

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
-

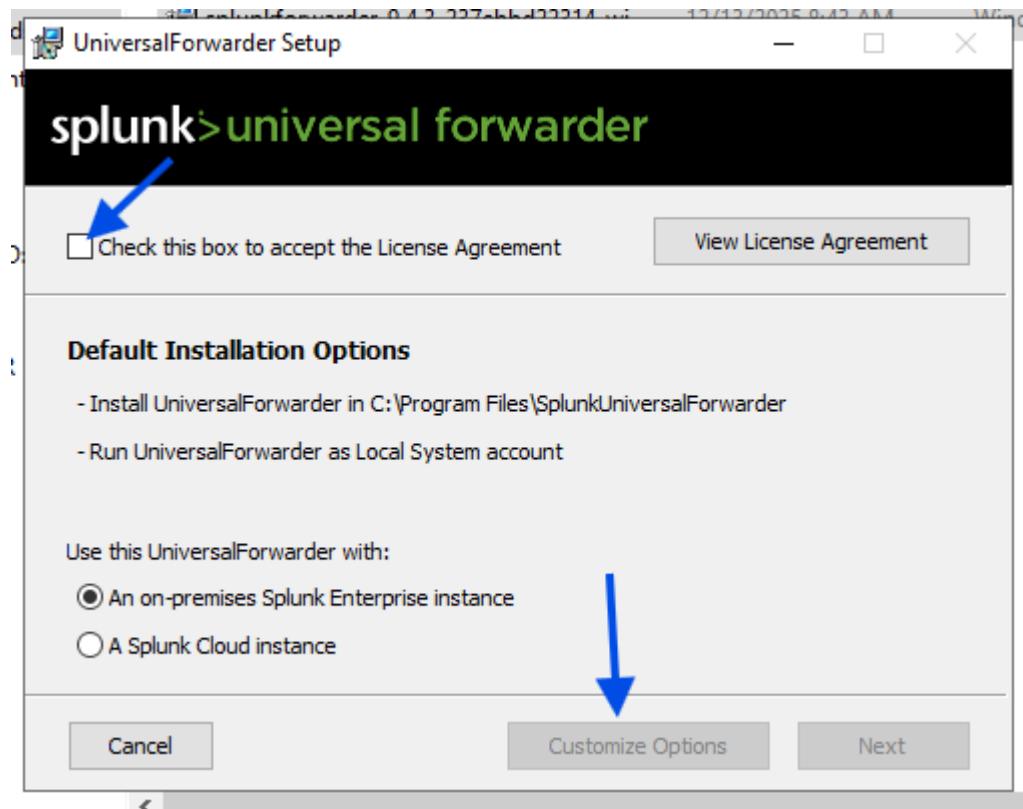
Why Organizations Use Splunk SIEM

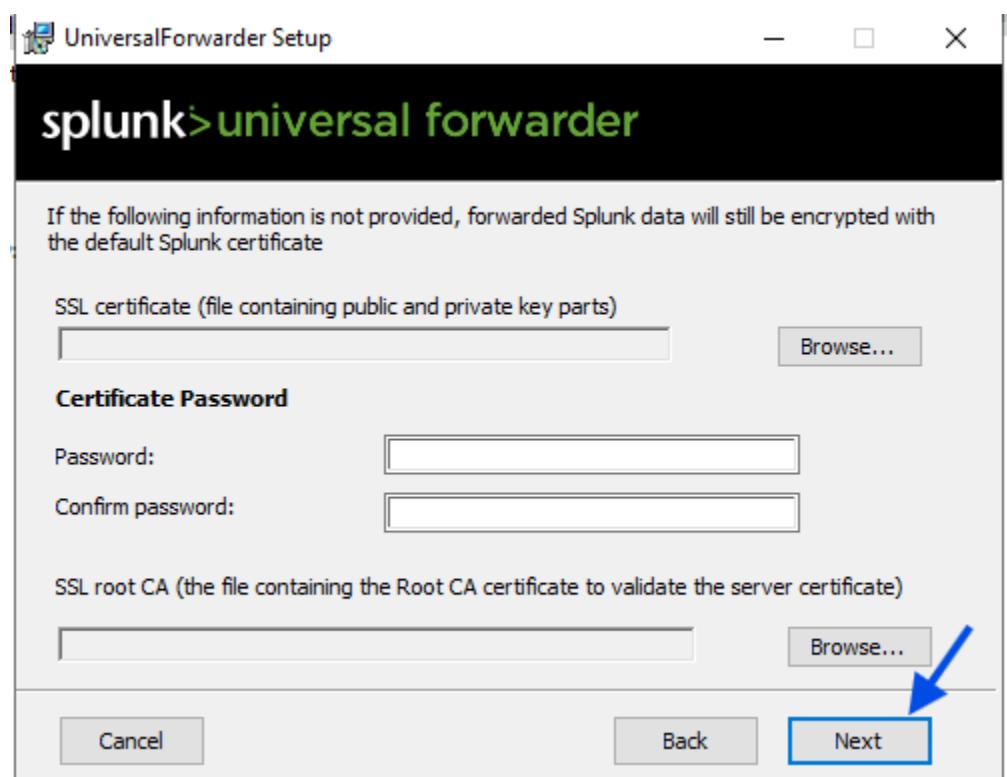
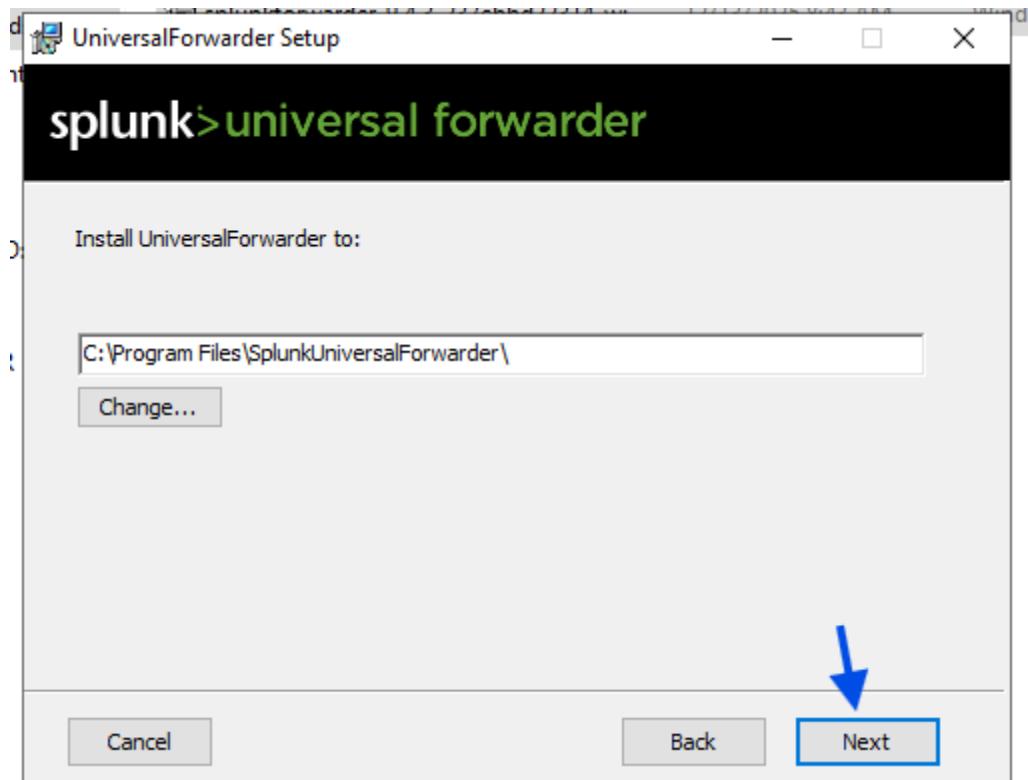
- Scales to very large environments
- Fast search and powerful analytics
- Highly customizable dashboards
- Strong threat detection and investigation
- Widely adopted in SOC environments

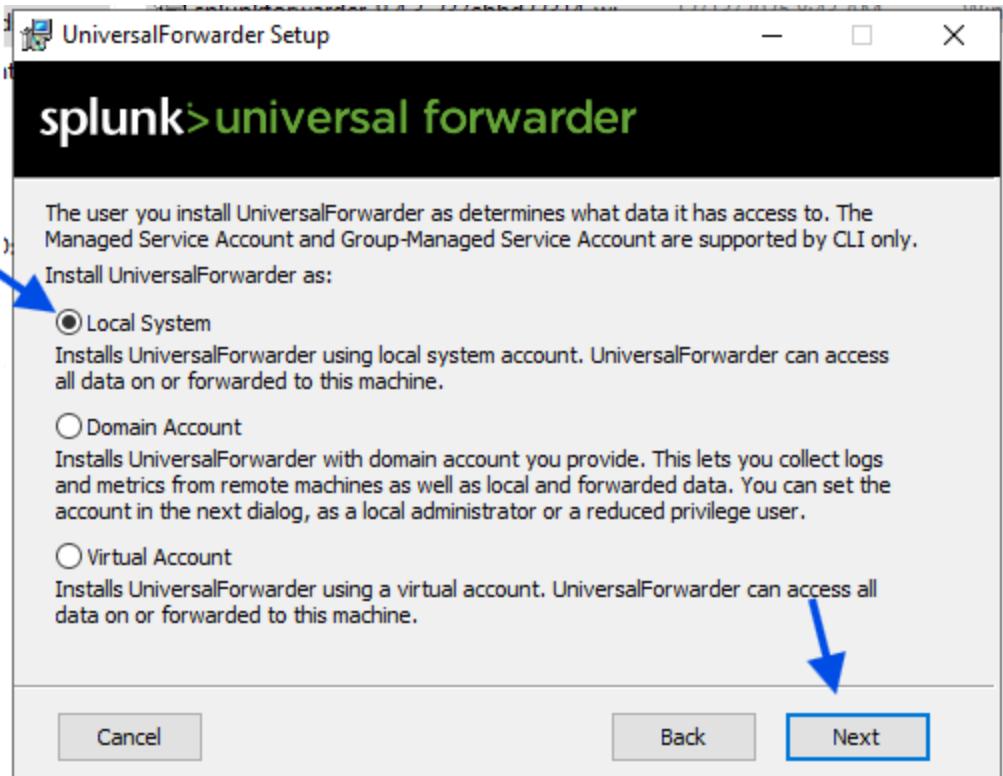
Below is a guide on installation and use of splunk

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

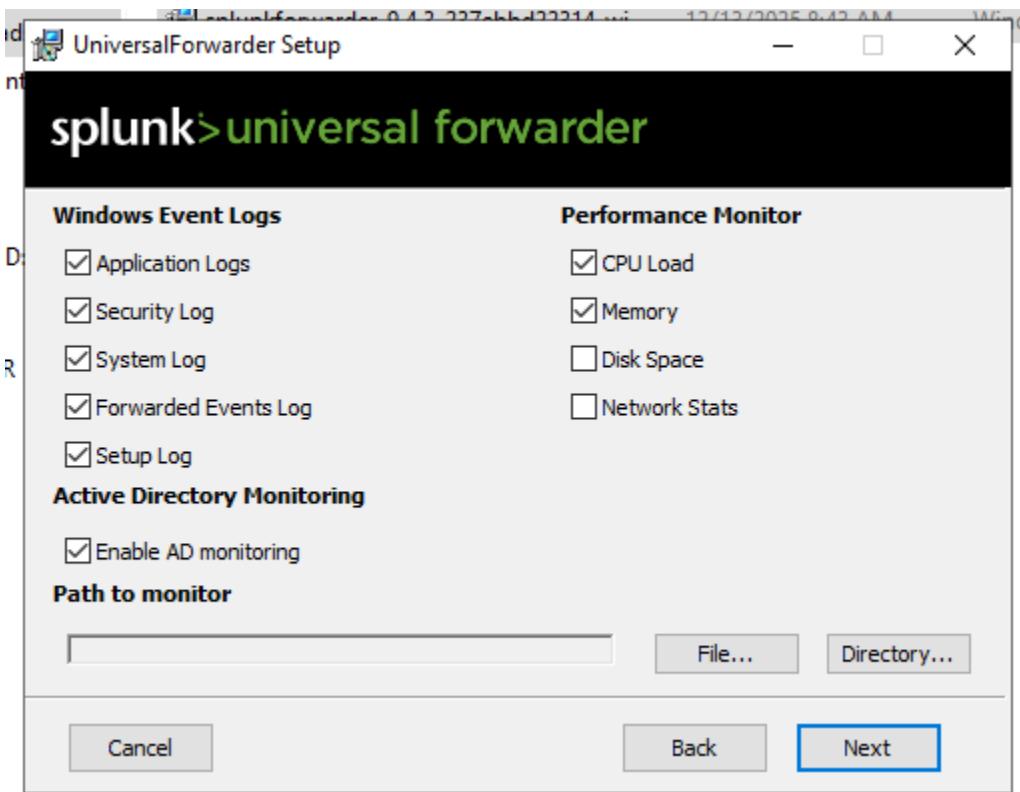
Install splunk forwarder on server



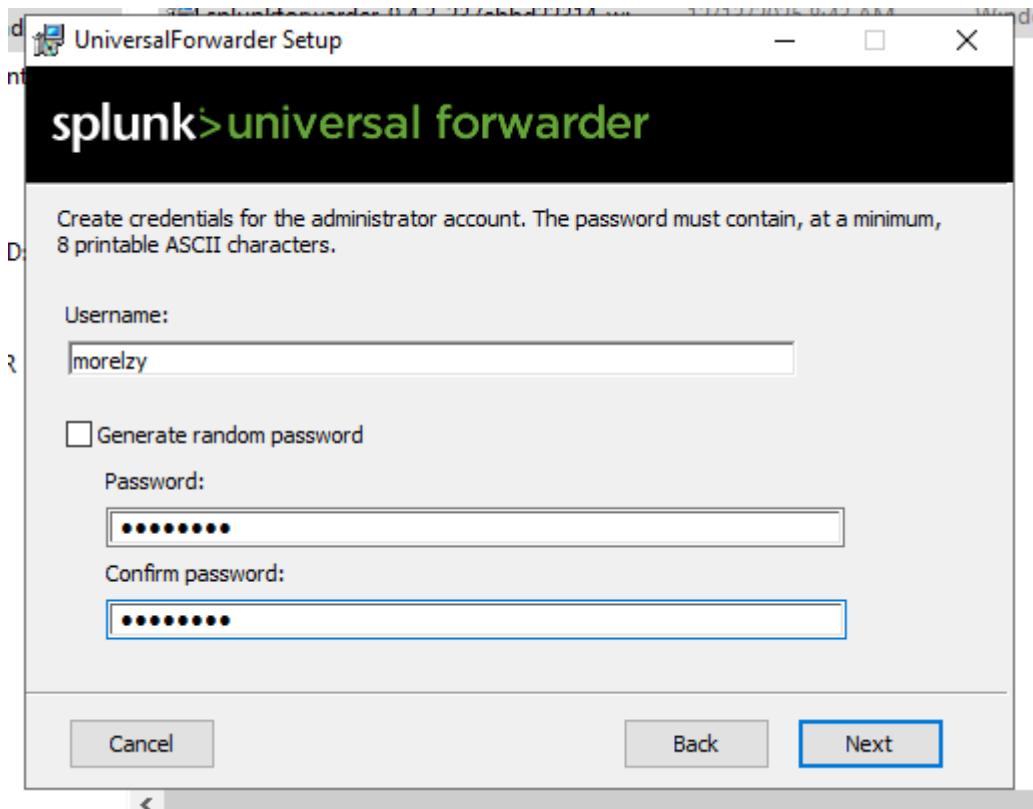




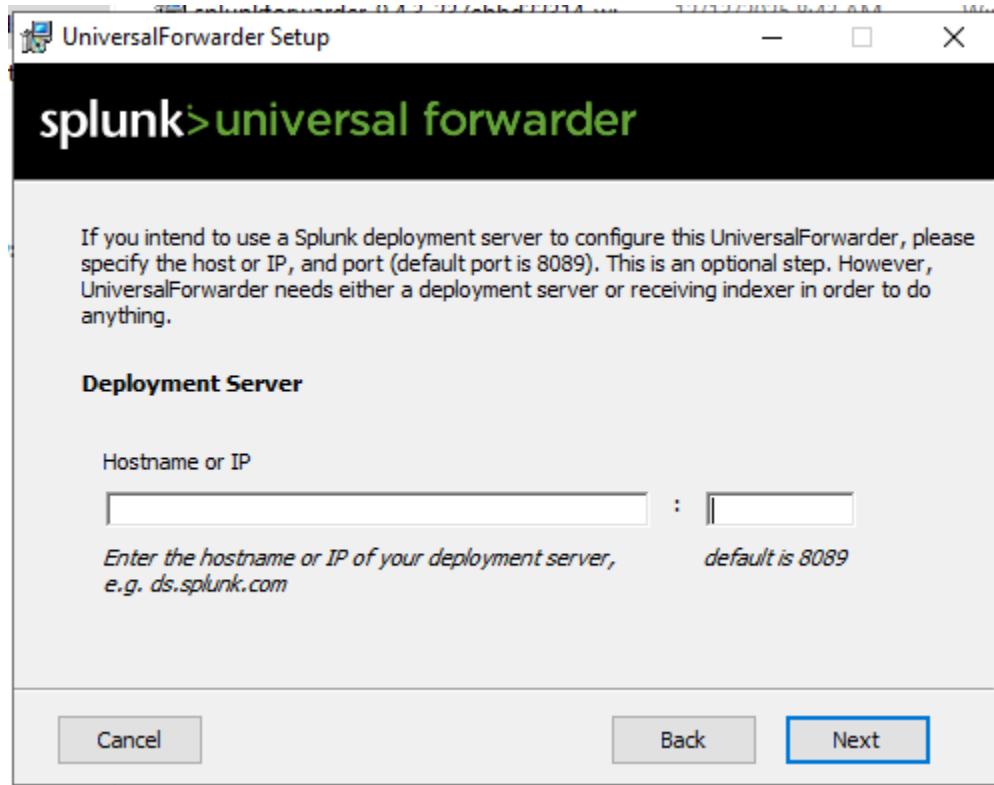
Check the logs we want reported and click next



Create username and password



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

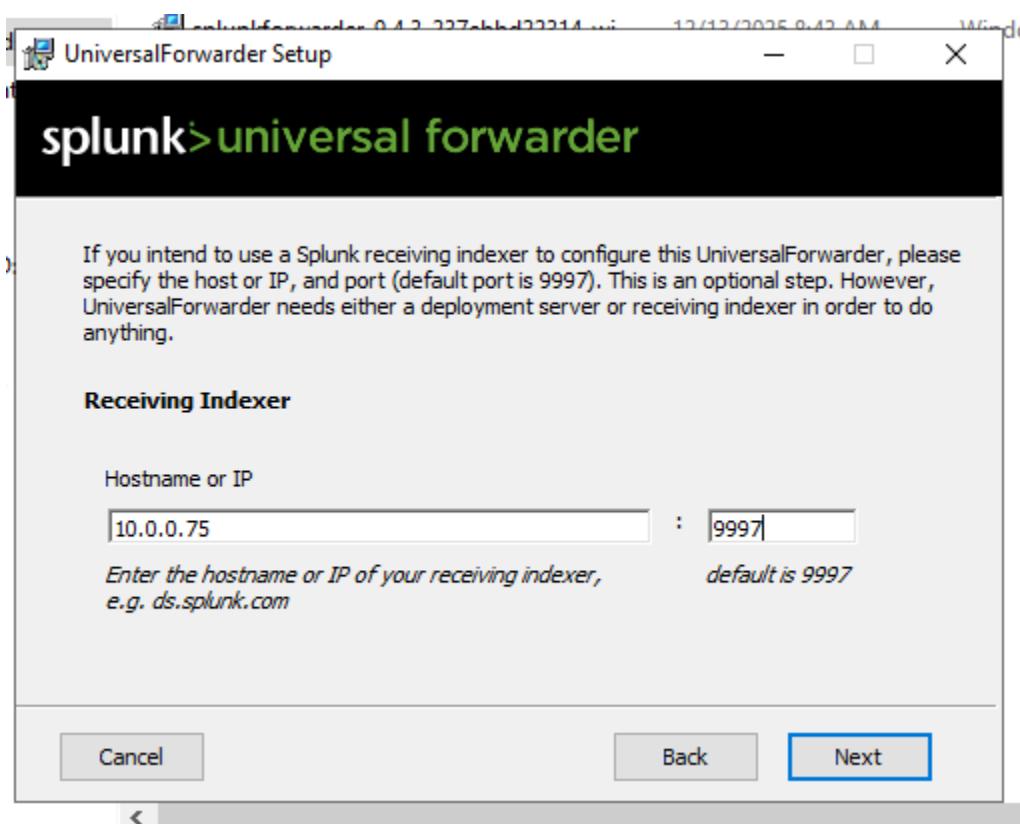


For the receiver indexer, provide the ip address of the host PC and use default port

```
Wireless LAN adapter Wi-Fi:

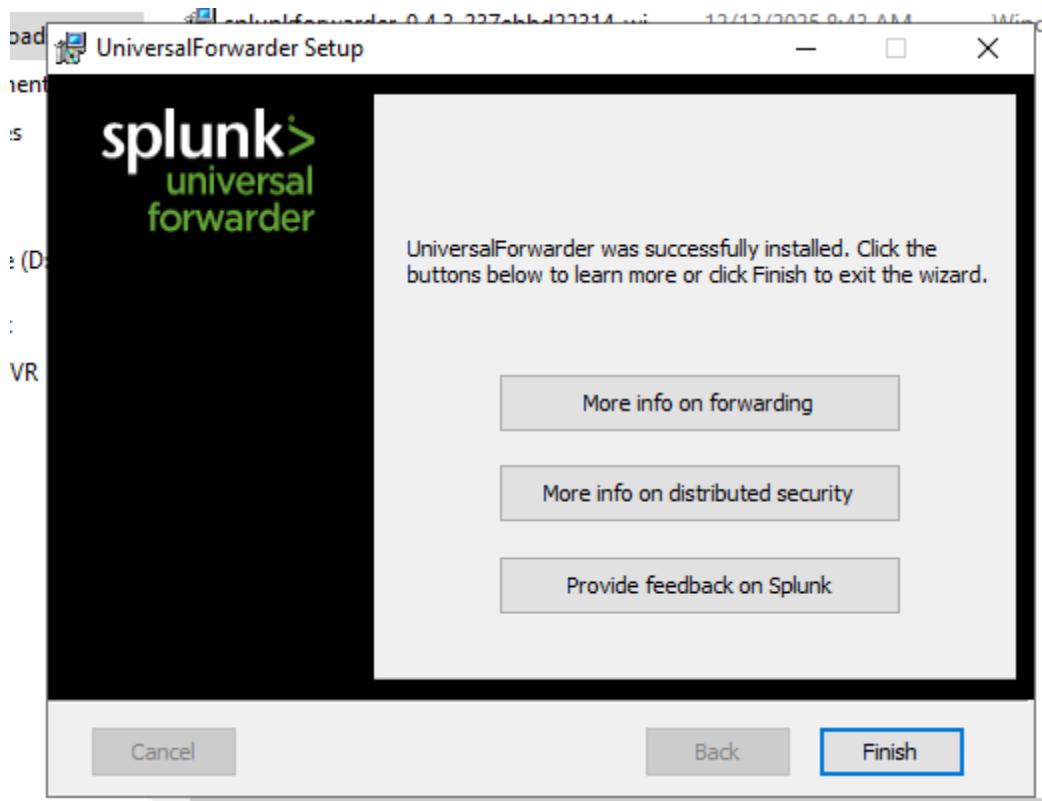
Connection-specific DNS Suffix . :
IPv6 Address . . . . . : 2604:3d09:888:1800::e408
IPv6 Address . . . . . : 2604:3d09:888:1800:e39c:a5d6:3dde:3b9c
Temporary IPv6 Address . . . . . : 2604:3d09:888:1800:2074:fe87:5e4a:b404
Link-local IPv6 Address . . . . . : fe80::b39b:7ef5:eb05:179%8
IPv4 Address . . . . . : 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:
```

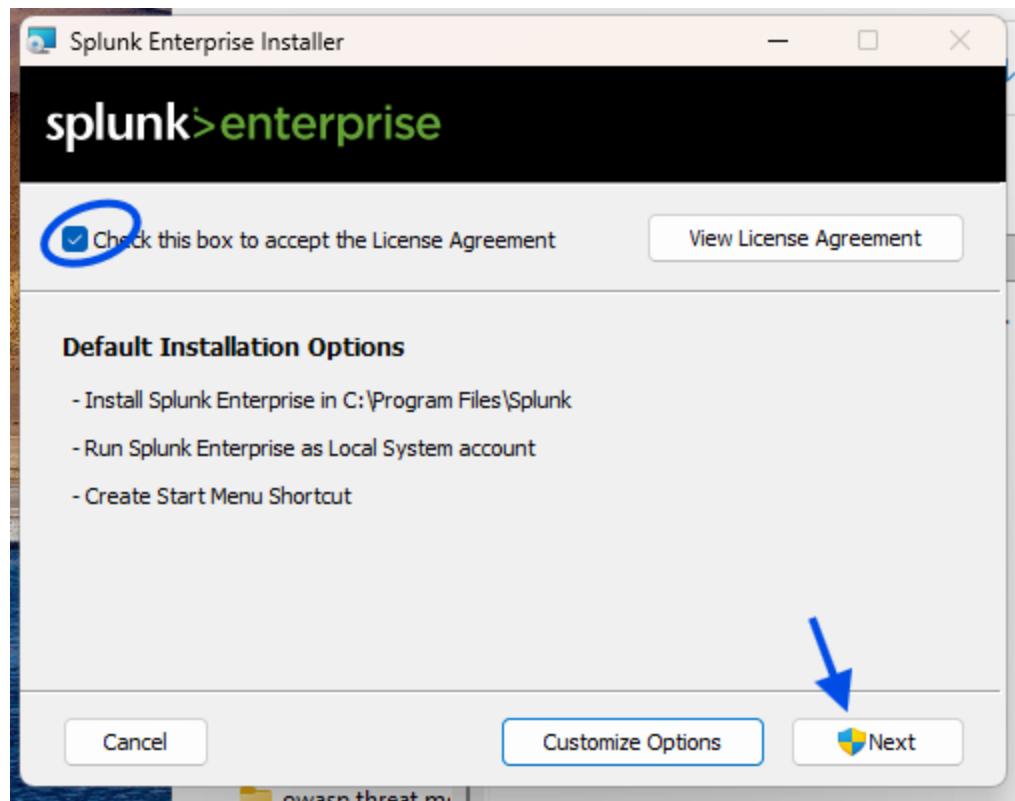


Click next and install

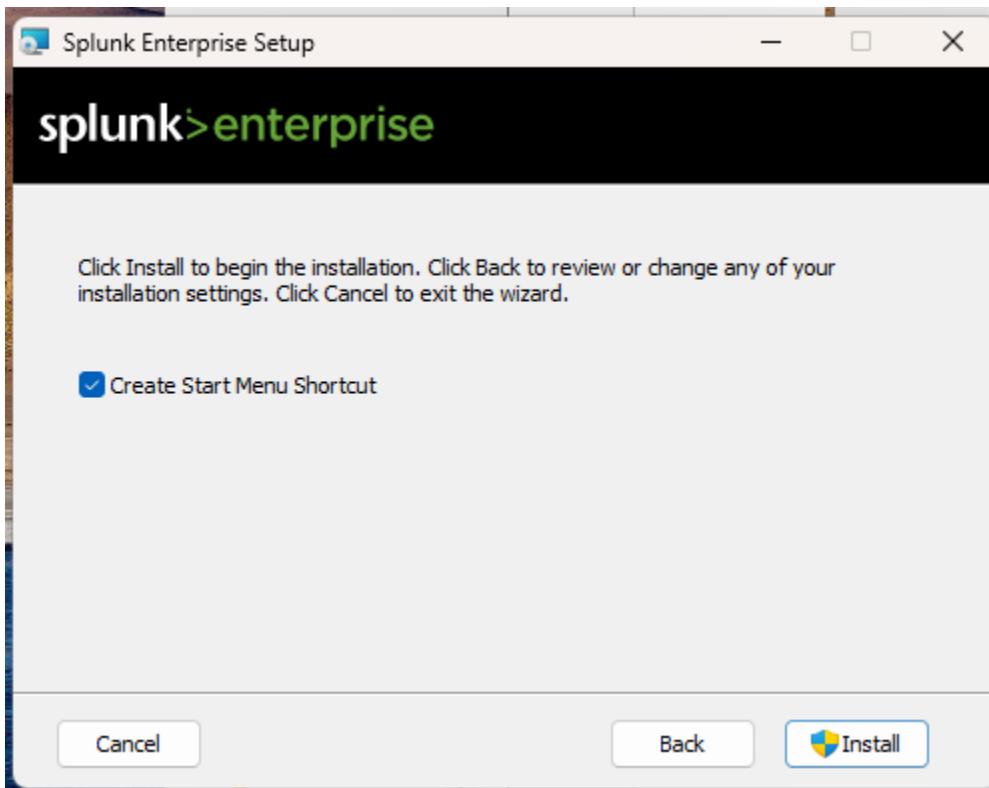
Click finish



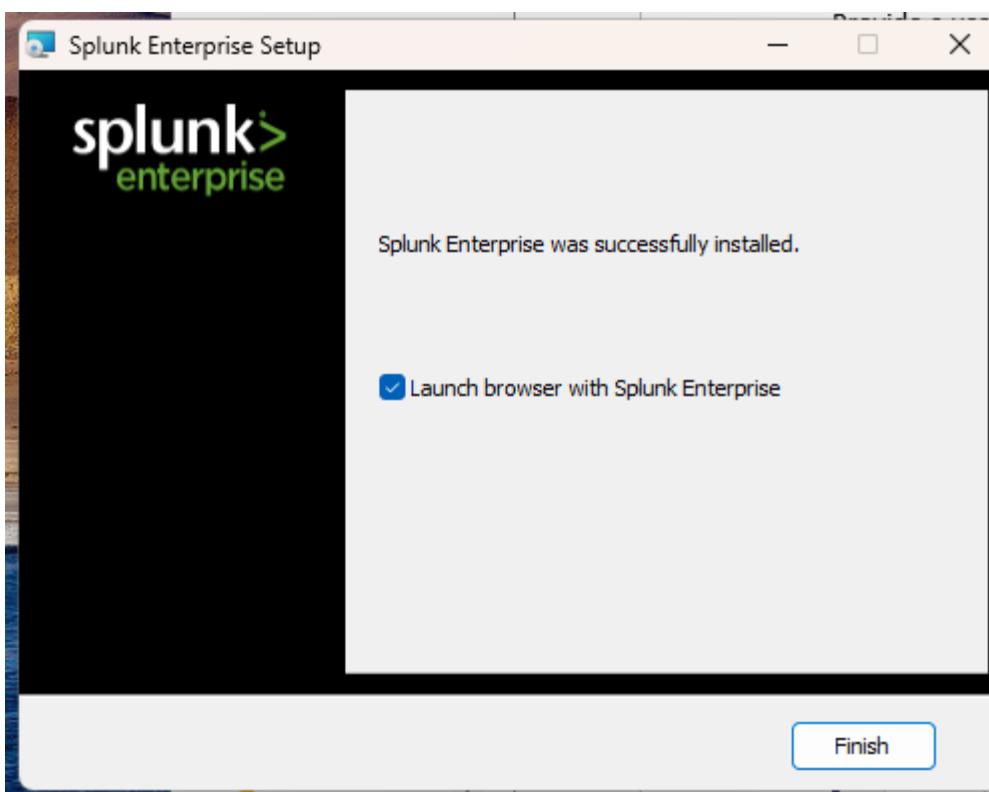
Next we install splunk enterprise on host machine



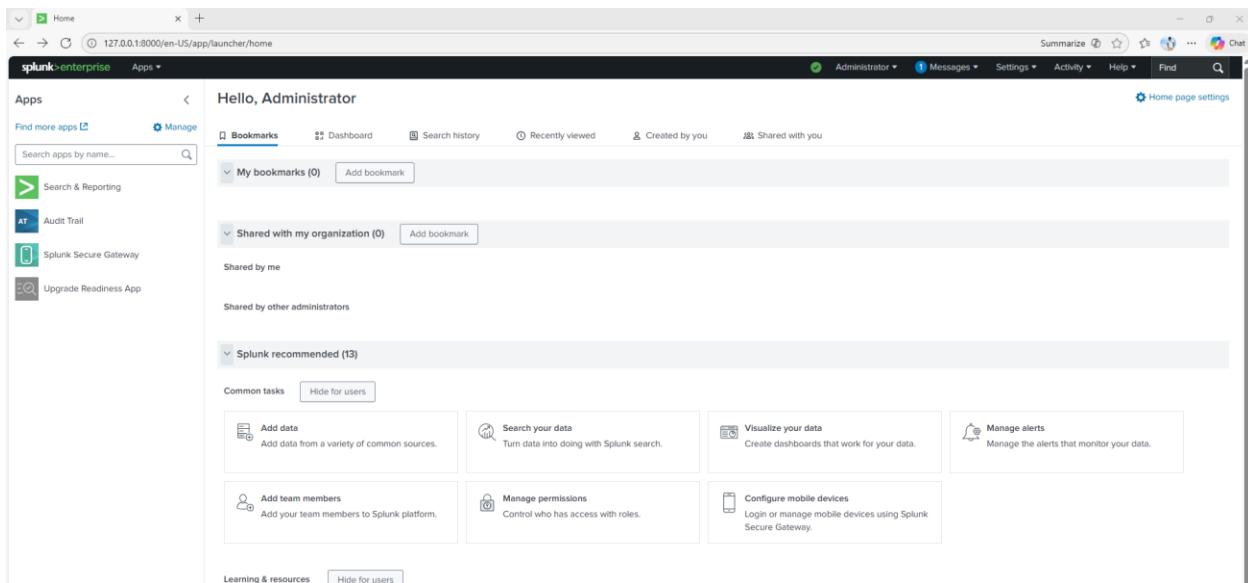
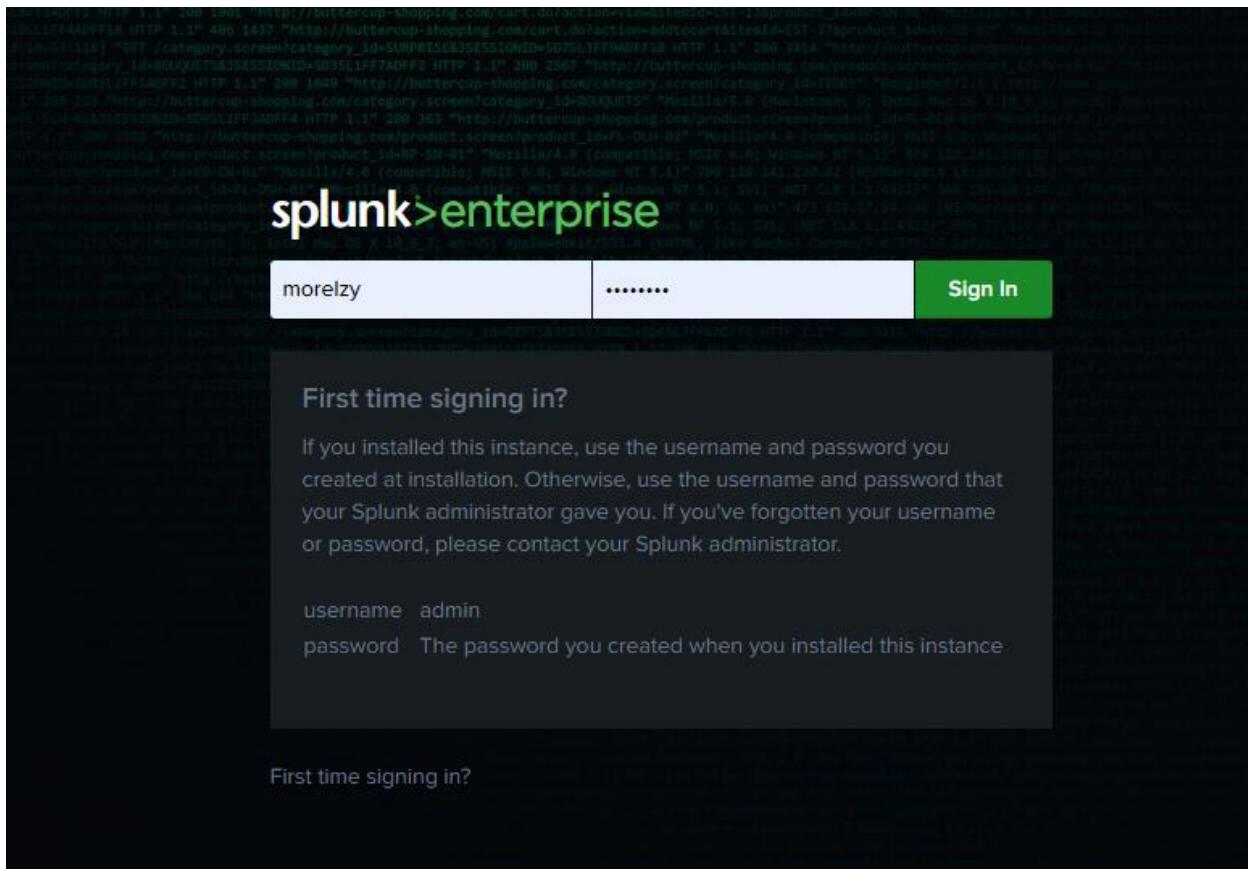
Provide a user name and password, then click install



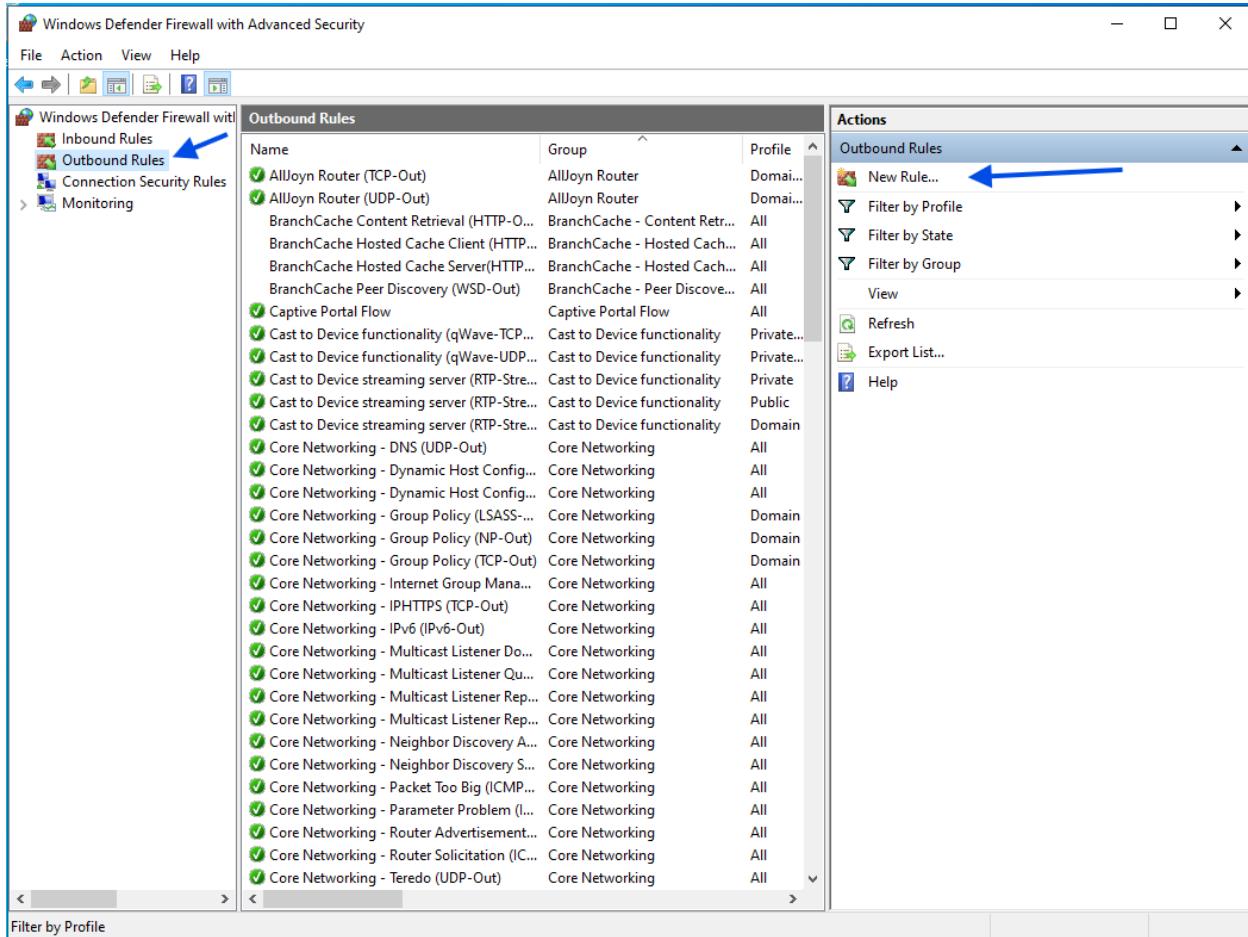
Click finish to launch splunk

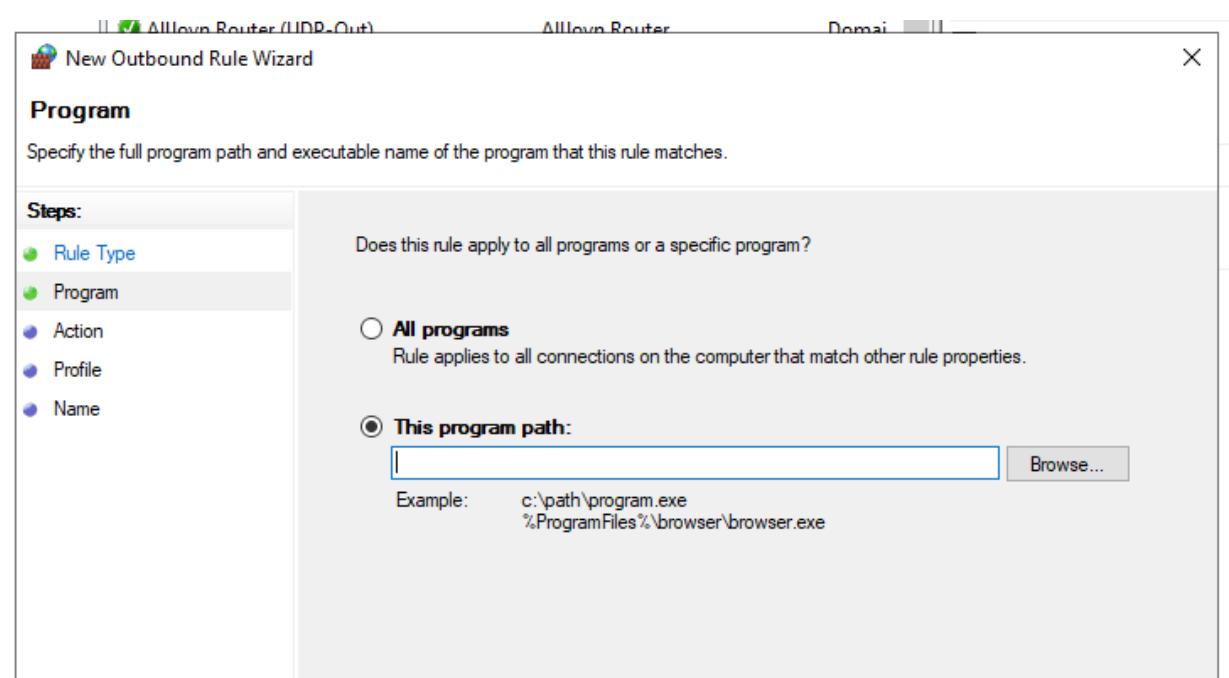
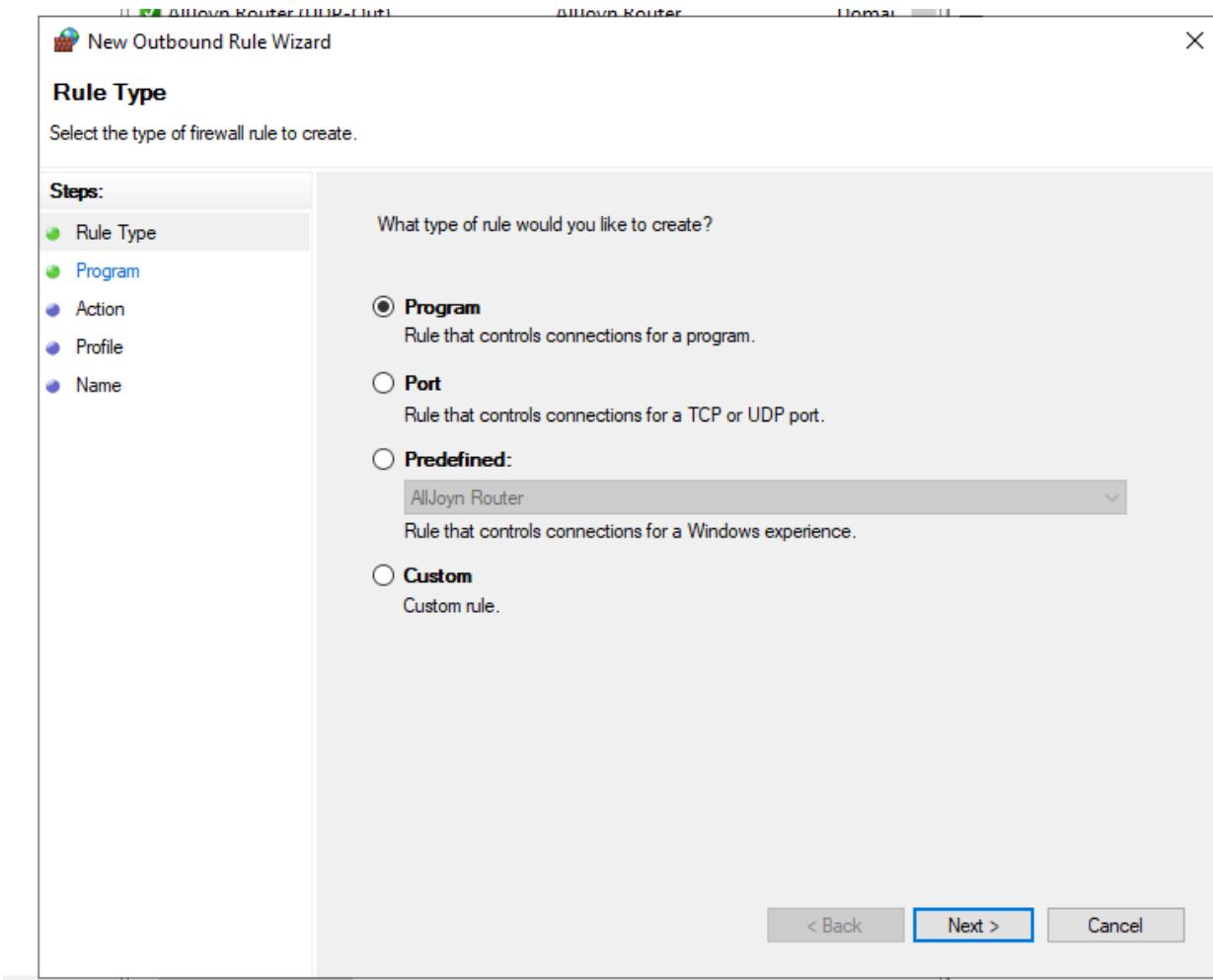


It opens up in a browser and requests for the username and password inputted while setting up



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





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:

%ProgramFiles%\Splunk UniversalForwarder\bin\splunkd.exe

[Browse...](#)

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.

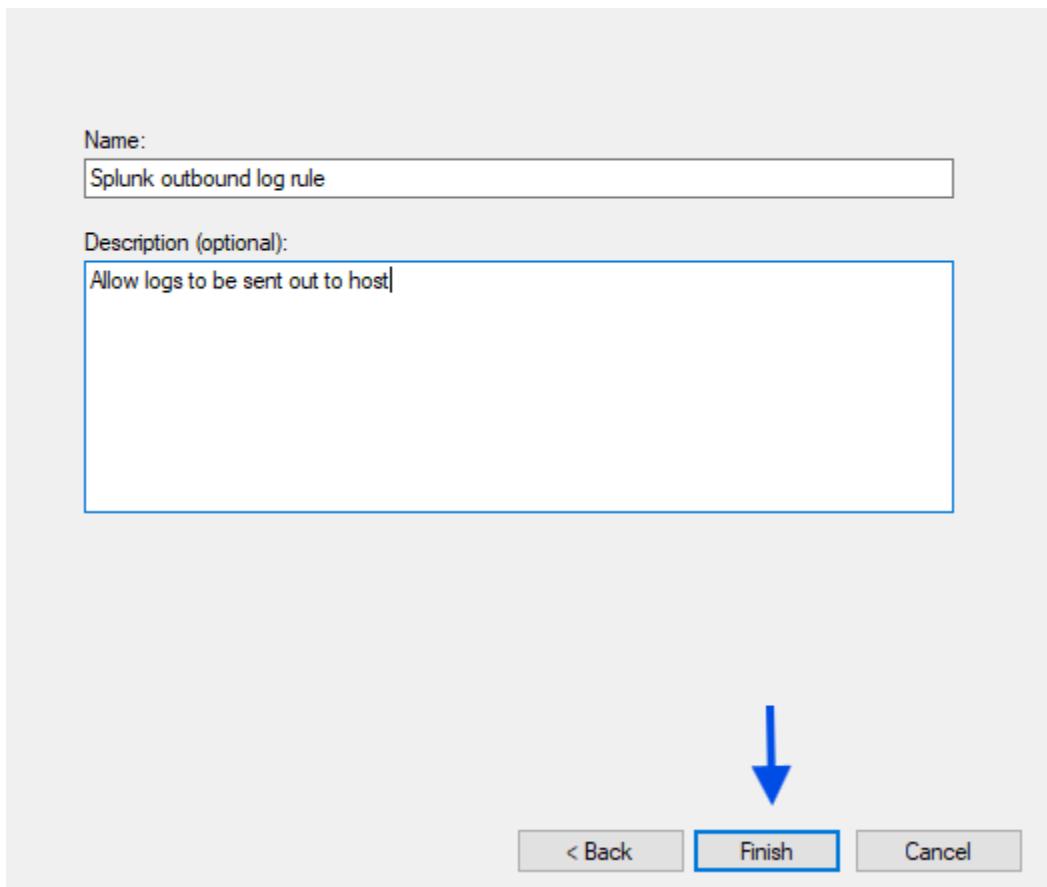
[Customize...](#)

Block the connection

< Back

[Next >](#)

Cancel



Name	Group	Profile
Splunk outbound log rule	All	
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...
BranchCache Content Retrieval (HTTP-O...)	BranchCache - Content Retr...	All
BranchCache Hosted Cache Client (HTTP...	BranchCache - Hosted Cach...	All
BranchCache Hosted Cache Server(HTTP...	BranchCache - Hosted Cach...	All
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove...	All
Captive Portal Flow	Captive Portal Flow	All
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...

Actions

- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

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

Launch splunk on host

Click settings and select forwarding and receiving

The screenshot shows the Splunk Settings page. At the top, there are navigation links: Administrator, Messages (with 1 notification), Settings (circled in blue), Activity, Help, and Find. Below the navigation is a search bar labeled "Search settings...". On the left, there's a sidebar with "Add Data" (represented by a database icon) and "Monitoring Console" (represented by a gauge icon). The main content area is divided into sections: KNOWLEDGE (Searches, reports, and alerts; Data models; Event types; Tags; Fields; Lookups; User interface; Alert actions; Advanced search; All configurations), DATA (Data inputs; Forwarding and receiving (highlighted with a blue arrow); Indexes; Report acceleration summaries; Source types; Ingest actions), and DISTRIBUTED ENVIRONMENT (Forwarder management; Indexer clustering).

This screenshot shows the "Forwarding and receiving" configuration page under the "Receive data" section. It includes a table with a single row for "Configure receiving" and a "+ Add new" button.

Type	Actions
Configure receiving	+ Add new

Add new, use port selected during installation

This screenshot shows the "Configure receiving" dialog box. It asks to set up the instance to receive data from forwarder(s). A text input field "Listen on this port*" contains the value "9997". Below the input field is a note: "For example, 9997 will receive data on TCP port 9997." At the bottom right are "Cancel" and "Save" buttons.

Receive data

Forwarding and receiving > Receive data

Successfully saved "9997".

Show 1 of 1 item

filter	Status	Actions
Listener on this port	Enabled Disable	Delete
9997		

25 per page ▾

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

splunk-enterprise Apps ▾

Search Analytics Datasets Reports Alerts Dashboards

Administrator Messages Settings Activity Help Find

New Search

index=*

3,976 events (1/29/26 3:00:00.000 AM to 1/30/26 3:23:18.000 AM) No Event Sampling ▾

Events (3,976) Patterns Statistics Visualization

Timeline format ▾ Zoom Out ▾ Zoom to Selection ▾ Deselect

1 hour per column

Format ▾ Show: 20 Per Page ▾ View: List ▾

1 2 3 4 5 6 7 8 Next ▾

SELECTED FIELDS

- ↳ All Fields
- ↳ host 1
- ↳ source 5
- ↳ sourcetype 5

INTERESTING FIELDS

- ↳ collection 2
- ↳ counter 3
- ↳ index 1
- ↳ instance 2
- ↳ #linecount 9
- ↳ object 2
- ↳ punct 30
- ↳ splunk_server 1
- ↳ # Value 100+
- + Extract New Fields

47 more fields

Activate Windows
Go to Settings to activate Windows.

i	Time	Event
>	1/30/26 3:22:16.000 AM	01/30/2026 02:22:16.347 -0800 collection="Available Memory" object="Memory" counter="Available Bytes" instance="0" Show all 6 lines host = WIN-5VE4GC1U4LE source = Perfmon.Available Memory sourcetype = Perfmon.Available Memory
>	1/30/26 3:22:16.000 AM	01/30/2026 02:22:16.347 -0800 collection="CPU Load" object="Processor" counter="% User Time" instance="Total" Show all 6 lines host = WIN-5VE4GC1U4LE source = Perfmon.CPU Load sourcetype = Perfmon.CPU Load
>	1/30/26 3:22:16.000 AM	01/30/2026 02:22:16.347 -0800 collection="CPU Load" object="Processor" counter="% Processor Time" instance="Total" Show all 6 lines host = WIN-5VE4GC1U4LE source = Perfmon.CPU Load sourcetype = Perfmon.CPU Load
>	1/30/26 3:22:07.000 AM	01/30/2026 02:22:07 AM LogName=Security

We can dig deeper or search for specific ports or keywords