



INSTALLING SPLUNK FORWARDER (Windows)

By: SAMEER HASSAN

GitHub-link: [GitHub - sameerhassancode/Wazuh-labs](https://github.com/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.

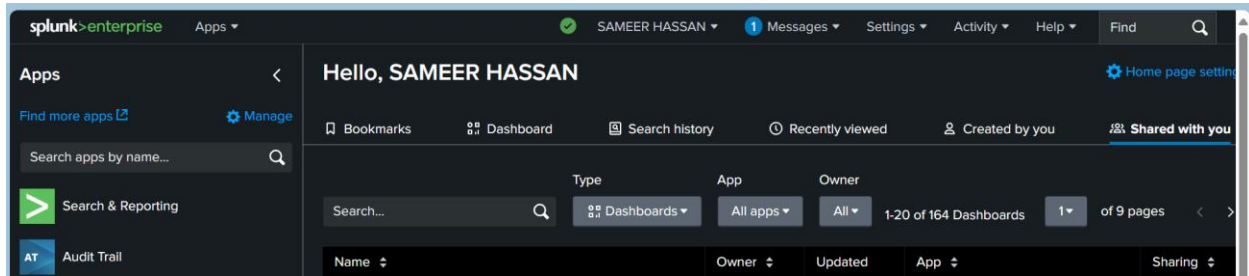
Types of Splunk Forwarders

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:

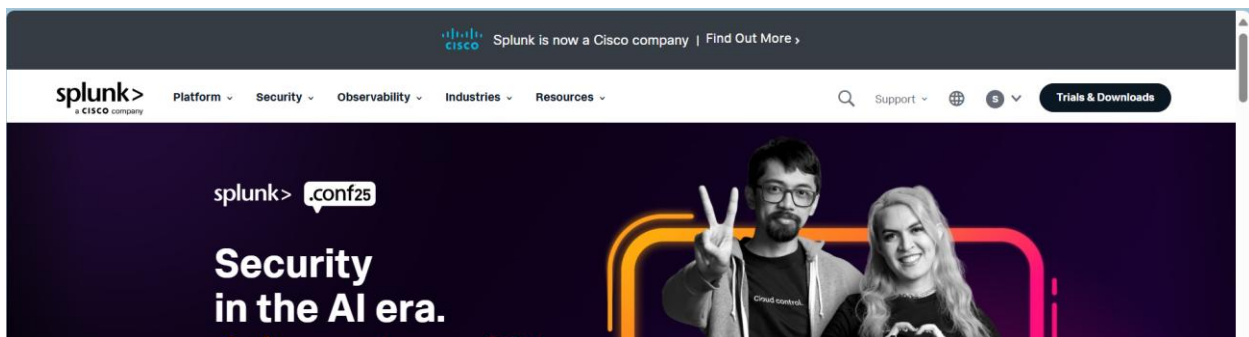
Install Splunk Universal Forwarder on a Windows server. Configure it to monitor event logs. Forward those logs to your central Splunk server for search, alerting, and dashboards.

Splunk:

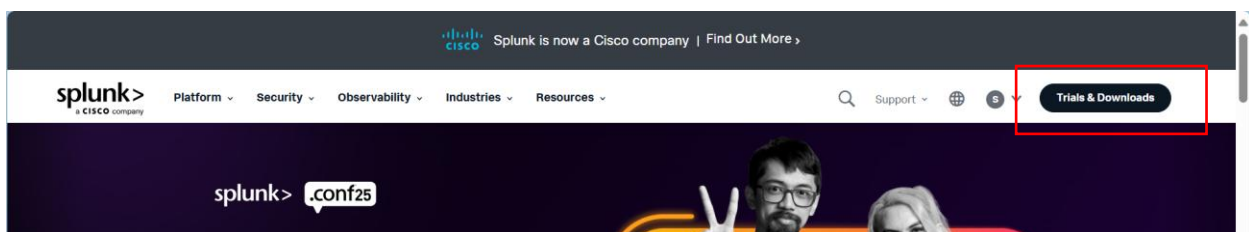


1: Install Splunk Universal Forwarder on Windows

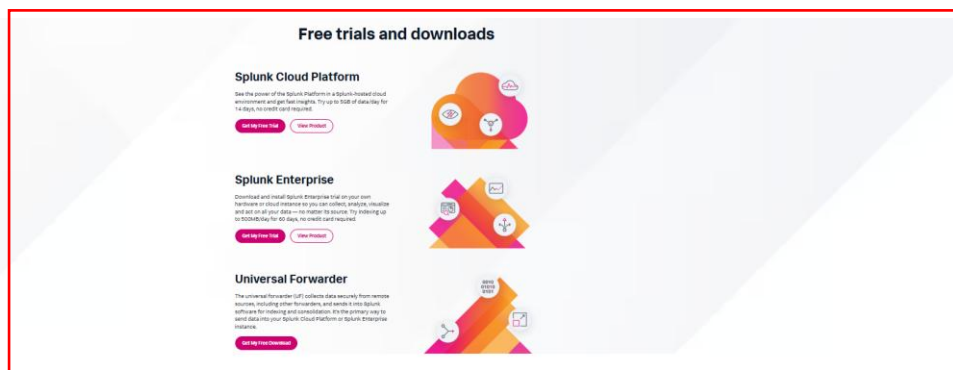
Open Splunk official website.



Click on Trails & Download button



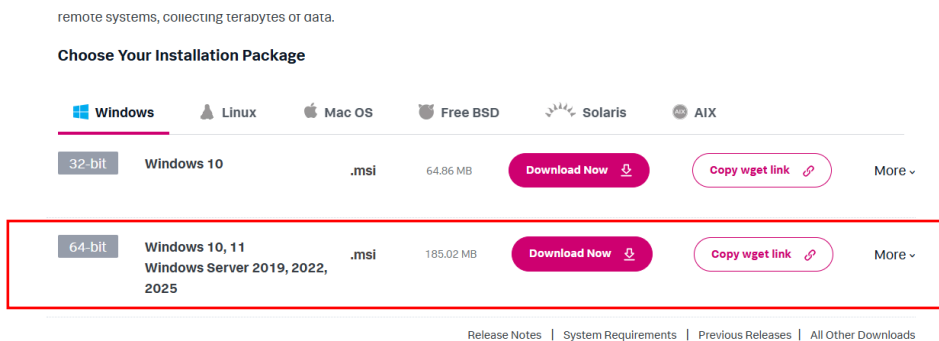
It will redirect you to download page. (if not login it will ask for login)



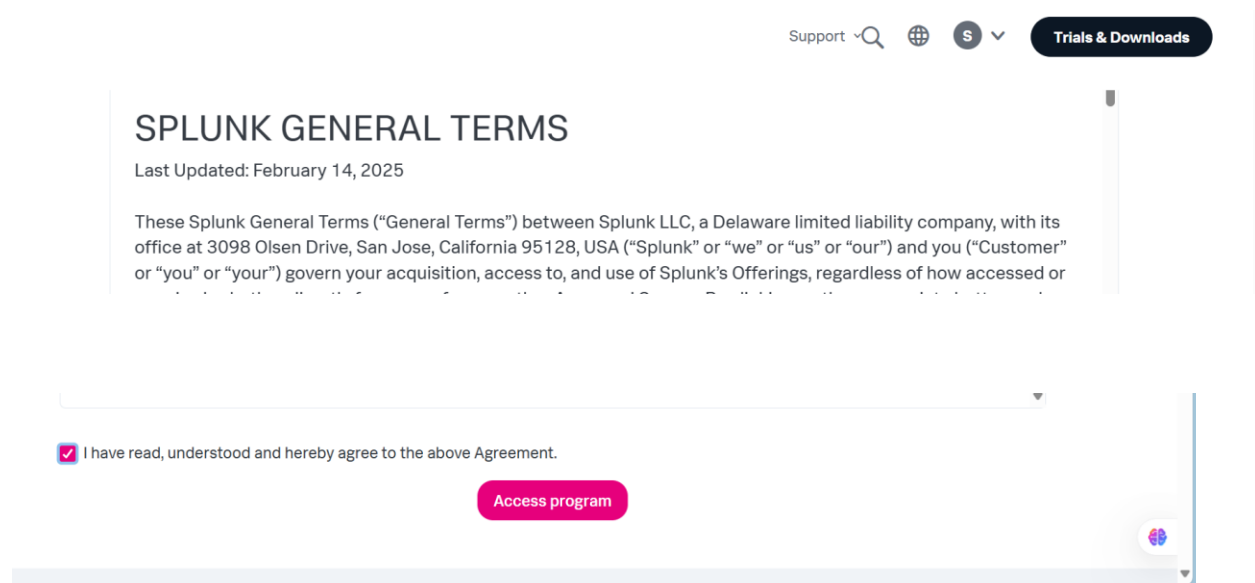
Now click on Get my Free Download Under Universal Forwarder section:



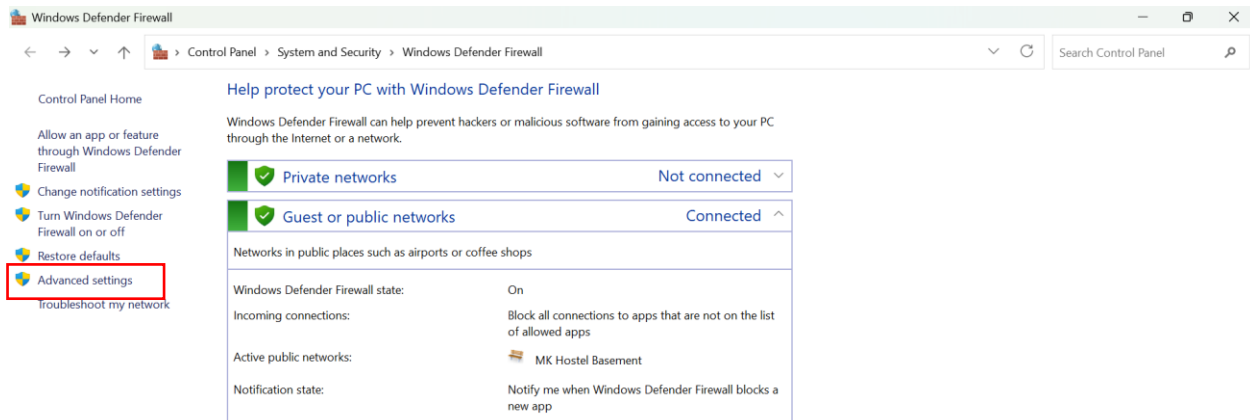
Now after clicking the download button it will redirect to main download page here select suitable version of windows universal forwarder and click download



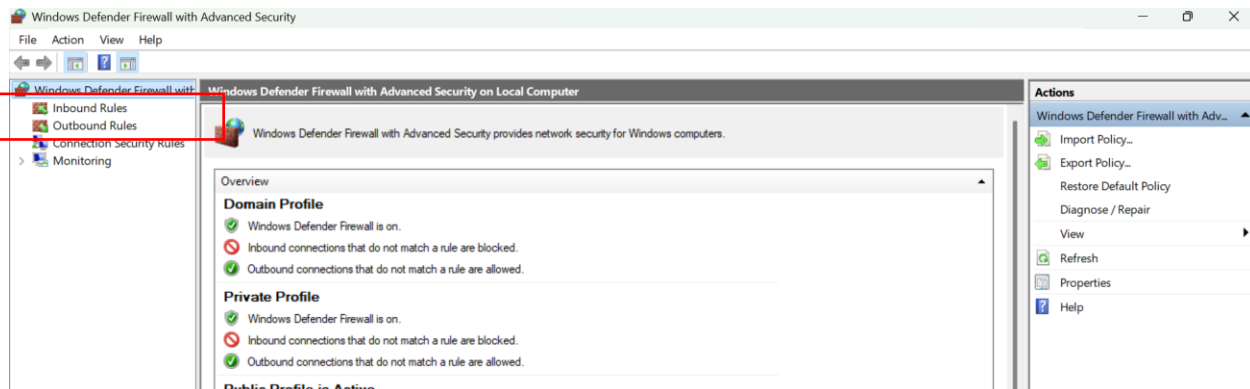
After clicking download you will redirect to license and agreement page accept and download



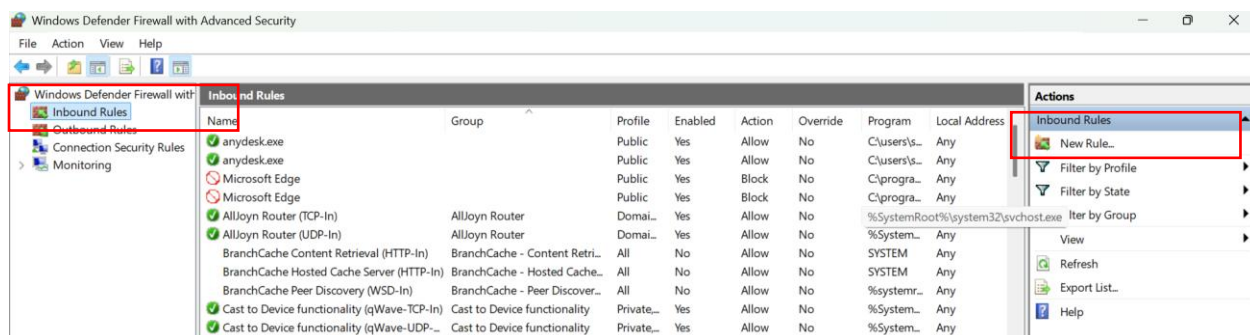
Now open windows firewall to allow 9997 and 8089 port for Splunk
Open- Windows Firewall then click on Advance settings



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

The screenshot shows a dialog box titled "What type of rule would you like to create?". On the left, there is a sidebar with the following steps: Rule Type (selected), Protocol and Ports, Action, Profile, and Name. The main area contains four radio button options:

- Program**: Rule that controls connections for a program.
- Port** (selected): Rule that controls connections for a TCP or UDP port.
- Predefined:**: A dropdown menu showing "AllJoyn Router". Rule that controls connections for a Windows experience.
- Custom**: Custom rule.

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

The screenshot shows a dialog box titled "Does this rule apply to TCP or UDP?". On the left, the sidebar shows: Steps: Rule Type, Protocol and Ports (selected), Action, Profile, and Name. The main area contains two radio button options:

- TCP** (selected)
- UDP**

Below these, it asks "Does this rule apply to all local ports or specific local ports?". There are two radio button options:

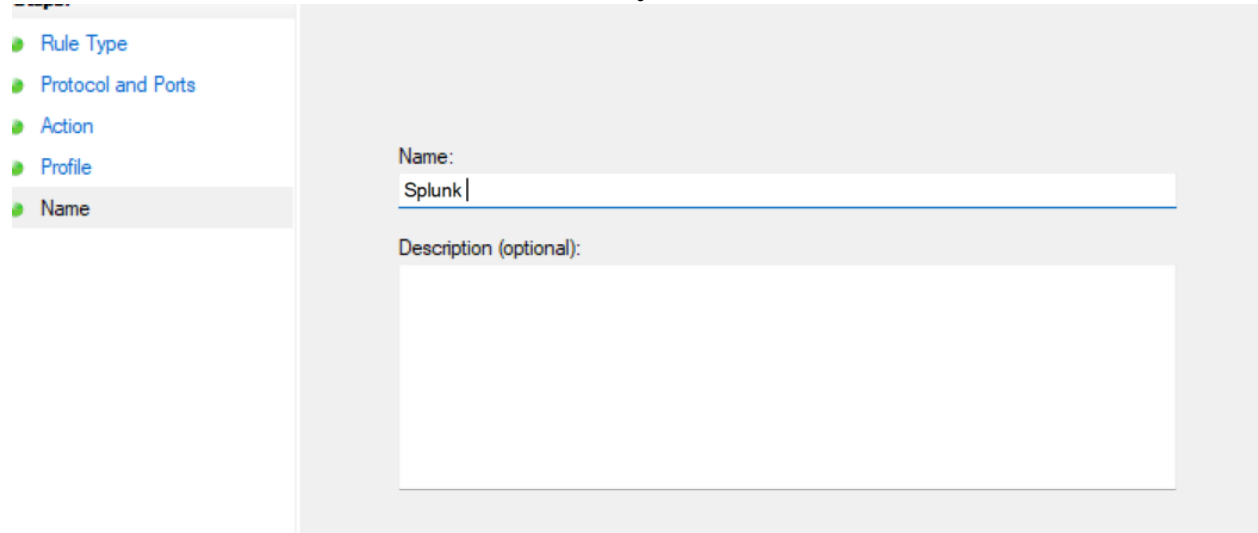
- All local ports**
- Specific local ports:** (selected) with a text input field containing "8089,9997". Below the input field, it says "Example: 80, 443, 5000-5010".

Now select Allow the connection

The screenshot shows a dialog box titled "What action should be taken when a connection matches the specified conditions?". On the left, the sidebar shows: Steps: Rule Type, Protocol and Ports, Action (selected), Profile, and Name. The main area contains three radio button options:

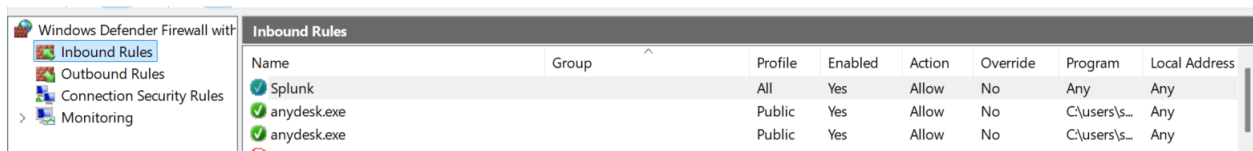
- Allow the connection** (selected): This includes connections that are protected with IPsec as well as those are not.
- Allow the connection if it is secure**: This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node. Below this option is a "Customize..." button.
- Block the connection**

Now write the rule name and hit okay!



The screenshot shows the 'Name' step of the Windows Firewall rule creation wizard. On the left, a sidebar lists the steps: Rule Type, Protocol and Ports, Action, Profile, and Name (which is currently selected). The main area has a 'Name:' label followed by a text box containing 'Splunk'. Below it, there is a 'Description (optional):' label followed by a larger empty text box.

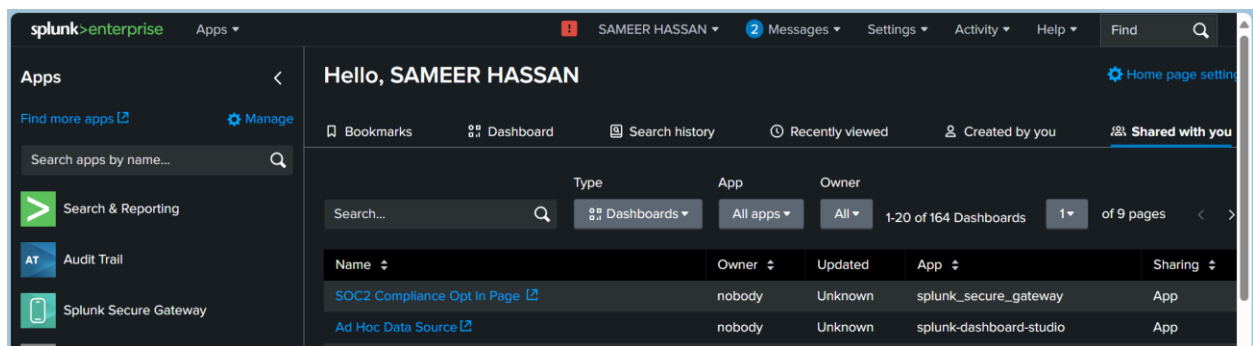
Rule is created:



The screenshot shows the 'Inbound Rules' list in Windows Firewall. The table below represents the data visible in the screenshot.

Name	Group	Profile	Enabled	Action	Override	Program	Local Address
Splunk		All	Yes	Allow	No	Any	Any
anydesk.exe		Public	Yes	Allow	No	C:\users\s...	Any
anydesk.exe		Public	Yes	Allow	No	C:\users\s...	Any

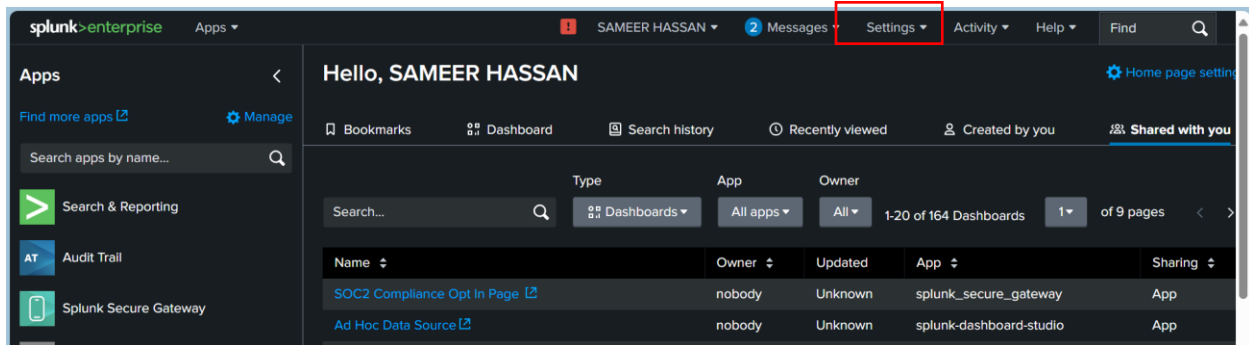
Now open Splunk dashboard



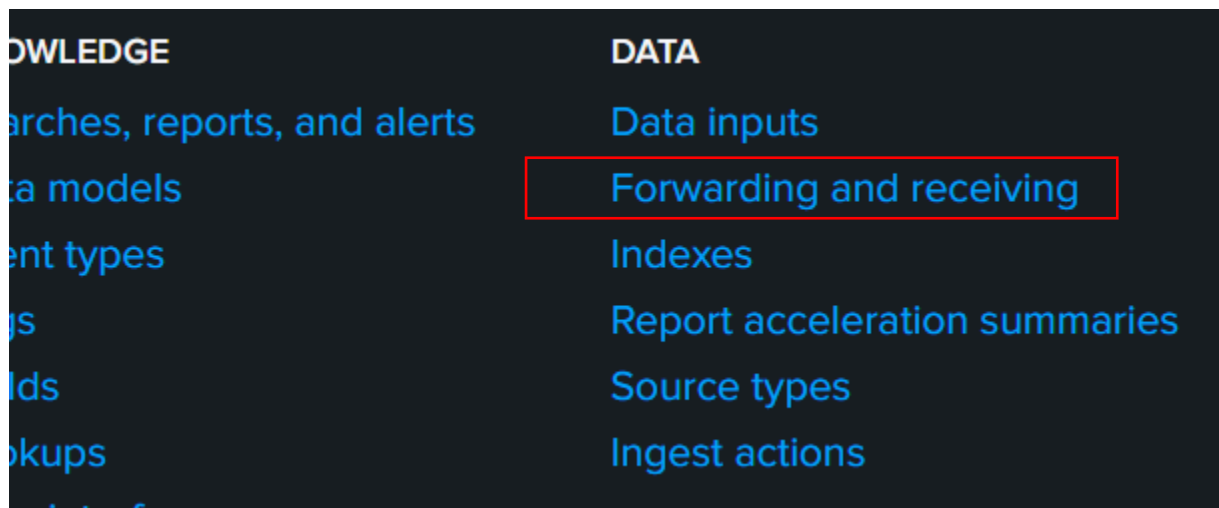
The screenshot shows the Splunk Enterprise dashboard interface. The top navigation bar includes the Splunk logo, user name 'SAMEER HASSAN', and various menu items like Messages, Settings, Activity, and Help. The main content area is titled 'Hello, SAMEER HASSAN' and displays a list of dashboards. The left sidebar shows the 'Apps' menu with options like Search & Reporting, Audit Trail, and Splunk Secure Gateway.

Name	Owner	Updated	App	Sharing
SOC2 Compliance Opt In Page	nobody	Unknown	splunk_secure_gateway	App
Ad Hoc Data Source	nobody	Unknown	splunk-dashboard-studio	App

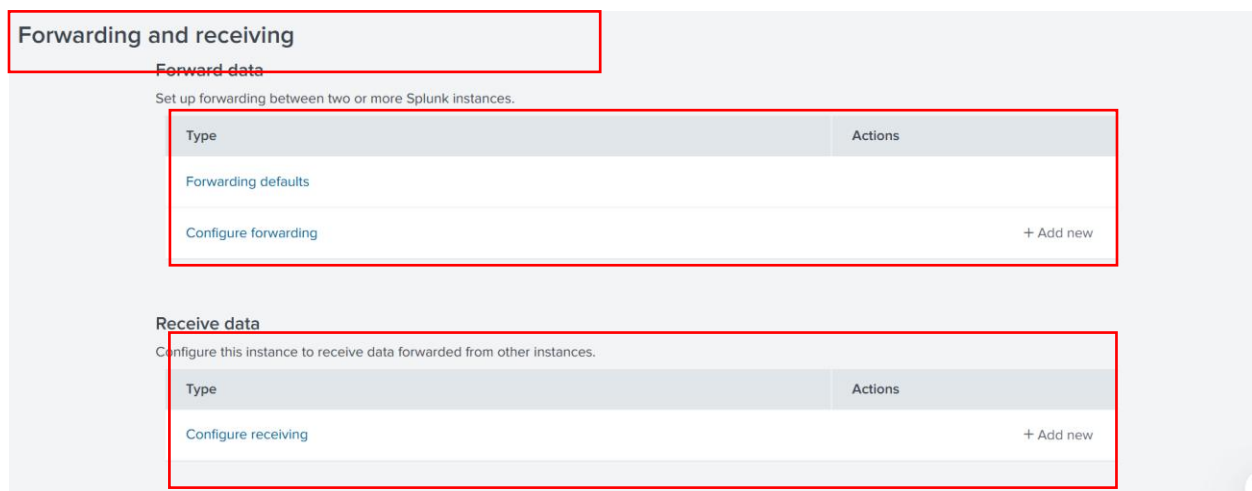
Click on setting



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:

Receive data
Configure this instance to receive data forwarded from other instances.

Type	Actions
Configure receiving	+ Add new

Type the port 9997 and click save

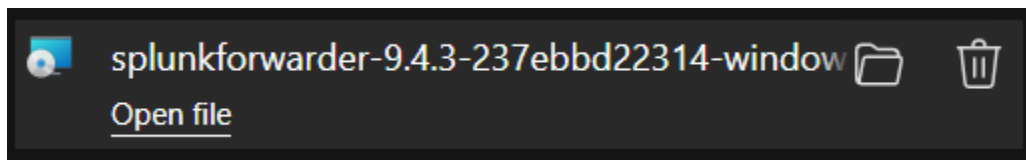
Configure receiving
Set up this Splunk instance to receive data from forwarder(s).

Listen on this port *

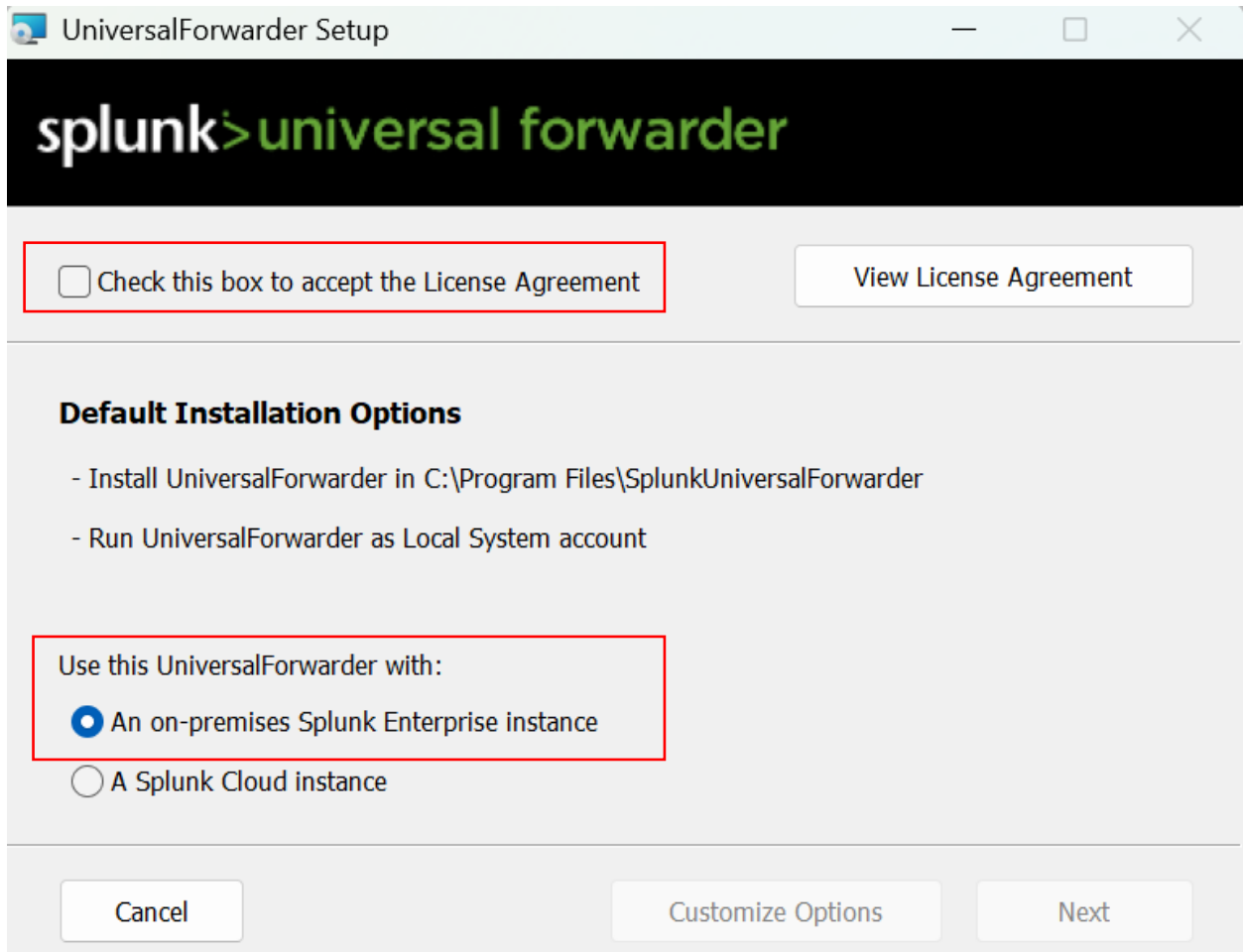
For example, 9997 will receive data on TCP port 9997.

[Cancel](#) [Save](#)

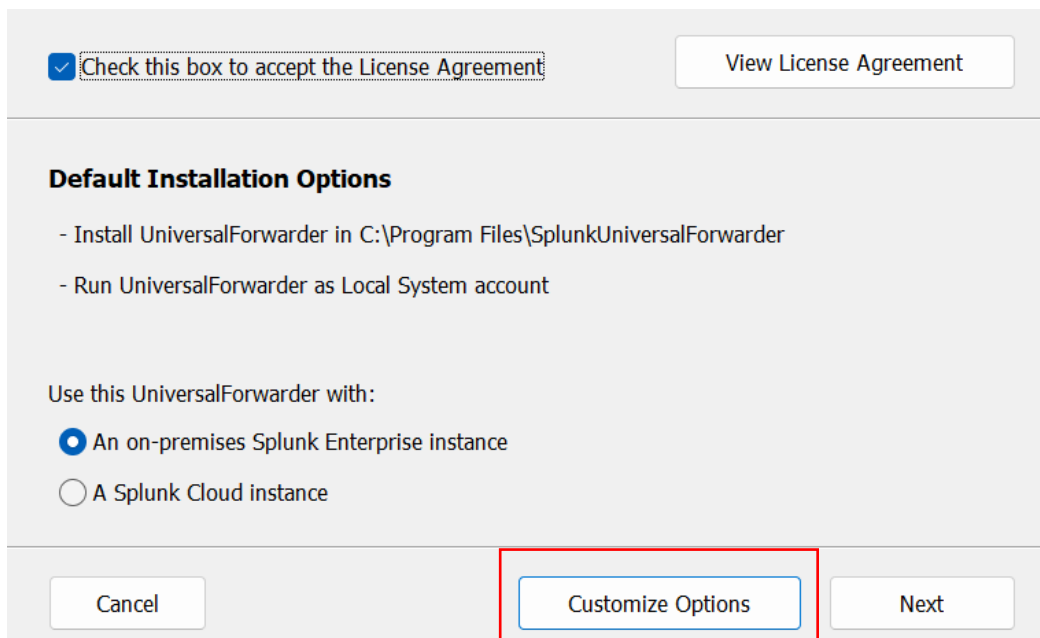
After Successful download start the forwarder



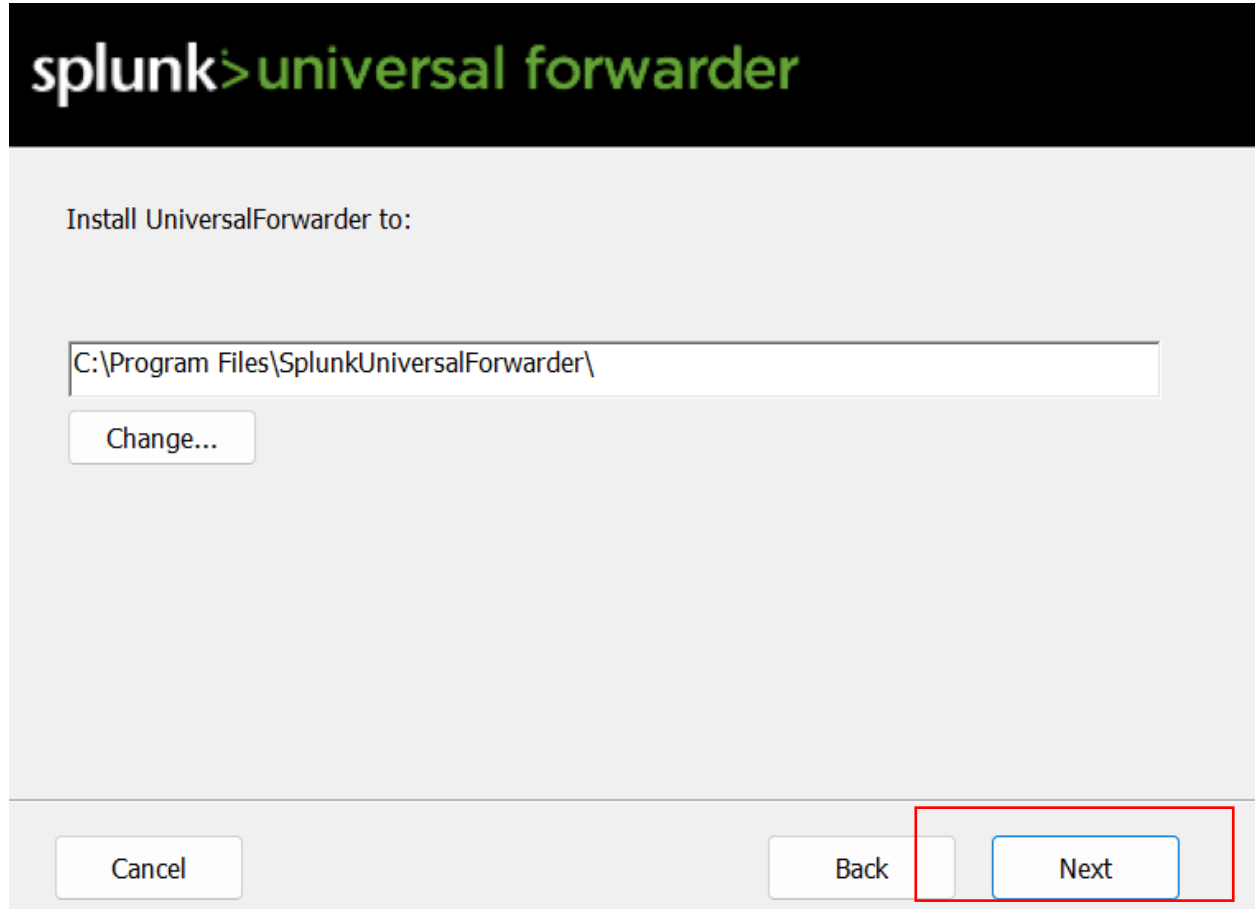
While installing it will ask you to accept the term check box. And another option of Splunk enterprise or cloud instance so I go with enterprise.



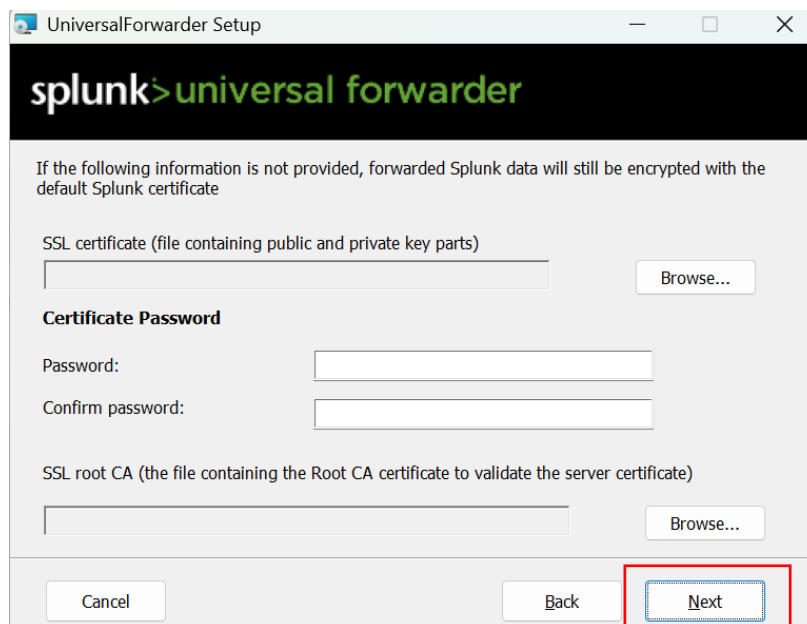
After checking the License box click on customize options



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

splunk>universal forwarder

Windows Event Logs

- ☐ Application Logs
- ☐ Security Log
- ☐ System Log
- ☐ Forwarded Events Log
- ☐ Setup Log

Performance Monitor

- ☐ CPU Load
- ☐ Memory
- ☐ Disk Space
- ☐ Network Stats

Active Directory Monitoring

- ☐ Enable AD monitoring

Path to monitor

File...Directory...

Cancel

Back

Next

Create a Simple username and password for latter access

Username:

☐ Generate random password
Password:

Confirm password:

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. ds.splunk.com *default is 8089*

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

:

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

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

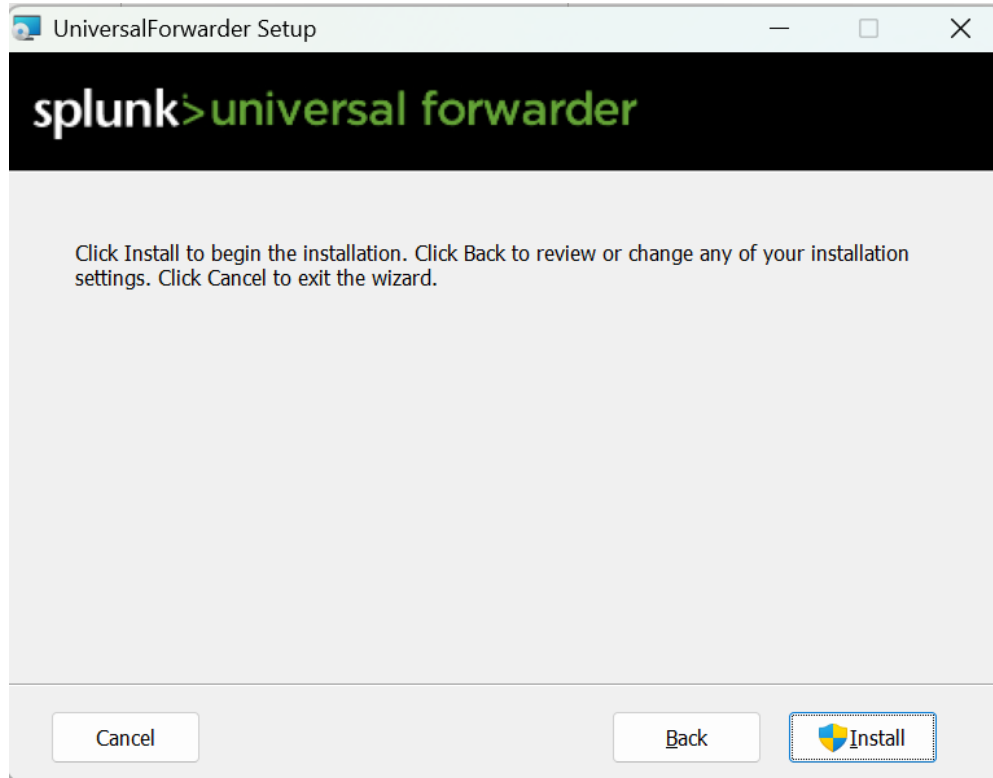
Receiving Indexer

Hostname or IP

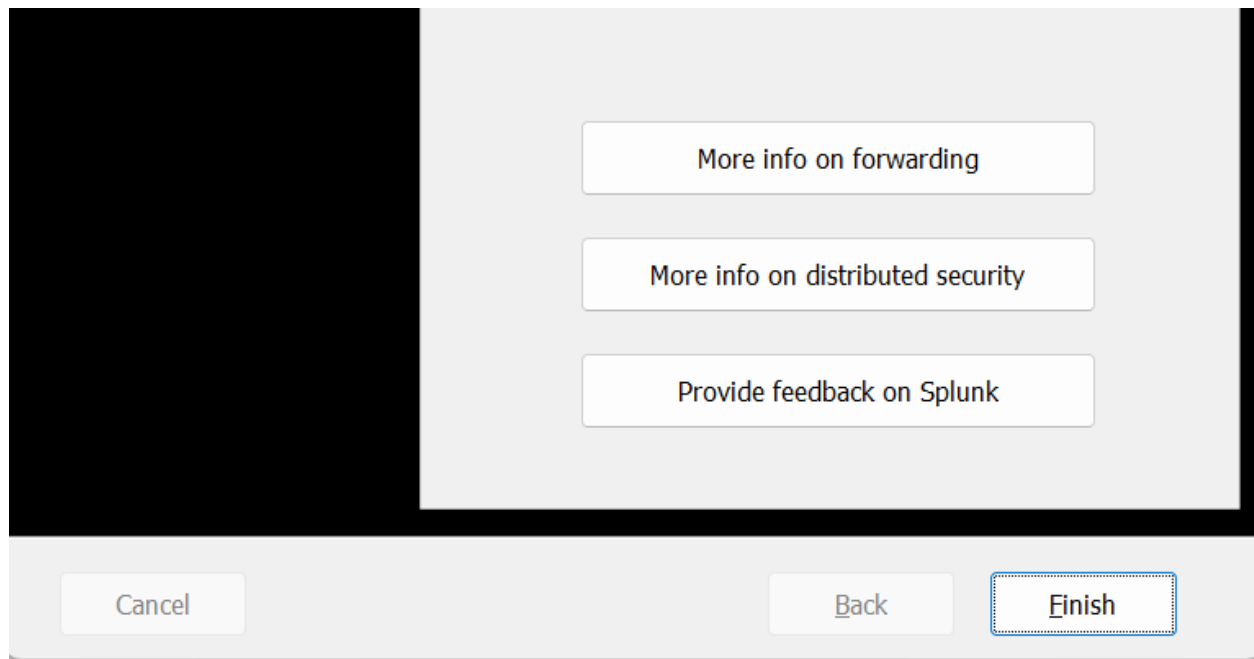
:

Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com *default is 9997*

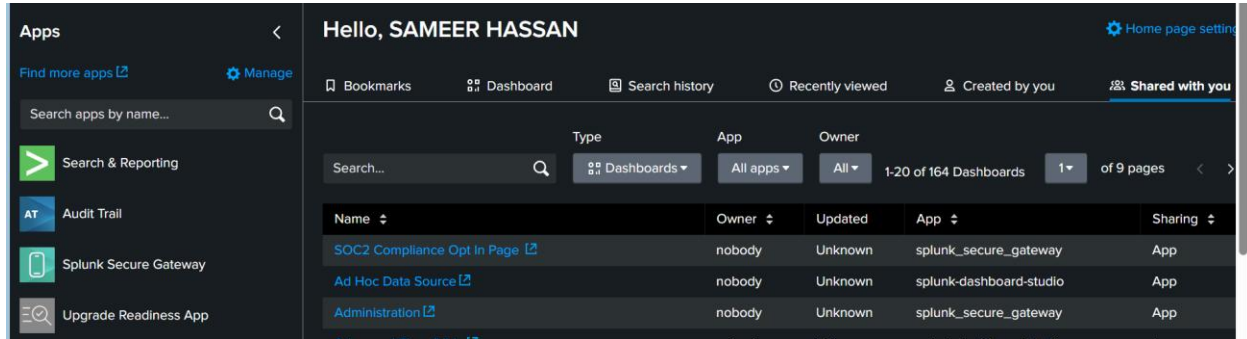
After adding the ip of Receiving and sending server click install



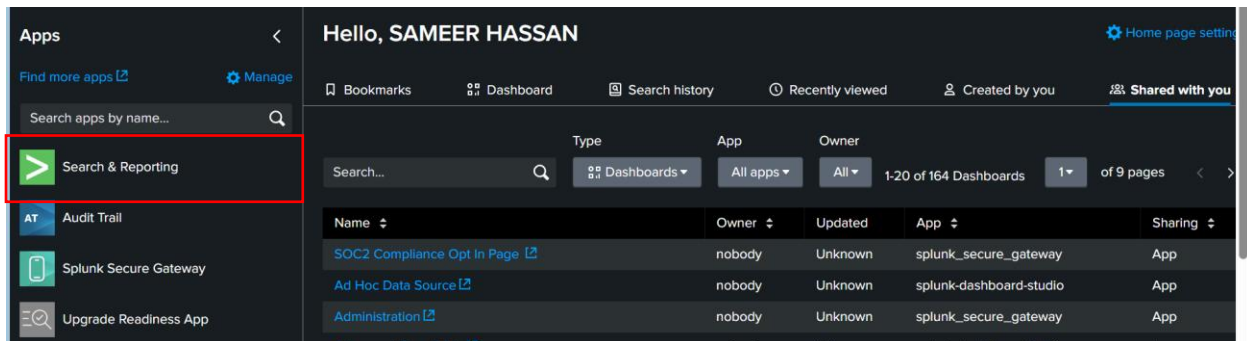
After successful installation click finish



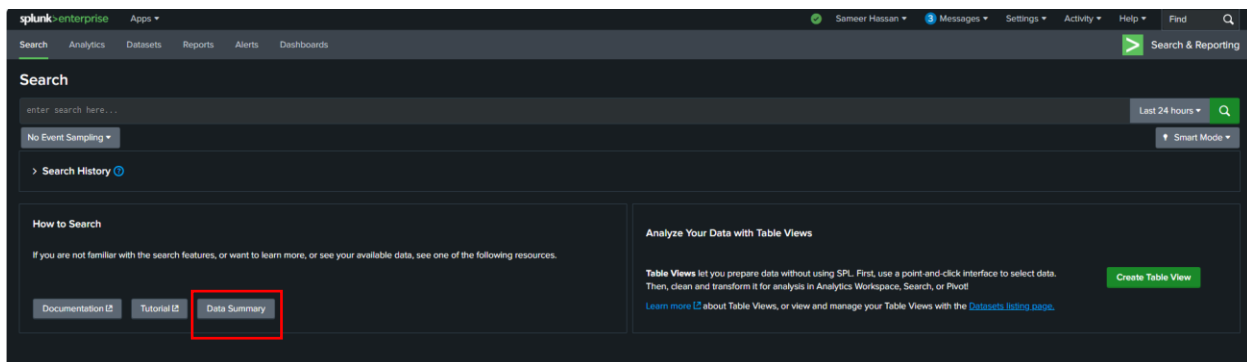
Now again open **Splunk Dashboard**



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

Data Summary ×			
Hosts (1) Sources (7) Sourcetypes (7)			
<input type="text" value="filter"/>			
Host ↕		Count ↕	Last Update ↕
DESKTOP-GR6BQDN		47,405	6/22/25 4:20:22.000 AM

Ubuntu Forwarder

Start the machine.



Open Splunk download page and go to Splunk forwarder section

Splunk Universal Forwarder 9.4.3

Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

Choose Your Installation Package

Windows	Linux	Mac OS	Free BSD	Solaris	AIX	
PPC64	4.x+, or 5.x+ kernel Linux distributions	.rpm	32.47 MB	Download Now	Copy wget link	More
		.tgz	32.6 MB	Download Now	Copy wget link	More
ARM	4.14+, 5.4+ kernel Linux distributions with libc v2.21+, 6.x+ kernel, Graviton+ Servers 64-bit	.deb	52.17 MB	Download Now	Copy wget link	More
		.rpm	84.76 MB	Download Now	Copy wget link	More

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

Splunk Universal Forwarder 9.4.3

Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

Choose Your Installation Package

Windows Linux Mac OS Free BSD Solaris AIX

PPC64	4.x+, or 5.x+ kernel Linux distributions	.rpm	32.47 MB	Download Now	Copy wget link	More
		.tgz	32.6 MB	Download Now	Copy wget link	More
ARM	4.14+, 5.4+ kernel Linux distributions with libc v2.21+, 6.x+ kernel, Graviton+ Servers 64-bit	.deb	52.17 MB	Download Now	Copy wget link	More
		.rpm	84.76 MB	Download Now	Copy wget link	More

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

```
File Actions Edit View Help
kali@kali: ~/Desktop
$ wget -O splunkforwarder-9.4.3-237ebbd22314-linux-arm64.deb "https://download.splunk.com/products/universalforwarder/releases/9.4.3/linux/splunkforwarder-9.4.3-237ebbd22314-linux-arm64.deb"
```

Forwarder Downloaded:

```
kali@kali: ~/Desktop
$ wget -O splunkforwarder-9.4.3-237ebbd22314-linux-arm64.deb "https://download.splunk.com/products/universalforwarder/releases/9.4.3/linux/splunkforwarder-9.4.3-237ebbd22314-linux-arm64.deb"
--2025-06-22 07:38:01-- https://download.splunk.com/products/universalforwarder/releases/9.4.3/linux/splunkforwarder-9.4.3-237ebbd22314-linux-arm64.deb
Resolving download.splunk.com (download.splunk.com)... 108.139.79.68, 108.139.79.44, 108.139.79.70, ...
Connecting to download.splunk.com (download.splunk.com)|108.139.79.68|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 54786294 (52M) [binary/octet-stream]
Saving to: 'splunkforwarder-9.4.3-237ebbd22314-linux-arm64.deb'

splunkforwarder-9.4.3-237ebbd22314-linux-arm64.deb 100%[=====] 52.17M 3.74MB/s in 24s

2025-06-22 07:38:26 (2.19 MB/s) - 'splunkforwarder-9.4.3-237ebbd22314-linux-arm64.deb' saved [54786294/54786294]
```

Now type ls to view the .tgz file. Extract 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.

```
(root@kali)-[/opt]
└─$ sudo /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 [8080]: 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]
└─$ sudo /opt/splunkforwarder/bin/splunk enable 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

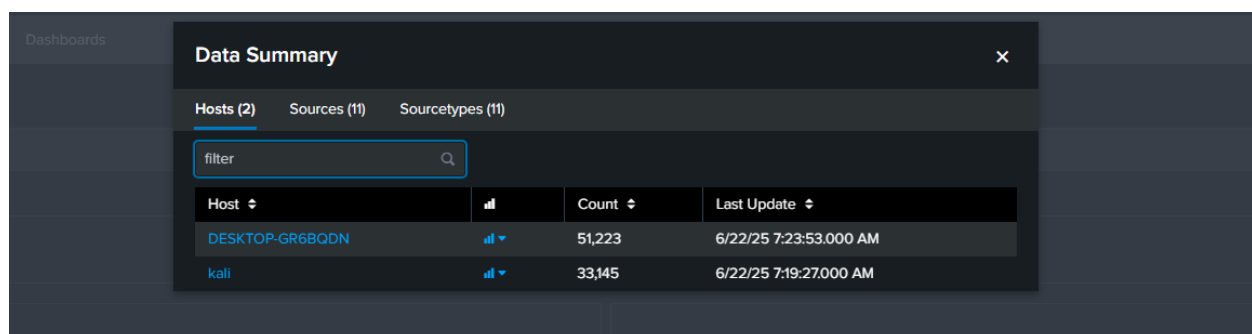
Command: add monitor [path]

```
(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.



The screenshot shows the Splunk Data Summary dashboard. It has a sidebar with 'Dashboards' and a main area with a 'Data Summary' window. The window has tabs for 'Hosts (2)', 'Sources (11)', and 'Sourcetypes (11)'. Below the tabs is a search filter box. The main table displays data for two hosts: 'DESKTOP-GR6BQDN' and 'kali'. Each row includes a host name, a status icon, a count, and a last update timestamp.

Host	Count	Last Update
DESKTOP-GR6BQDN	51,223	6/22/25 7:23:53.000 AM
kali	33,145	6/22/25 7:19:27.000 AM

