splunk®

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.
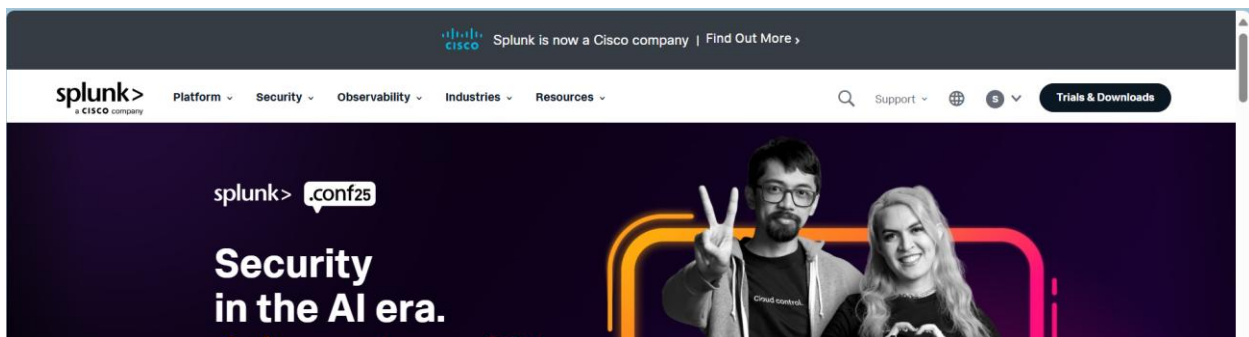
Use Case Example:

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.
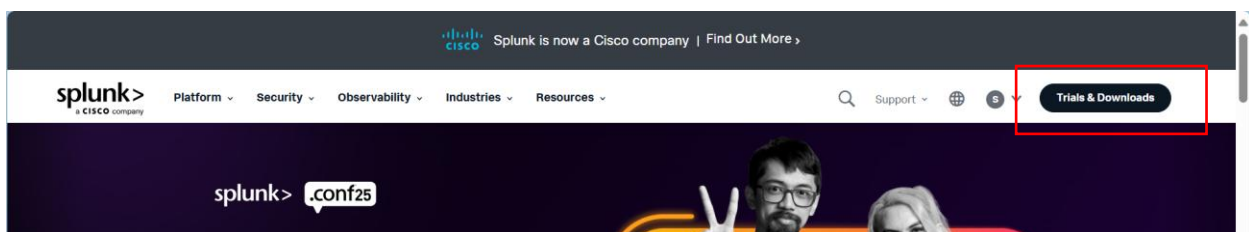
Splunk:
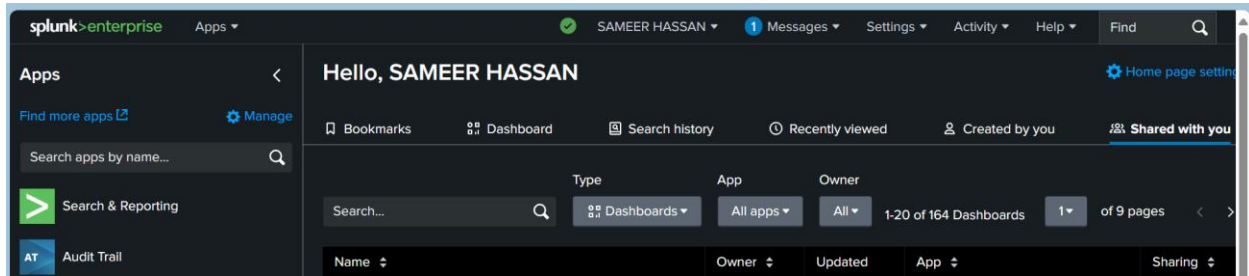
1: **Install Splunk Universal Forwarder on Windows**
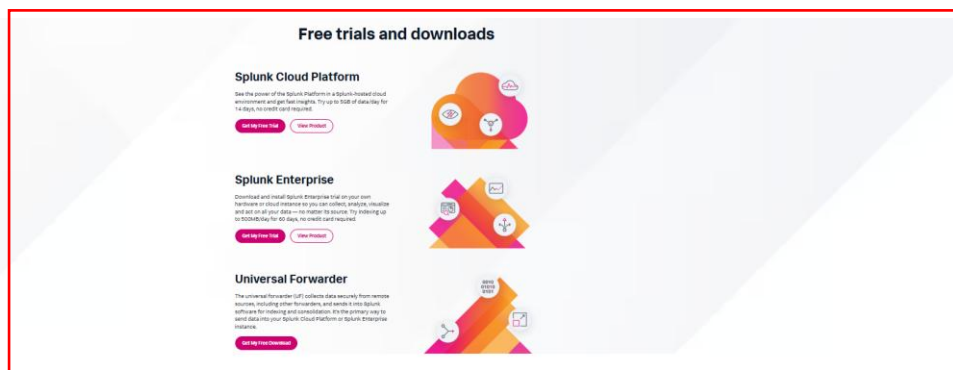
Open Splunk official website.

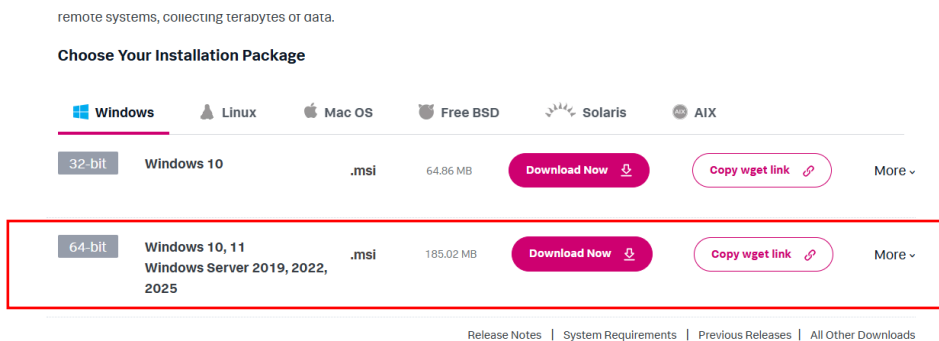Click on Trails & Download button

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
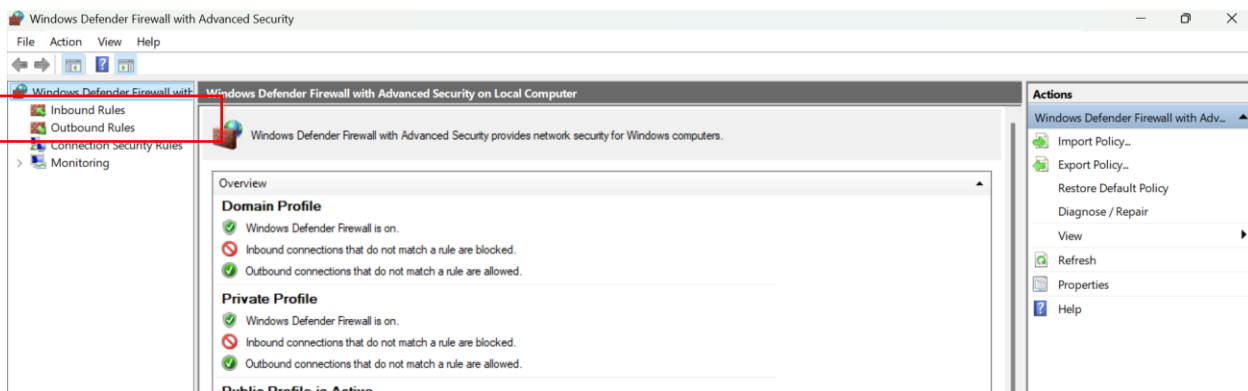

After clicking download you will redirect to license and agreement page accept and download
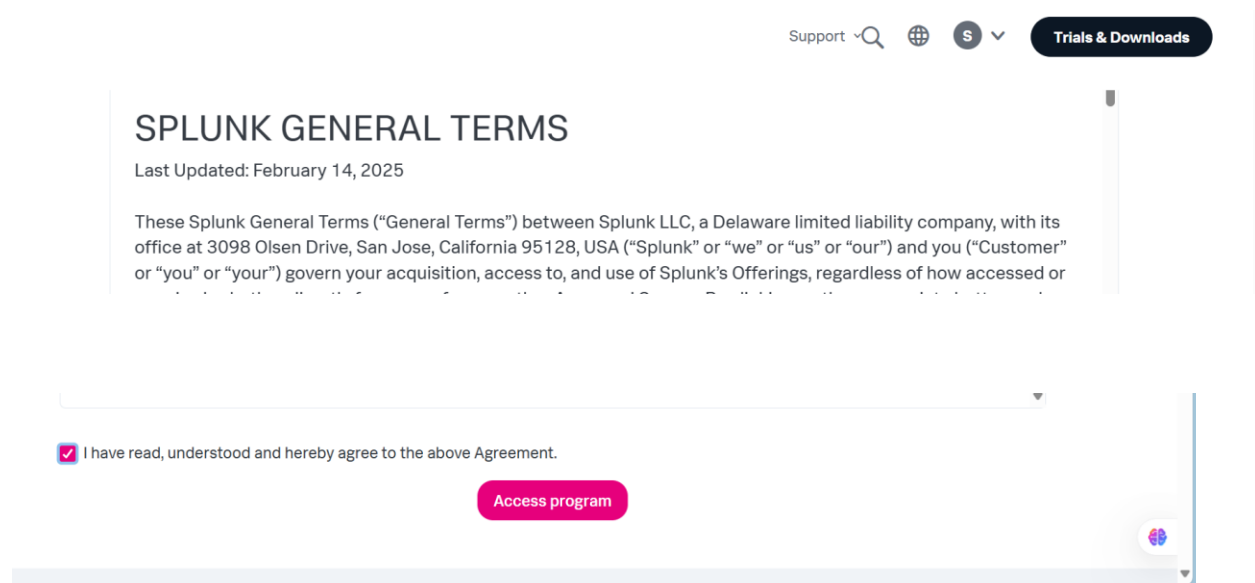
Now open windows firewall to allow 9997 and 8089 port for Splunk

Open- Windows Firewall then click on Advance settings
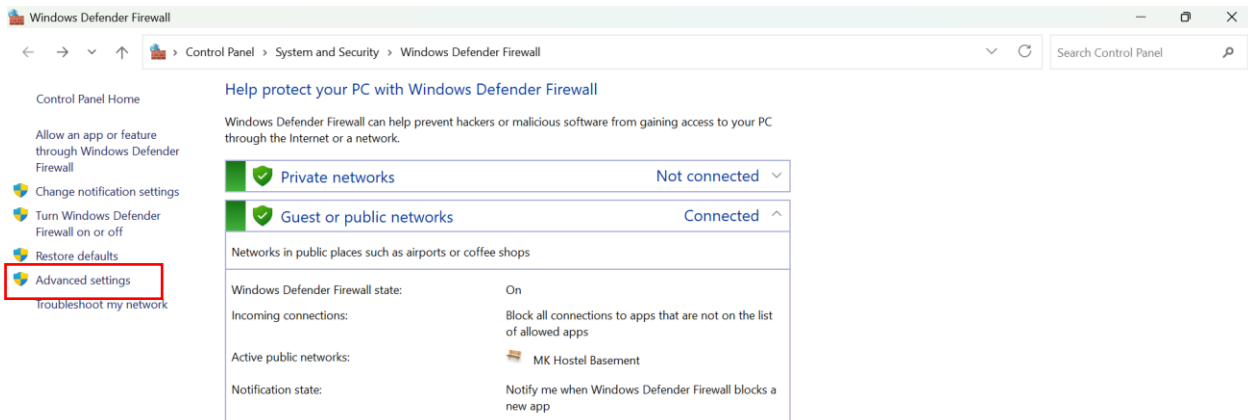
In advance setting you can see the inbound and outbound rules to allow or block any port or app.

Now click on inbound rules and then **New Rules**
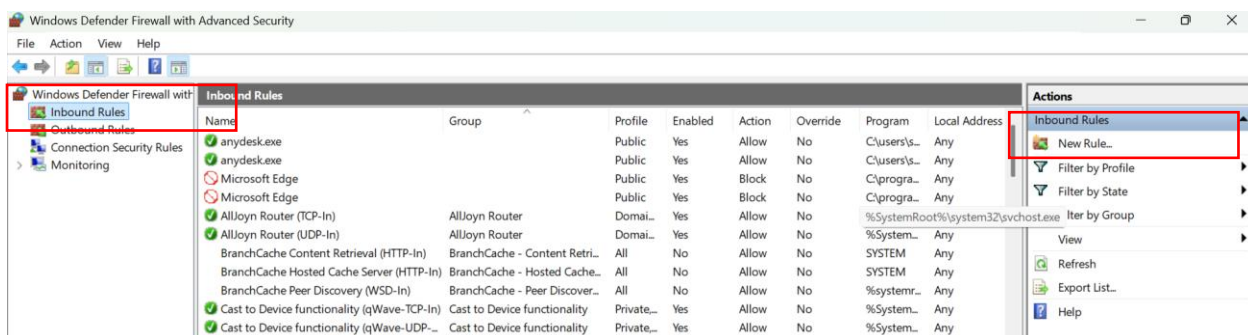
After clicking new rule it will show a popup select port

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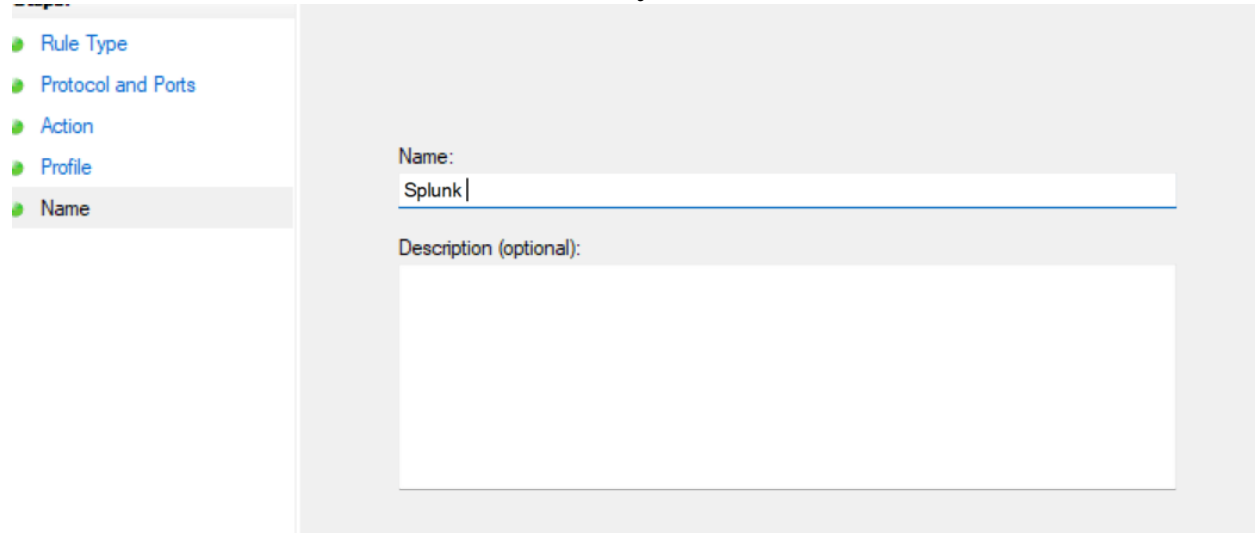
Now select Allow the connection

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
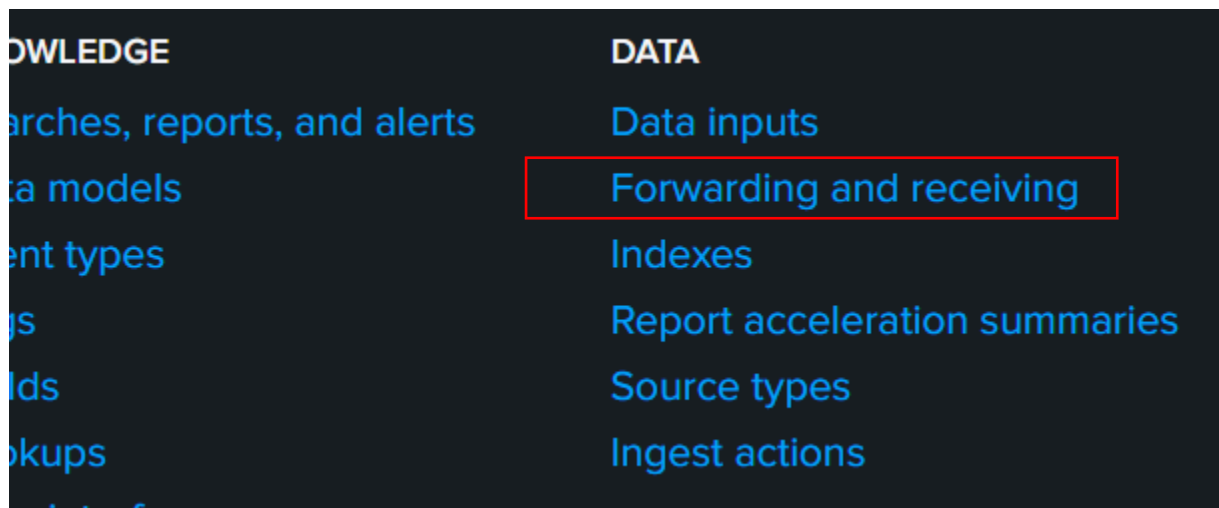
After opening forwarding and receiving page you will see two type **forwarding data and receiving data**
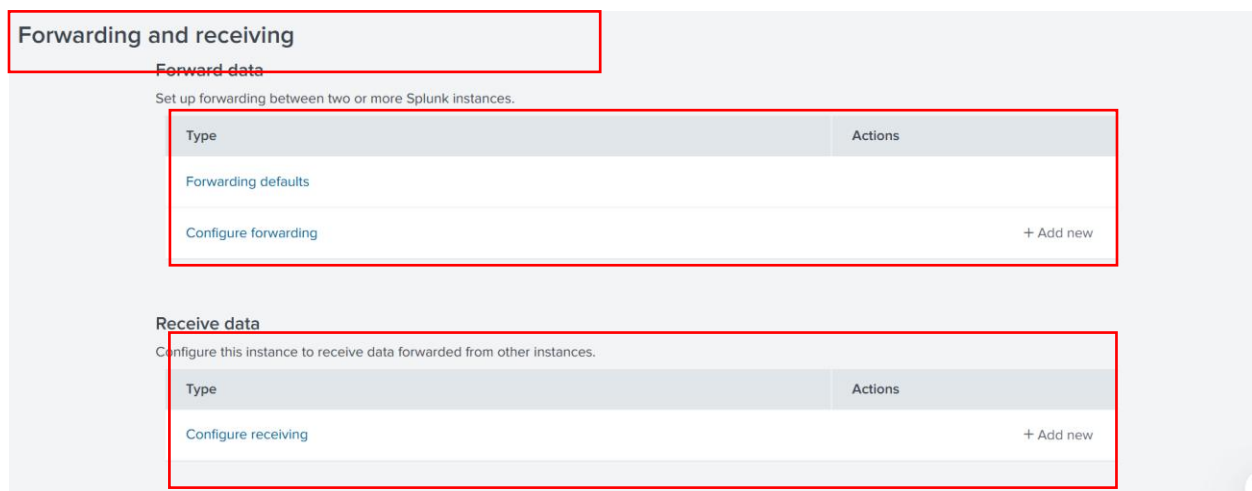
Click on add new in receive data section:

Type the port 9997 and click save

After Successful download start the forwarder
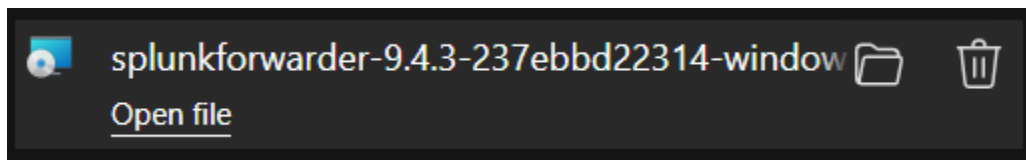
While installing it will ask you to accept the term check box. And another option of Splunk enterprise or cloud instance so I go with enterprise.
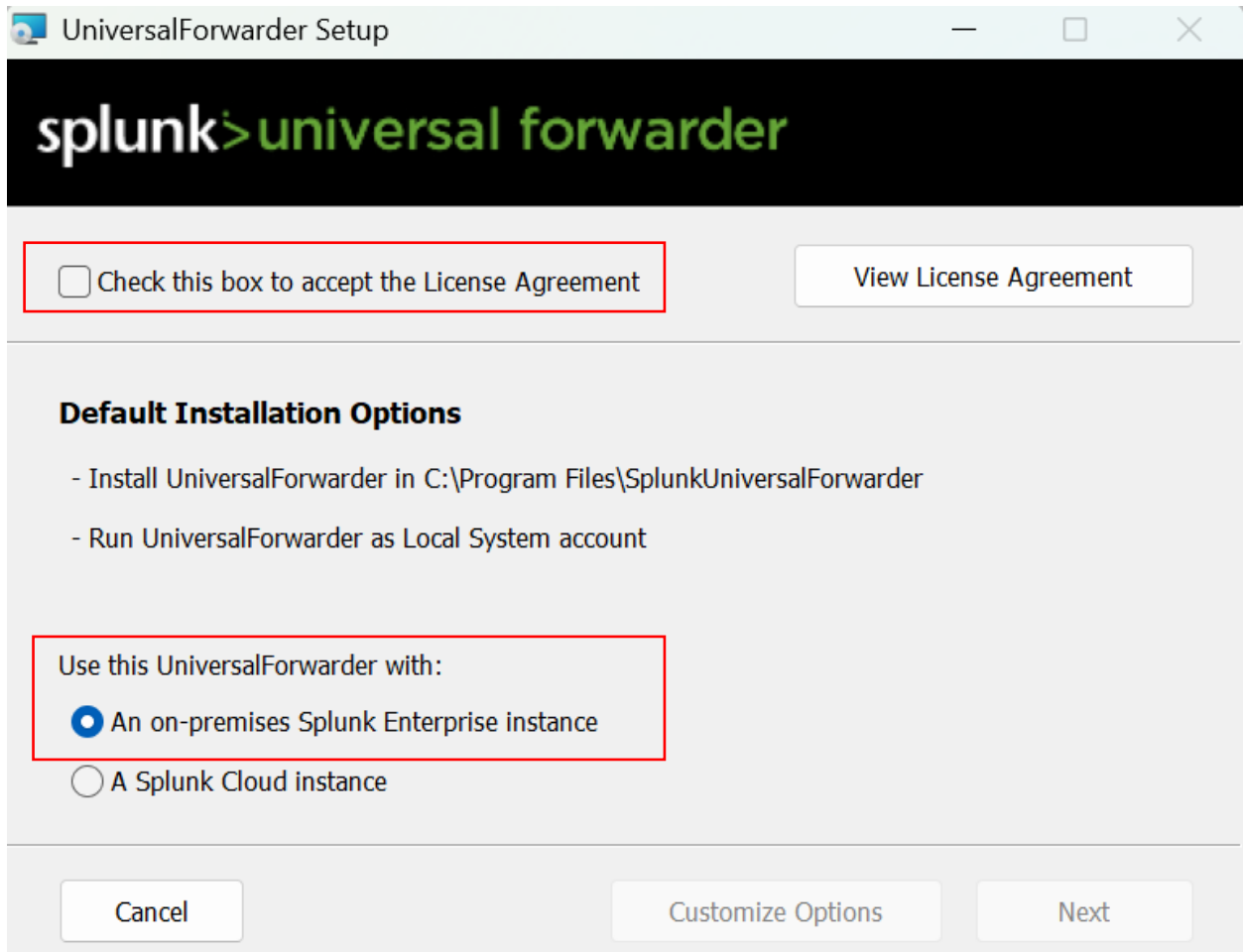
After checking the License box click on customize options

Click next:

Next

Select local and click next

The user you install UniversalForwarder as determines what data it has access to. The Managed Service Account and Group-Managed Service Account are supported by CLI only.

Install UniversalForwarder as:

○ Local System

Installs UniversalForwarder using local system account. UniversalForwarder can access all data on or forwarded to this machine.

○ Domain Account

Installs UniversalForwarder with domain account you provide. This lets you collect logs and metrics from remote machines as well as local and forwarded data. You can set the account in the next dialog, as a local administrator or a reduced privilege user.

● Virtual Account

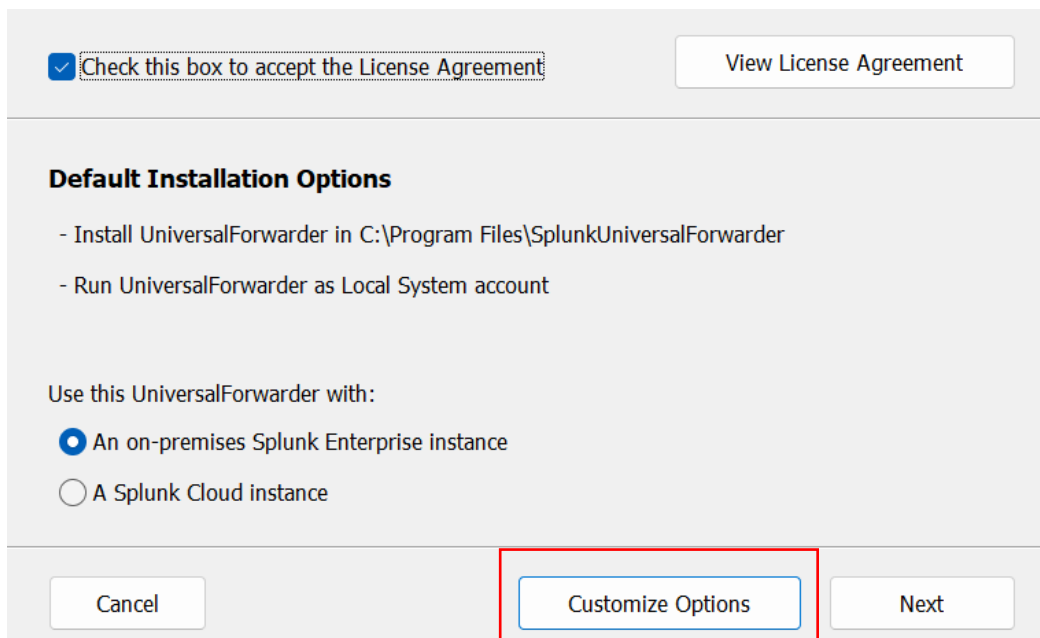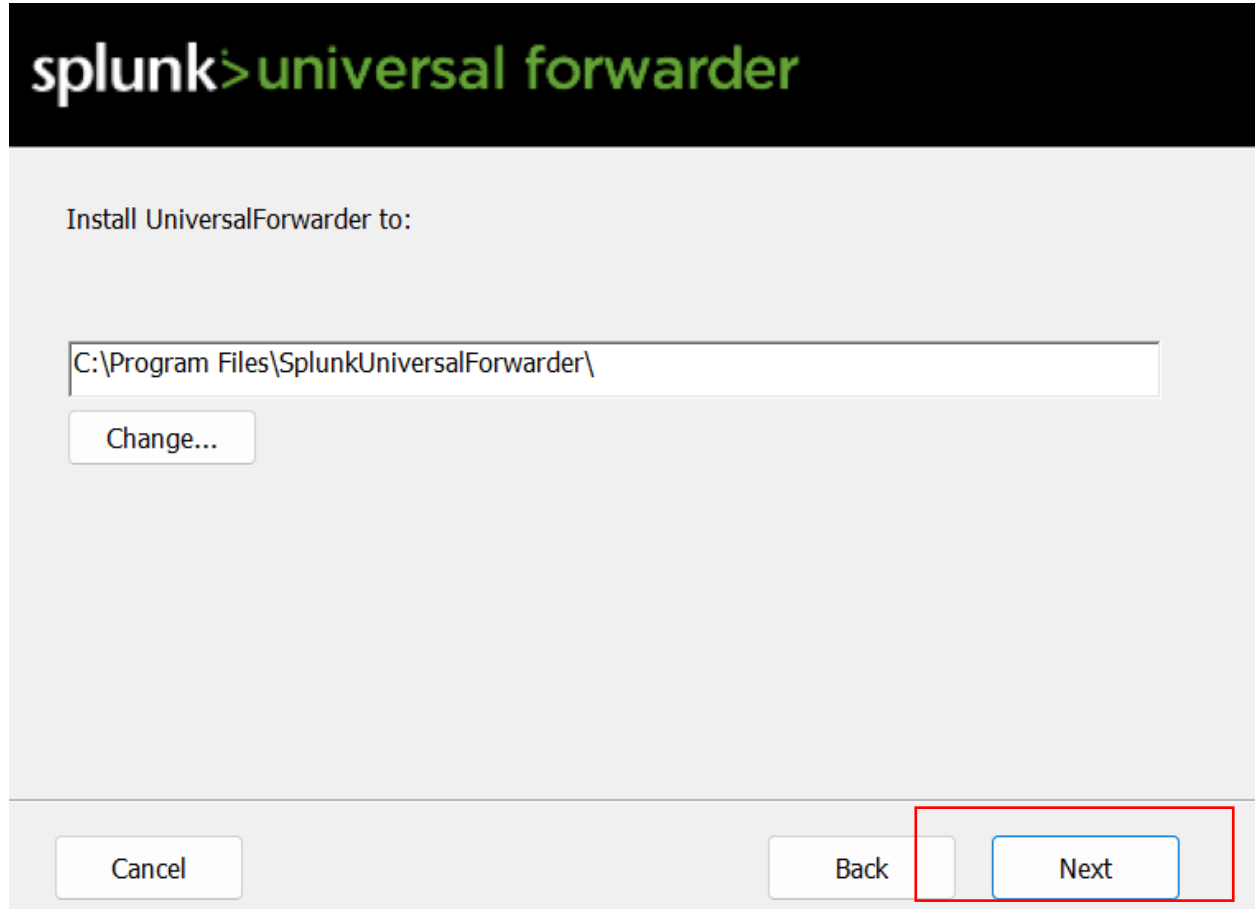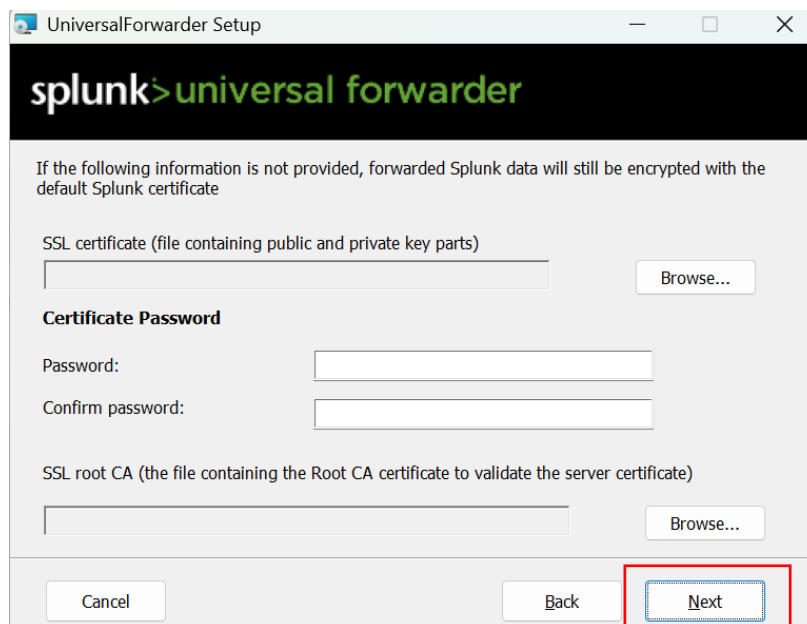Installs UniversalForwarder using a virtual account. UniversalForwarder can access all data on or forwarded to this machine.

Cancel		Back	Next

● Local System

Installs UniversalForwarder using local system account. UniversalForwarder can access all data on or forwarded to this machine.

○ Domain Account

Installs UniversalForwarder with domain account you provide. This lets you collect logs and metrics from remote machines as well as local and forwarded data. You can set the account in the next dialog, as a local administrator or a reduced privilege user.

○ Virtual Account

Installs UniversalForwarder using a virtual account. UniversalForwarder can access all data on or forwarded to this machine.

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

Create a Simple username and password for latter access

Username:

admin

☐ Generate random password

Password:

••••••••

Confirm password:

••••••••

Cancel   Back   Next

Now enter the ip of your Splunk server

If you intend to use a Splunk deployment server to configure this UniversalForwarder, please specify the host or IP, and port (default port is 8089). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

Deployment Server

Hostname or IP

[   ] : [   ]

Enter the hostname or IP of your deployment server, e.g.   default is 8089
ds.splunk.com

Cancel   Back   Next

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
```

Deployment Server

Hostname or IP

| 192.168.0.103 | : | 8089 |

Enter the hostname or IP of your deployment server, e.g.   default is 8089
ds.splunk.com

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

Receiving Indexer

Hostname or IP

| 192.168.0.103 | : | 9997 |

Enter the hostname or IP of your receiving indexer, e.g.   default is 9997
ds.splunk.com
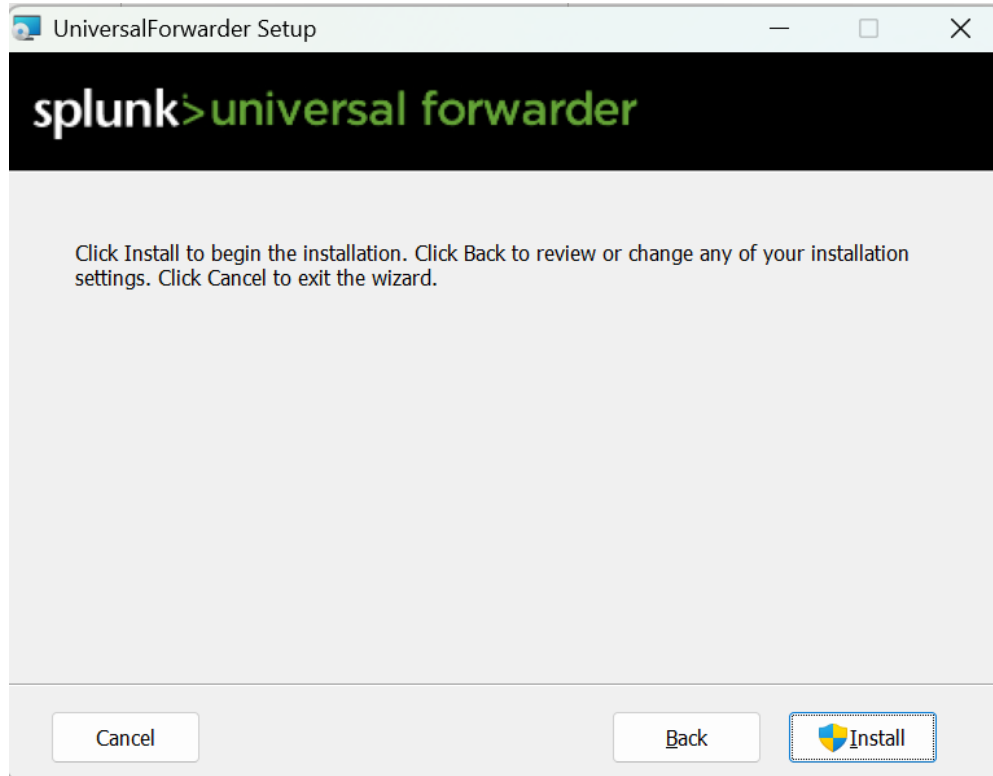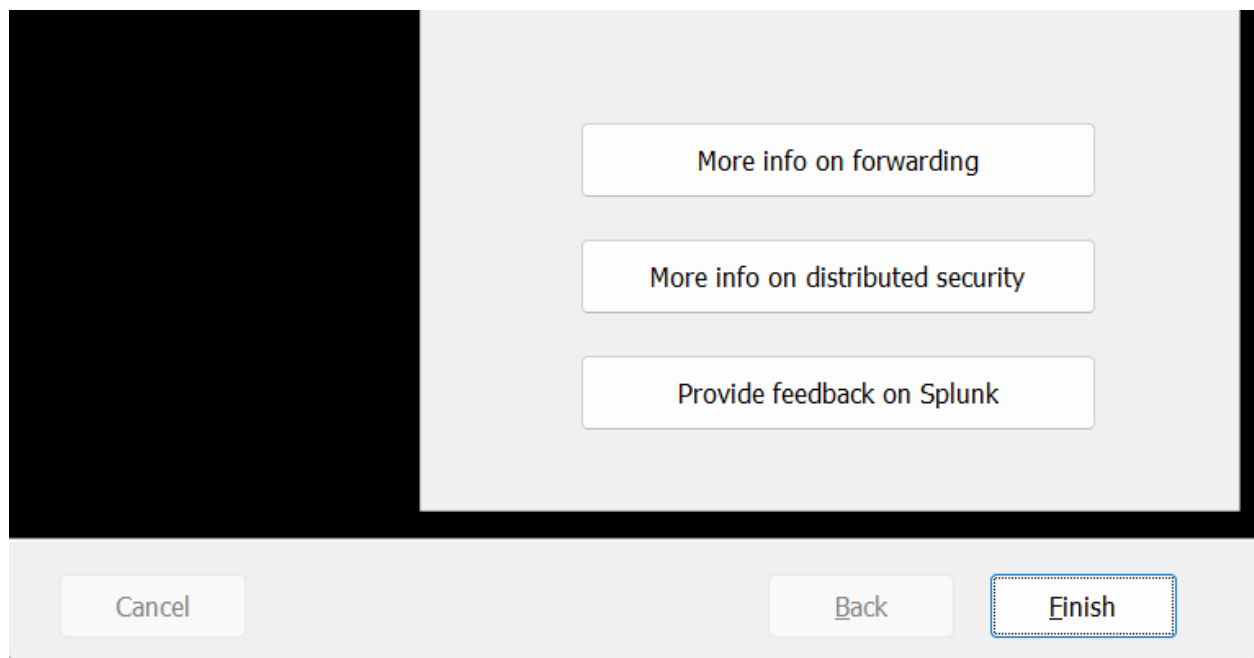
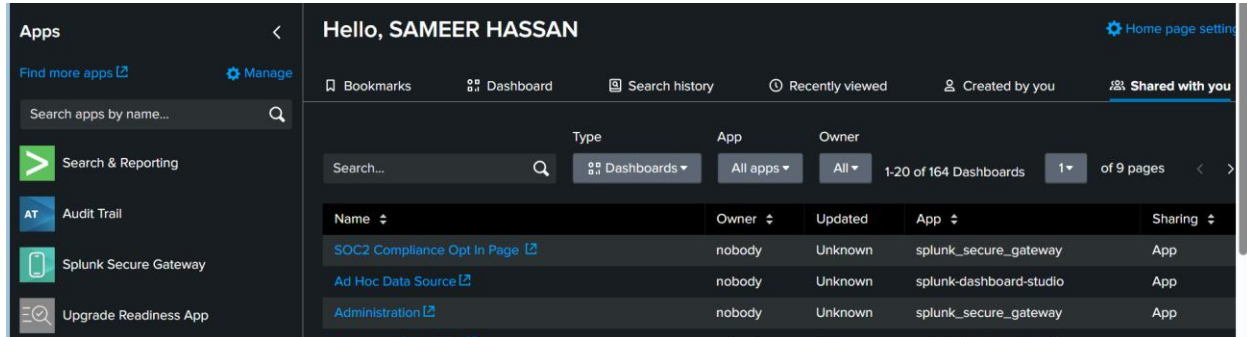| Cancel | | Back | Next |

After adding the ip of Receiving and sending server click install
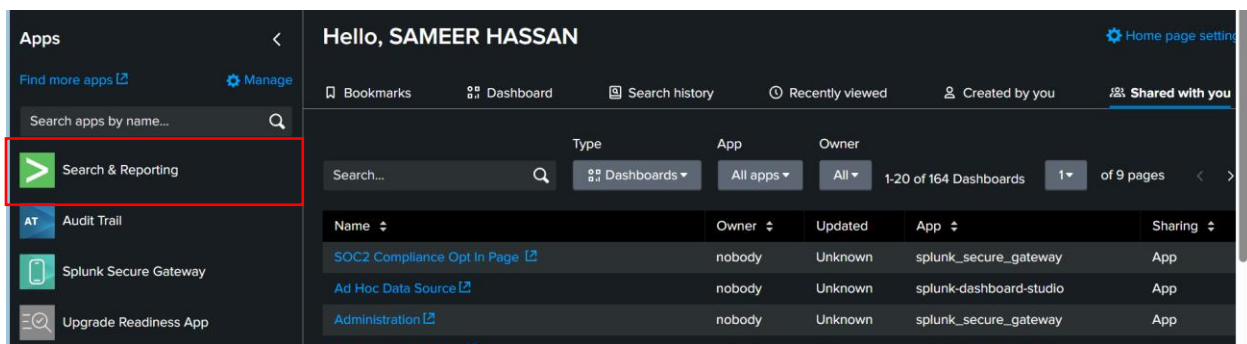

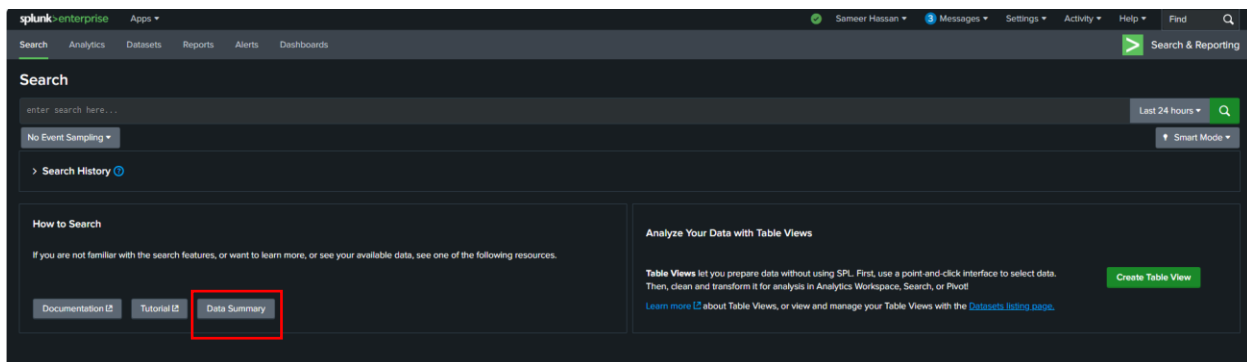After successful installation click finish

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