

What is Splunk?

Splunk is a powerful **data analytics platform** that can function as a **SIEM** when used with **Splunk Enterprise Security (ES)**.

Splunk ingests machine data such as:

- Server and application logs
 - Network device logs (firewalls, routers, IDS/IPS)
 - Endpoint and cloud logs
 - Authentication and access logs
-

Splunk as a SIEM

When Splunk is deployed with **Splunk Enterprise Security (ES)**, it provides full SIEM capabilities:

- Real-time security monitoring
 - Correlation searches and alerts
 - Security dashboards and visualizations
 - Incident review and investigation workflows
 - Risk-based alerting
 - MITRE ATT&CK mapping
-

Splunk SIEM Architecture (High Level)

1. **Data Sources** – Servers, endpoints, firewalls, cloud services
 2. **Forwarders** – Send logs to Splunk
 3. **Indexers** – Store and index data
 4. **Search Head** – Query, analyze, and visualize data
 5. **Enterprise Security App** – SIEM features and detections
-

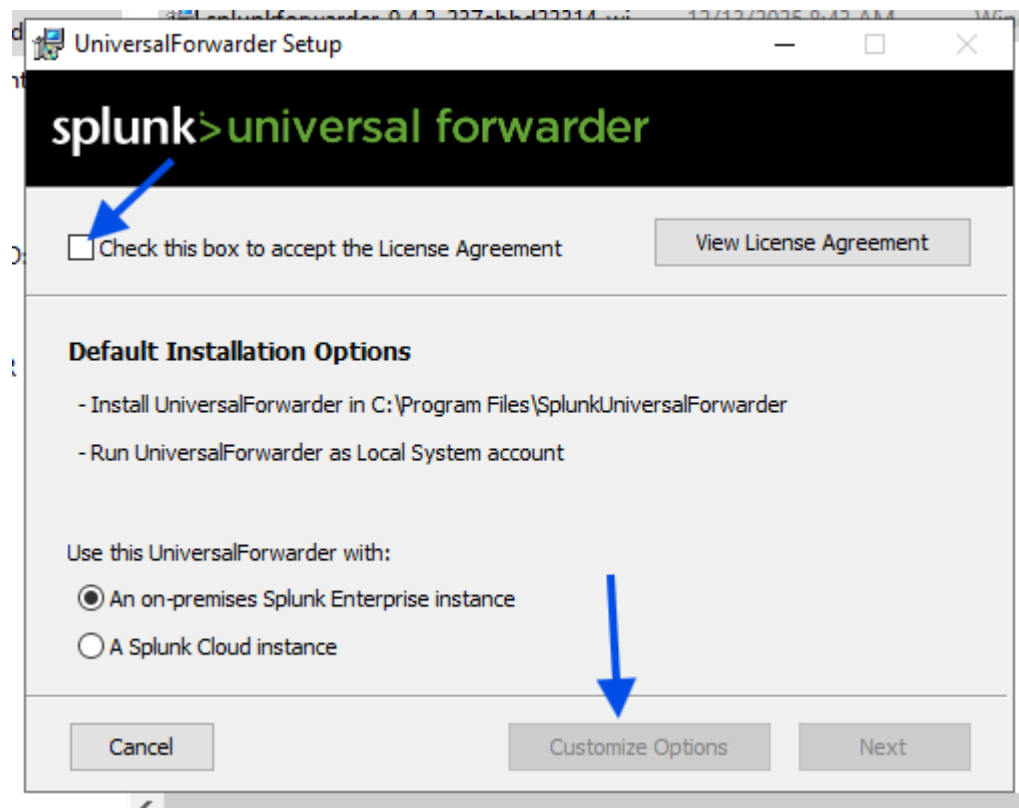
Why Organizations Use Splunk SIEM

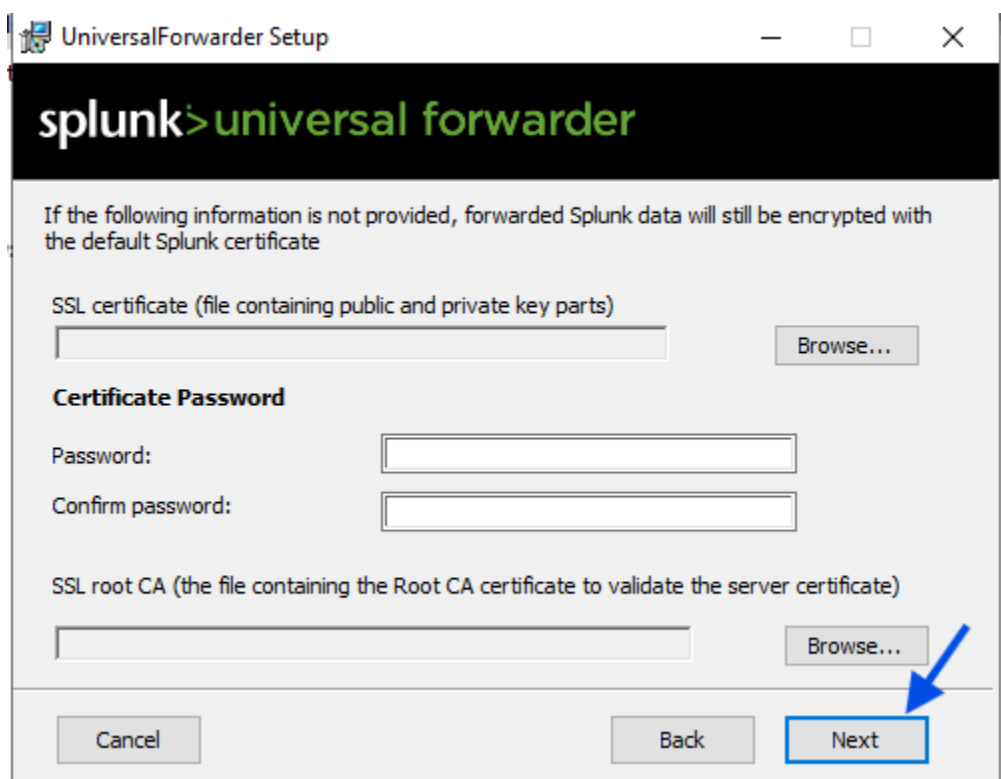
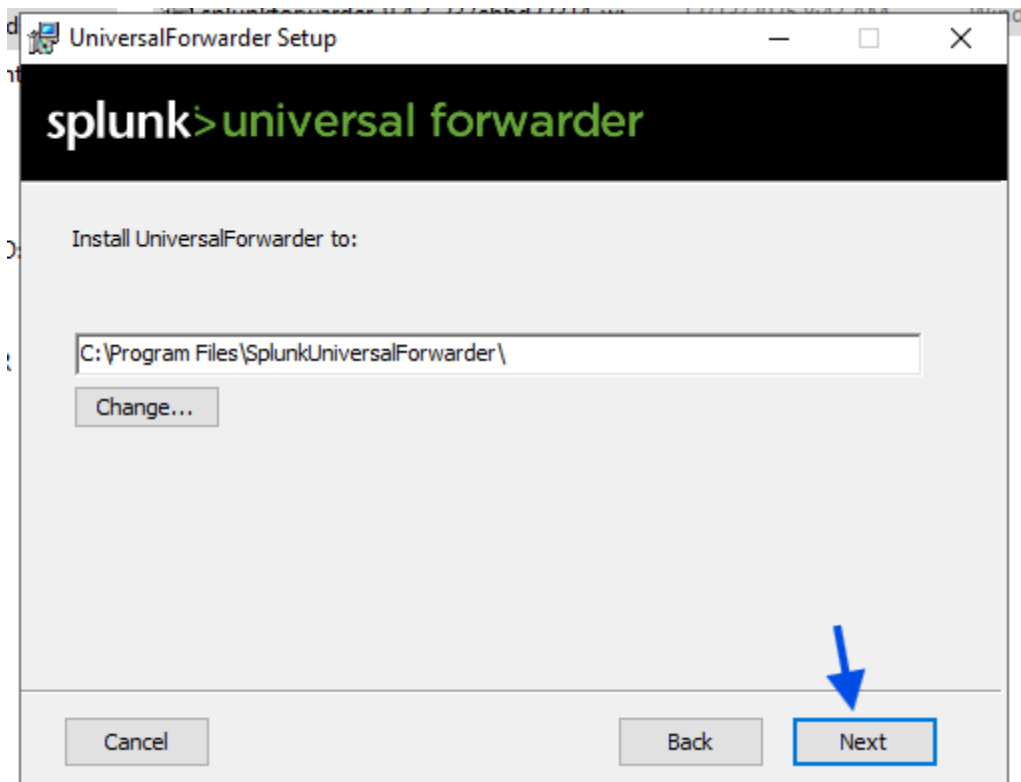
- Scales to very large environments
- Fast search and powerful analytics
- Highly customizable dashboards
- Strong threat detection and investigation
- Widely adopted in SOC environments

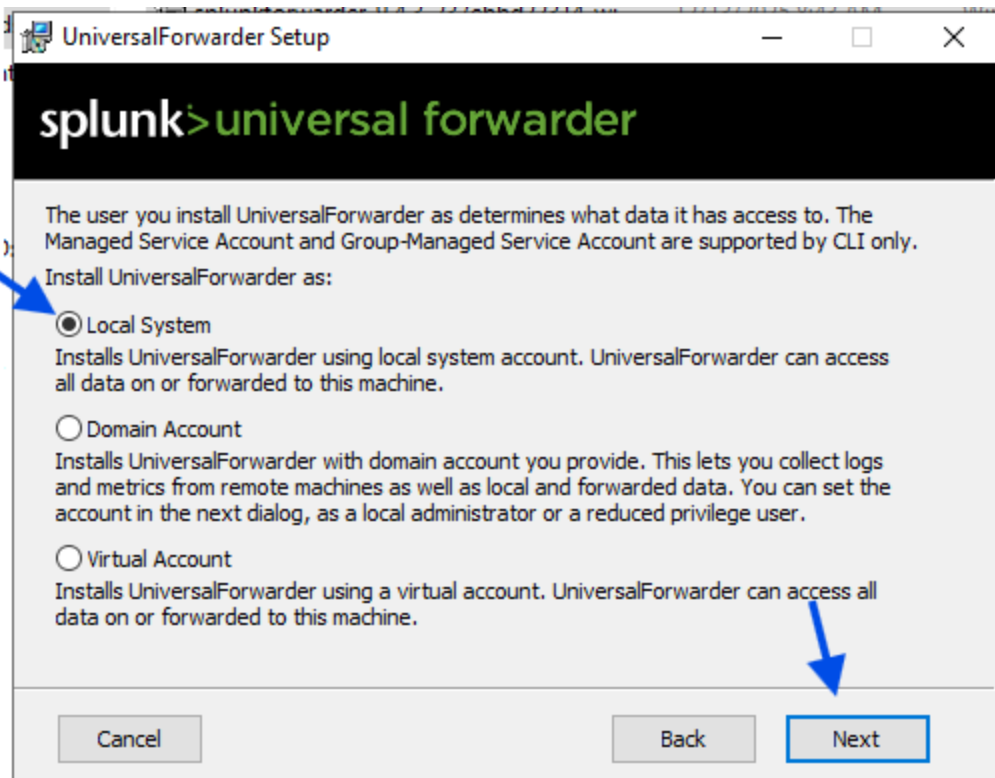
Below is a guide on installation and use of splunk

In this example we will install splunk enterprise on a host machine and we will install splunk forwarder on endpoint pc (server in this case) which will send the logs to host machine for analysis

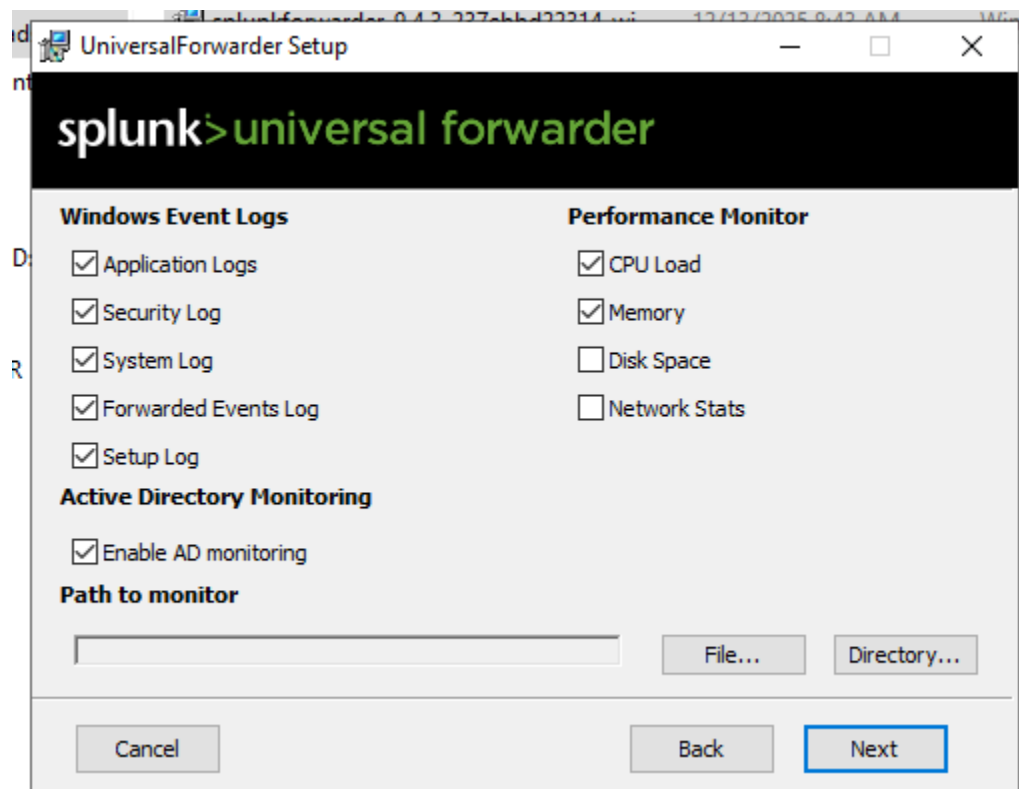
Install splunk forwarder on server







Check the logs we want reported and click next



Create username and password

UniversalForwarder Setup

splunk>universal forwarder

Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.

Username:
morelzy

☐ Generate random password

Password:
●●●●●●●●

Confirm password:
●●●●●●●●

Cancel Back Next

We don't need a deployment server, so we click next

UniversalForwarder Setup

splunk>universal forwarder

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*

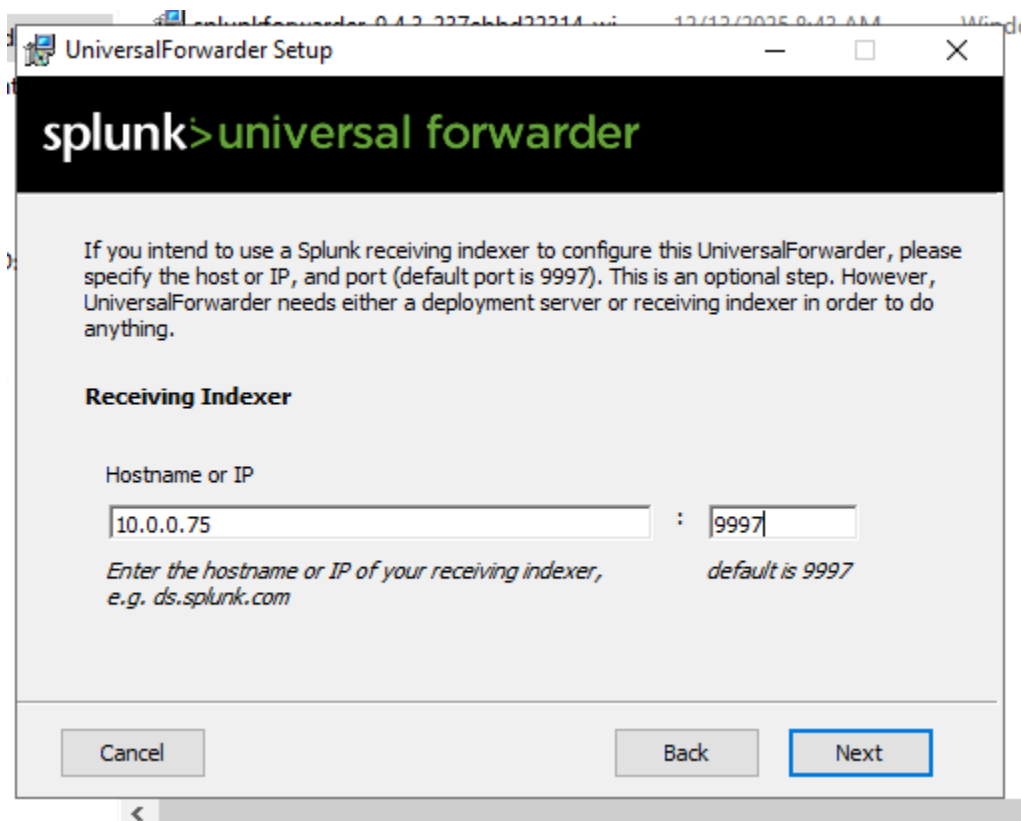
Cancel Back Next

For the receiver indexer, provide the ip address of the host PC and use default port

```
Wireless LAN adapter Wi-Fi:

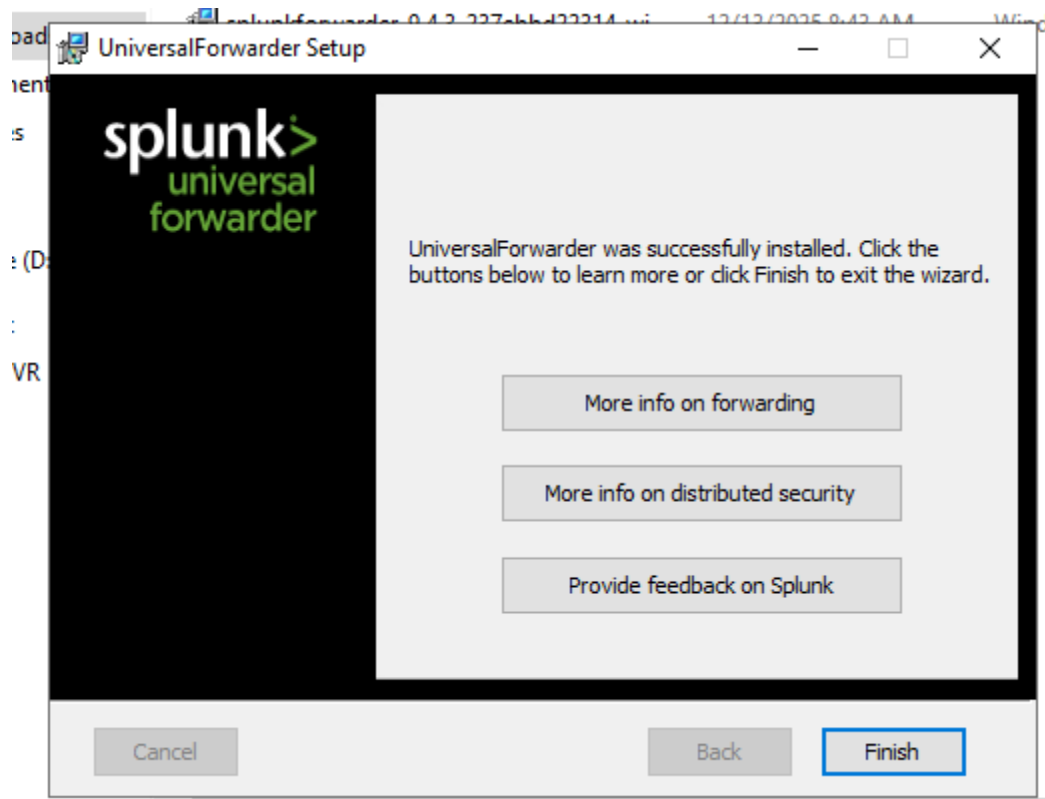
Connection-specific DNS Suffix . : 
IPv6 Address. . . . . : 2604:3d09:888:1800::e408
IPv6 Address. . . . . : 2604:3d09:888:1800:e39c:a5d6:3dde:3b9c
Temporary IPv6 Address. . . . . : 2604:3d09:888:1800:2074:fe87:5e4a:b404
Link-local IPv6 Address . . . . . : fe80::b39b:7ef5:eb05:179%8
IPv4 Address. . . . . : 10.0.0.75
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::c650:9cff:fe22:530f%8
                             10.0.0.1

Ethernet adapter Bluetooth Network Connection:
```

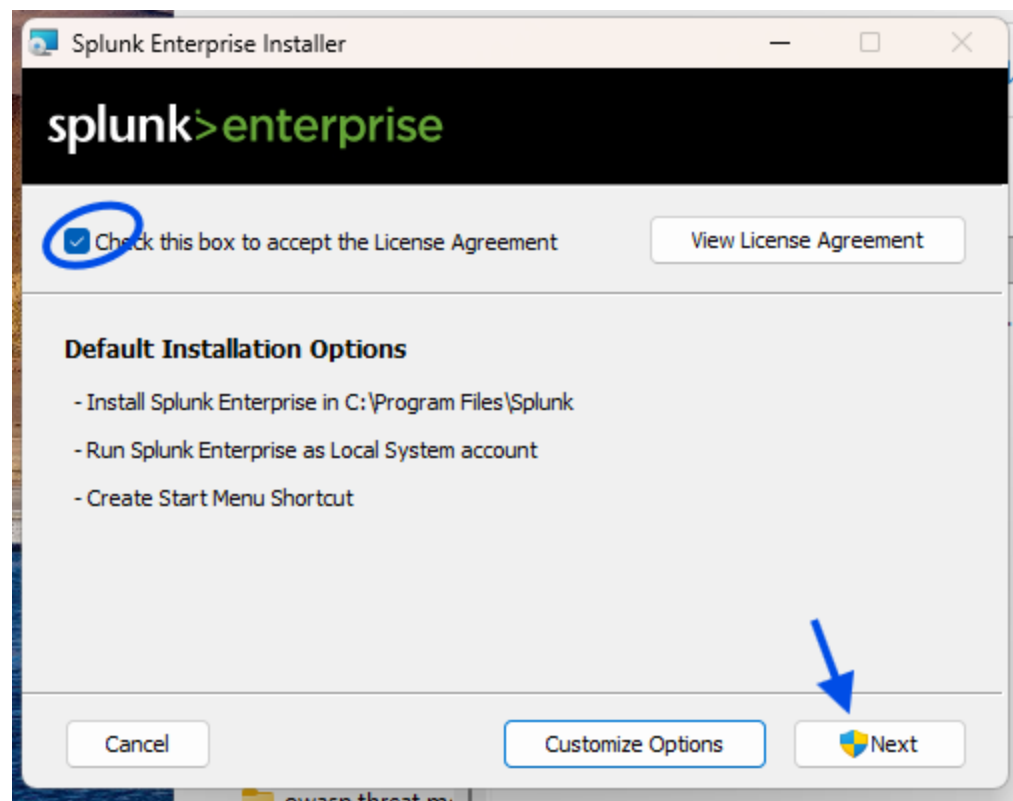


Click next and install

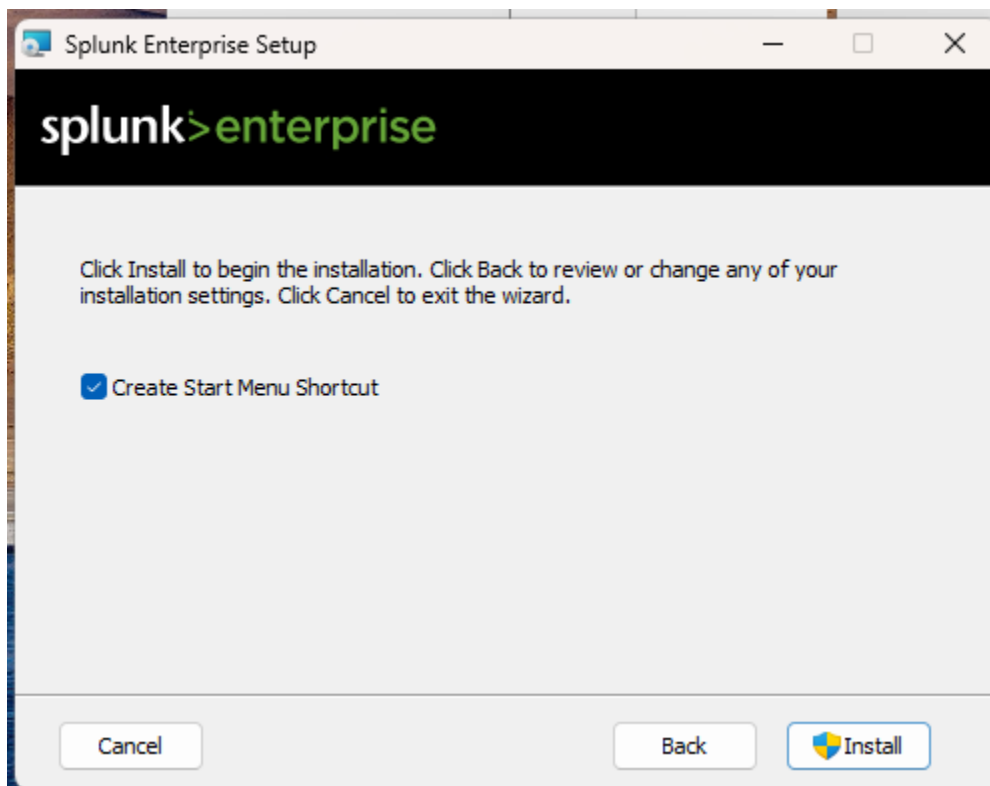
Click finish



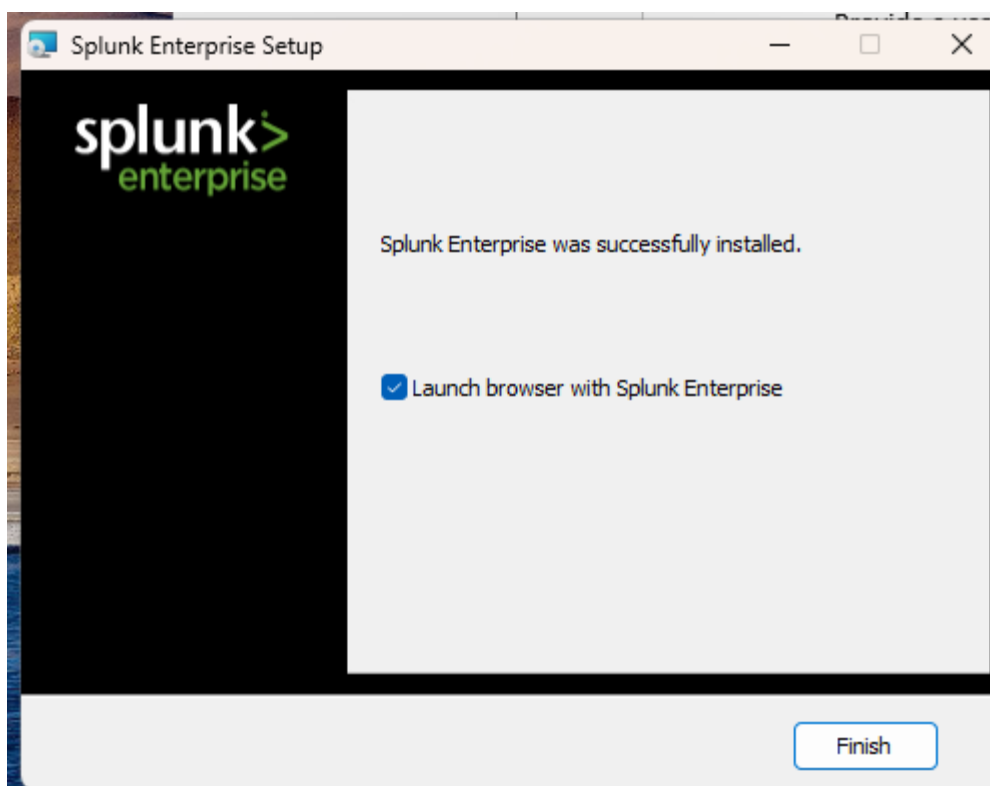
Next we install splunk enterprise on host machine



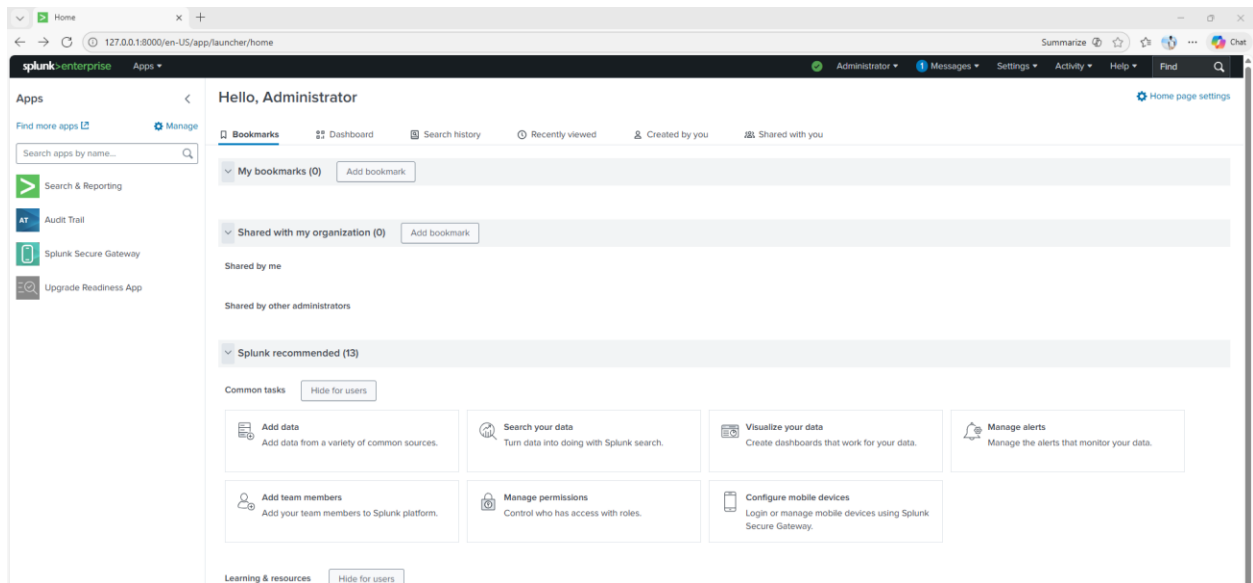
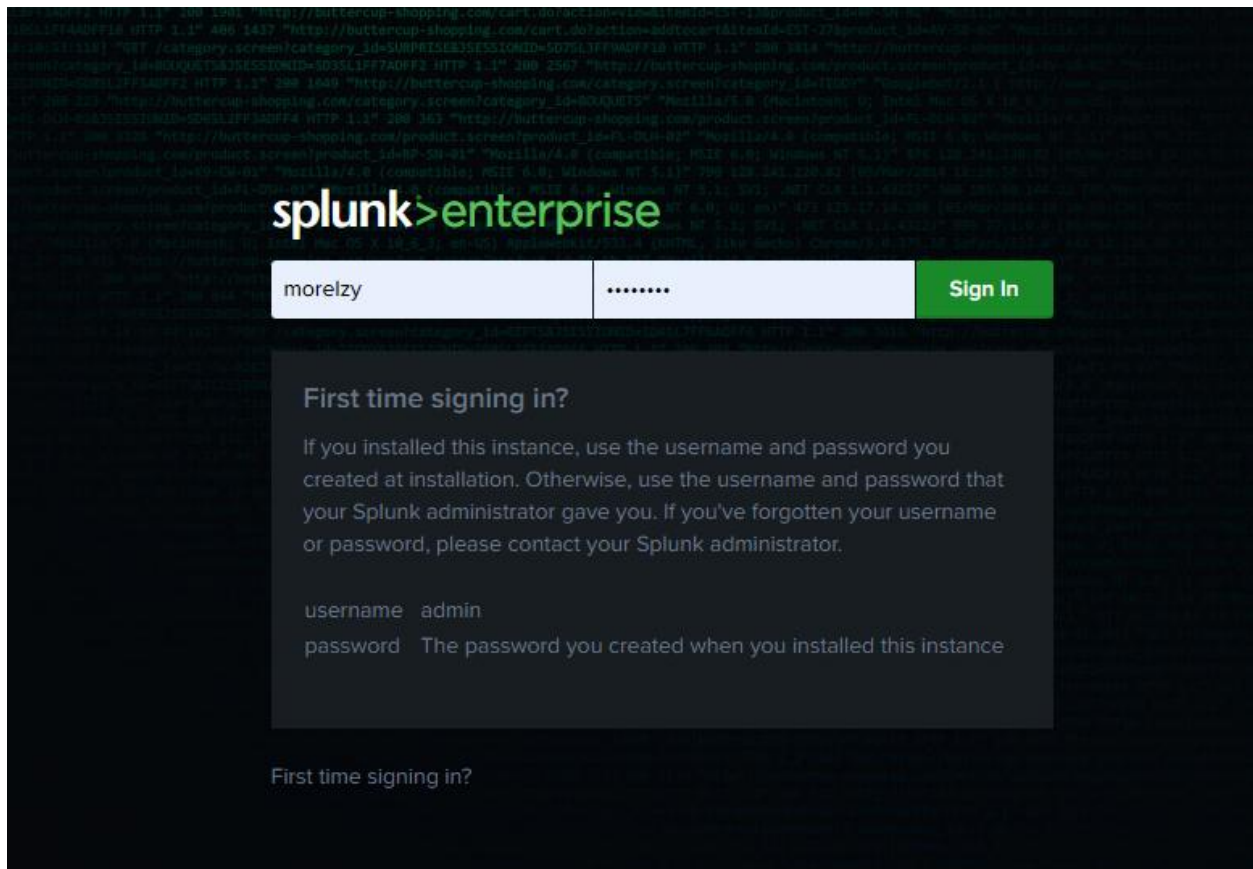
Provide a user name and password, then click install



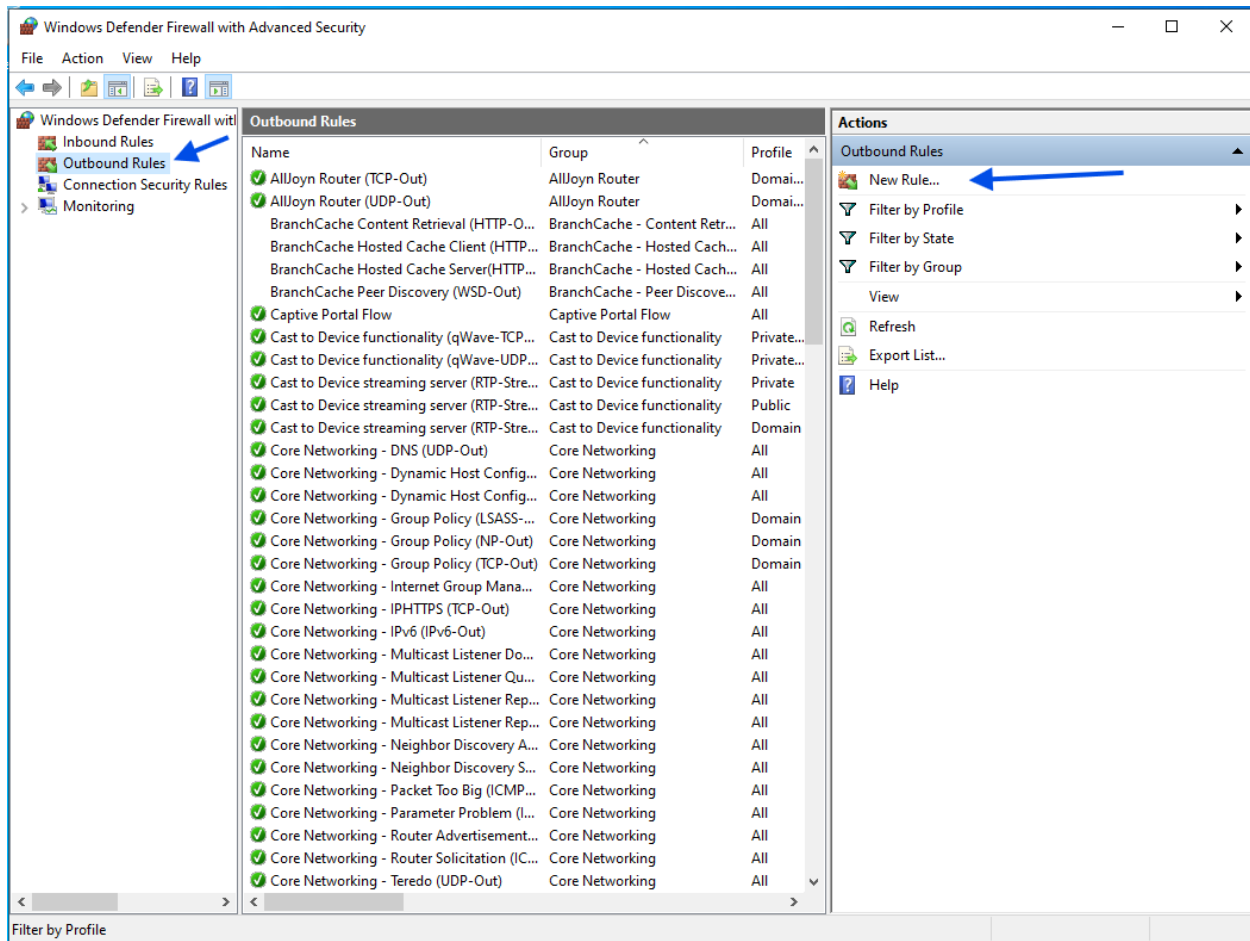
Click finish to launch splunk



It opens up in a browser and requests for the username and password inputted while setting up



In Order to have the system send logs to the host we need to set firewall outbound rules by creating a rule in the endpoint pc



New Outbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Program
- Action
- Profile
- Name

What type of rule would you like to create?

☒ **Program**
Rule that controls connections for a program.

☐ **Port**
Rule that controls connections for a TCP or UDP port.

☐ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

☐ **Custom**
Custom rule.

< Back Next > Cancel

New Outbound Rule Wizard

Program

Specify the full program path and executable name of the program that this rule matches.

Steps:

- Rule Type
- Program
- Action
- Profile
- Name

Does this rule apply to all programs or a specific program?

☐ **All programs**
Rule applies to all connections on the computer that match other rule properties.

☒ **This program path:**

Browse...

Example: c:\path\program.exe
 %ProgramFiles%\browser\browser.exe

Find the path to the executable file of the program

Does this rule apply to all programs or a specific program?

☐ **All programs**
Rule applies to all connections on the computer that match other rule properties.

☒ **This program path:**

Example: c:\path\program.exe
 %ProgramFiles%\browser\browser.exe

Allow connection, name and save rule

What action should be taken when a connection matches the specified conditions?

☒ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

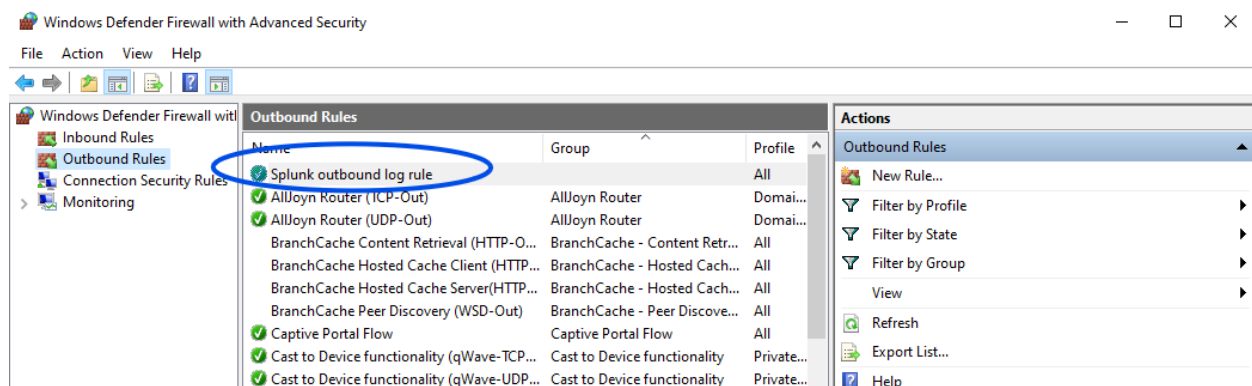
☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

☐ **Block the connection**

Name:
Splunk outbound log rule

Description (optional):
Allow logs to be sent out to host

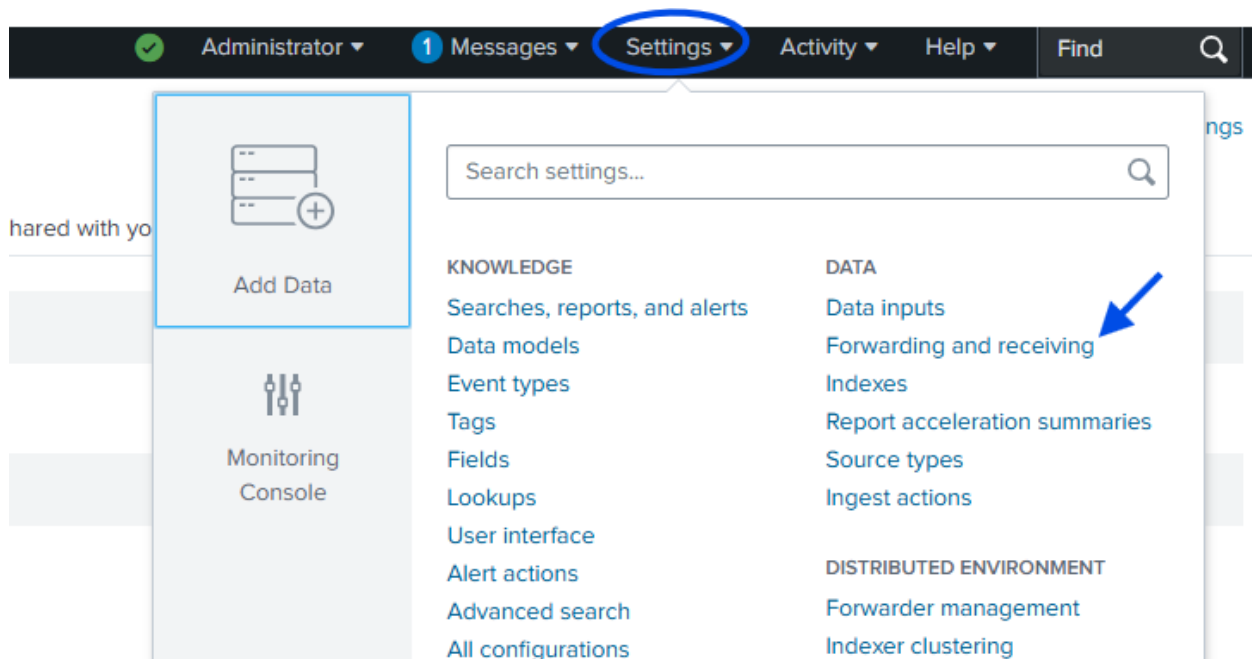
< Back Finish Cancel



Next, on the HOST we set up our receiving index,

Launch splunk on host

Click settings and select forwarding and receiving



Forward data

Set up forwarding between two or more Splunk instances.

Type	Actions
Forwarding defaults	
Configure forwarding	+ Add new

Receive data

Configure this instance to receive data forwarded from other instances.

Type	Actions
Configure receiving	+ Add new

Add new, use port selected during installation

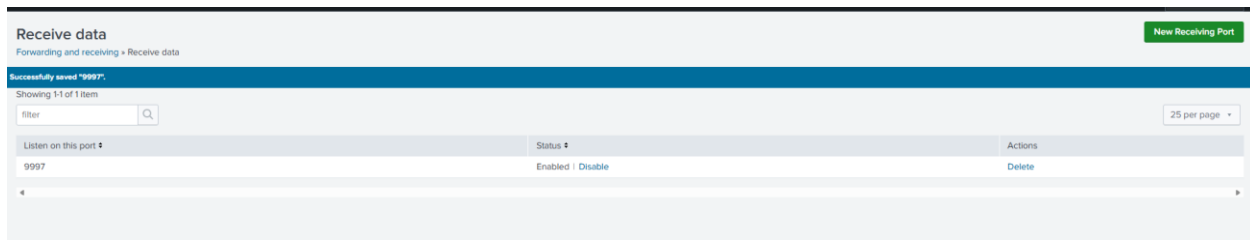
Add new

Forwarding and receiving > Receive data > Add new

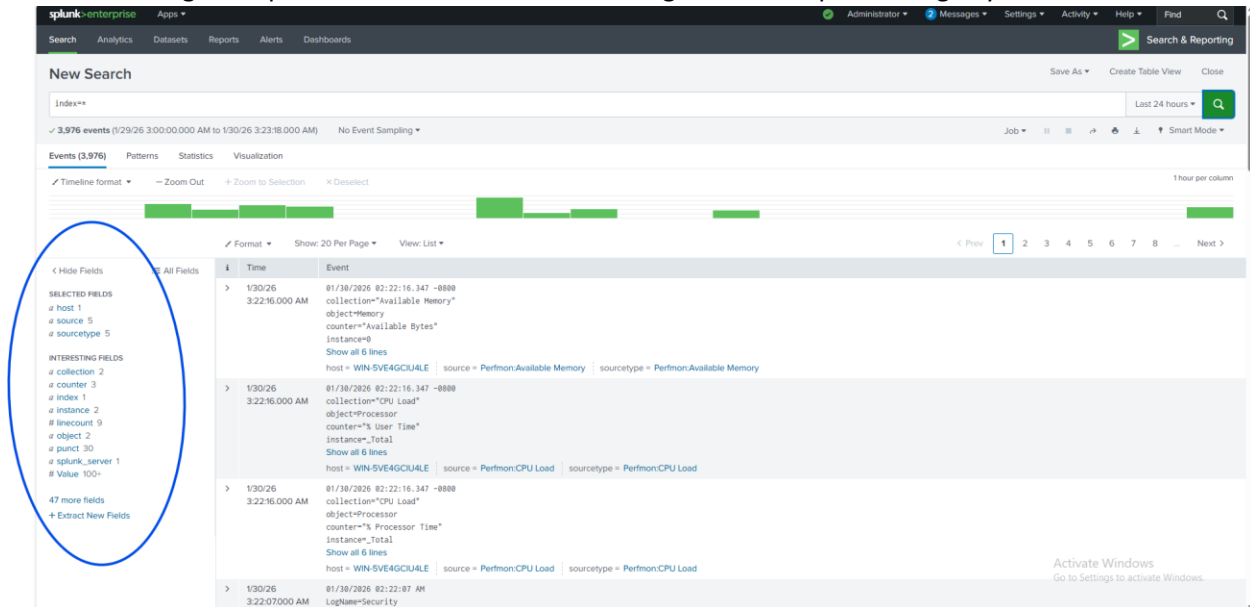
Configure receiving
Set up this Splunk instance to receive data from forwarder(s).

Listen on this port *

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



Now we can log into splunk on host machine to view logs and run reports using key words



We can dig deeper or search for specific ports or keywords