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

---

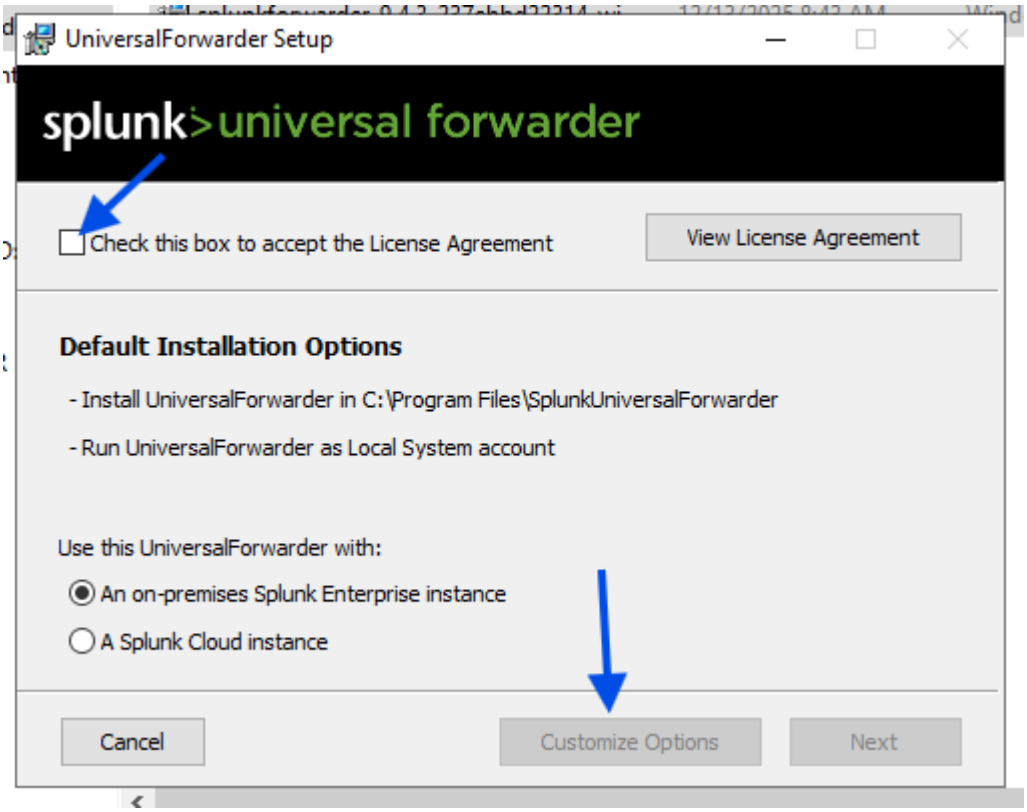
Why Organizations Use Splunk SIEM

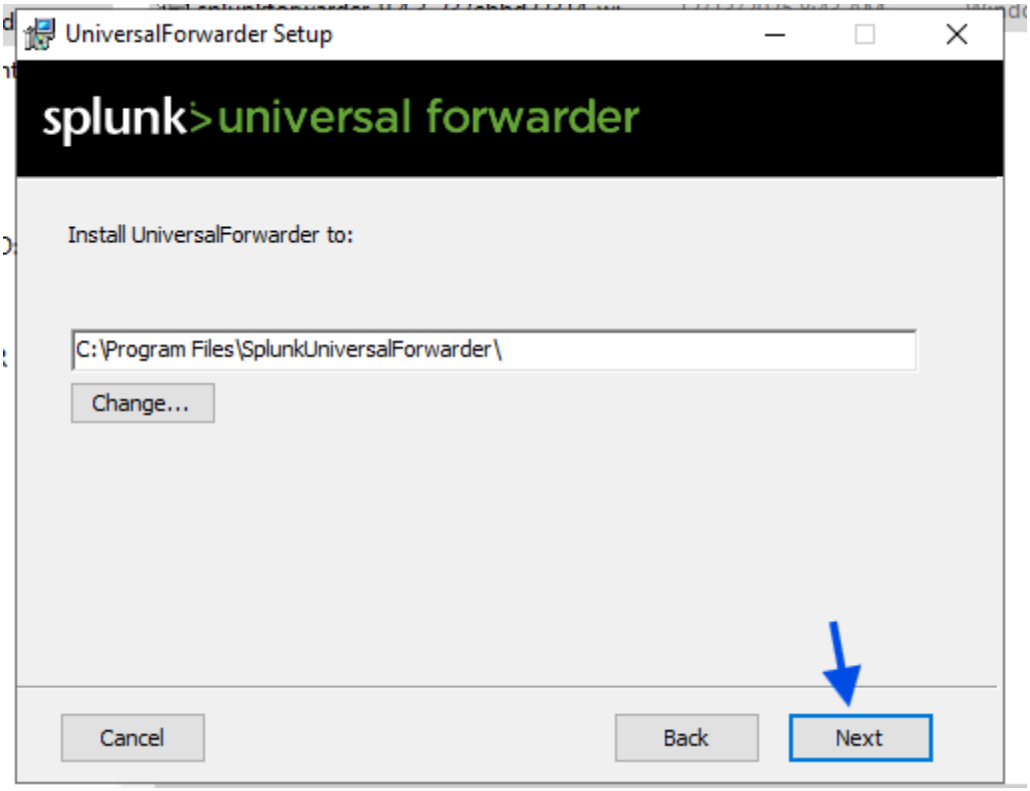
- Scales to very large environments
- Fast search and powerful analytics
- Highly customizable dashboards
- Strong threat detection and investigation
- Widely adopted in SOC environments

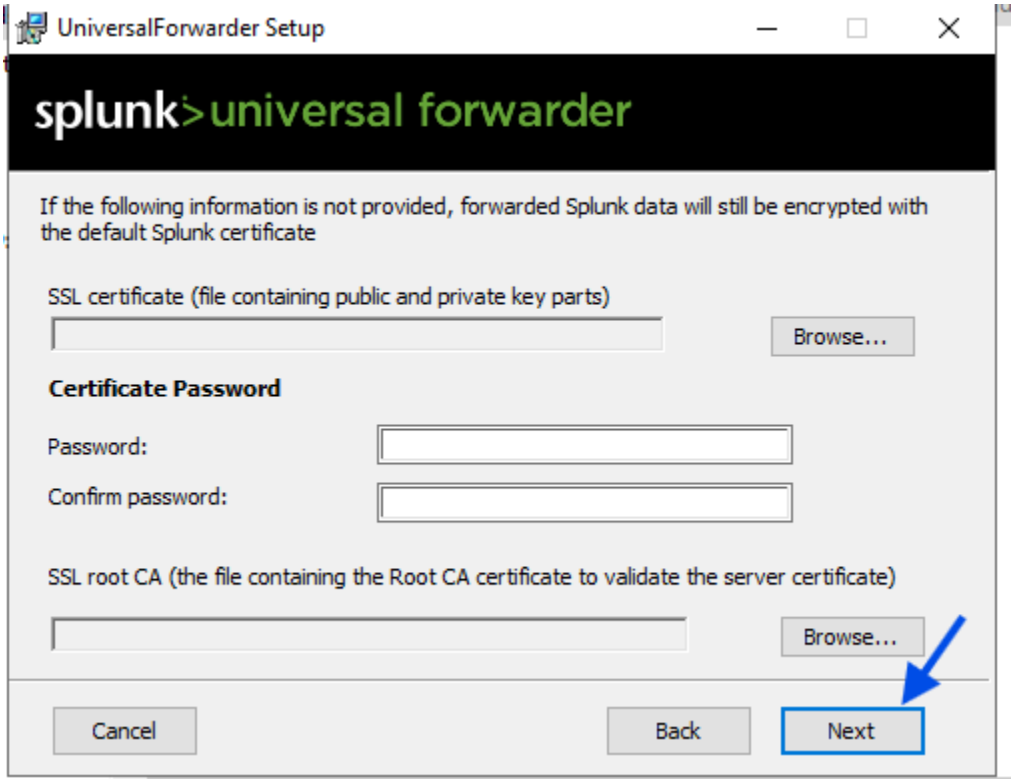
Below is a guide on installation and use of splunk

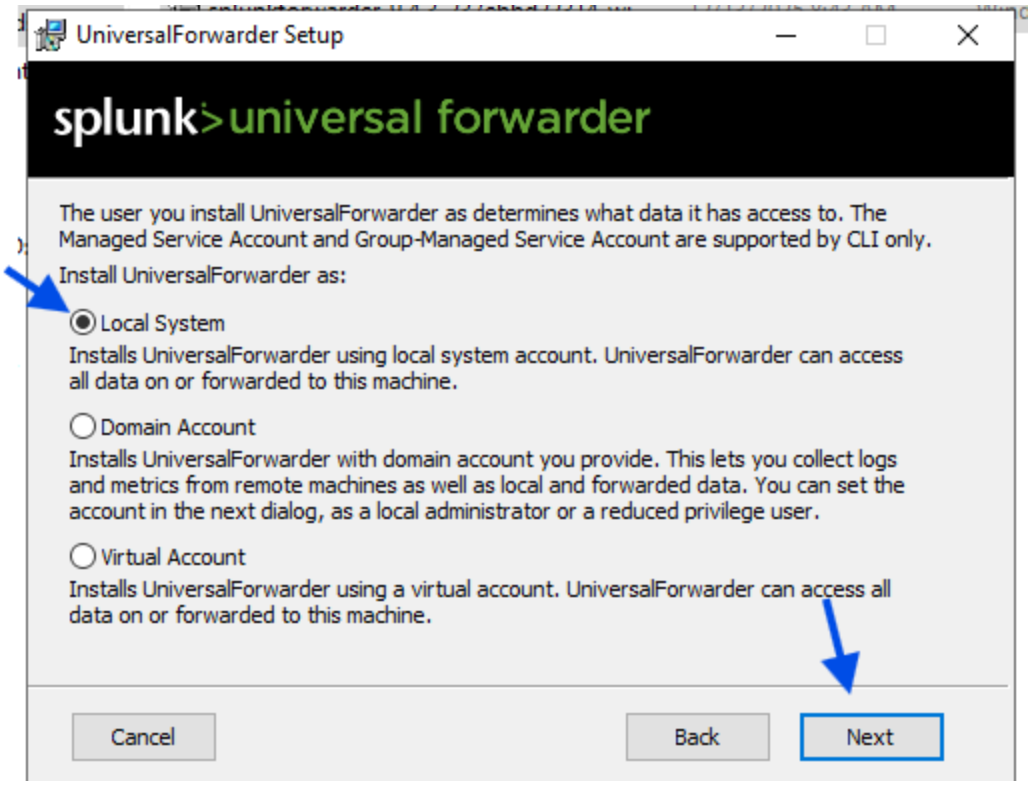
In this example we will install splunk enterprise on a host machine and we will install splunk forwarder on endpoint pc (server in this case) which will send the logs to host machine for analysis

Install splunk forwarder on server

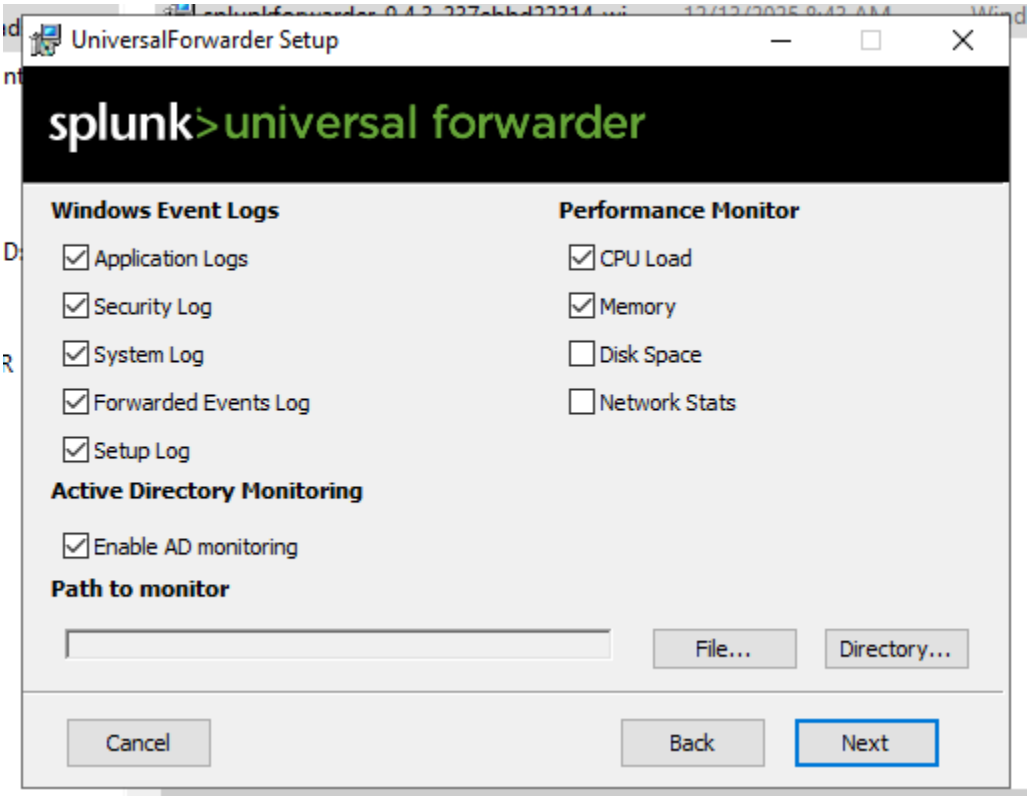



UniversalForwarder Setup
splunk>universal forwarder
Install UniversalForwarder to:
C:\Program Files\SplunkUniversalForwarder\
Change...
Cancel
Back
Next

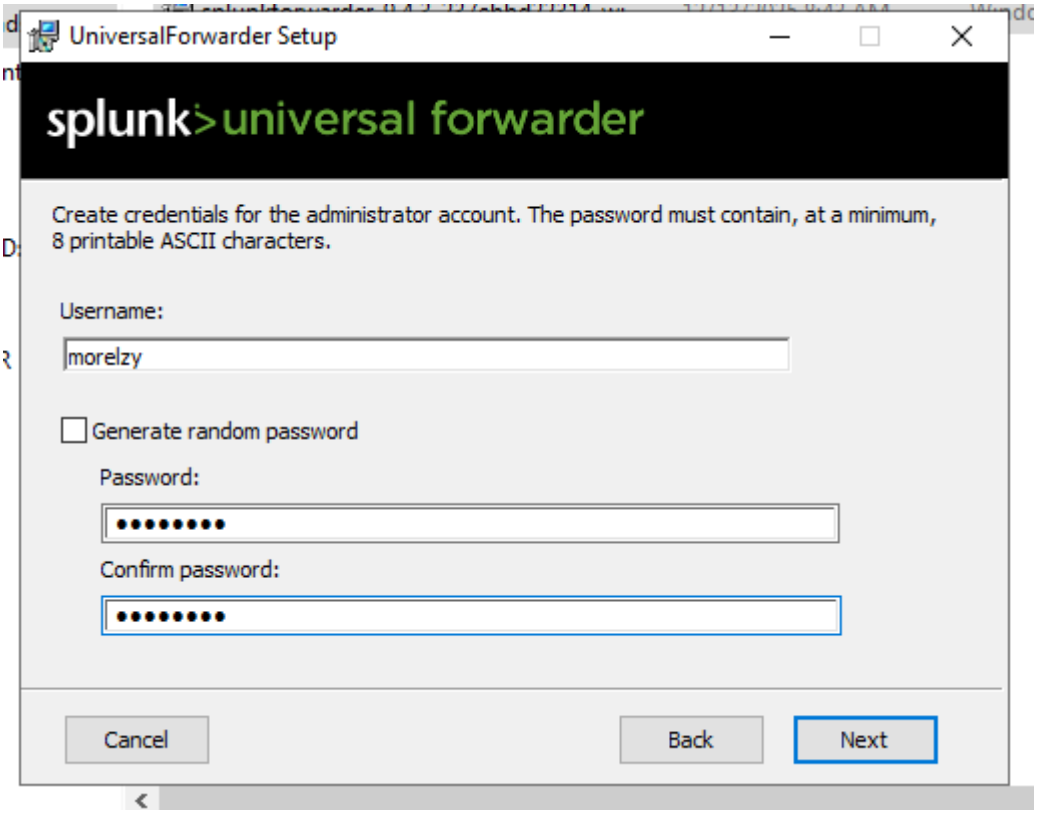

UniversalForwarder Setup
splunk>universal forwarder
If the following information is not provided, forwarded Splunk data will still be encrypted with the default Splunk certificate
SSL certificate (file containing public and private key parts)
Browse...
Certificate Password
Password:
Confirm password:
SSL root CA (the file containing the Root CA certificate to validate the server certificate)
Browse...
Cancel
Back
Next



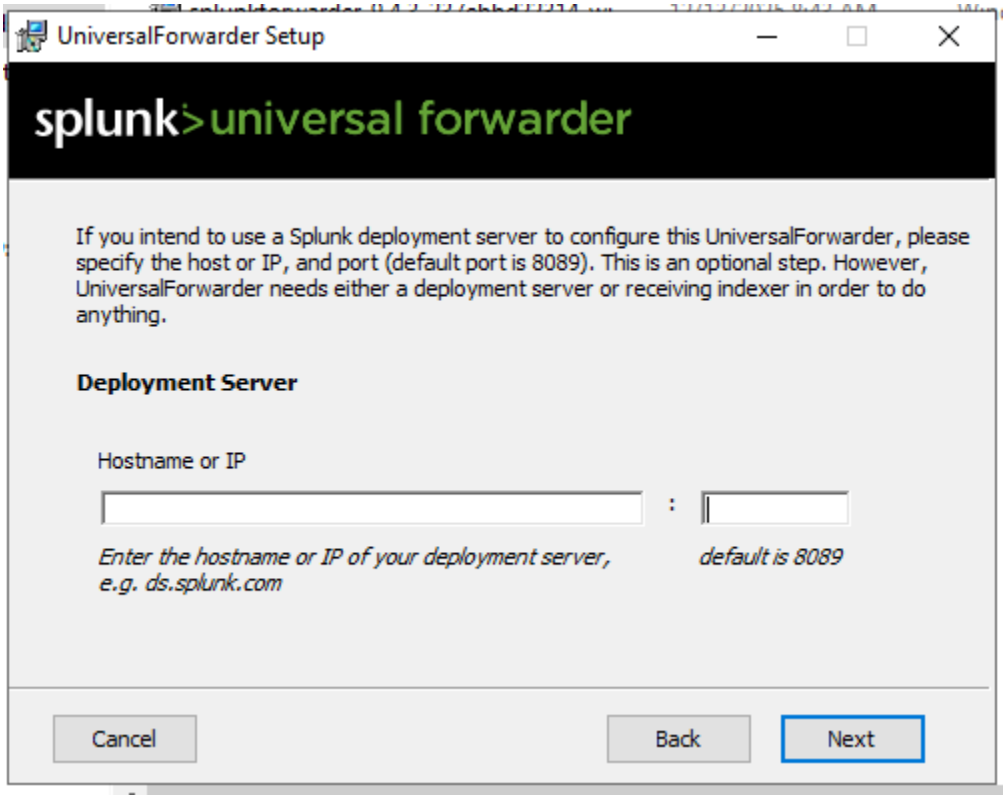
Check the logs we want reported and click next



Create username and password

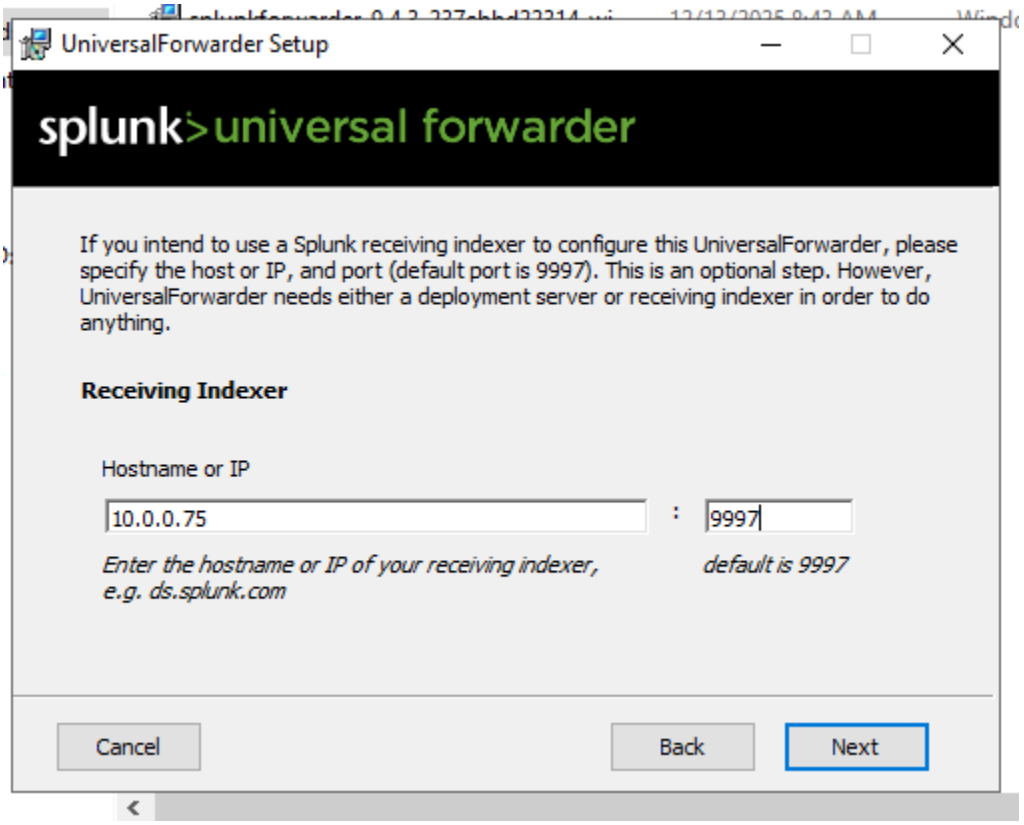


We don’t need a deployment server, so we click next



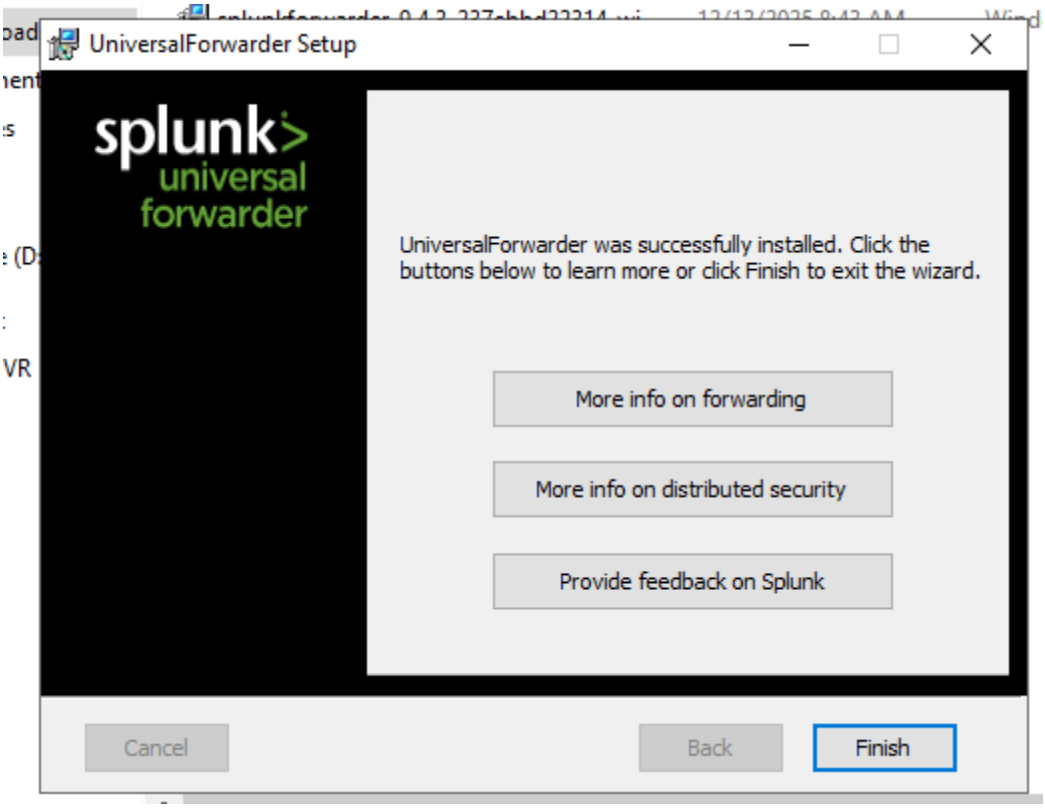
For the receiver indexer, provide the ip address of the host PC and use default port

```
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:
```

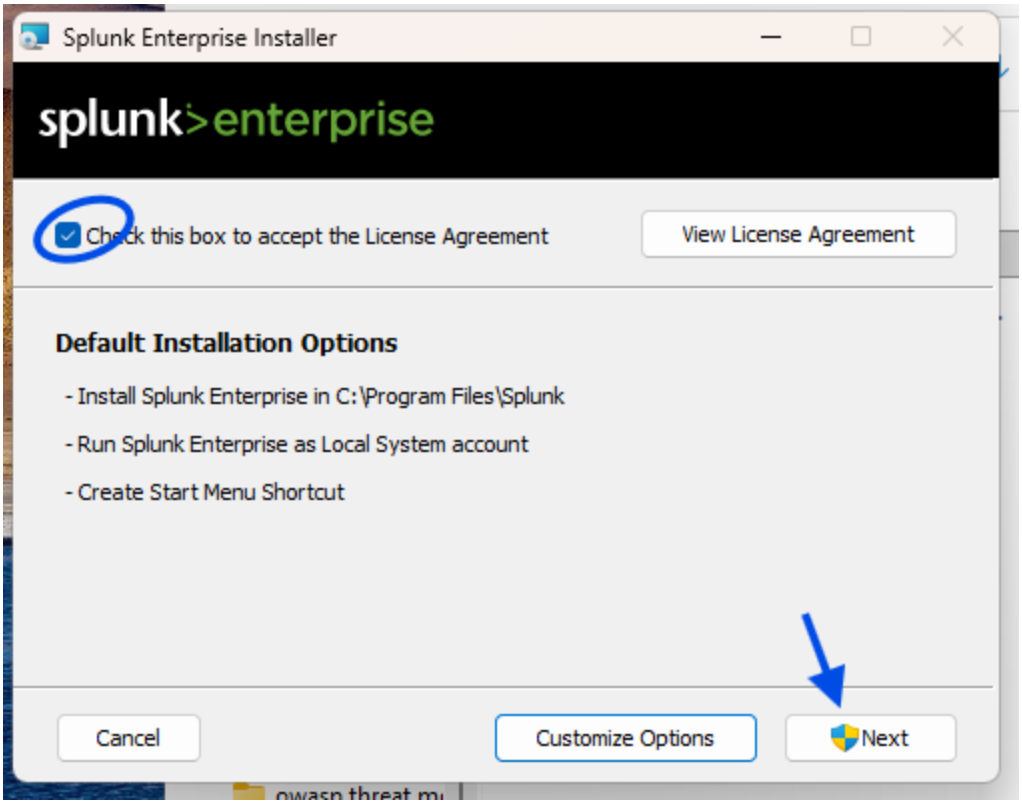


Click next and install

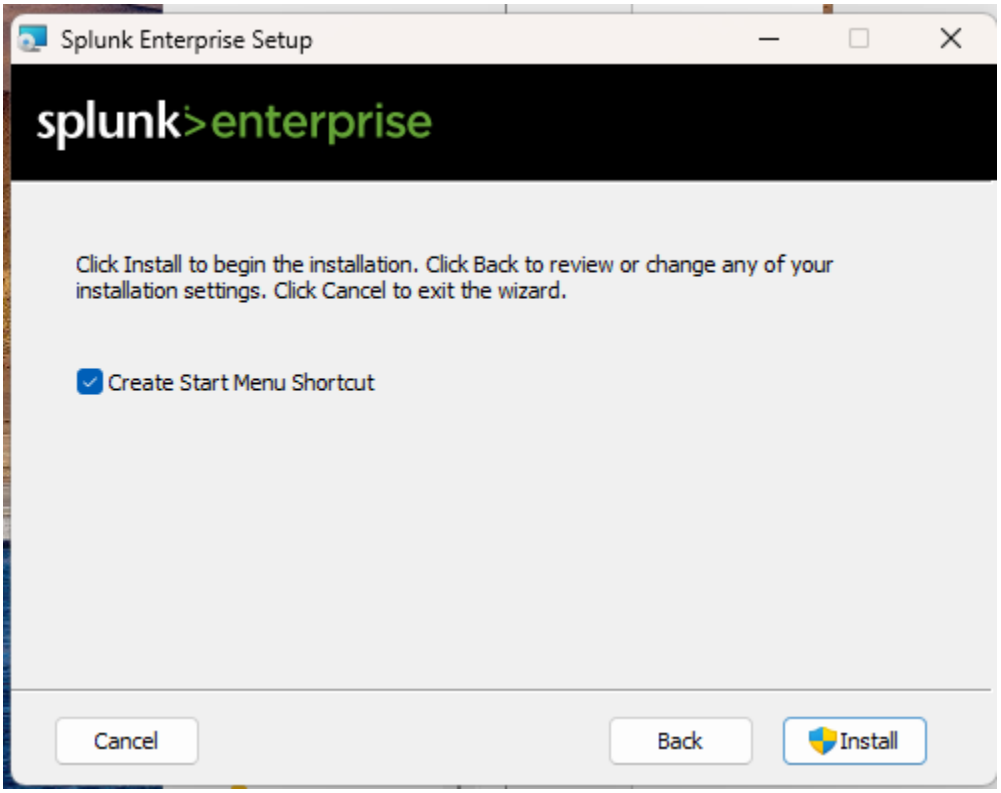
Click finish



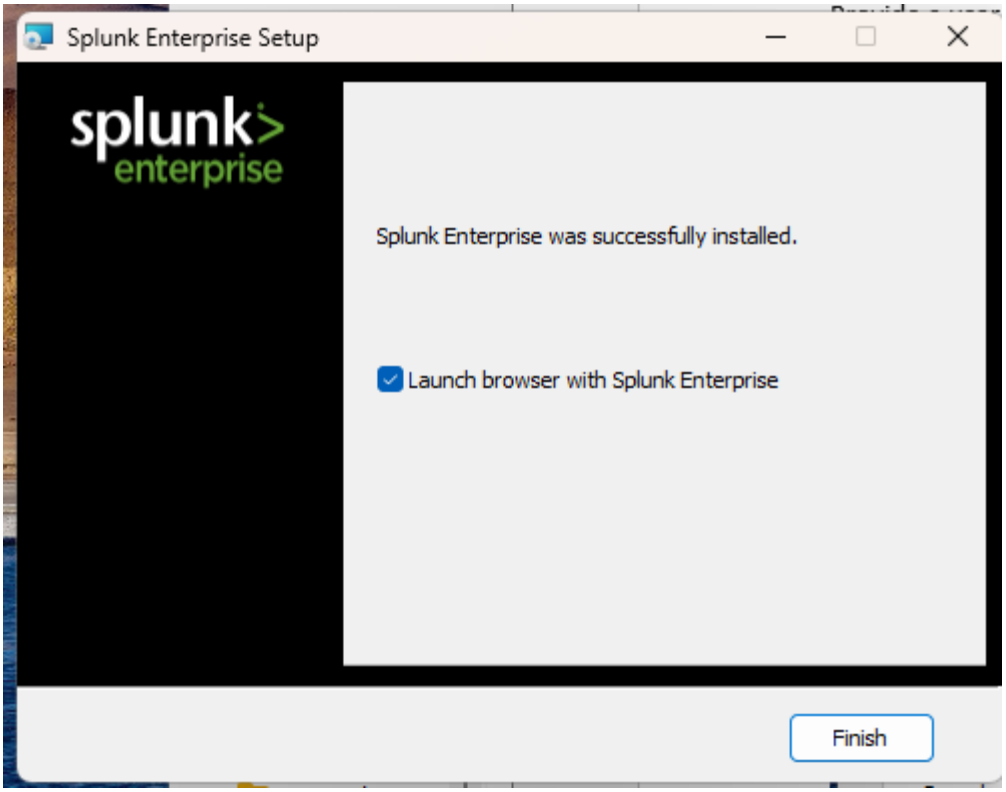
Next we install splunk enterprise on host machine



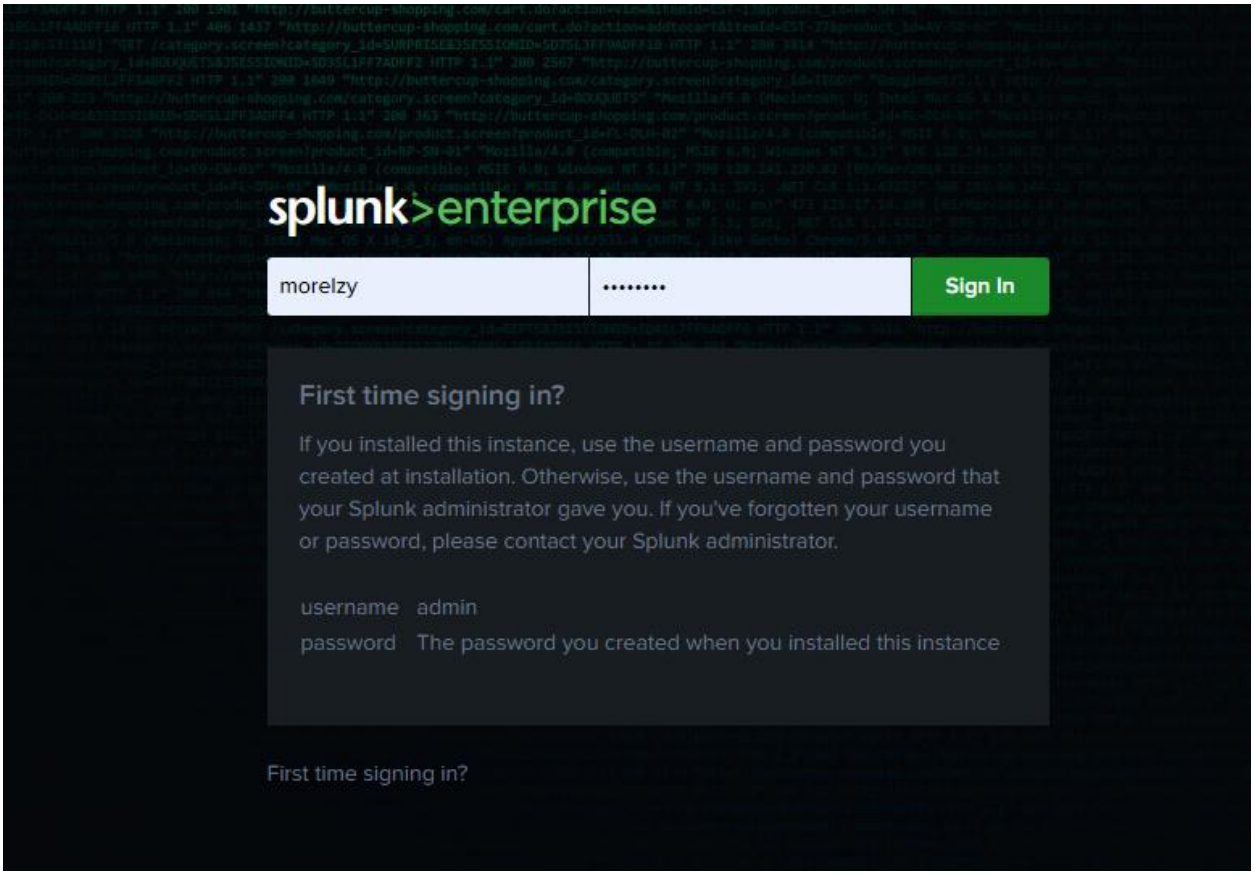
Provide a user name and password, then click install

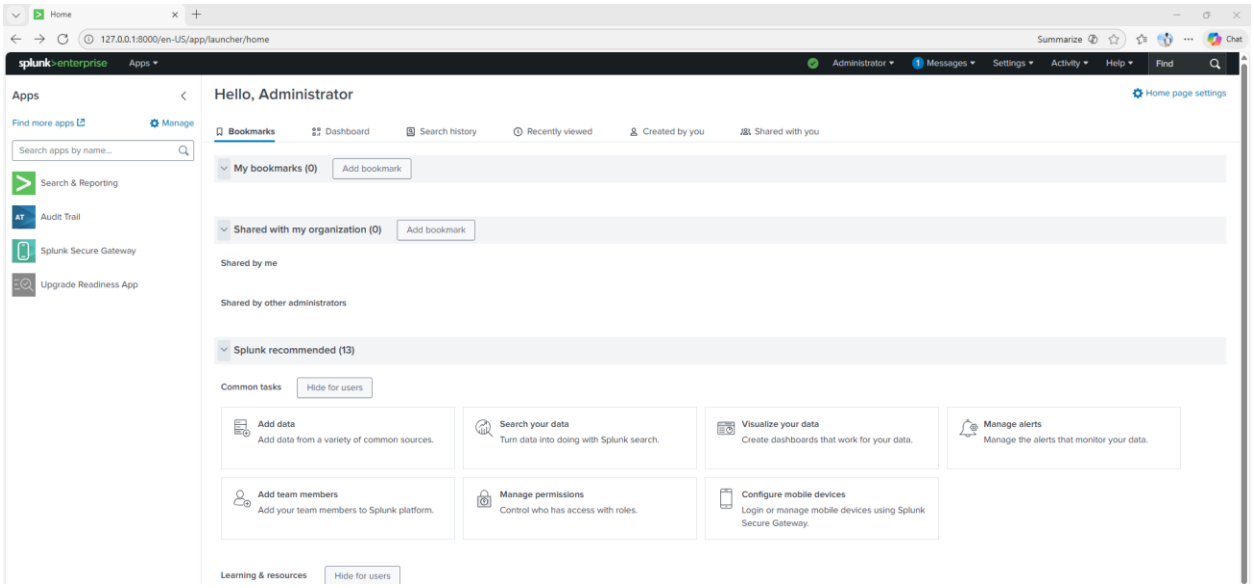


Click finish to launch splunk

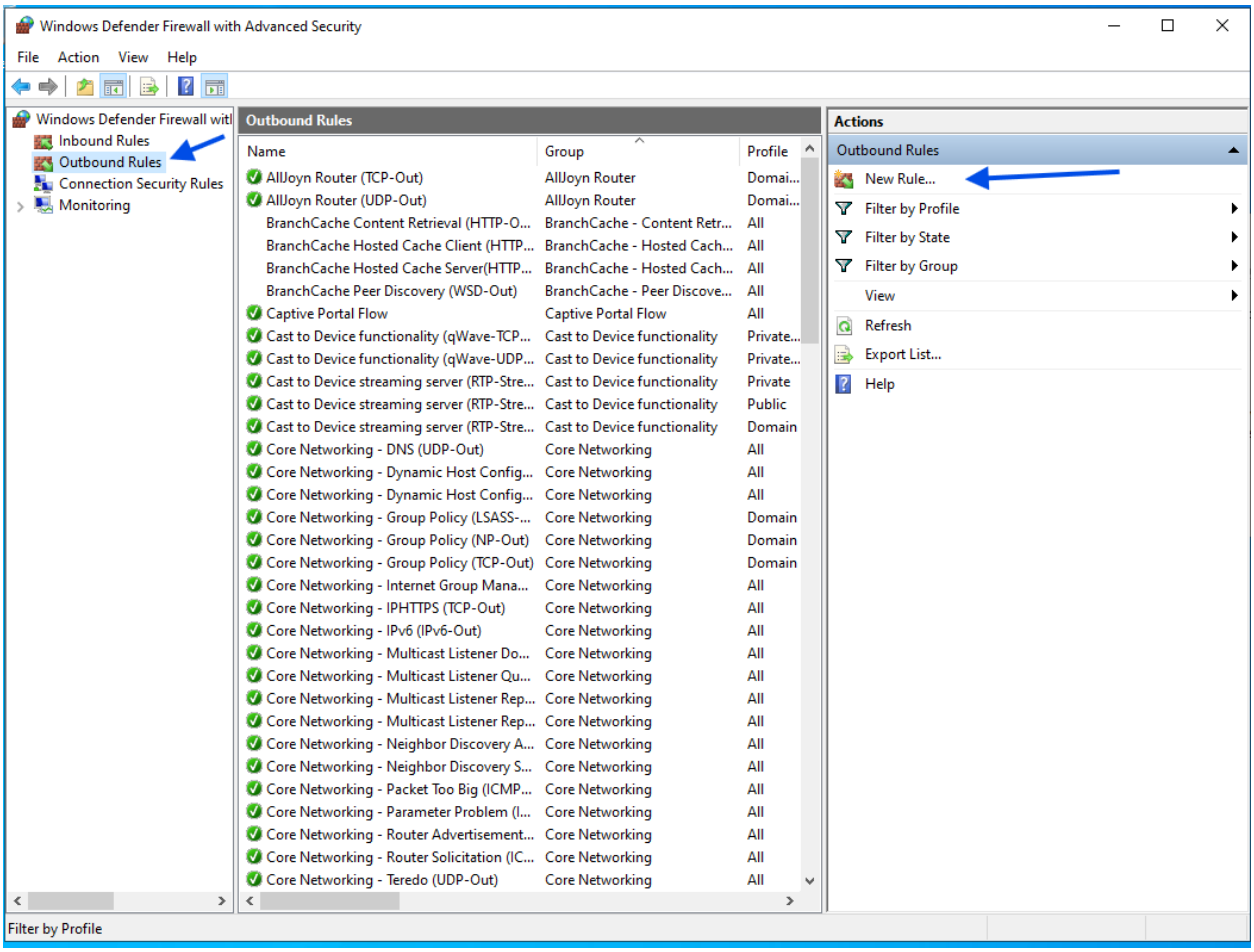


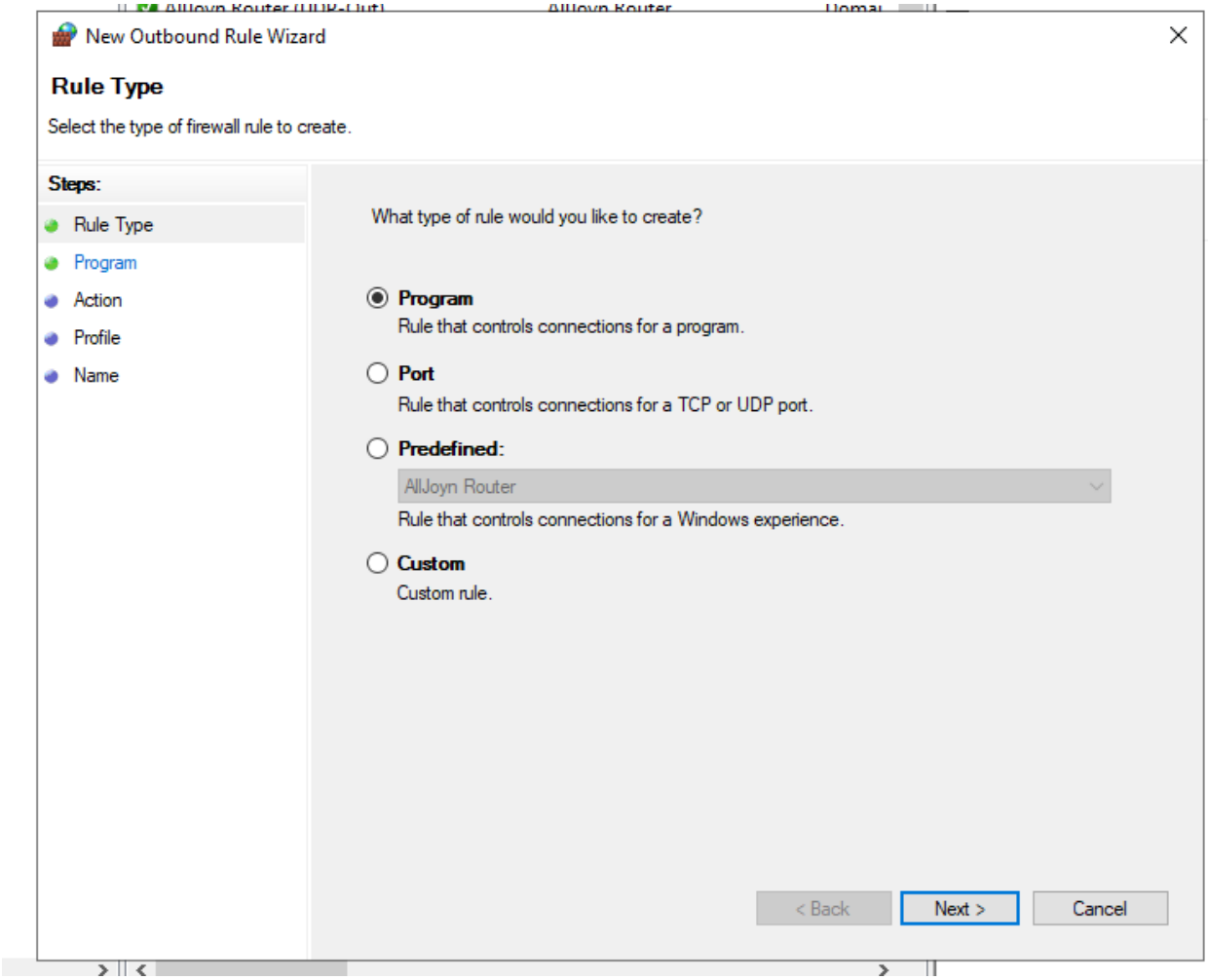
It opens up in a browser and requests for the username and password inputted while setting up

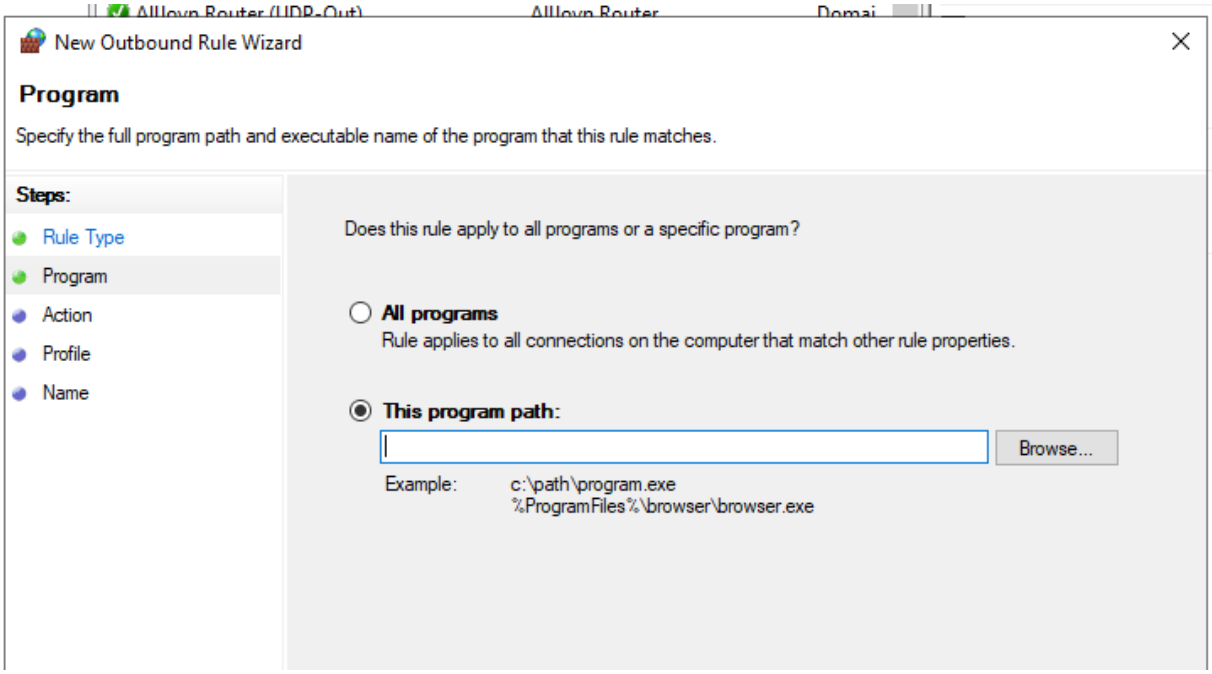




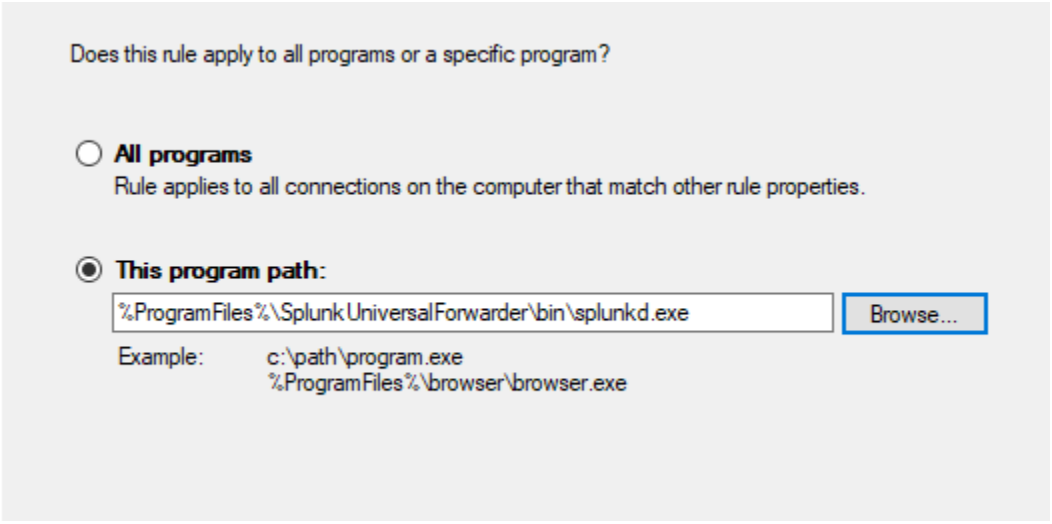
In Order to have the system send logs to the host we need to set firewall outbound rules by creating a rule in the endpoint pc



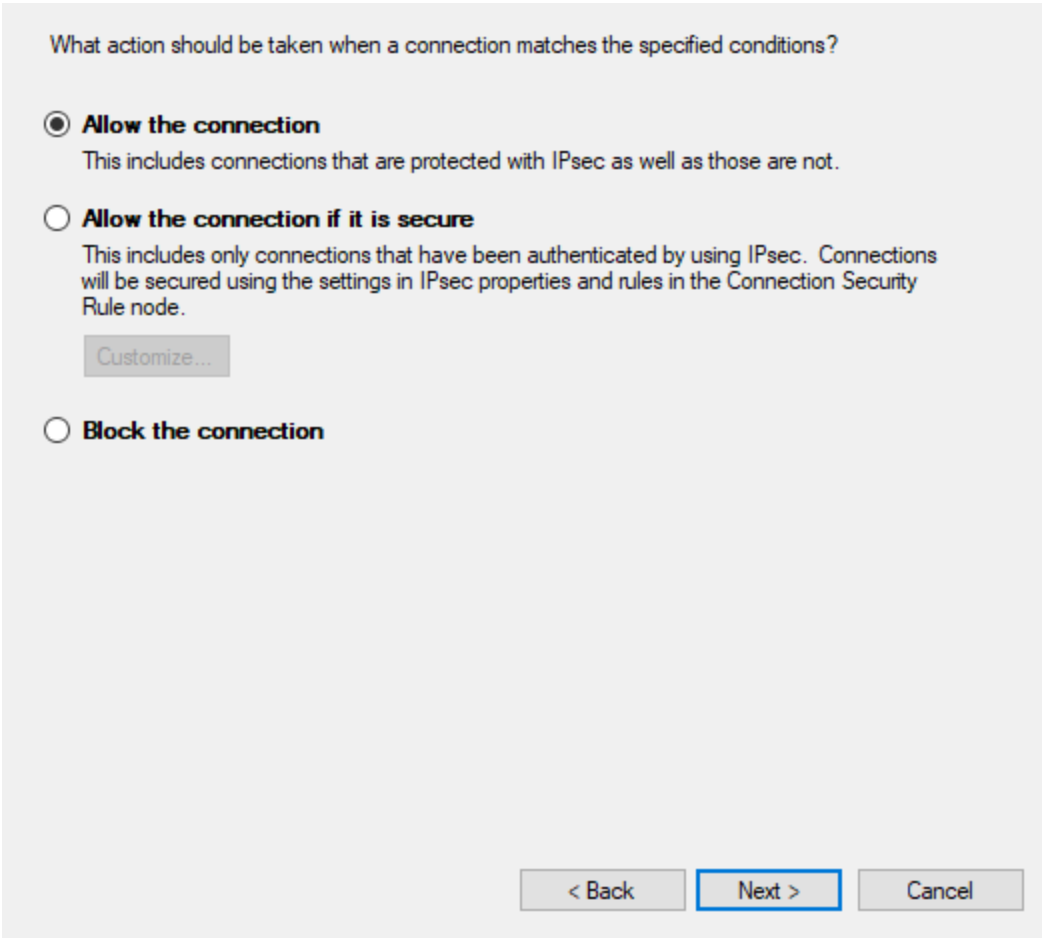

New Outbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Program
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
AllJoyn Router
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel

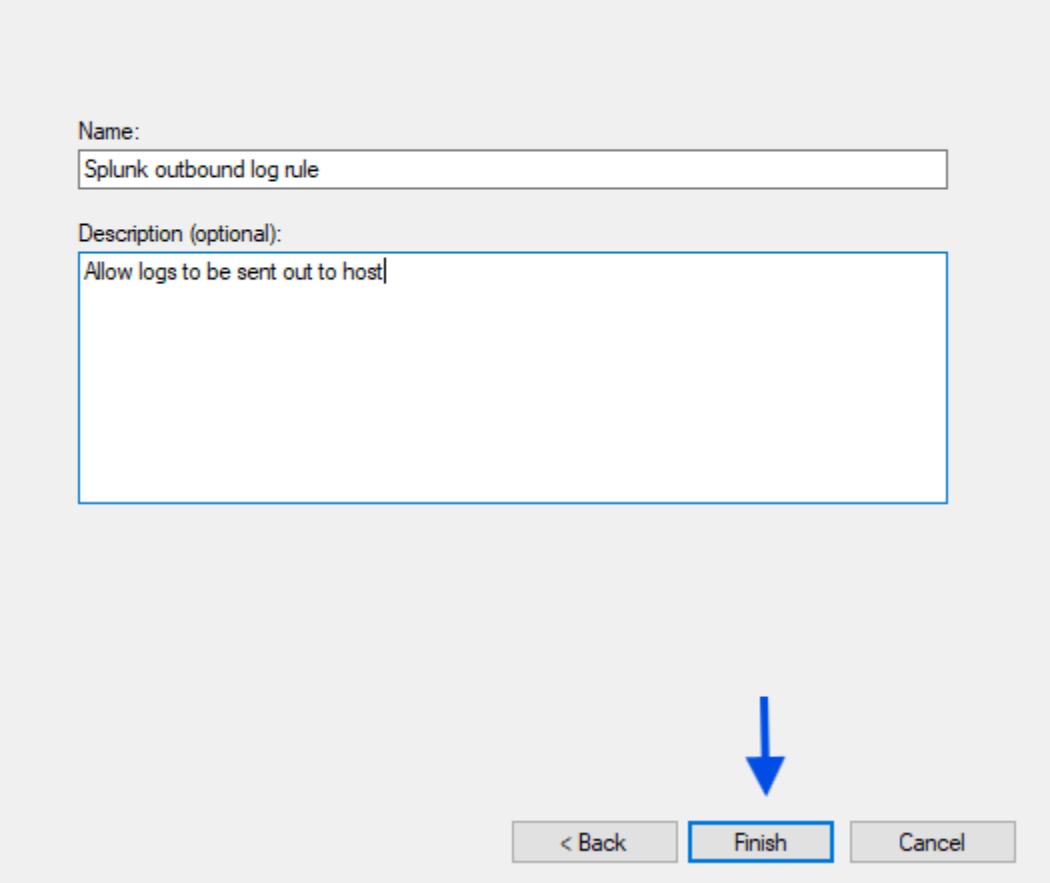

New Outbound Rule Wizard
Program
Specify the full program path and executable name of the program that this rule matches.
Steps:
Rule Type
Program
Action
Profile
Name
Does this rule apply to all programs or a specific program?
All programs
Rule applies to all connections on the computer that match other rule properties.
This program path:
Browse...
Example:
c:\path\program.exe
%ProgramFiles%\browser\browser.exe

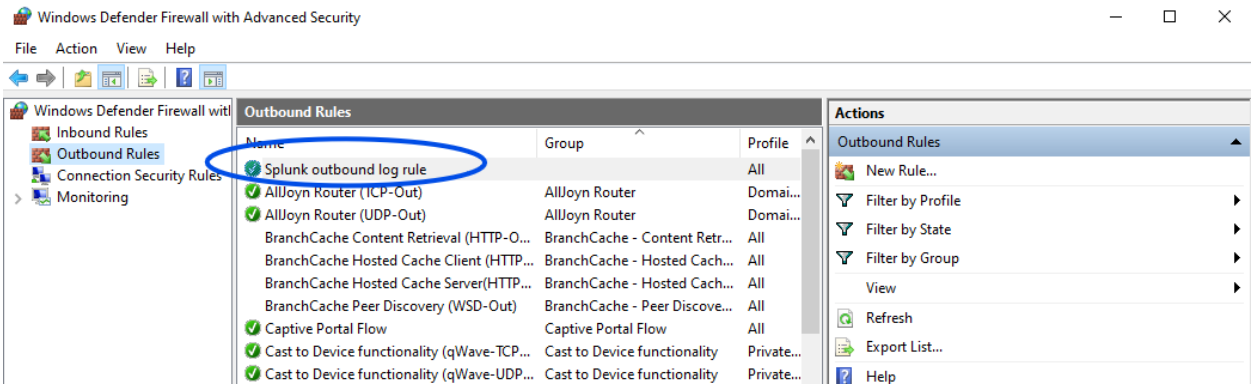
Find the path to the executable file of the program



Allow connection, name and save rule



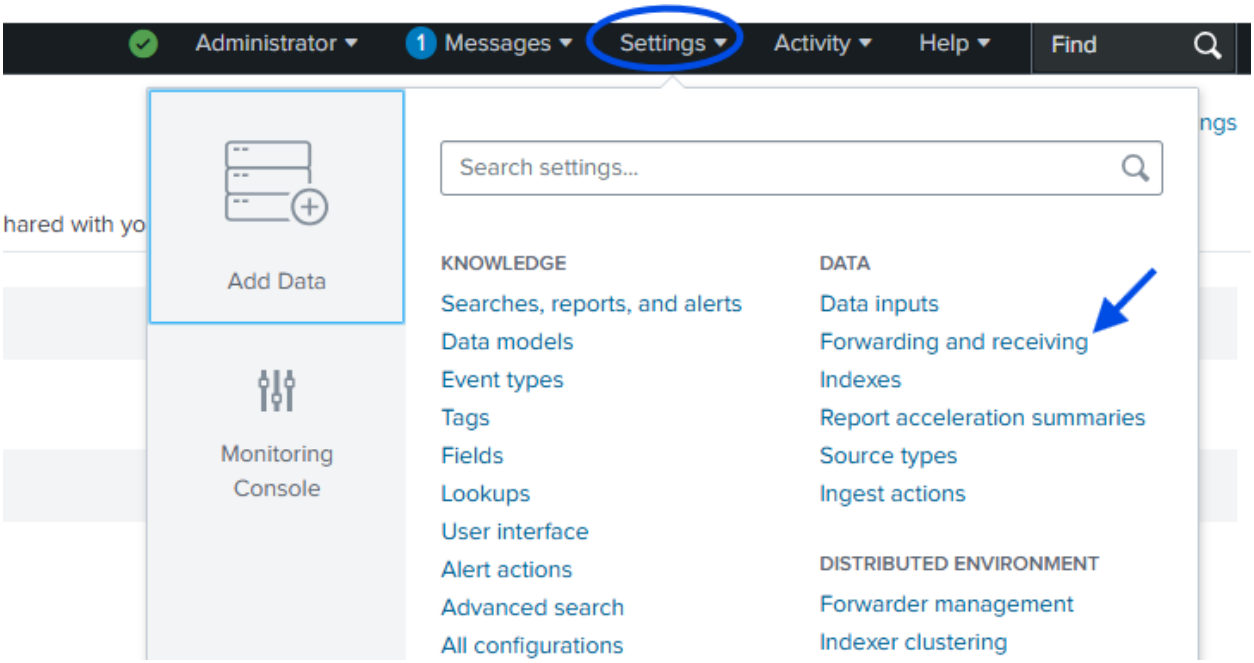


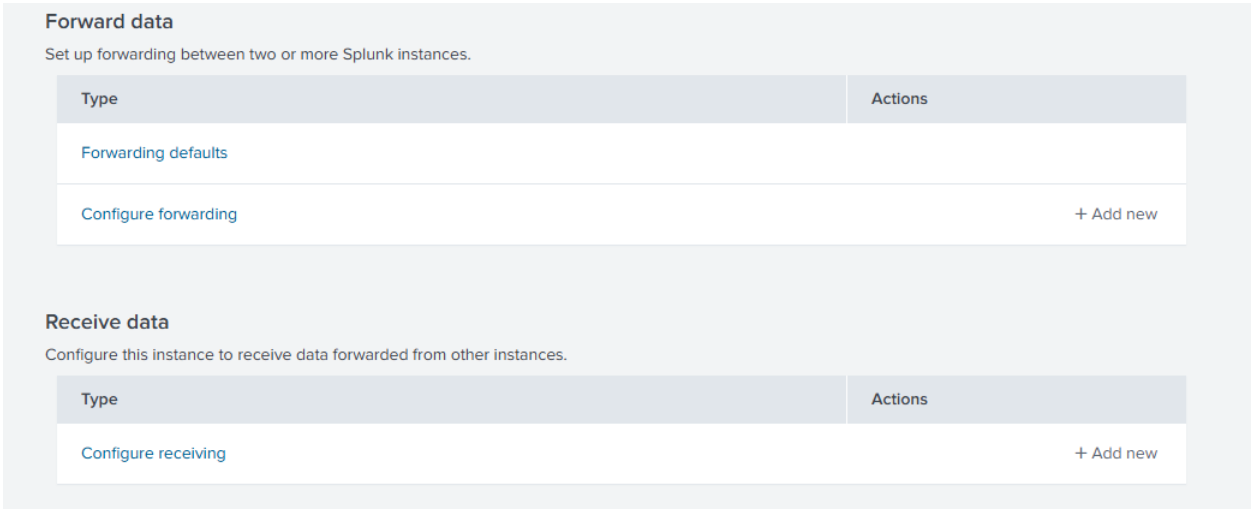


Next, on the HOST we set up our receiving index,

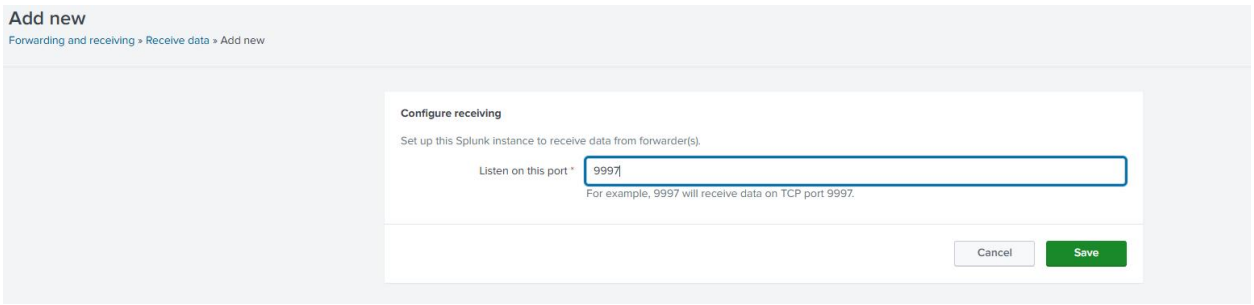
Launch splunk on host

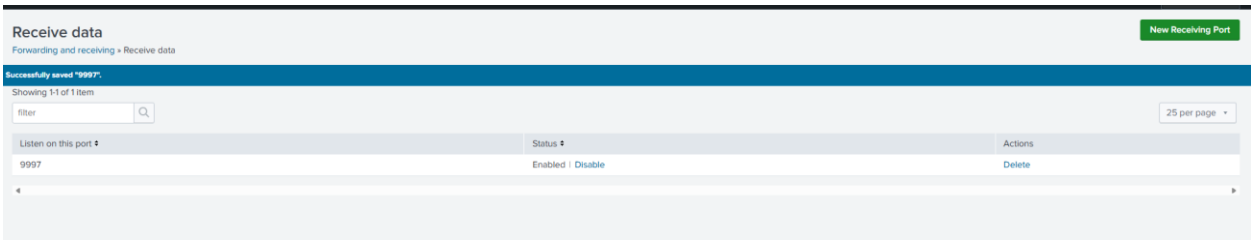
Click settings and select forwarding and receiving



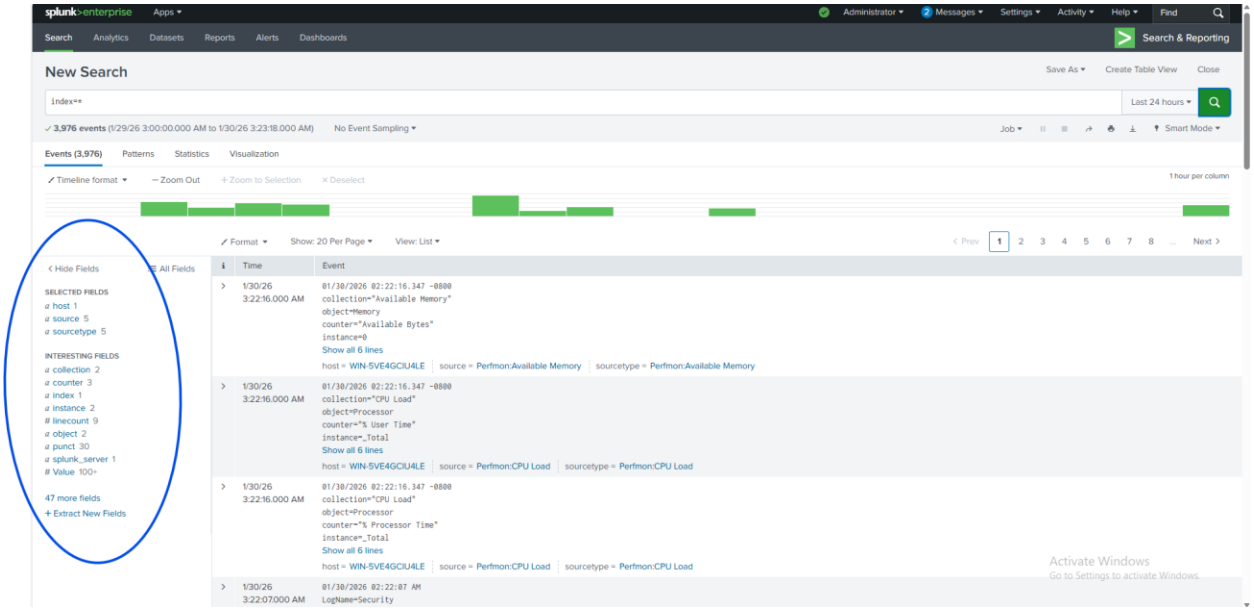


Add new, use port selected during installation





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