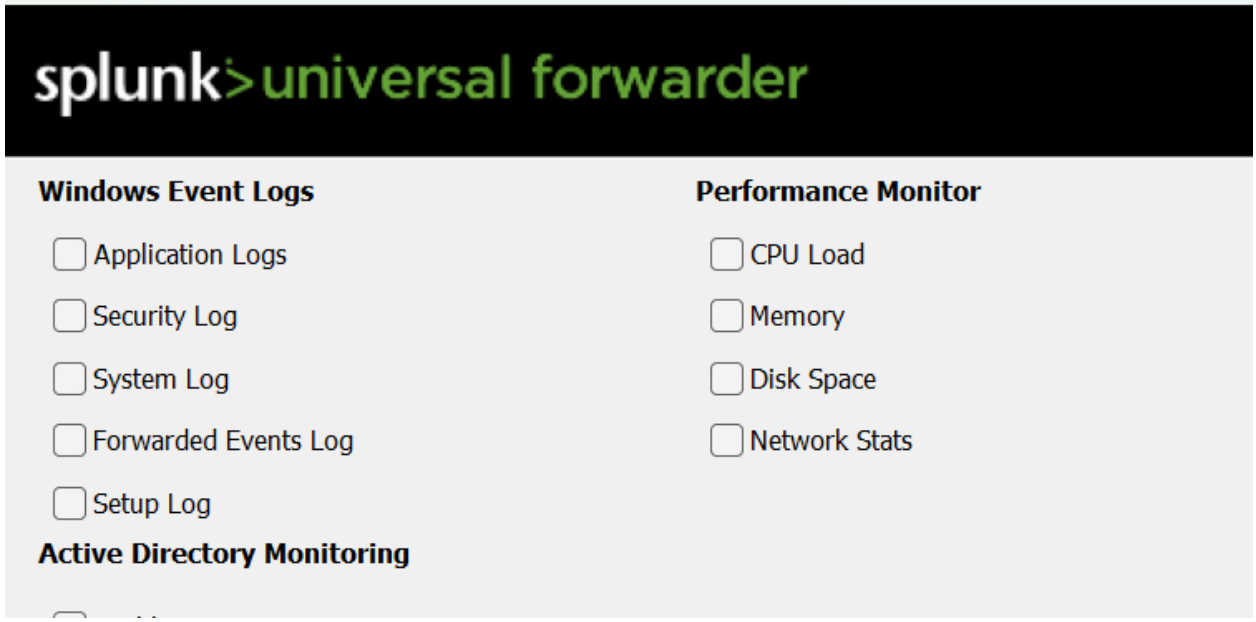


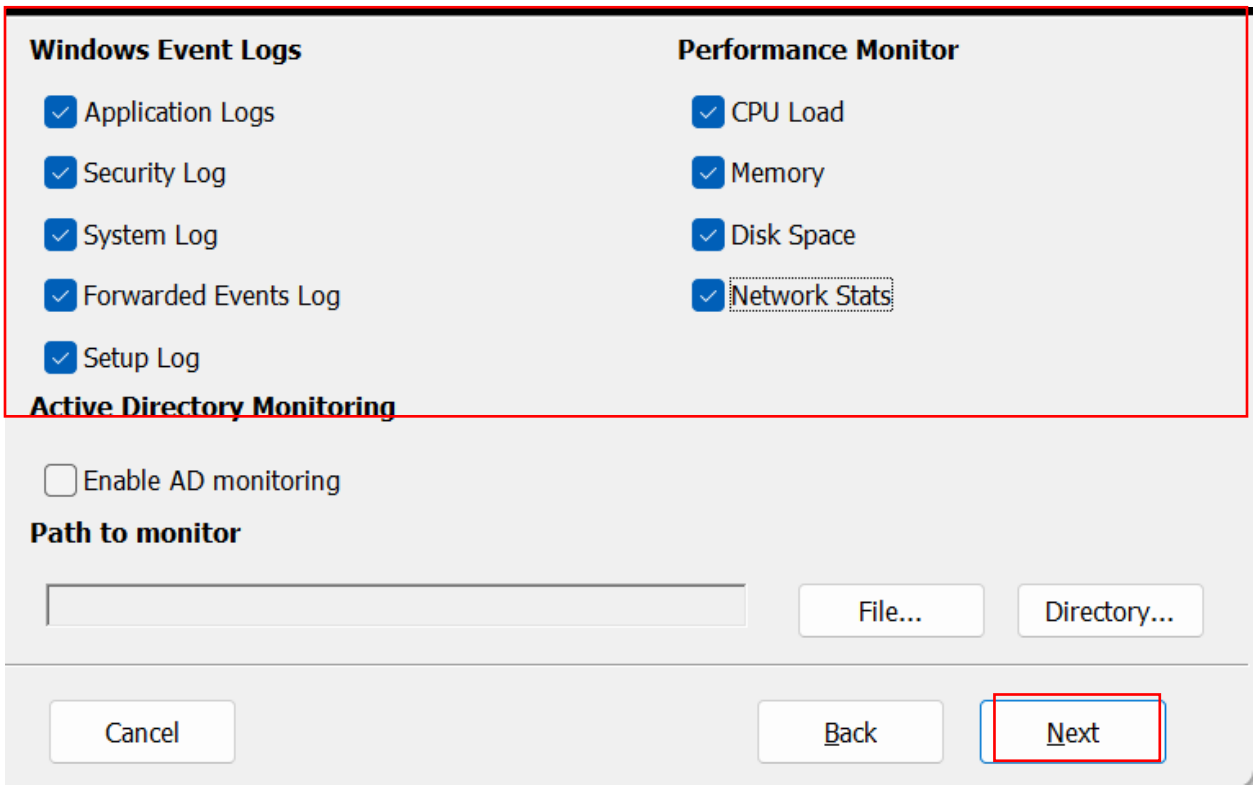
Select local and click next



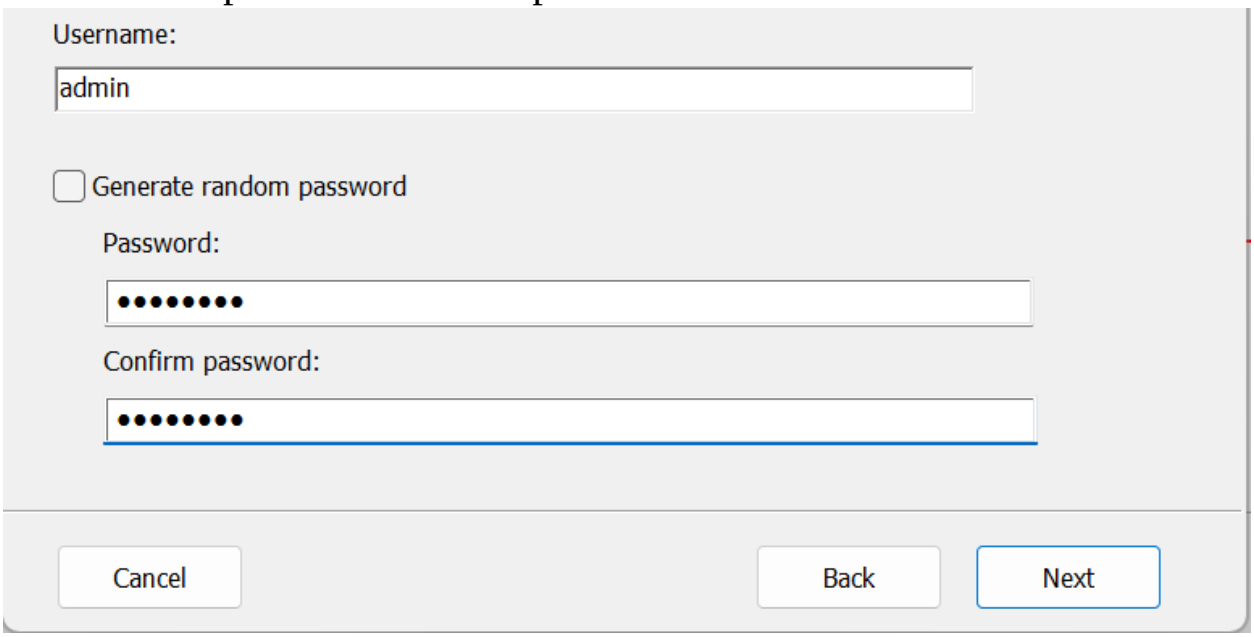


Here select all the logs type you want to forward and click next

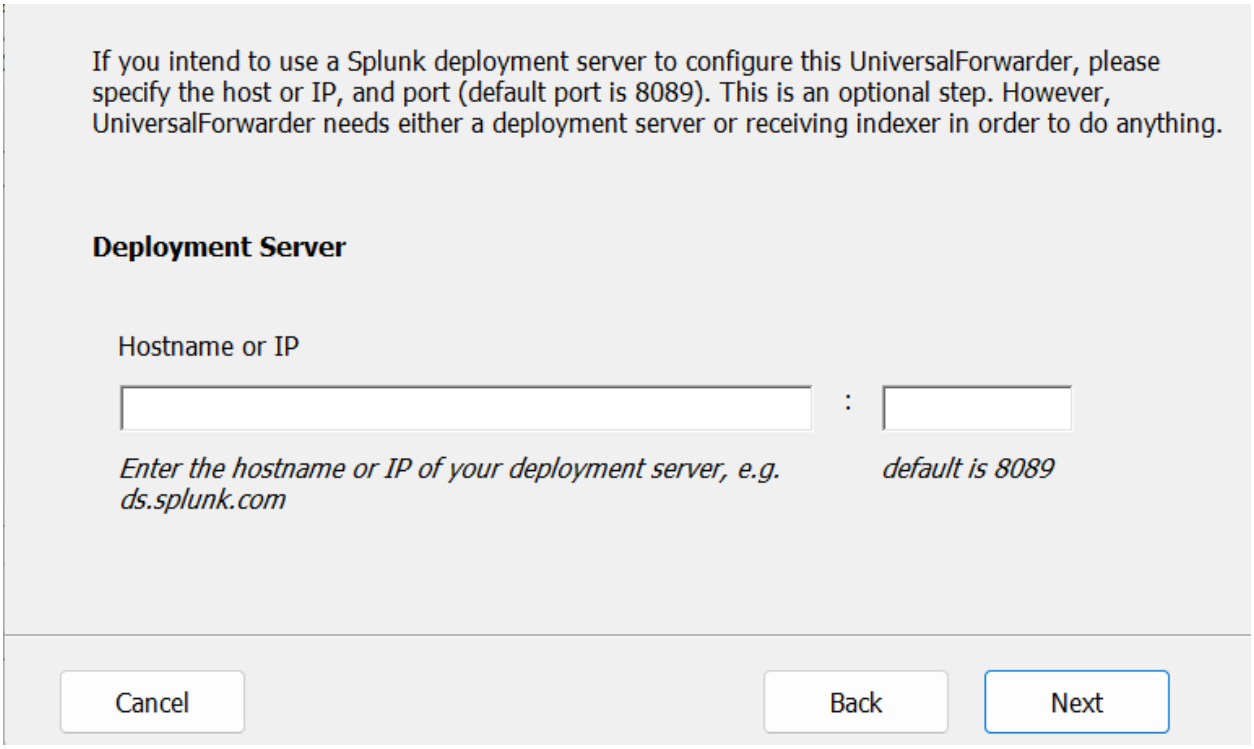




Create a Simple username and password for latter access



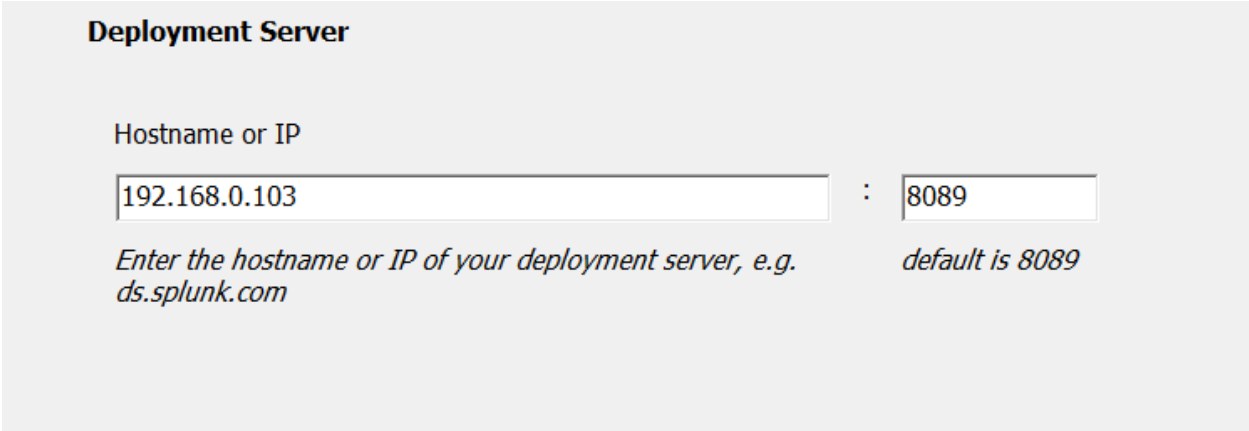
Now enter the ip of your Splunk server



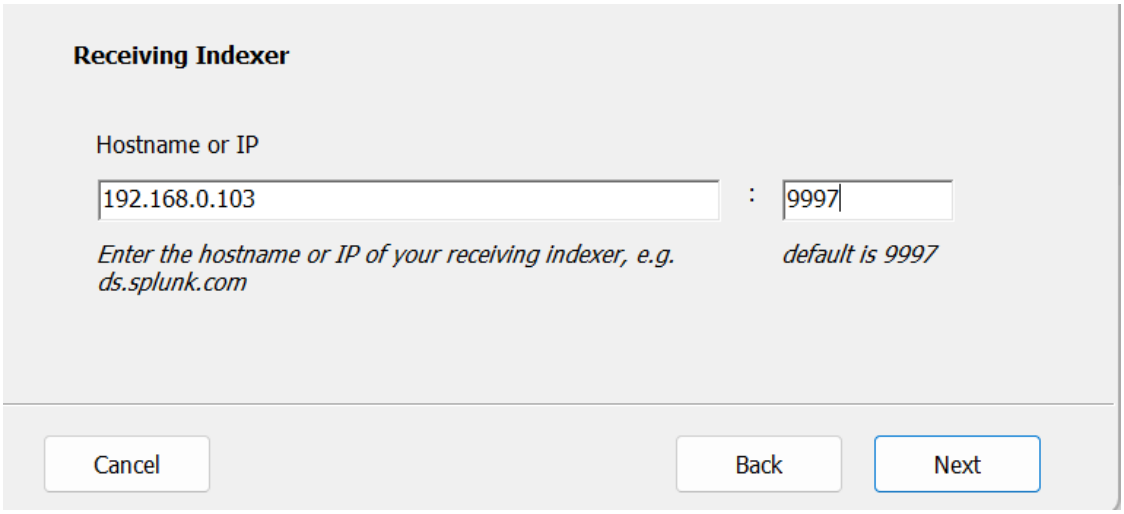
Open cmd and enter ipconfig to view the ip

```
C:\Users\Shifat>ipconfig

Windows IP Configuration
```

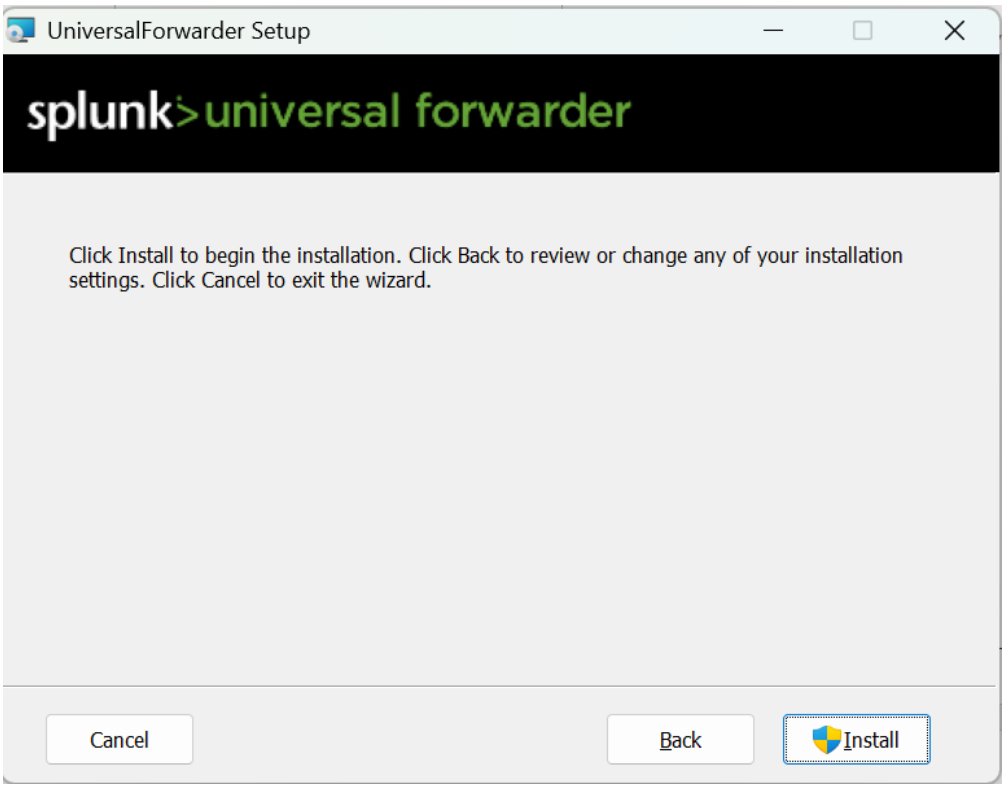
```
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::13f3:ad08:a7ed:f84b%14
   IPv4 Address. . . . . . . . . . . : 192.168.0.103
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```



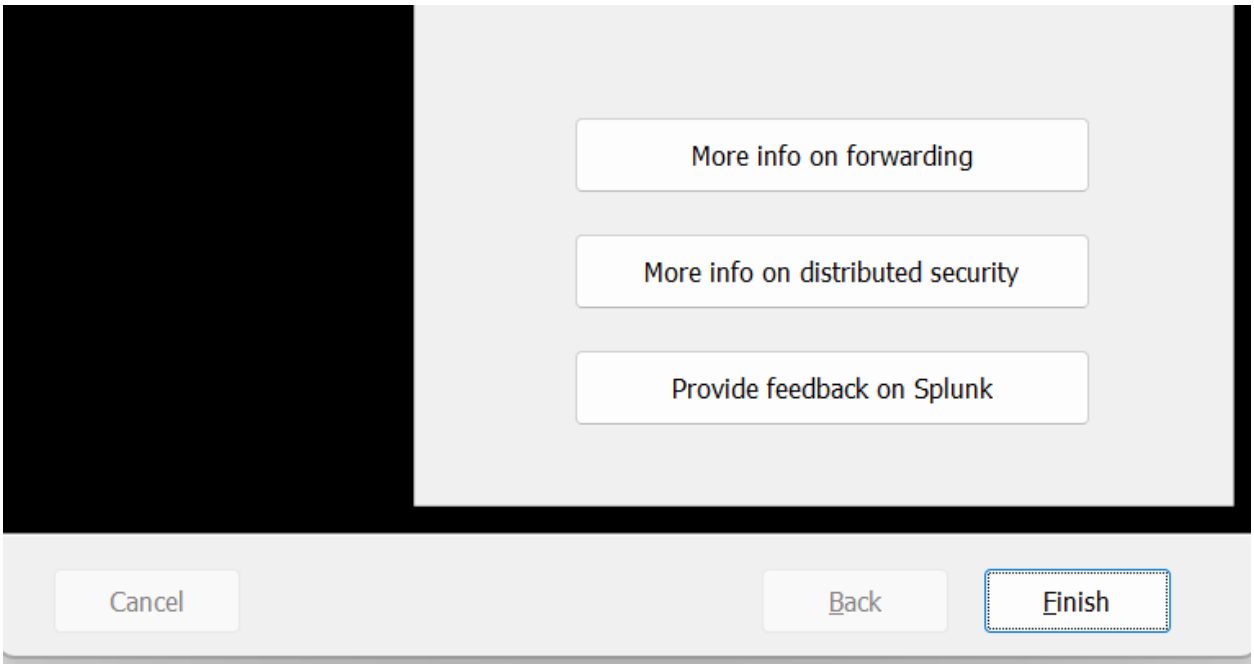
Now for the Receiving server add the same Ip and enter default port.



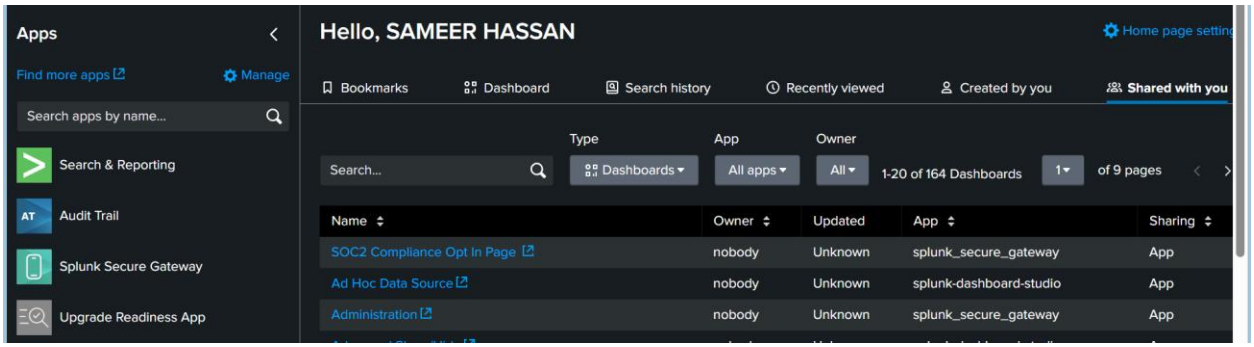
After adding the ip of Receiving and sending server click install



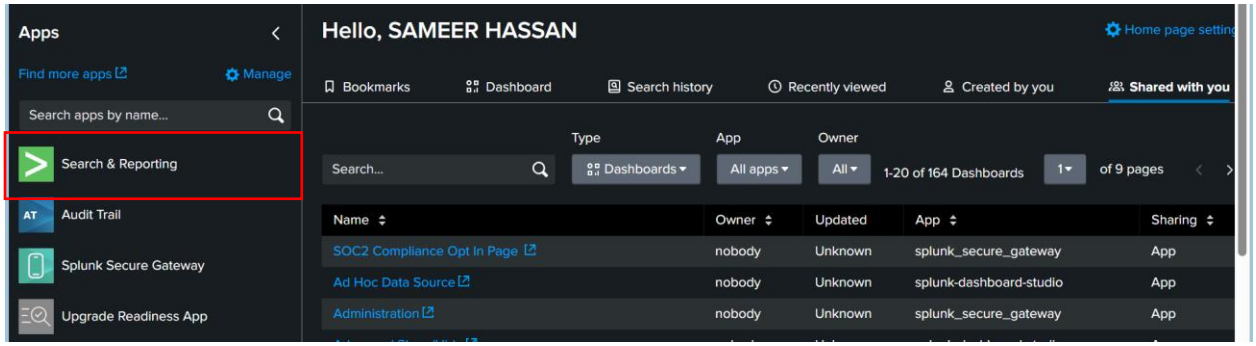
After successful installation click finish



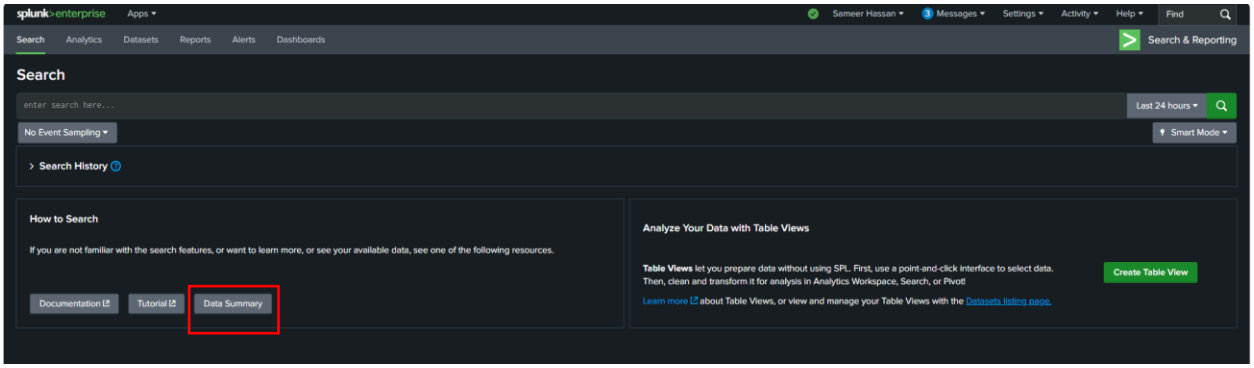
Now again open **Splunk Dashboard**



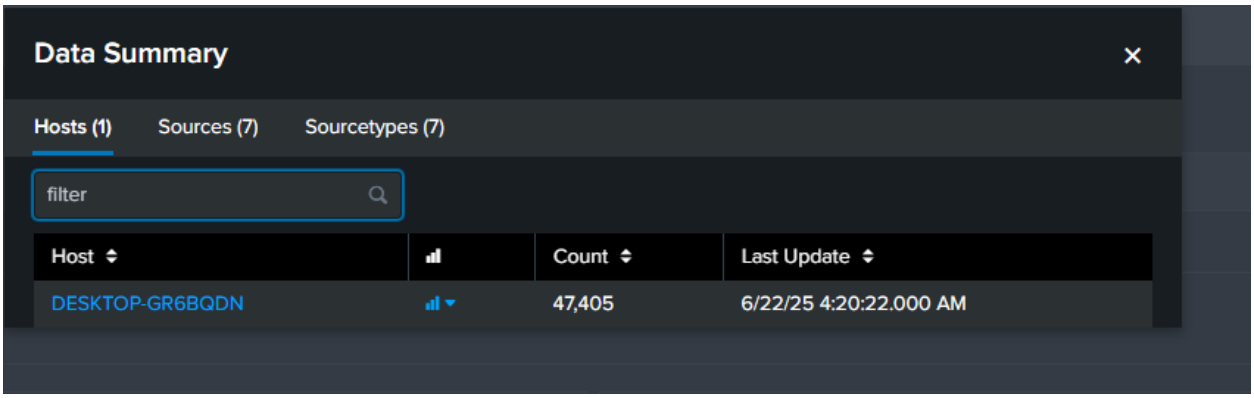
Click on Search and reporting!



Now you are at search page here click on data summary it will show you the forwarder host name.



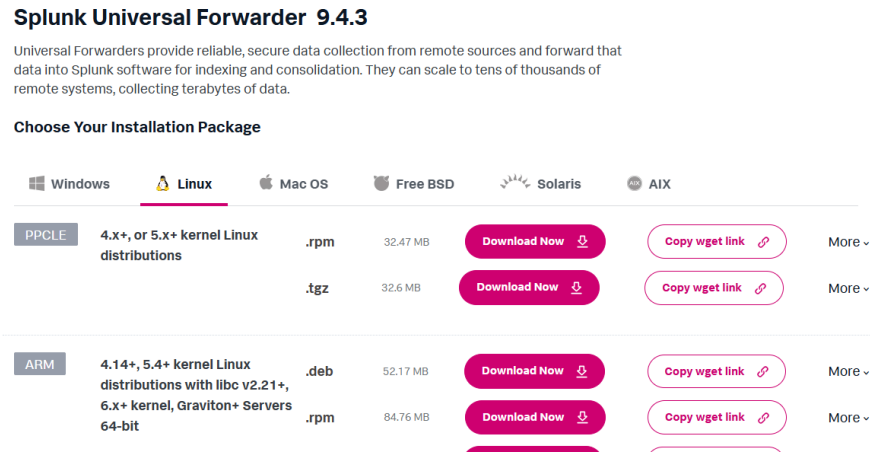
My Forwarder setup successfully



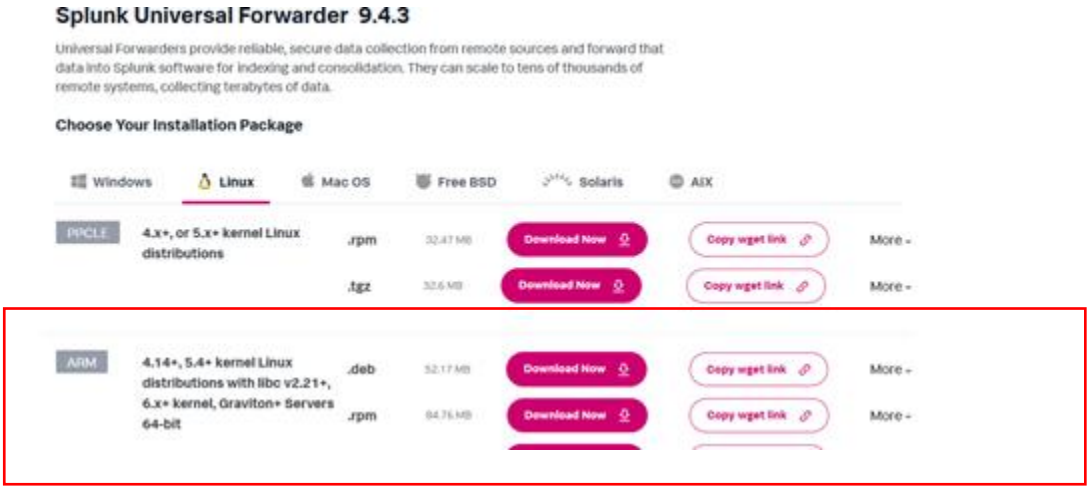
Ubuntu Forwarder

Start the machine.

Open Splunk download page and go to Splunk forwarder section

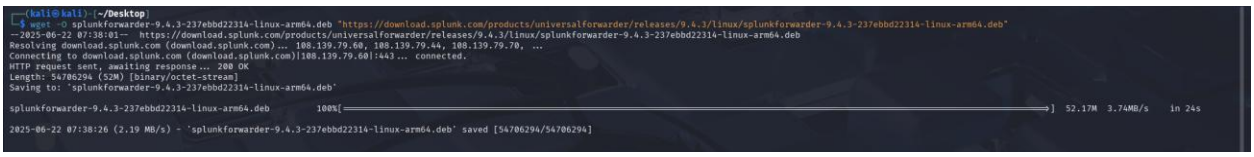


Here select **.tgz** and copy wget link to install it by using command line **check your system and then install**



After that open the terminal and paste this code and press enter

Forwarder Downloaded:



Now type ls to view the .**tgz** file. Extact the file

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ls
splunkforwarder  splunkforwarder-9.4.3-237ebbd22314-linux-arm64.tgz
```

Now move the directory to /opt path.

Command : sudo mv splunkforwarder /opt/

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# cd /opt

┌──(root㉿kali)-[/opt]
└─# ls
microsoft  splunkforwarder

┌──(root㉿kali)-[/opt]
└─#
```

Now go to bin folder and start the splunk with command

(my terminal is showing some glitches)

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

During installation it will ask for enter username and password.

```
t㉿kali)-[/opt]
osudo /opt/splunkforwarder/bin/splunkrt --ac--accept-license


pears to be your first time running this version of Splunk.

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

enter an administrator username: admin
d must contain at least:
total printable ASCII character(s).
enter a new password:
confirm new password:
g unit file ...
to auto-set default user.
to create the unit file. Please do it manually later.


 Winning the War on Error

g prerequisites ...
 Checking mgmt port [8089]: open
         Creating: /opt/splunkforwarder/var/lib/splunk
         Creating: /opt/splunkforwarder/var/run/splunk
         Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n
         Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/static/css
         Creating: /opt/splunkforwarder/var/run/splunk/upload
         Creating: /opt/splunkforwarder/var/run/splunk/search_telemetry
         Creating: /opt/splunkforwarder/var/run/splunk/search_log
         Creating: /opt/splunkforwarder/var/spool/splunk
         Creating: /opt/splunkforwarder/var/spool/dirmoncache
```

Now enable boot start for forwarder

./splunk enable boot-start

```
┌──(root㉿kali)-[/opt/splunkforwarder/bin]
└─# sudosudo /opt/splunkforwarder/bin/splunkble boot-start
```

Setup forwarding to your splunk server

sudo /opt/splunkforwarder/bin/splunk add forward-server 192.168.0.109:9997 -auth admin:Password

Note:

Replace you ip, admin and password

```
┌──(root㉿kali)-[/opt/splunkforwarder/bin]
└─# sudo /opt/splunkforwarder/bin/splunk add forward-server 192.168.0.109:9997 -auth admin:Password
tcp_conn_open_afux ossocket_connect failed with No such file or directory
tcp_conn_open_afux ossocket_connect failed with No such file or directory
tcp_conn_open_afux ossocket_connect failed with No such file or directory
Added forwarding to: 192.168.0.109:9997.

┌──(root㉿kali)-[/opt/splunkforwarder/bin]
└─#
```

Add logs to monitor

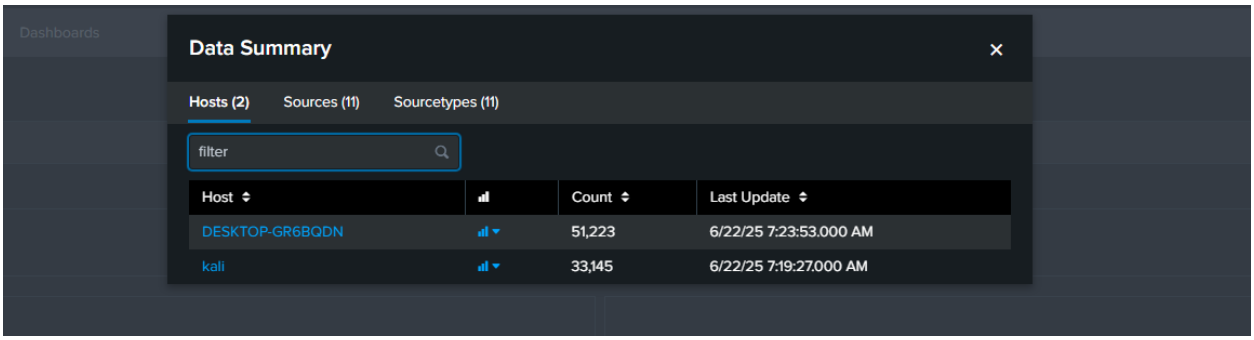
Command: add monitor [path]

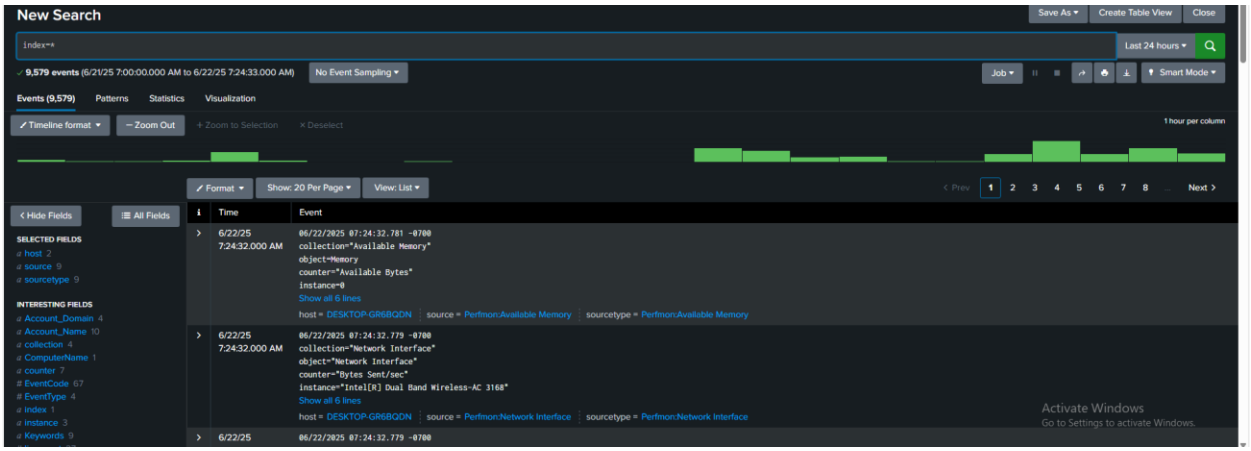
```
┌──(root㉿kali)-[/var/log]
└─# ls -sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/dpkg.log
sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/boot.log
sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/Xorg.0.log
sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/alternatives.log

Added monitor of '/var/log/dpkg.log'.
Added monitor of '/var/log/boot.log'.
Added monitor of '/var/log/Xorg.0.log'.
Added monitor of '/var/log/alternatives.log'.
```

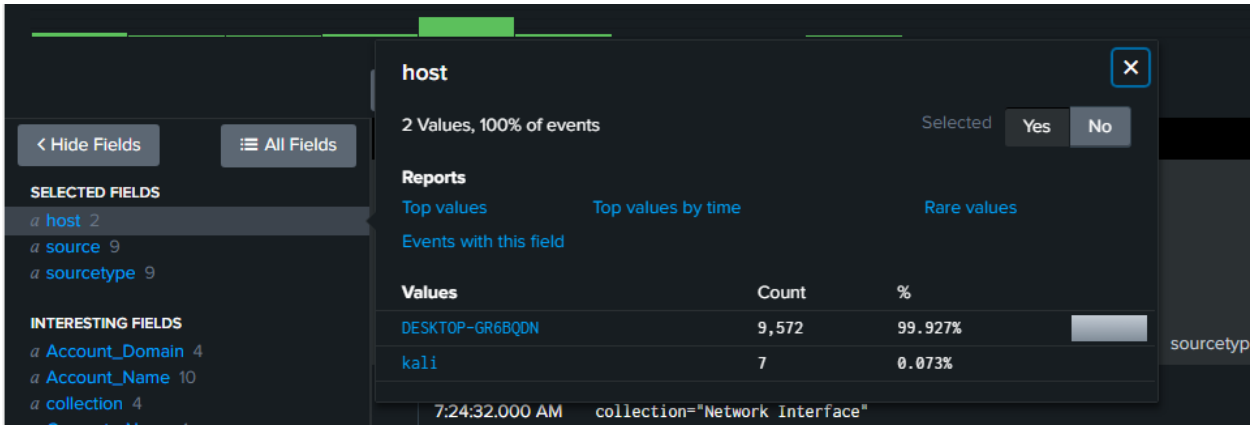
Now restart the Splunk

```
┌──(root㉿kali)-[/opt/splunkforwarder/bin]
└─# ./splunk restart
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
.
```

Now go back to Splunk and check the data summary for newly add machine.




New Search
Save As
Create Table View
Close
index=*
Last 24 hours
9,579 events (6/21/25 7:00:00.000 AM to 6/22/25 7:24:33.000 AM)
No Event Sampling
Job
Smart Mode
Events (9,579)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Format
Show: 20 Per Page
View: List
Prev
1 2 3 4 5 6 7 8
Next
Hide Fields
All Fields
SELECTED FIELDS
host 2
source 9
sourcetype 9
INTERESTING FIELDS
Account_Domain 4
Account_Name 10
collection 4
ComputerName 1
counter 7
EventCode 67
EventType 4
index 1
instance 3
Keywords 9
Time
Event
6/22/25 7:24:32.000 AM
06/22/2025 07:24:32.781 -0700
collection="Available Memory"
object=Memory
counter="Available Bytes"
instance=0
Show all 6 lines
host = DESKTOP-GR6BQDN
source = Perfmon:Available Memory
sourcetype = Perfmon:Available Memory
6/22/25 7:24:32.000 AM
06/22/2025 07:24:32.779 -0700
collection="Network Interface"
object="Network Interface"
counter="Bytes Sent/sec"
instance="Intel[R] Dual Band Wireless-AC 3168"
Show all 6 lines
host = DESKTOP-GR6BQDN
source = Perfmon:Network Interface
sourcetype = Perfmon:Network Interface
6/22/25
06/22/2025 07:24:32.779 -0700
Activate Windows
Go to Settings to activate Windows.


Hide Fields
All Fields
SELECTED FIELDS
host 2
source 9
sourcetype 9
INTERESTING FIELDS
Account_Domain 4
Account_Name 10
collection 4
host
2 Values, 100% of events
Selected
Yes
No
Reports
Top values
Top values by time
Rare values
Events with this field
Values
Count
%
DESKTOP-GR6BQDN
9,572
99.927%
kali
7
0.073%
sourcetyp
7:24:32.000 AM
collection="Network Interface"