

SITE-TO-SITE VPN AND LOG FORWARDING TO SPLUNK FOR TTI NETWORK

CISA 4390 – Enterprise Network Project

Instructors: John Ali, Kirksal Icoz, Rouzbeh Keshavarz, Travis Penner, Hamid Talebi, Areeb Yasir

Scott Bandy (A01366713)
Jason Chan (A01248750)
Nicholas Dunsmuir (A01325497)
Brian Hayter (A01356751)
Thomas Jelstad (A01357395)
Harsheen Kaur (A01363090)
Joey Lam (A00967230)
Yvonne Li (A00730798)
Suraj Nand (A01240738)
Andrei Tepei (A01384863)

Table of Contents

Table of Contents.....	2
Phase 1: Site-to-Site VPN between Vancouver and Burnaby.....	3
IP Addressing Table.....	3
FortiGate Setup (configure on both sites accordingly).....	3
Configure Site-to-Site VPN From Both Routers.....	8
Phase 2: Splunk Configuration.....	12
IP Configuration on Windows VM (Splunk Server and Forwarder) on both Sites.....	12
VMware Workstation Setup (on both Sites):.....	13
Splunk Server Setup:.....	16
Splunk Forwarder Setup.....	19
Splunk Server FG & Cisco, UDP & Index Setup on both Site VM.....	25
Splunk Forwarder Conf File Configuration.....	34
FortiGate Logging Setting Setup.....	36
Verification of Fortigate Logs Received.....	37
Cisco Logging Configuration.....	39
Verification of Cisco Logging.....	42
Active Directory Configuration.....	43
Verification of Active Directory Logs.....	44
SNMP Trap Configuration.....	45
Verification of SNMP Trap Logging.....	49

Phase 1: Site-to-Site VPN between Vancouver and Burnaby

IP Addressing Table

Site 2 - Vancouver	Address	172.31.64.0/20
Router WAN	To Fortigate	172.31.64.254/24
FortiGate	To Site Router	172.31.64.220/24
	To Vancouver LAN	172.31.65.10/24
	To Splunk LAN	172.31.66.99/24
	DHCP Server for Splunk LAN	172.31.66.10-80/24
Host PC	DHCP Client on Splunk LAN	
Splunk Server	Static	172.31.66.200/24
Splunk Forwarder	Static	172.31.66.201/24
Site 3 - Burnaby	Address	172.31.96.0/21
Router WAN	To Fortigate	172.31.96.254/24
FortiGate	To Site Router	172.31.96.220/24
	To Burnaby LAN	172.31.97.10/24
	To Splunk LAN	172.31.98.99/24
	DHCP Server for Splunk LAN	172.31.98.10-80/24
Host PC	DHCP Client on Splunk LAN	
Splunk Server	Static	172.31.98.200
Splunk Forwarder	Static	172.31.98.201

FortiGate Setup (configure on both sites accordingly)

This is the baseline configuration.

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
dmz	Physical Interface		10.10.1.255.255.255.0	PING HTTPS HTTP FMG-Access Security Fabric Connection			1
wan1	Physical Interface		192.168.64.26/255.255.255.0	PING FMG-Access			0
wan2	Physical Interface		0.0.0/0.0.0.0	PING FMG-Access			0

Double-click the ‘Internal’, change the IP Address, and configure the DHCP Server range for your LAN.

The screenshot shows the FortiGate 60E web interface with the URL <https://172.31.66.99/ng/interface/edit/internal>. The left sidebar is collapsed. The main content area is titled 'Edit Interface' for 'Internal LAN (internal)'. The 'Addressing mode' is set to 'DHCP'. In the 'Address' section, the IP/Netmask is listed as 172.31.66.99/255.255.255.0. Below this, there are fields for 'Name' (Internal), 'Destination' (172.31.66.99/255.255.255.0), and 'Secondary IP address'. Under 'Administrative Access', several checkboxes are checked: HTTPS, HTTP, PING, and SNMP. The 'DHCP Server' section at the bottom has an 'Address range' of 172.31.66.10-172.31.66.80. At the bottom right are 'OK' and 'Cancel' buttons.

On the Host PC, shutdown and then bring up the NIC that is connected to the FortiGate. The IP should change according to the DHCP Server. (Site 2 and 3)

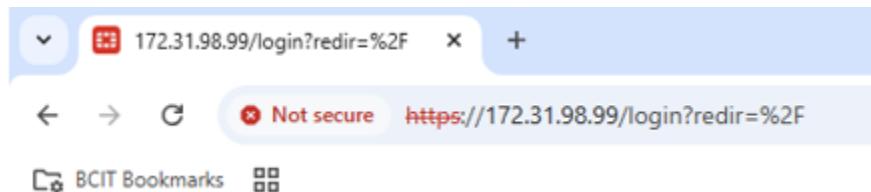
```
Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix . .
Link-local IPv6 Address . . . . . : fe80::91e:a5dd:1f50:6a6f%5
IPv4 Address . . . . . : 172.31.66.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.31.66.99
```

```
Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . . . : 
Description . . . . . : Intel(R) Ethernet 10G 2P X550-t Adapter
Physical Address. . . . . : B4-96-91-A8-C7-F0
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::2de5:f71c:ea32:aaea%7(Preferred)
IPv4 Address. . . . . : 172.31.98.10(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, May 22, 2025 11:20:33 AM
Lease Expires . . . . . : Thursday, May 29, 2025 11:20:34 AM
Default Gateway . . . . . : 172.31.98.99
DHCP Server . . . . . : 172.31.98.99
DHCPv6 IAID . . . . . : 129275537
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-DF-EF-01-B4-96-91-A8-C7-F0
DNS Servers . . . . . : 96.45.45.45
                                         96.45.46.46
NetBIOS over Tcpip. . . . . : Enabled
```

Go to the new Management IP on the browser which is the gateway address of the FortiGate.
Site2: <https://172.31.66.99/> or Site3: https://172.31.98.99/. Click ‘Advanced’ and proceed to the login page then sign in with your account.



Now you should see the Internal LAN IP has changed. 172.31.98.99 for Site 3.

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
fortilink	Hardware Switch			PING Security Fabric Connection		169.254.1.2-169.254.1.254	2
Internal LAN (internal)	Hardware Switch	internal1 internal3 internal4 internal5 internal6	172.31.66.99/255.255.255.0	PING HTTPS SNMP HTTP	1	172.31.66.10-172.31.66.80	5

Go to the WAN port and configure an IP address on the same subnet as the Site Router to connect to the local Site Router. Here, we configured a 172.31.64.220/24 address since the Site 2 Router is 172.31.64.254/24. 172.31.96.220/24 for Site 3.

To Router WAN (wan1)	Physical Interface	172.31.64.220/255.255.255.0	PING HTTPS SSH SNMP HTTP
----------------------	--------------------	-----------------------------	--------------------------------------

Go to ‘Network’ then ‘Static Routes’ as we will be manually defining the path the network traffic should follow to reach their destination.

Destination	Gateway IP	Interface
No results		

Click 'Create New' and configure the following where Gateway Address is the WAN Router's IP. 172.31.96.254 for Site 3.

Destination	<input checked="" type="radio"/> Subnet	<input type="radio"/> Named Address	<input type="radio"/> Internet Service
Gateway Address	0.0.0/0.0.0		
	172.31.64.254		
Interface	To Router WAN (wan1)		
Administrative Distance	10		
Comments	Write a comment... / 0/255		
Status	Enabled Disabled		

Configure the Firewall Policy like so. Name it appropriately, specifying incoming and outgoing traffic (interface), specifying the source and destination IPs, and defining the type of protocol allowed (service).

Name	In-to-Out
Incoming Interface	Internal LAN (internal)
Outgoing Interface	To Router WAN (wan1)
Source	all
Destination	all
Schedule	always
Service	ALL
Action	ACCEPT DENY

Verify connectivity with a ping test to the local Router from Fortigate.

```
FG-SITE2 # execute ping 172.31.64.254
PING 172.31.64.254 (172.31.64.254): 56 data bytes
64 bytes from 172.31.64.254: icmp_seq=0 ttl=255 time=0.4 ms
64 bytes from 172.31.64.254: icmp_seq=1 ttl=255 time=0.2 ms
64 bytes from 172.31.64.254: icmp_seq=2 ttl=255 time=0.3 ms
64 bytes from 172.31.64.254: icmp_seq=3 ttl=255 time=0.2 ms
64 bytes from 172.31.64.254: icmp_seq=4 ttl=255 time=0.2 ms

--- 172.31.64.254 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.4 ms

FG-SITE2 #
```

```
FG-SITE3 # execute ping 172.31.96.254
PING 172.31.96.254 (172.31.96.254): 56 data bytes
64 bytes from 172.31.96.254: icmp_seq=0 ttl=255 time=0.4 ms
64 bytes from 172.31.96.254: icmp_seq=1 ttl=255 time=0.3 ms
64 bytes from 172.31.96.254: icmp_seq=2 ttl=255 time=0.3 ms
64 bytes from 172.31.96.254: icmp_seq=3 ttl=255 time=0.2 ms
64 bytes from 172.31.96.254: icmp_seq=4 ttl=255 time=0.3 ms

--- 172.31.96.254 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.3/0.4 ms

FG-SITE3 #
```

Then you will do the same on the Burnaby side but with the proper IP addressing scheme.

Configure Site-to-Site VPN From Both Routers

Go to 'VPN' on the sidebar, then click 'IPsec Wizard' and configure the following. Configure a policy name, select 'No NAT' to disable address translation, and apply the settings to FortiGate devices. For Site 3, name it 'SITE3-SITE2'

The screenshot shows the 'VPN Creation Wizard' interface. The current step is '1 VPN Setup'. The configuration includes:

- Name: SITE2-SITE3
- Template type: Site to Site
- NAT configuration: No NAT between sites (selected)
- Remote device type: FortiGate

To the right, there is a diagram titled 'Site to Site - FortiGate' showing two FortiGate units connected via the Internet.

Enter the remote device's IP address, select the outgoing interface, choose "Pre-shared Key" authentication, enter the key, then click "Next." Make sure it matches on both sides. Remote IP 172.31.64.220 on Site 3 side.

VPN Creation Wizard

2 Authentication > 3 Policy & Routing > 4 Review Settings

Remote device

IP Address Dynamic DNS

Remote IP address 172.31.96.220

Outgoing Interface To Router WAN (wan1)

Authentication method Pre-shared Key Signature

Pre-shared key *****

Site to Site - FortiGate

This FortiGate

Internet

Remote FortiGate

< Back Next > Cancel

Specify the local interface and subnets, add the remote subnets, select the desired internet access option, and click "Next." Reverse it for Site 3.

VPN Creation Wizard

3 Policy & Routing > 4 Review Settings

Local interface Internal LAN (internal)

Local subnets 172.31.66.0/24

Remote Subnets 172.31.98.0/24

Internet Access None Share Local Use Remote

Site to Site - FortiGate

This FortiGate

Internet

Remote FortiGate

< Back Next > Cancel

Review and confirm it.

VPN Creation Wizard

4 Review Settings

The following settings should be reviewed prior to creating the VPN.

Object Summary

Phase 1 interface	SITE2-SITE3
Local address group	SITE2-SITE3_local
Remote address group	SITE2-SITE3_remote
Phase 2 interface	SITE2-SITE3
Static route	static
Blackhole route	static
Local to remote policies	vpn_SITE2-SITE3_local
Remote to local policies	vpn_SITE2-SITE3_remote

VPN Creation Wizard

✓ VPN Setup > ✓ Authentication > ✓ Policy & Routing > ✓ Review Settings

✓ The VPN has been set up

Object Summary

Phase 1 interface	✓ SITE2-SITE3
Local address group	✓ SITE2-SITE3_local Edit
Remote address group	✓ SITE2-SITE3_remote Edit
Phase 2 interface	✓ SITE2-SITE3
Static route	✓ 2 Edit
Blackhole route	✓ 3 Edit
Local to remote policies	✓ vpn_SITE2-SITE3_local_0 (3)
Remote to local policies	✓ vpn_SITE2-SITE3_remote_0 (5)

You can see it here in the tunnel list.

IPsec						
Name		Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1
Site to Site - FortiGate	1					
SITE2-SITE3	172.31.96.220			0 B	0 B	✓ SITE2-SITE3

Double-click the SITE2-SITE3, then click Bring Up, then bring up All Phase 2 Selectors. You should see the tunnel is up as well as the icons being green confirming it.

IPsec						
Site to Site - FortiGate						
Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
SITE2-SITE3	172.31.96.220		0 B	0 B	✓ SITE2-SITE3	✓ SITE2-SITE3
						Reset Statistics Bring Up Bring Down Locate on VPN Map
						Phase 2 Selector: SITE2-SITE3 Bring Up Bring Down
						All Phase 2 Selectors Locate on VPN Map
Site to Site - FortiGate						
SITE3-SITE2	172.31.64.220	172.31.64.220	0 B	0 B	✓ SITE3-SITE2	✓ SITE3-SITE2

Do a ping test from VM on one site to the other site to verify Site-to-Site VPN connectivity.

W11 - SServer - VMware Workstation

File Edit View VM Tabs Help || + | X |

W11 - SServer W11 - SForwarder

Command Prompt

```
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>ping 172.31.98.200 -S 172.31.66.200 -n 3

Pinging 172.31.98.200 from 172.31.66.200 with 32 bytes of data:
Reply from 172.31.98.200: bytes=32 time=1ms TTL=126
Reply from 172.31.98.200: bytes=32 time=4ms TTL=126
Reply from 172.31.98.200: bytes=32 time=1ms TTL=126

Ping statistics for 172.31.98.200:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 2ms

C:\Users\admin>ping 172.31.98.201 -S 172.31.66.200 -n 3

Pinging 172.31.98.201 from 172.31.66.200 with 32 bytes of data:
Reply from 172.31.98.201: bytes=32 time=1ms TTL=126
Reply from 172.31.98.201: bytes=32 time=2ms TTL=126
Reply from 172.31.98.201: bytes=32 time=1ms TTL=126

Ping statistics for 172.31.98.201:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\admin>ping 172.31.98.10 -S 172.31.66.200 -n 3

Pinging 172.31.98.10 from 172.31.66.200 with 32 bytes of data:
Reply from 172.31.98.10: bytes=32 time=1ms TTL=126
Reply from 172.31.98.10: bytes=32 time=1ms TTL=126
Reply from 172.31.98.10: bytes=32 time<1ms TTL=126

Ping statistics for 172.31.98.10:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\admin>
```

```
Home < W11-SPLUNK < W11-FORWARDER <
Command Prompt + ▾

Primary Dns Suffix . . . . . : 
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . . . . . : 
Description . . . . . : Intel(R) 8257UL Gigabit Network Connection
Physical Address . . . . . : 00-0C-29-1E-B8-75
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::ab56:3d35:1d72:dd09%14(PREFERRED)
IPv4 Address . . . . . : 172.31.98.200(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.31.98.99
DHCPv6 IAID . . . . . : 83889193
DHCPv6 Client DUID. . . . . : 00-01-00-01-2F-BE-58-07-00-0C-29-1E-B8-75
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                        fec0:0:0:ffff::2%1
                        fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\user>ping 172.31.66.200 -S 172.31.98.200

Pinging 172.31.66.200 from 172.31.98.200 with 32 bytes of data:
Reply from 172.31.66.200: bytes=32 time=1ms TTL=126

Ping statistics for 172.31.66.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\user>
```

Phase 2: Splunk Configuration

IP Configuration on Windows VM (Splunk Server and Forwarder) on both Sites

On the **Splunk Server VM**, we change the IP address as followed from the table. The following IP configured is for the Vancouver Site. Configure the correct IP on the other side.

The screenshot shows two windows side-by-side. On the left is the 'Internet Protocol Version 4 (TCP/IPv4) Properties' dialog box for the 'W11 - SForwarder' VM. It displays the 'General' tab with the following settings:

- Obtain an IP address automatically (radio button)
- Use the following IP address (radio button): IP address: 172.31.66.200, Subnet mask: 255.255.255.0, Default gateway: 172.31.66.99
- Obtain DNS server address automatically (radio button)
- Use the following DNS server addresses (radio button): Preferred DNS server: (empty), Alternate DNS server: (empty)
- Validate settings upon exit (checkbox)

On the right is the 'Windows IP Configuration' window for the 'W11-SPLUNK' host. It lists the following details for the 'Ethernet adapter Ethernet0':

Setting	Value
Host Name	W11-SPLUNK
Primary Dns Suffix	
Node Type	Hybrid
IP Routing Enabled	No
WINS Proxy Enabled	No
Ethernet adapter Ethernet0:	
Connection-specific DNS Suffix	
Description	Intel(R) 82574L Gigabit Network Connection
Physical Address	00-0C-29-1E-B8-75
DHCP Enabled	No
Autoconfiguration Enabled	Yes
Link-local IPv6 Address	fe80::ab56:3d35:1d72:dd09%14(Preferred)
IPv4 Address	172.31.98.200(Preferred)
Subnet Mask	255.255.255.0
Default Gateway	172.31.98.99
DHCPv6 IAID	83889193
DHCPv6 Client DUID	00-01-00-01-2F-BE-5B-07-00-0C-29-1E-B8-75
DNS Servers	fec0:0:0:ffff::1%1 fec0:0:0:ffff::2%1 fec0:0:0:ffff::3%1
NetBIOS over Tcpip	Enabled

On the **Splunk Forwarder VM**, we change the IP address as followed from the table. No DNS. Configure the correct IP on the other side.

The screenshot shows two windows side-by-side. On the left is the 'Internet Protocol Version 4 (TCP/IPv4) Properties' dialog box for the 'W11 - SForwarder' VM. It displays the 'General' tab with the following settings:

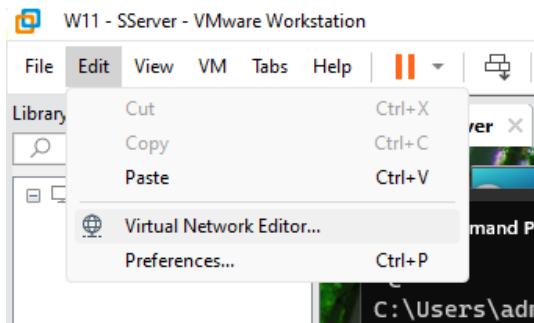
- Obtain an IP address automatically (radio button)
- Use the following IP address (radio button): IP address: 172.31.66.201, Subnet mask: 255.255.255.0, Default gateway: 172.31.66.99

On the right is the 'Windows IP Configuration' window for the 'W11-FORWARDER' host. It lists the following details for the 'Ethernet adapter Ethernet0':

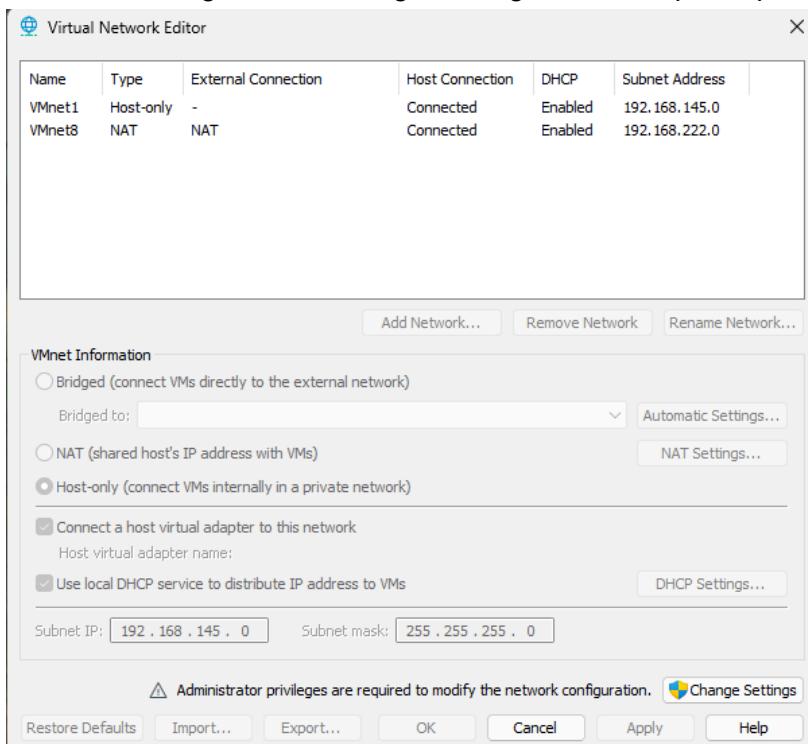
Setting	Value
Name	W11-FORWARDER
Primary Dns Suffix	
Type	Hybrid
Routing Enabled	No
Proxy Enabled	No
adapter Ethernet0:	
Connection-specific DNS Suffix	
Description	Intel(R) 82574L Gigabit Network Connection
Physical Address	00-0C-29-C2-4E-67
DHCP Enabled	No
Autoconfiguration Enabled	Yes
Link-local IPv6 Address	fe80::13b5:fe60:d54d:83c9%9(Preferred)
IPv4 Address	172.31.98.201(Preferred)
Subnet Mask	255.255.255.0
Default Gateway	172.31.98.99
DHCPv6 IAID	100666409
DHCPv6 Client DUID	00-01-00-01-2F-BE-5F-95-00-0C-29-C2-4E-67
DNS Servers	fec0:0:0:ffff::1%1 fec0:0:0:ffff::2%1 fec0:0:0:ffff::3%1
NetBIOS over Tcpip	Enabled

VMware Workstation Setup (on both Sites):

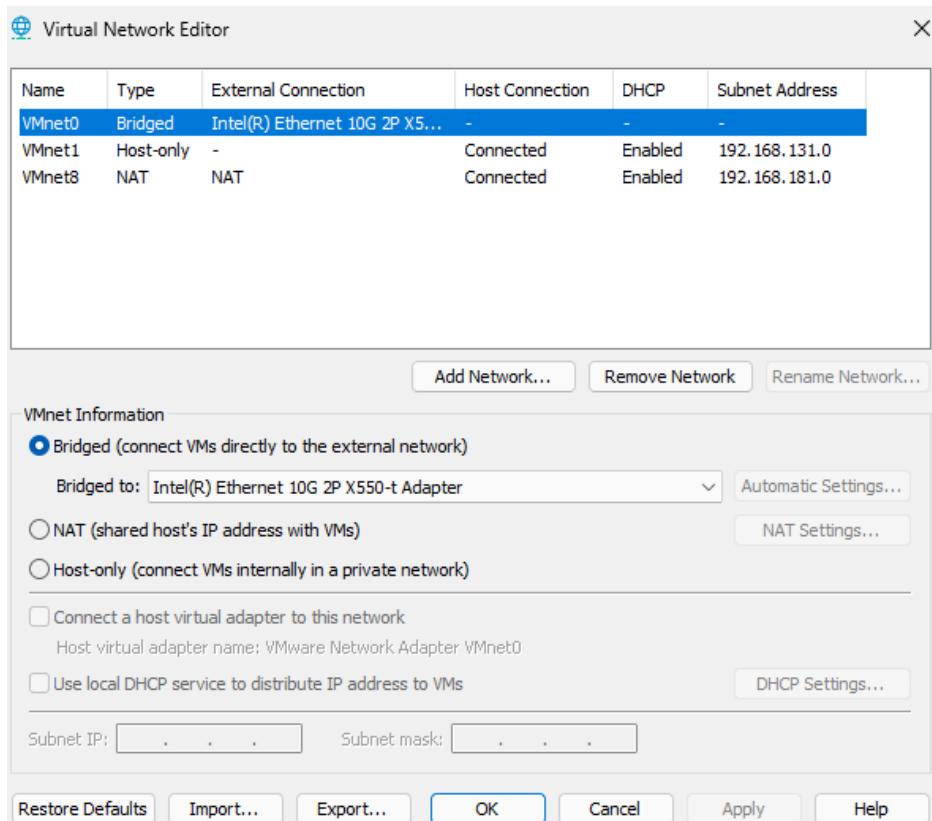
On the VMware Workstation itself, go to Virtual Network Editor. You will change the default NIC that the bridge connection will use.



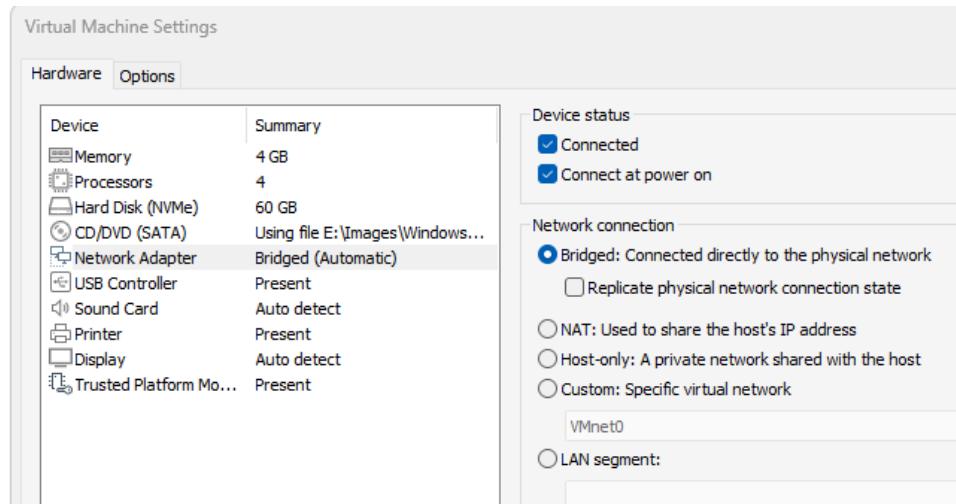
At the bottom right, click Change Settings, and accept the prompt for administrator access.



Change the Bridged Adapter from Automatic to the physical NIC on the Host



On the VMs that will connect to your physical network, in the VM Settings, change the Network Connection to Bridged allowing it to communicate directly with other devices on the network like a physical computer.



Verify connectivity with a Ping Test between VM and Host. Here, we are pinging the host (172.32.66.10) from the Splunk Server (172.32.66.200)

```

W11 - SServer x W11 - SForwarder x
Command Prompt x + v

C:\Users\admin>
C:\Users\admin>
C:\Users\admin>
C:\Users\admin>ping 172.31.66.10

Pinging 172.31.66.10 with 32 bytes of data:
Reply from 172.31.66.10: bytes=32 time=2ms TTL=128
Reply from 172.31.66.10: bytes=32 time<1ms TTL=128
Reply from 172.31.66.10: bytes=32 time<1ms TTL=128
Reply from 172.31.66.10: bytes=32 time<1ms TTL=128

Ping statistics for 172.31.66.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Users\admin>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::d6f4:b8dd:656e:1d01%14
    IPv4 Address . . . . . : 172.31.66.200
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.31.66.99

C:\Users\admin>

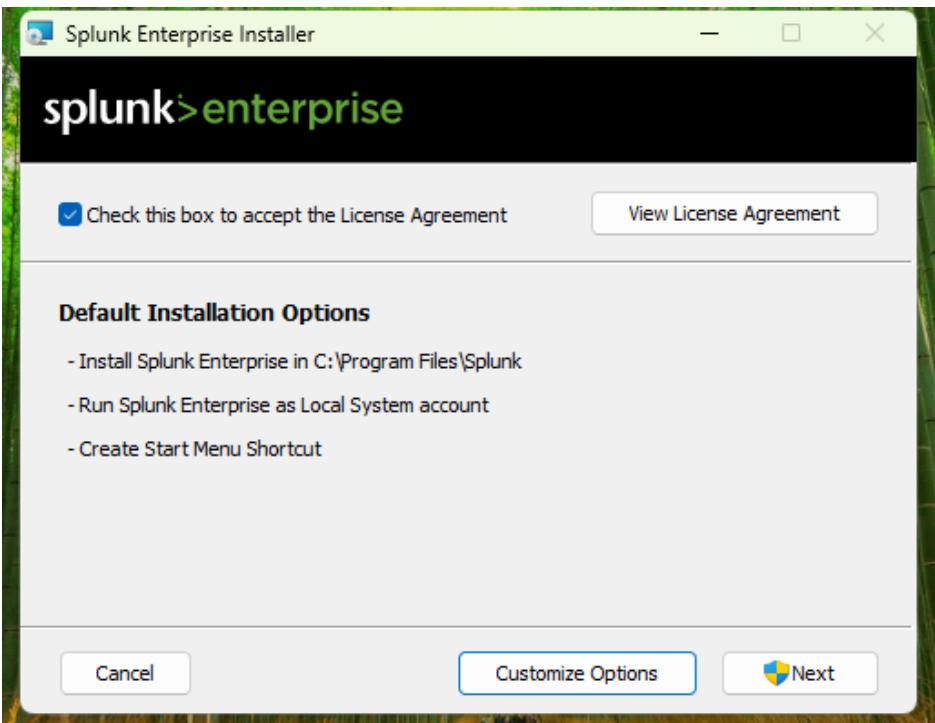
```

Splunk Server Setup:

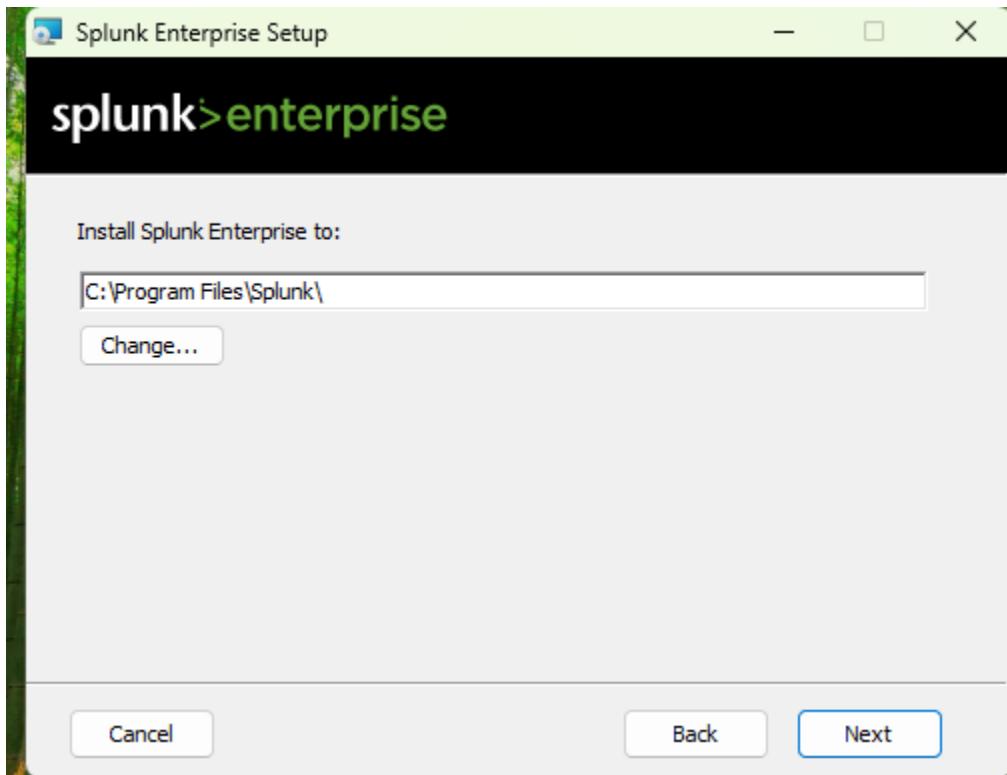
You download the official Splunk application and run it located wherever you downloaded it. In this case, we saved it to the desktop for easier access.



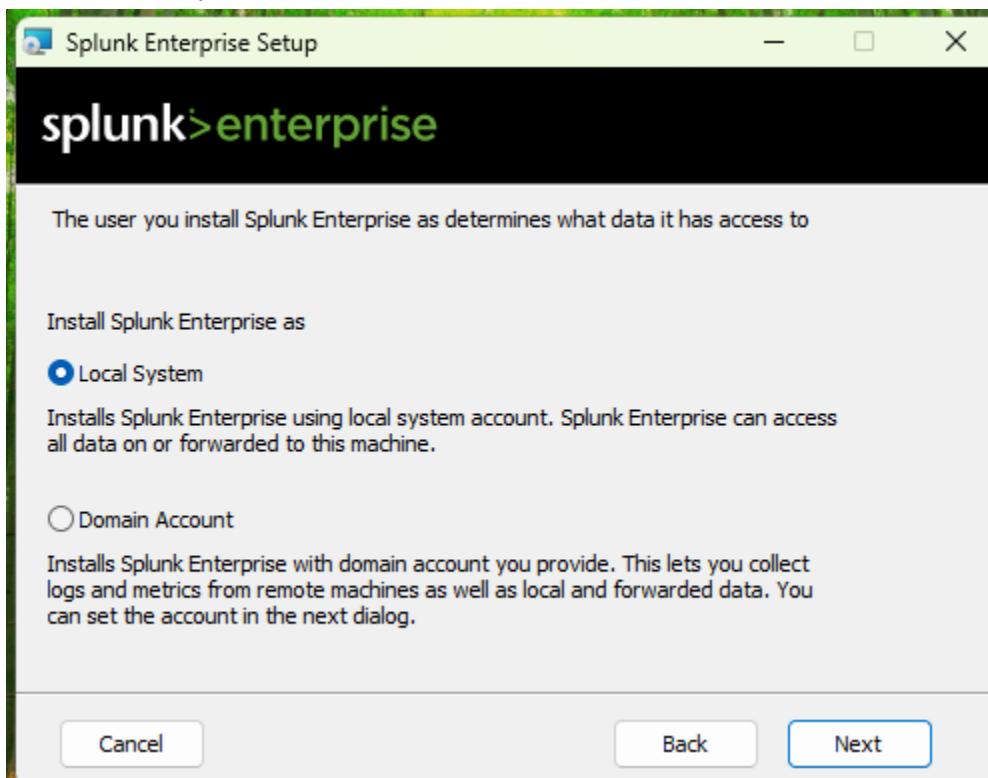
We check the box accepting the license agreement and click 'Next'



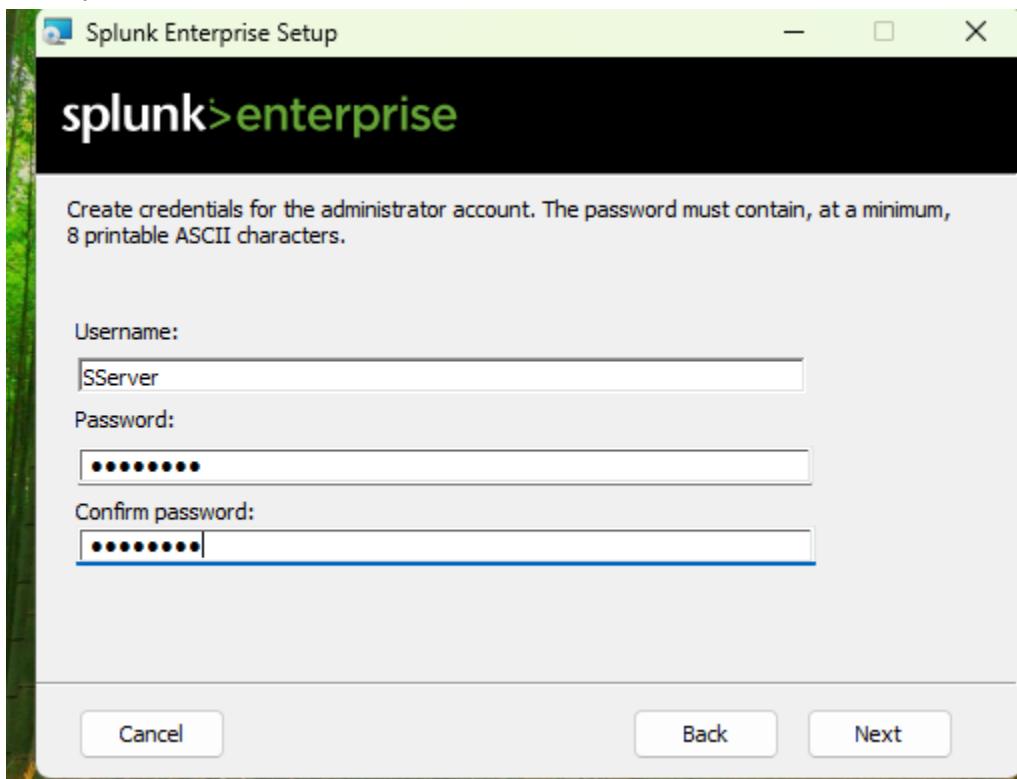
Click 'Next'



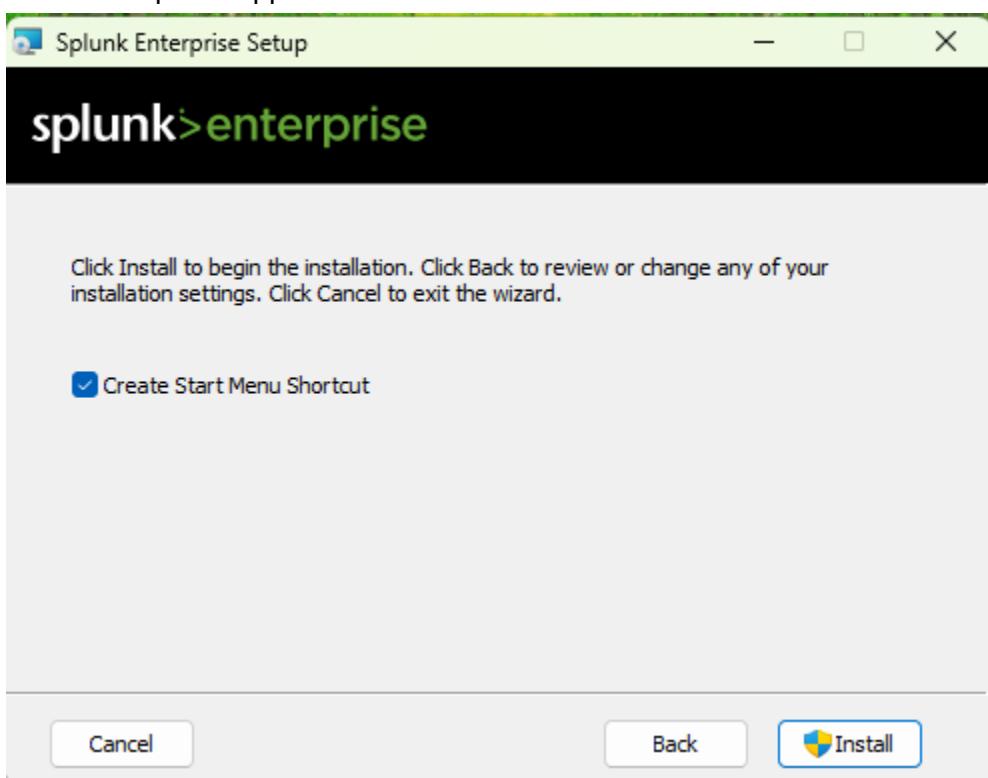
Check 'Local System' and click 'Next'



Make your administrator account.

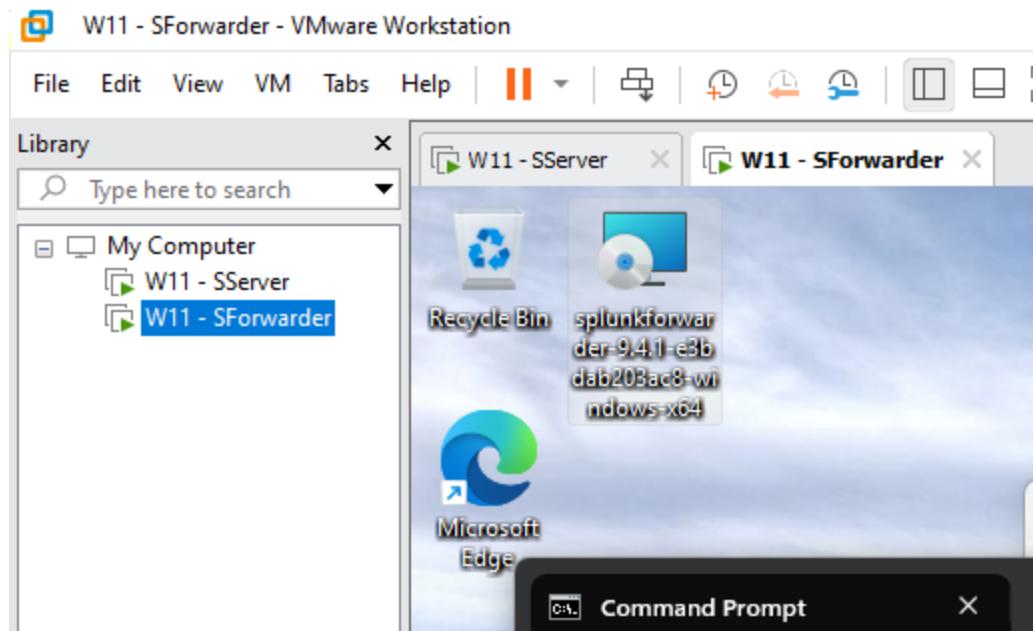


Install the Splunk Application.

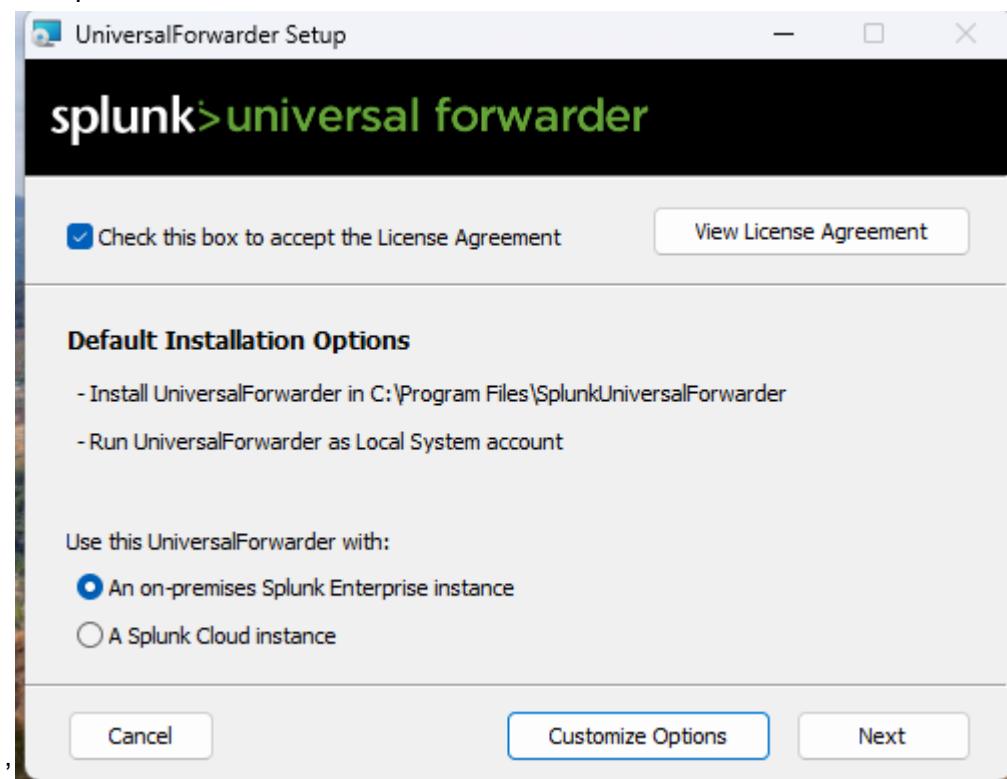


Splunk Forwarder Setup

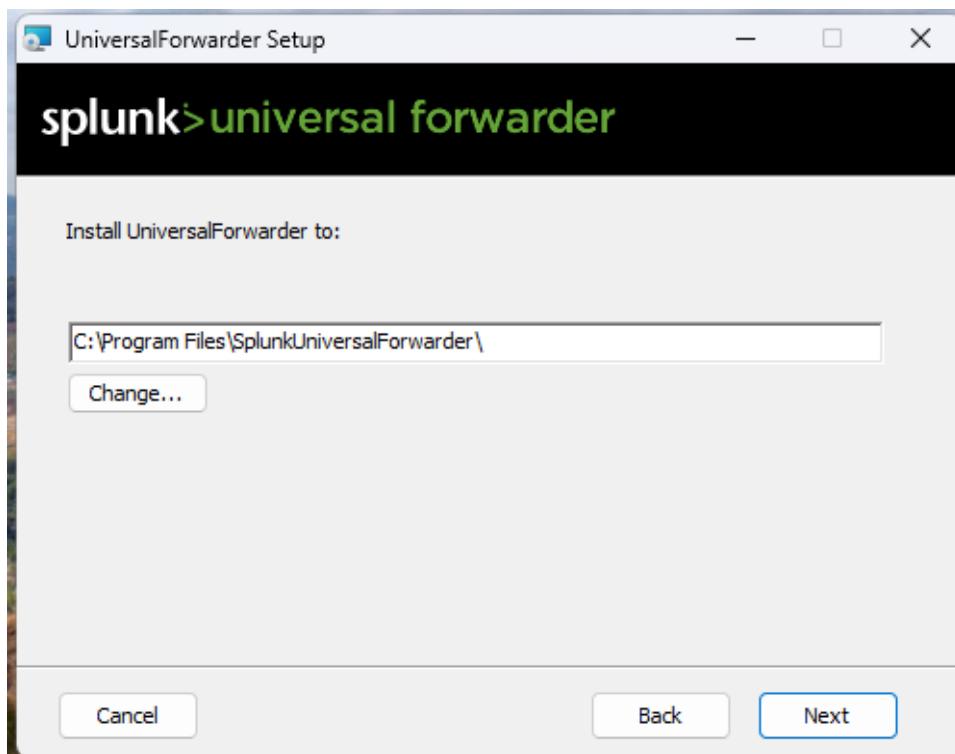
You download the official Splunk Universal Forwarder and run the application located wherever you downloaded it. In this case, we saved it to desktop for easier access.



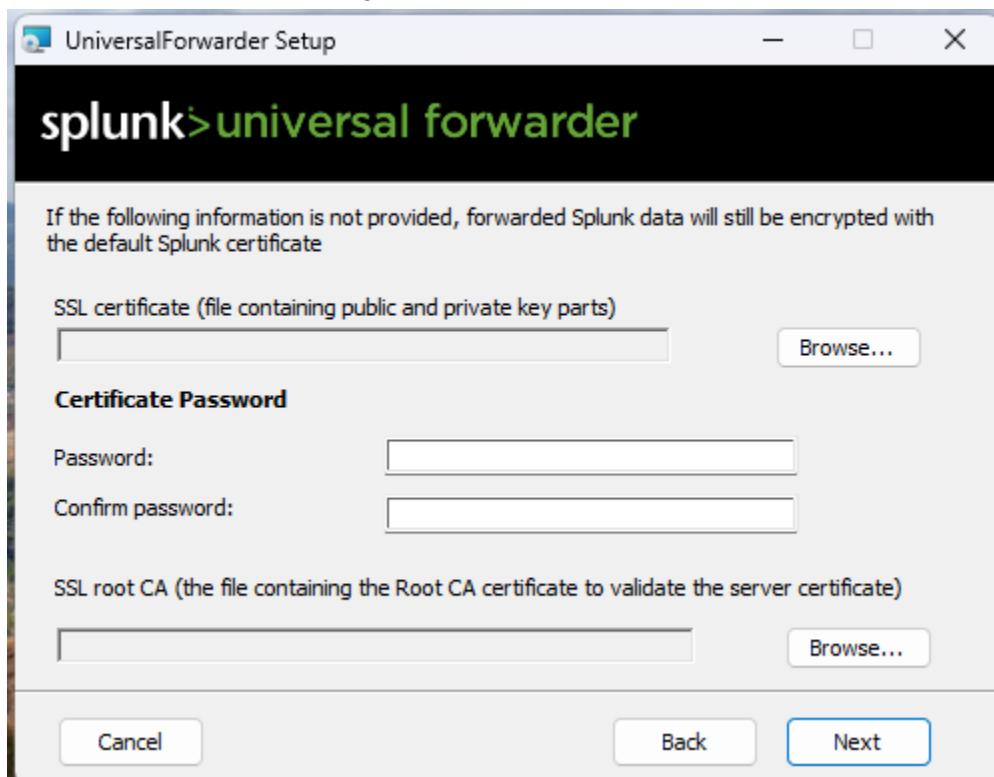
We check the box to accept the license agreement and select 'An on-premises Splunk Enterprise Instance'



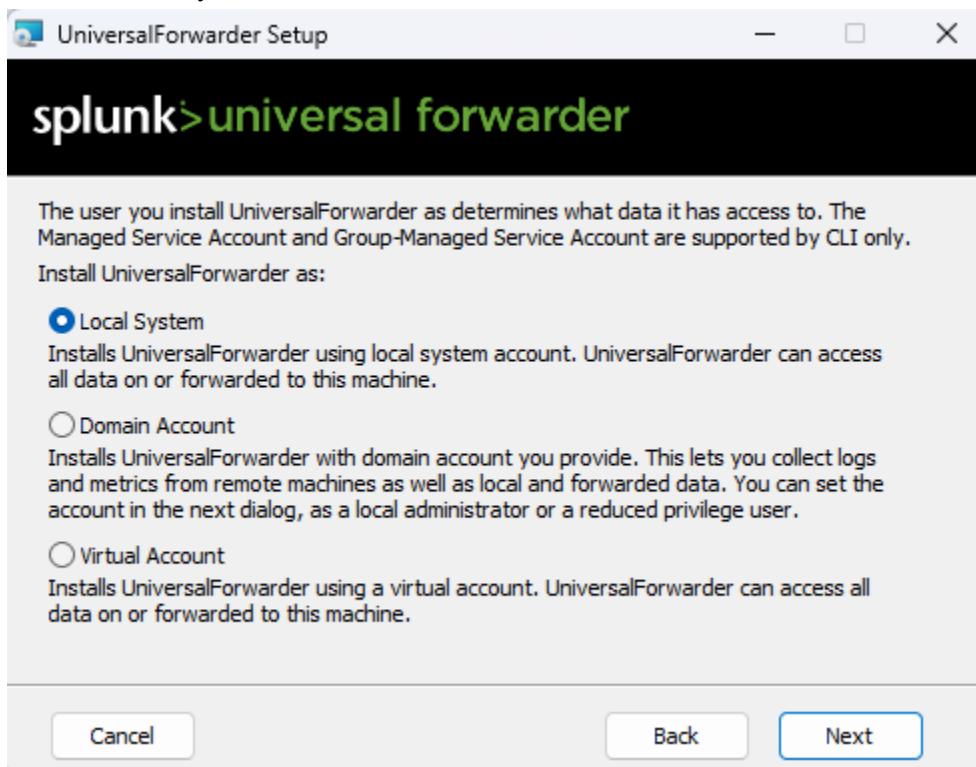
Click 'Next'



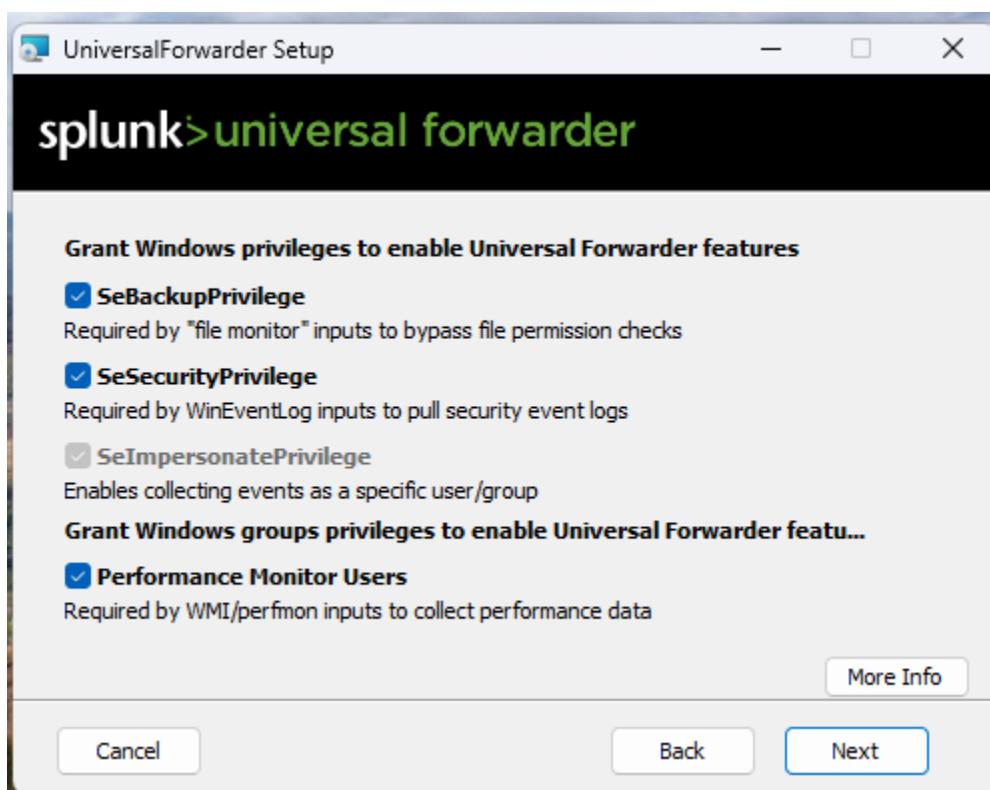
Select 'Next' on the SSL page.



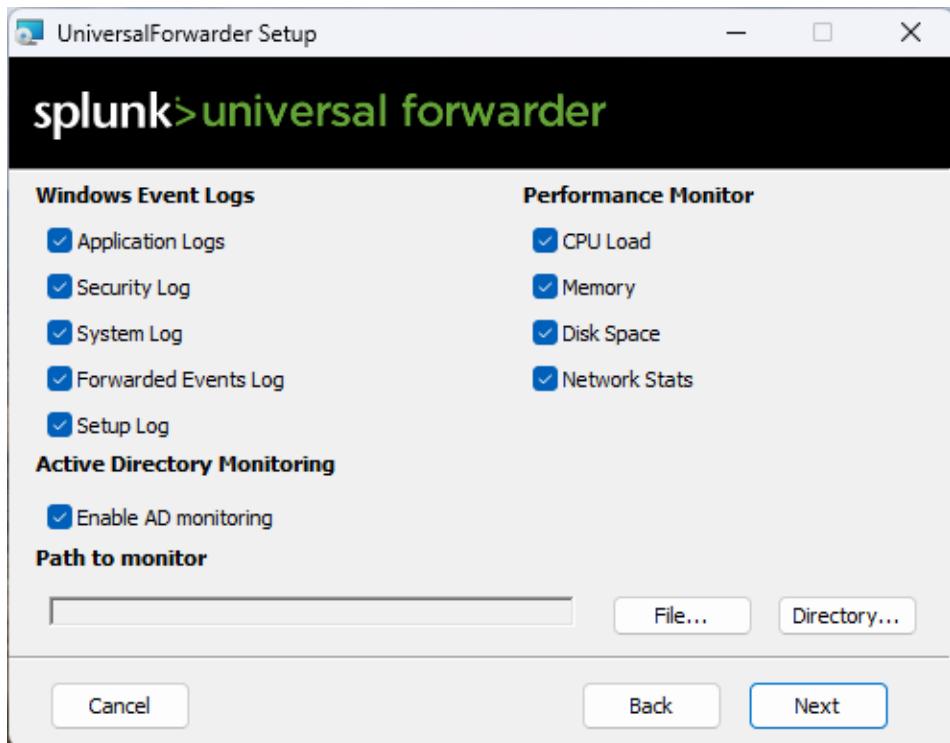
Select 'Local System'



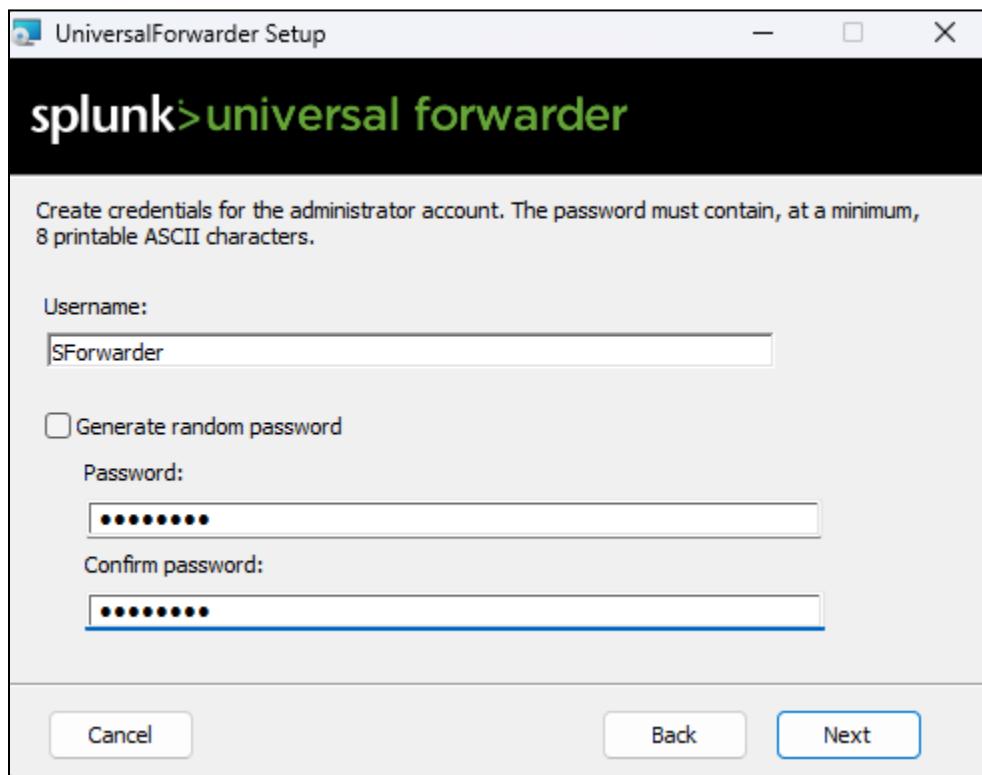
The default is fine. Click 'Next'



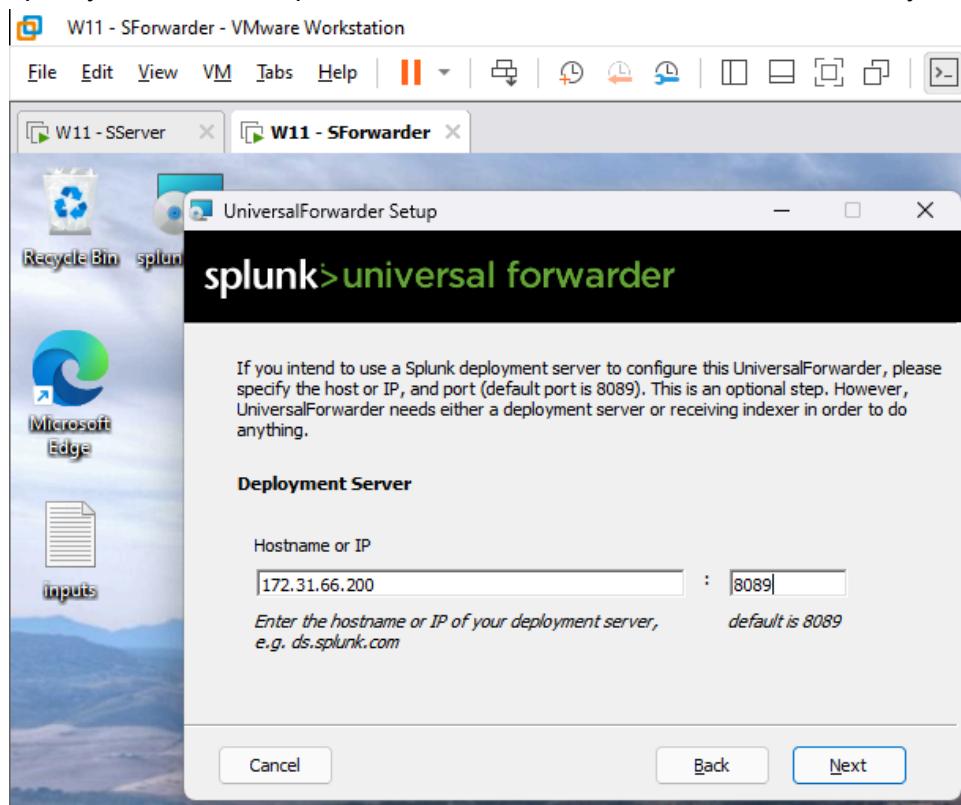
Check all the boxes to get all the logs to forward.



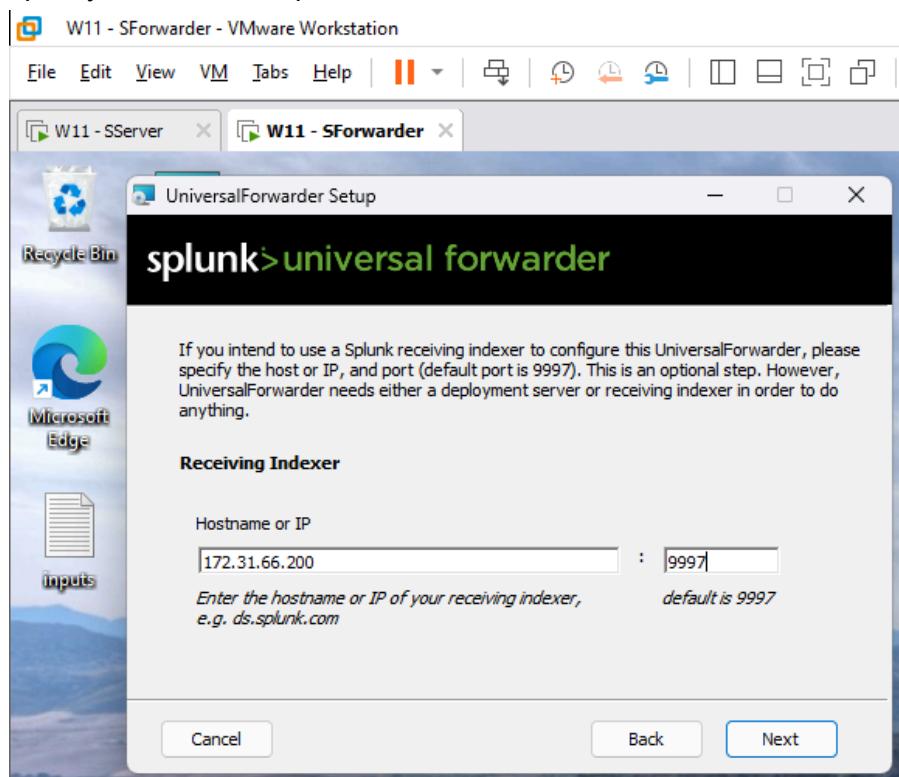
Make your administrator account.



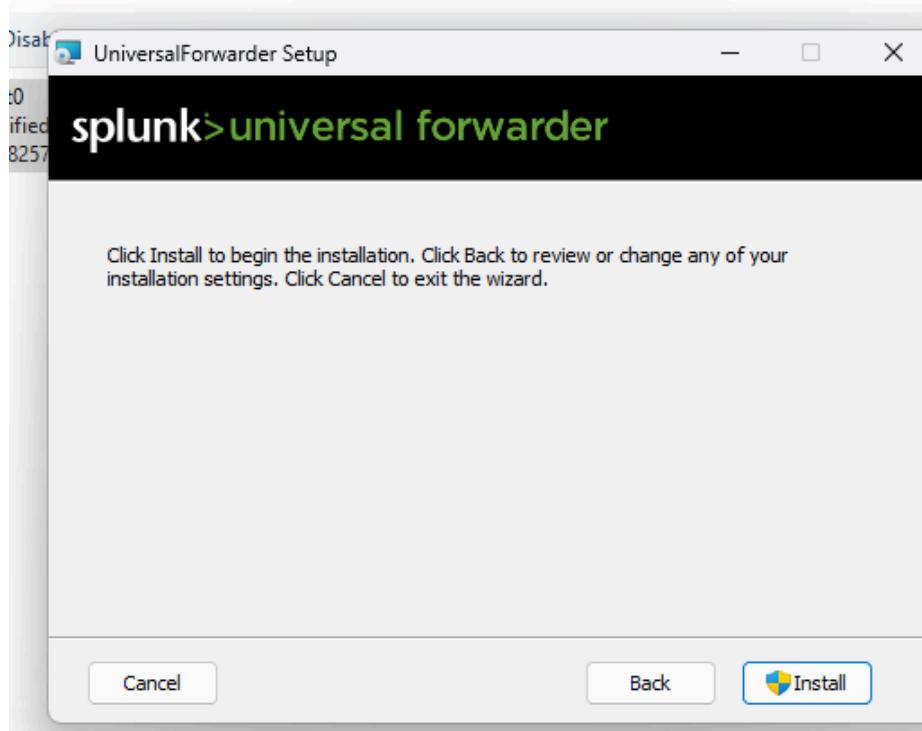
Specify the IP of the Splunk Server at 8089.172.31.98.200 for Burnaby.



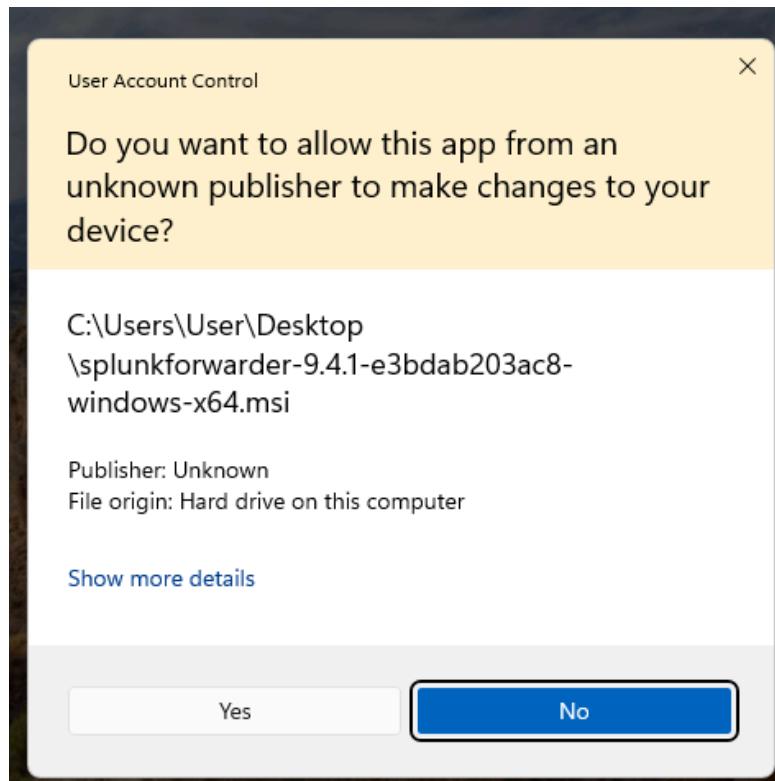
Specify the IP of the Splunk Server at 9997. 172.31.98.200 for Burnaby.



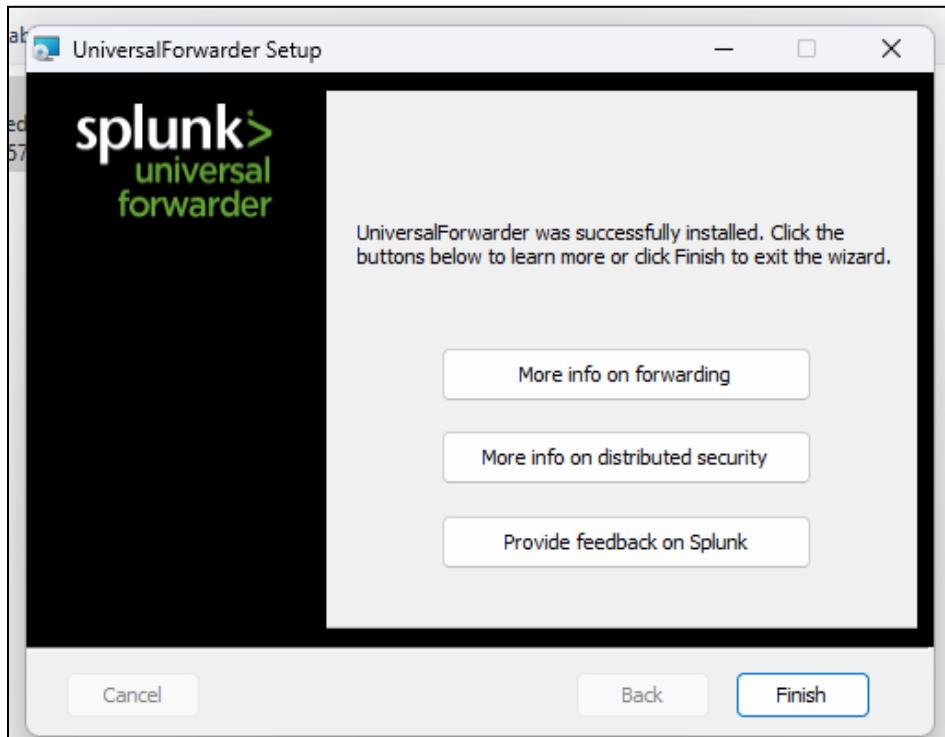
Click 'Install.'



Click 'Yes' on the prompt.



Click 'Finish'

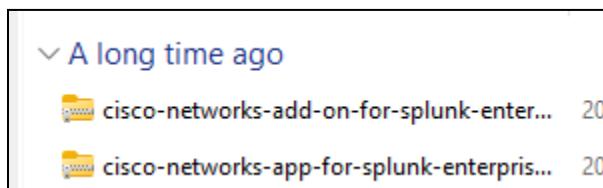


Splunk Server FG & Cisco, UDP & Index Setup on both Site VM

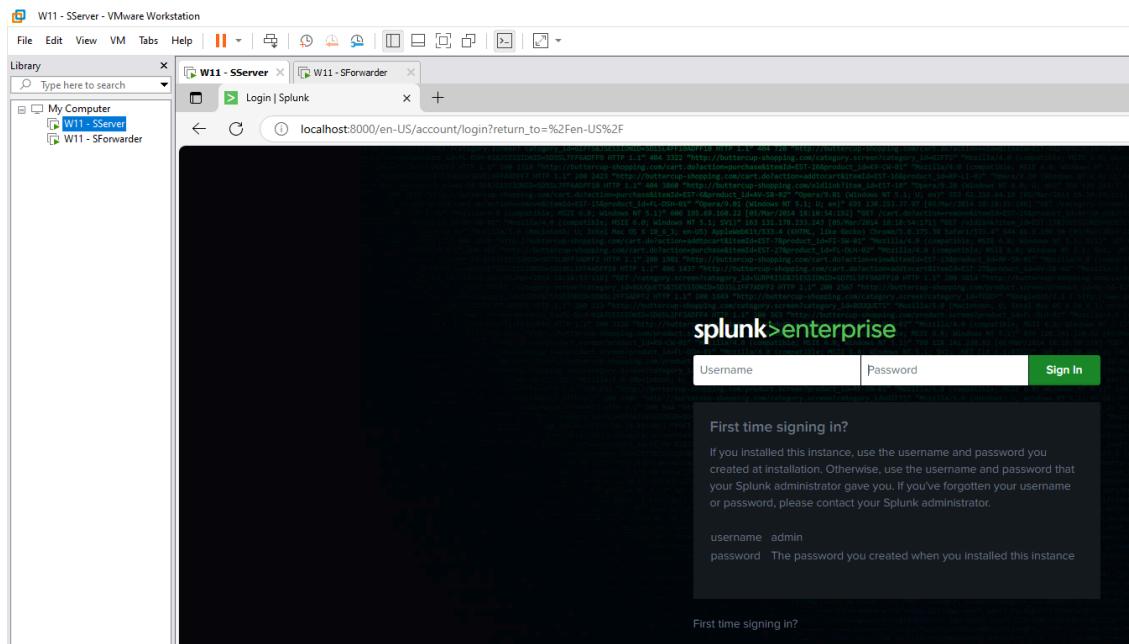
Download your own FortiGate Apps and Add-On and save it to your Server



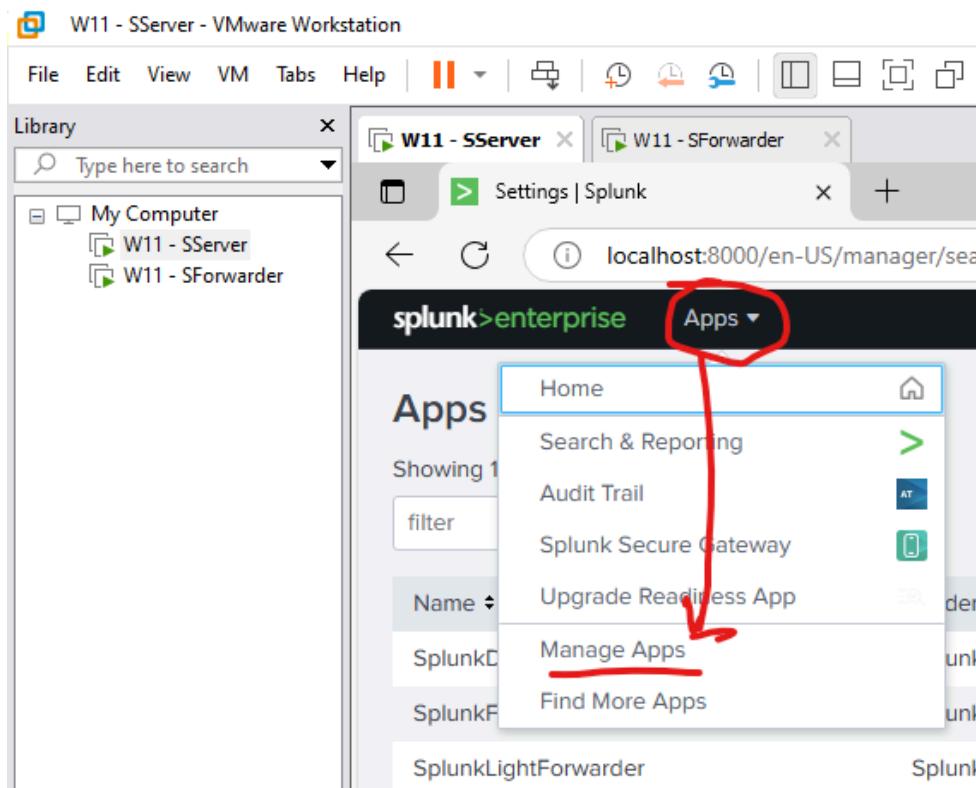
Download Cisco Network Apps and Add-On as well.



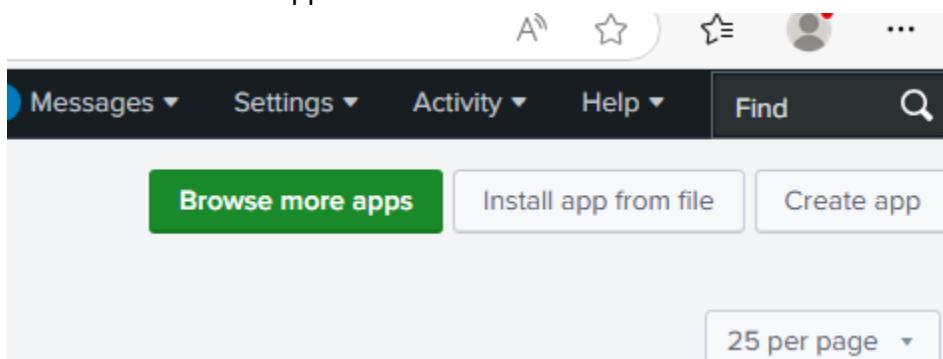
Go to either 'localhost:8000' or '127.0.0.1:8000' which will bring you to the Splunk Login page.
Sign in.



Go to 'Apps' and then 'Manage Apps'



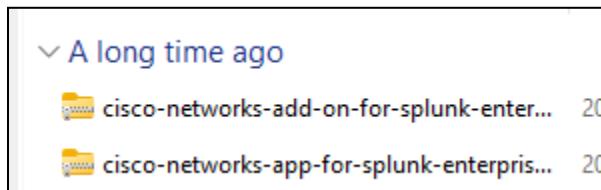
Then click on 'Install app from file'



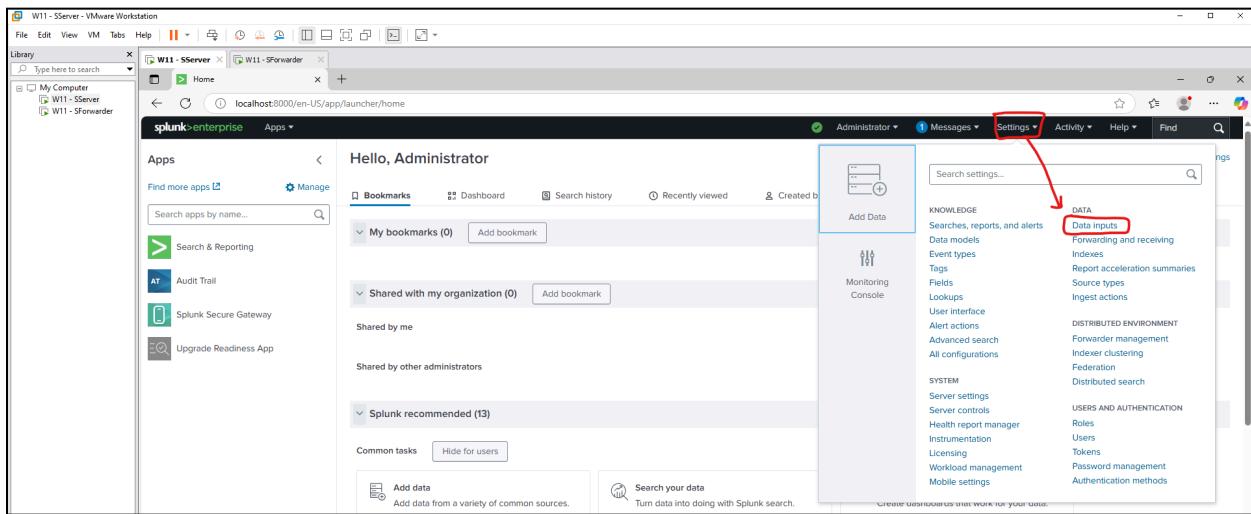
Click 'Choose File' and select the **FortiGate App ZIP** file then Upload. You will then do the same for the **Add-On ZIP** file after.

The image contains two screenshots. The top screenshot shows a 'File Explorer' window titled 'Open' with the path 'Downloads'. It lists two files: 'fortinet-fortigate-app-for-splunk_163' and 'fortinet-fortigate-add-on-for-splunk_167'. Both files are compressed archives (Type: Compressed Arch...). The bottom screenshot shows a 'Install App From File' form. It has a 'File' section with a 'Choose File' button containing the path 'fortinet-fortigat...-splunk_167.tgz'. There is also a checked checkbox for 'Upgrade app. Checking this will overwrite the app if it already exists.' At the bottom are 'Cancel' and 'Upload' buttons.

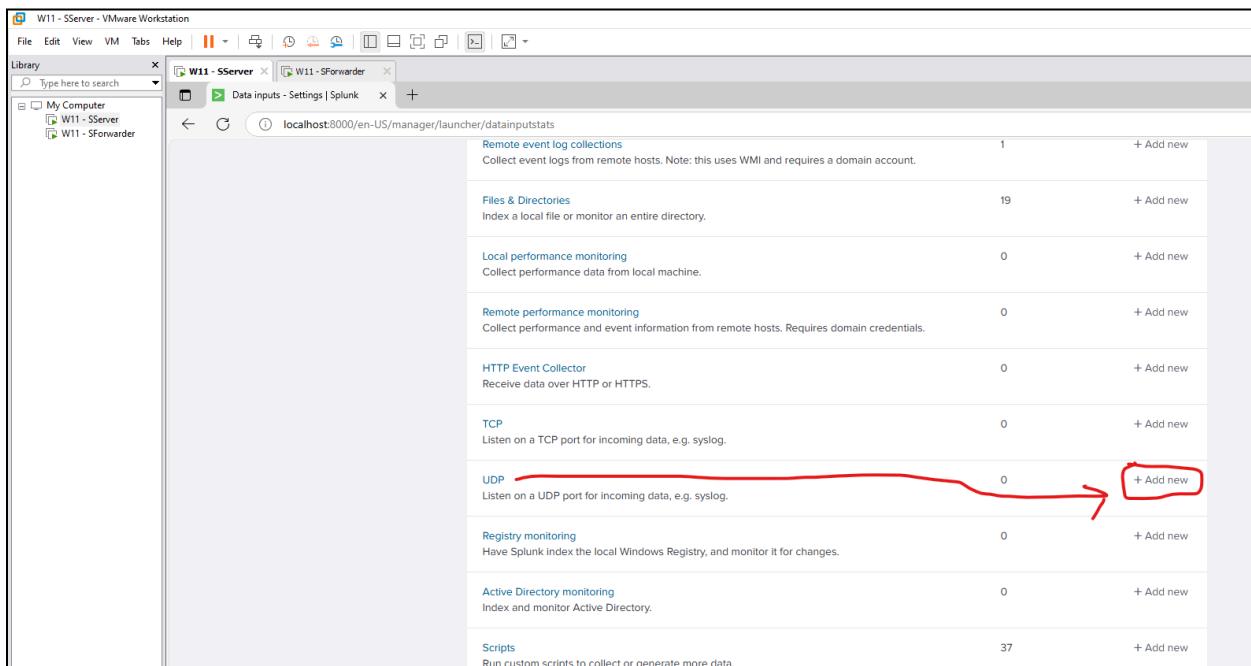
Do the same previous steps but this time for **Cisco Network Apps and Add-On**.



Go to 'Settings' then 'Data Inputs'



Then scroll down and click 'Add New' at the UDP section.



Then for ‘Port’, enter a custom Port number for your Apps, so, in our case, we do 514 for the FortiGate. Click ‘Next.’

Add Data

Select Source Input Settings Review Done < Back **Next >**

Local Event Logs Collect event logs from this machine.	Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). Learn More
Remote Event Logs Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.	<input type="checkbox"/> TCP <input type="checkbox"/> UDP
Files & Directories Upload a file, index a local file, or monitor an entire directory.	Port ? <input type="text" value="514"/> Example: 514
HTTP Event Collector Configure tokens that clients can use to send data over HTTP or HTTPS.	Source name override ? <input type="text" value="optional"/> hostport
TCP / UDP Configure the Splunk platform to listen on a network port.	Only accept connection from ? <input type="text" value="optional"/> example: 10.1.2.3, !badhost.splunk.com, *.splunk.com
Local Performance Monitoring Collect performance data from this machine.	F&Q

For Source Type, type “fgt_log”. For App Context, select the FortiGate App. Review and Submit.

Add Data

Select Source **Input Settings** Review Done < Back **Review >**

Input Settings

Optionally set additional input parameters for this data input as follows:

Source type
The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

App context
Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. [Learn More](#)

Host

Source type:

App Context:

We will do the same previous steps again but this time for **port 515**, **sourcetype: cisco:ios**, and **App Context: Cisco Networks**. Complete the steps.

Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). [Learn More](#)

TCP UDP

Port ? 515
Example: 514

Source name override ? optional
host:port

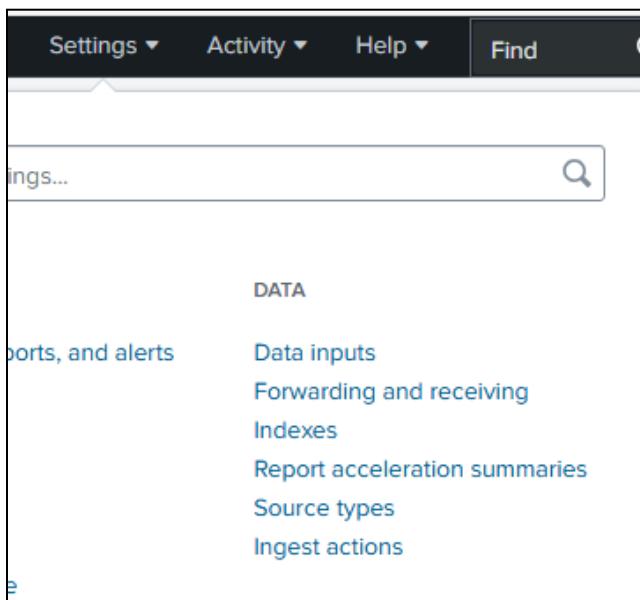
Only accept connection from ? optional

Select New

cisco:ios ▾

App Context Cisco Networks (cisco_ios) ▾

After, go to 'Settings' then 'Forwarding and Receiving.'



Under ‘Receive Data’, for ‘Configure Receiving’, click ‘+Add New.’

The screenshot shows two sections of the configuration interface. The top section, 'Forward data', has a table with rows for 'Forwarding defaults' and 'Configure forwarding'. A '+ Add new' button is located at the bottom right of this section. The bottom section, 'Receive data', also has a table with rows for 'Type' and 'Configure receiving'. A '+ Add new' button is located at the bottom right of this section. A red circle highlights the '+ Add new' button in the 'Receive data' section.

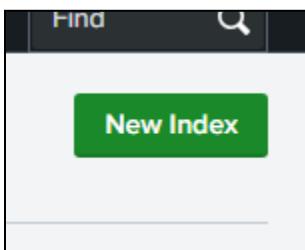
Type in ‘9997’ as we set it up earlier in the initial Splunk Forwarder setup.

The screenshot shows the 'Configure receiving' dialog box. It contains a field labeled 'Listen on this port *' with the value '9997' highlighted by a blue border. Below the field is a note: 'For example, 9997 will receive data on TCP port 9997.' At the bottom right are 'Cancel' and 'Save' buttons.

Then go to ‘Settings’, ‘Indexes’

The screenshot shows the Splunk Settings menu. The left sidebar lists 'KNOWLEDGE' and 'DATA' categories. Under 'KNOWLEDGE', options include 'Searches, reports, and alerts', 'Data models', 'Event types', 'Tags', 'Fields', 'Lookups', and 'User interface'. Under 'DATA', options include 'Data inputs', 'Forwarding and receiving', 'Indexes', 'Report acceleration summaries', 'Source types', and 'Ingest actions'. The 'Indexes' option is highlighted.

Click 'New Index'



Configure the 'Index Name' and 'App' like so accordingly. We use the index name '**splunk-FortiGate-site2**' and '**splunk-cisco-site2**' for our Index name and App Fortinet and Cisco Networks respectively. **Change the 'site2' to 'site3' for Burnaby.**

New Index

Index Name Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type Events Metrics

The type of data to store (event-based or metrics).

Home Path optional

Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).

Cold Path optional

Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path optional

Thawed/resurrected db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check Enable Disable

Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index 500 GB ▾

Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket auto GB ▾

Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path optional

Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App Fortinet FortiGate App for Splunk ▾

Save **Cancel**

New Index

Index Name splunk-cisco-site2
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type Events Metrics
The type of data to store (event-based or metrics).

Home Path
Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).

Cold Path
Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path
Thawed/resurrected db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check Enable Disable
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index GB ▾
Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket GB ▾
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path
Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App Cisco Networks ▾

You should see this in **Indexes** and **UDP** if done correctly. Site3 for Burnaby.

splunk-cisco-site2	Edit	Delete	Disable	<input type="radio"/> Events	cisco_ios
splunk-fortigate-site2	Edit	Delete	Disable	<input type="radio"/> Events	SplunkAppForFortinet

UDP

[Data inputs](#) » UDP

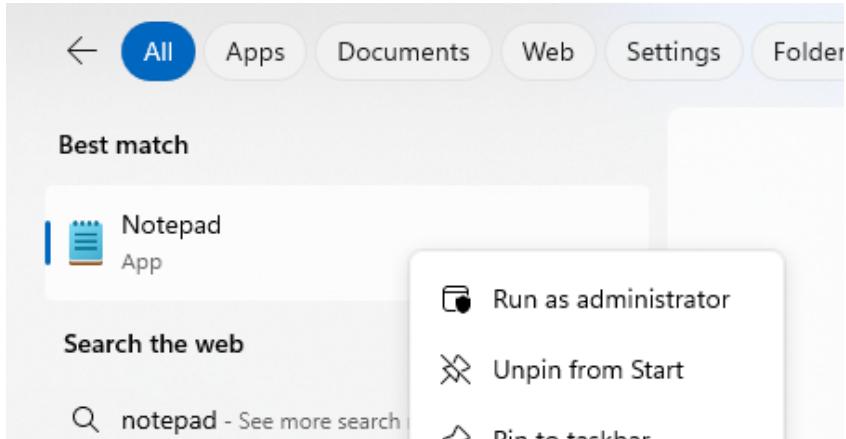
Showing 1-2 of 2 items

filter

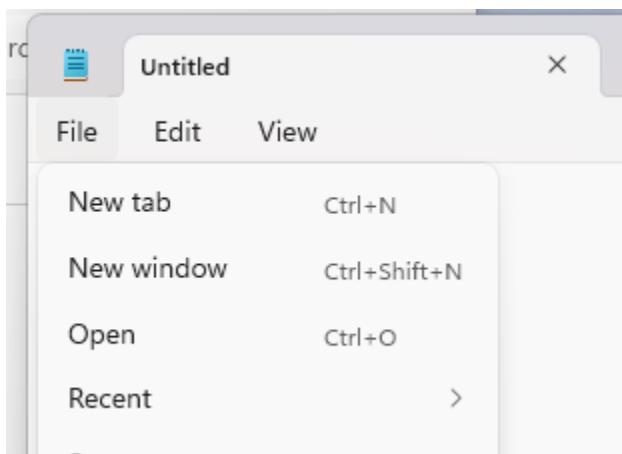
UDP port ▾	Source type ▾
514	fgt_log
515	cisco:ios

Splunk Forwarder Conf File Configuration

Open Notepad in Administrator Mode

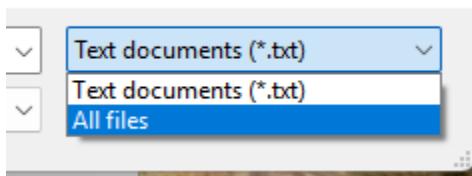


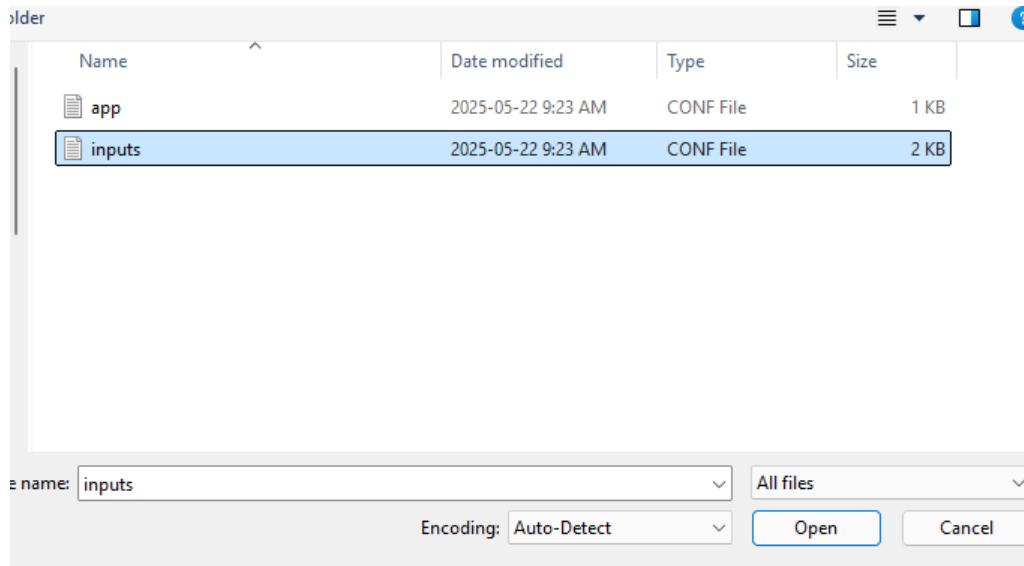
Go to 'Files' then 'Open'



Go to **C:\Program**

Files\SplunkUniversalForwarder\etc\apps\SplunkUniversalForwarder\local. Change the
.txt to 'All Files' then select the 'inputs.conf' file.





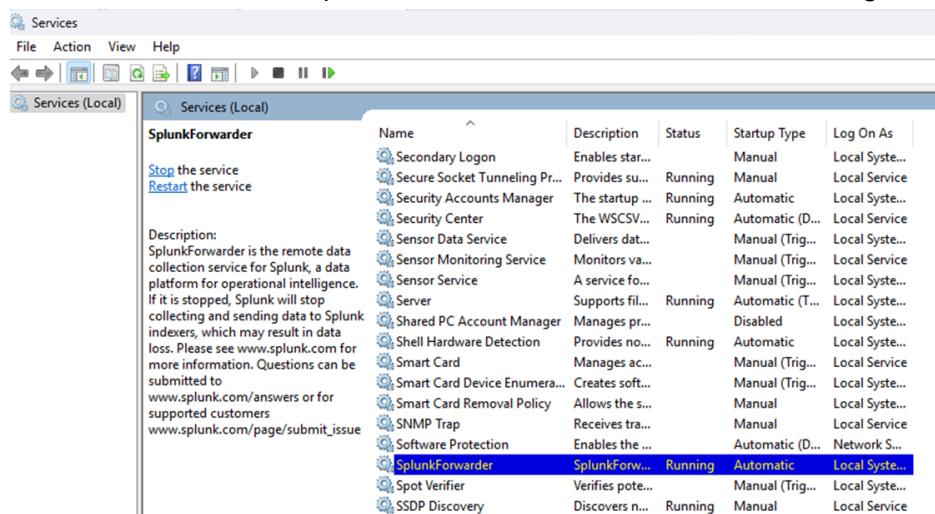
Add the following at the top with proper spacing and save. This will allow the forwarder to listen and send logs at the specified ports to the proper index on Splunk Server with appropriate sourcetypes for each log source.

A screenshot of a text editor window titled 'Untitled' with the file name 'inputs.conf' in the tab bar. The menu bar includes 'File', 'Edit', and 'View'. The code in the editor is as follows:

```
[udp://514]
disabled = false
connection_host = ip
sourcetype = fgt_log
index = splunk-fortigate-site2

[udp://515]
disabled = false
connection_host = ip
sourcetype = cisco:ios
index = splunk-cisco-site2
```

We need to restart the SplunkForwarder service because we configured the inputs.conf file.



FortiGate Logging Setting Setup

Go to 'Log & Report' then 'Log Settings'. Enable the 'Send logs to syslog' and enter the IP address of the Splunk Forwarder which will then forward the logs to the Splunk Server. We also change 'Local Traffic Log' to 'All' so that all traffic logs are logged.

The screenshot shows the FortiGate 60E Log Settings configuration page. On the left, there is a navigation sidebar with various settings like Dashboard, Security Fabric, Network, System, Policy & Objects, Security Profiles, VPN, User & Authentication, WiFi & Switch Controller, and Log & Report. Under Log & Report, Log Settings is selected. The main pane shows the 'Log Settings' section with 'Local Log' and 'Memory' options. Below that is the 'Remote Logging and Archiving' section, where 'Send logs to FortiAnalyzer/FortiManager' is set to 'Enabled' and 'Send logs to syslog' is set to 'Enabled' with the IP address '172.31.66.201' entered. There are also sections for 'Cloud Logging Settings', 'UUIDs in Traffic Log', 'Address', 'Event Logging' (set to 'All'), 'Local Traffic Log' (set to 'All'), and 'GUI Preferences'.

Verification of Fortigate Logs Received

Now, we go search for some FortiGate Logs like shown using queries like **index="splunk-fortigate-site2"** and keywords with '**snmp**', replacing site2 for site3 on Burnaby

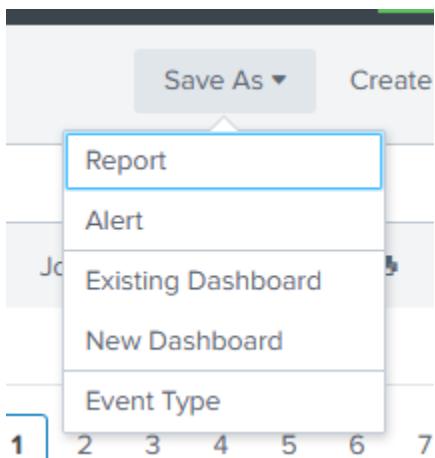
The screenshot shows the Splunk 9.4.1 interface with a search bar containing 'index="splunk-fortigate-site2"'. The results section displays 519 events from May 22, 2025, between 12:43:37 and 12:43:52. The events are listed in a table with columns for Time, Event, and several other fields. The interface includes a timeline at the top, search and reporting buttons, and a status bar at the bottom indicating 1:01 PM, ENG US, and 2025-05-22.

Time	Event
May 22 12:43:37 172.31.66.99	devname="FG-SITE2" devid="FGT60ETK21018735" eventtime="1747943016570048594 tz="-0700" logid="0001000014" type="traffic" subtype="local" level="no notice" vd="root" srcip=f680::2c1:64ff:fed4:e484 srcport=0 srlntrole="wan" dstip=ff02::1:dsport=0 dstlnf="root" dstlnfrole="undefined" sessionid=35319 proto=88 action="deny" policyid=0 politype="local-in-policy" service="other" transdp="noop" app="other" duration=0 sentby=0 rcvby=0 sentpk=0 rcvpkt=0 appcat="unscanned" host="172.31.66.99" source=udp:514 sourcetype=fortigate_traffic
May 22 12:43:38 172.31.66.99	devname="FG-SITE2" devid="FGT60ETK21018735" eventtime="174794301522398821 tz="-0700" logid="0001000014" type="traffic" subtype="local" level="no notice" vd="root" ssrcip=127.0.0.1 srport=24716 srlntrole="unknown" ssrcnrlrole="undefined" dstip=127.0.0.1 dsport=88 dstlnf="unknown" dstlnfrole="undefined" sccountry="Reserved" sessionid=160437 proto=6 action="client-rst" policyid=6 service="HTTP" transdp="noop" app="HTTP" duration=0 sentby=355 rcvby=258 sentpk=5 rcvpkt=5 appcat="unscanned" host="172.31.66.99" source=udp:514 sourcetype=fortigate_traffic
May 22 12:43:38 172.31.66.99	devname="FG-SITE2" devid="FGT60ETK21018735" eventtime="1747943014252405598 tz="-0700" logid="0001000014" type="traffic" subtype="local" level="no notice" vd="root" ssrcip=127.0.0.1 srport=24715 srlntrole="unknown" ssrcnrlrole="undefined" dstip=127.0.0.1 dsport=88 dstlnf="unknown" dstlnfrole="undefined" sccountry="Reserved" sessionid=160437 proto=6 action="client-rst" policyid=6 service="HTTP" transdp="noop" app="HTTP" duration=0 sentby=355 rcvby=258 sentpk=5 rcvpkt=5 appcat="unscanned" host="172.31.66.99" source=udp:514 sourcetype=fortigate_traffic
May 22 12:43:38 172.31.66.99	devname="FG-SITE2" devid="FGT60ETK21018735" eventtime="1747943011742913916 tz="-0700" logid="0001000014" type="traffic" subtype="local" level="no notice" vd="root" ssrcip=127.0.0.1 srport=24715 srlntrole="wan" ssrcnrlrole="undefined" dstip=127.0.0.1 dsport=88 dstlnf="root" dstlnfrole="undefined" sessionid=35318 proto=88 action="deny" policyid=0 politype="local-in-policy" service="other" transdp="noop" app="other" duration=0 sentby=0 rcvby=0 sentpk=0 rcvpkt=0 appcat="unscanned" host="172.31.66.99" source=udp:514 sourcetype=fortigate_traffic
May 22 12:43:32 172.31.66.99	devname="FG-SITE2" devid="FGT60ETK21018735" eventtime="1747943011742913916 tz="-0700" logid="0001000014" type="traffic" subtype="local" level="no notice" vd="root" ssrcip=127.0.0.1 srport=24715 srlntrole="wan" ssrcnrlrole="undefined" dstip=127.0.0.1 dsport=88 dstlnf="root" dstlnfrole="undefined" sessionid=35318 proto=88 action="deny" policyid=0 politype="local-in-policy" service="other" transdp="noop" app="other" duration=0 sentby=0 rcvby=0 sentpk=0 rcvpkt=0 appcat="unscanned" host="172.31.66.99" source=udp:514 sourcetype=fortigate_traffic

The screenshot shows the Splunk 9.4.1 interface with a search bar containing 'index="splunk-fortigate-site2" snmp'. The results section displays 5 events from May 22, 2025, between 12:42:40 and 12:42:46. The events are listed in a table with columns for Time, Event, and several other fields. The interface includes a timeline at the top, search and reporting buttons, and a status bar at the bottom indicating 1:01 PM, ENG US, and 2025-05-22.

Time	Event
May 22 12:42:52 172.31.66.99	devname="FG-SITE2" devid="FGT60ETK21018735" eventtime="1747942971272561216 tz="-0700" logid="0100044547" type="event" subtype="system" level="info" orname="vd="root" logdesc="Object attribute configured" user="user" ui="GUI(172.31.66.10)" action="Edit" cfgid=6685048 cfpnath="system.snmp.community" cfgobj="1" cfgattr="trap-v1-report[513->514]" msg="#Edit system.snmp.community 1" host="172.31.66.99" source=udp:514 sourcetype=fortigate_event
May 22 12:42:46 172.31.66.99	devname="FG-SITE2" devid="FGT60ETK21018735" eventtime="174794295162686885 tz="-0700" logid="0100044547" type="event" subtype="system" level="info" orname="vd="root" logdesc="Object attribute configured" user="user" ui="GUI(172.31.66.10)" action="Edit" cfgid=6685048 cfpnath="system.snmp.community" cfgobj="1" cfgattr="trap-v1-report[514->513]events [cpu-high mem-low log-full int-ip vnp-tun-up ha-switch ha-hb-failure los-signature los-anomaly av-virus av-overrise av-pattern av-fragmented fe-if-change hpn-established hpn-backward-transition ha-member-up ha-member-down ent-conf-change av-conserve av-bypass av-overrise-passed av-overrise-blocked ips-pkg-update lns-fall-open faz-disconnect wc-ap-up wc-ap-down fswcl-session-up fwcl-session ion-down load-balance-real-server-down per-cpu-high dhcp pool-useage >cpu-high mem-low log-full int-ip vnp-tun-up ha-switch ha-hb-failure los-signature los-anomaly av-virus av-overrise av-pattern av-fragmented fm-if-change hpn-established hpn-backward-transition ha-member-up ha-member-down ent-conf-change av-conserve av-bypass av-overrise-passed av-overrise-blocked ips-pkg-up dat ips-fall-open faz-disconnect wc-ap-up wc-ap-down fswcl-session-down load-balance-real-server-down device-new per-cpu-high dhcp pool-useage]" msg="#Edit system.snmp.community 1" host="172.31.66.99" source=udp:514 sourcetype=fortigate_event
May 22 12:42:27 172.31.66.99	devname="FG-SITE2" devid="FGT60ETK21018735" eventtime="1747942946652518948 tz="-0700" logid="0100044547" type="event" subtype="system" level="info" orname="vd="root" logdesc="Object attribute configured" user="user" ui="GUI(172.31.66.10)" action="Edit" cfgid=6685046 cfpnath="system.snmp.user" cfgobj="user" cfgattr="trap-report[513->514]" msg="#Edit system.snmp.user" host="172.31.66.99" source=udp:514 sourcetype=fortigate_event

We can see that we are correctly receiving logs. Add this to a dashboard by going ‘Save As’, then ‘New Dashboard’.



Give a Dashboard Title, and select Classic Dashboards, then Save to Dashboard.

The screenshot shows the 'Save Panel to New Dashboard' dialog box. It contains the following fields:

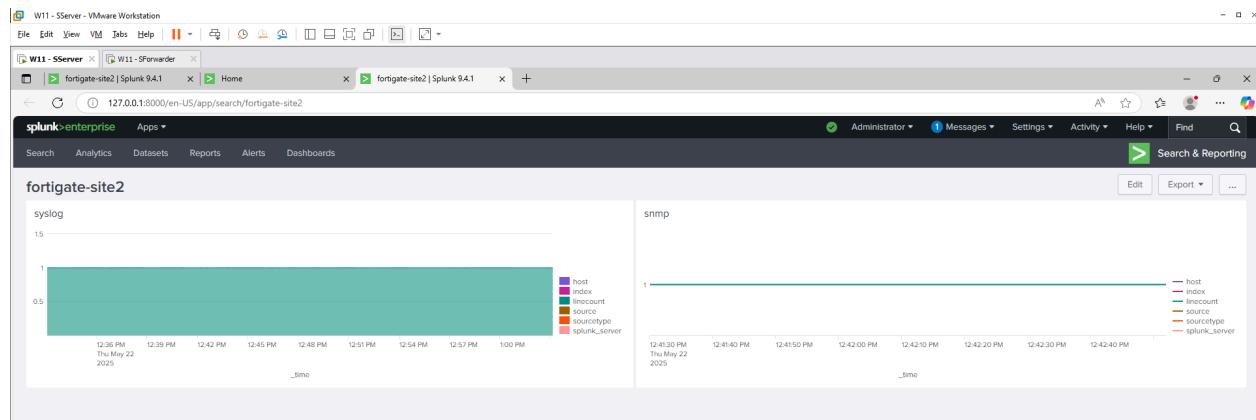
- Dashboard Title: fortigate
- Description: Optional
- Permissions: Private

Below these fields, there are two options for building the dashboard:

- Classic Dashboards**: The traditional Splunk dashboard builder.
- Dashboard Studio** (NEW): A new builder to create visually-rich, customizable dashboards.

At the bottom of the dialog box, there are buttons for 'Cancel' and 'Save to Dashboard'.

Repeat like so with the corresponding searches. Then you can view your dashboard with your custom queries in one place for easy viewing.



Cisco Logging Configuration

Configure a Virtual IP DNAT as followed. Give it a name, External IP is the Fortigate's WAN-facing interface IP, Mapped IP address is the Splunk Server IP, enable Port Forwarding for protocol UDP at External Service Port 514 to Mapped Port 515. Change the IP as accordingly.

VIP type	IPv4
Name	<input type="text" value="DNAT-WAN-TO-LAN"/>
Comments	<input type="text" value="Write a comment..."/> 0/255
Color	<input type="button" value="Change"/>
Network	
Interface	<input type="button" value="To Router WAN (wan1)"/>
Type	Static NAT
External IP address/range	<input type="text" value="172.31.64.220"/>
Mapped IP address/range	<input type="text" value="172.31.66.201"/>
Optional Filters	
Port Forwarding	
Protocol	<input type="radio" value="TCP"/> TCP <input checked="" type="radio" value="UDP"/> UDP <input type="radio" value="SCTP"/> SCTP <input type="radio" value="ICMP"/> ICMP
External service port	<input type="text" value="514"/>
Map to port	<input type="text" value="515"/>

Configure a Firewall Policy for the Cisco to Server with NAT enabled. The Destination is the Nat we created above. Follow it like so. You will do the same on the **other Site**.

The screenshot shows the FortiGate 60E web interface with the title "Edit Policy". The left sidebar navigation includes "Dashboard", "Security Fabric", "Network", "System", "Policy & Objects" (selected), "Firewall Policy" (highlighted green), "Addresses", "Internet Service Database", "Services", "Schedules", "Virtual IPs", "IP Pools", "Protocol Options", "Traffic Shapers", "Traffic Shaping Policy", "Traffic Shaping Profile", "Security Profiles", "VPN", "User & Authentication", "WIFI & Switch Controller", and "Log & Report".

The main configuration area is titled "Edit Policy" and contains the following fields:

- Name:** Syslog
- Incoming Interface:** To Router WAN (wan1)
- Outgoing Interface:** Internal LAN (internal)
- Source:** all
- Destination:** DNAT-WAN-TO-LAN
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT DENY

Below these fields are tabs for "Inspection Mode" (Flow-based selected) and "Proxy-based".

The "Firewall / Network Options" section includes:

- NAT:** IP Pool Configuration (selected), Use Outgoing Interface Address, Use Dynamic IP Pool
- Preserve Source Port:** Off
- Protocol Options:** PROT default

The "Security Profiles" section includes:

- AntiVirus: Off
- Web Filter: Off
- DNS Filter: Off
- Application Control: Off
- File Filter: Off

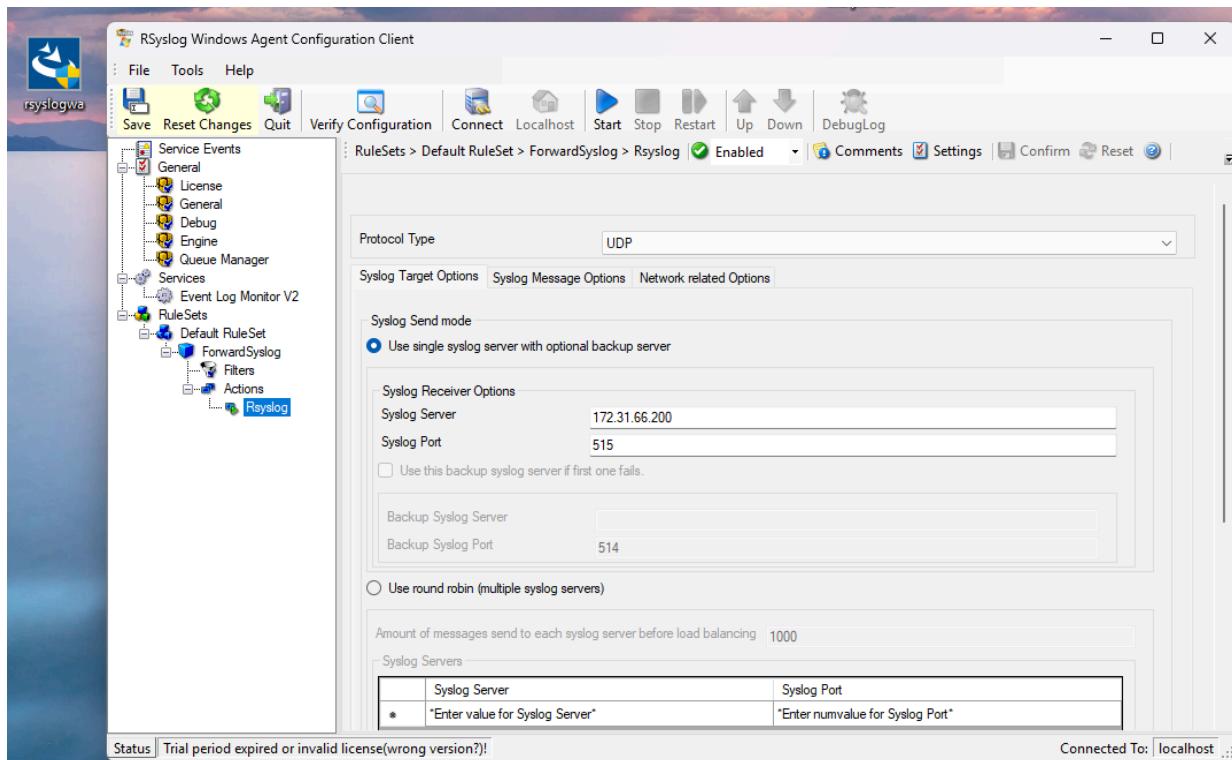
The "SSL Inspection" field is set to "ssl no-inspection".

The "Logging Options" section includes:

- Log Allowed Traffic: On
- Security Events: On
- All Sessions: On

At the bottom right are "OK" and "Cancel" buttons.

On the SForwarder, we will need to download **rsyslog**, an open source log processing system which will collect and forward log messages over the network to listen on port 515 (coming from the Cisco Routers) and forwarding to the Splunk Server. Once you execute and install **rsyslog** from accepting the default configurations, open the program, and expand the path: RuleSets→Default RuleSet→ForwardSyslog→Actions→Rsyslog, then change the Syslog Server IP to the Splunk Server IP, and Syslog Port to 515 because of our inputs.conf configuration.



Verification of Cisco Logging

Generate some logs from the Cisco Router using:

**logging host *FirewallIP*towardsRouter transport udp port *CustomPort*
send log *yourtestmessage***

In our case:

- logging host 172.31.64.220 transport udp port 514
- send log hamid

Below is the proof that it works. We searched for **index="splunk-cisco-site2"** as we configured earlier for Cisco. Change the name 'site2' for 'site3' for Burnaby.

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** Index="splunk-cisco-site2"
- Results Summary:** 32 events (before 5/23/25 11:20:28.000 AM) No Event Sampling
- Event List:** The list displays 32 events, each with a timestamp (e.g., May 23 11:20:25 172.31.66.99 502), source (host = 172.31.66.99), and source type (udp:515). The logs are categorized under "INTERESTING FIELDS" as ciscoios.
- Fields Panel:** Shows selected fields (a host 1, a source 1, a sourcetype 1) and interesting fields (a app 1, # date_hour 2, # date_mday 1).

Dashboard Proof of Cisco and Fortigate logs

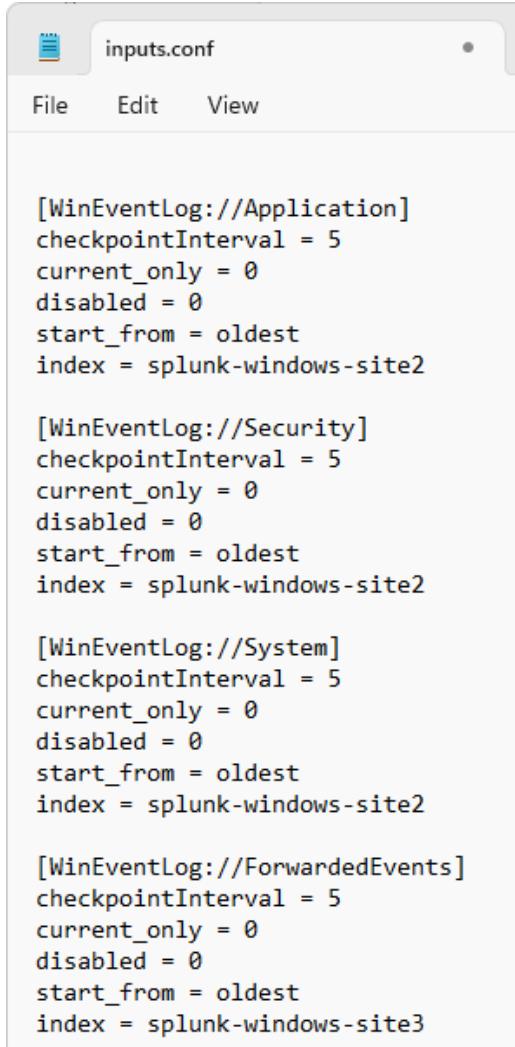
The screenshot shows the Splunk Dashboard Studio interface with the following details:

- Dashboard Studio Header:** W11 - SServer - VMware Workstation, 127.0.0.1:8000/en-US/app/search/dashboards
- Resources Section:** Examples for Dashboard Studio, Intro to Dashboard Studio, Intro to Classic Dashboards.
- Dashboard List:** A list of available dashboards:
 - Title *
 - cisco logs site2
 - fortigate-site2
 - Integrity Check of Installed Files
 - Job Details Dashboard
 - jQuery Upgrade
 - Orphaned Scheduled Searches, Reports, and Alerts
 - Scheduled export is now available for Dashboard Studio
- Actions Table:** A table showing dashboard details:

Actions	Owner	App	Sharing	Type
Edit	sserver	search	Private	Classic
Edit	sserver	search	Private	Classic
Edit	nobody	search	App	Dashboard Studio
Edit	nobody	search	App	Dashboard Studio
Edit	nobody	search	App	Dashboard Studio
Edit	nobody	search	Global	Dashboard Studio

Active Directory Configuration

On the domain controllers, follow the same above listed steps under Splunk Forwarder Setup as well as the Splunk Forwarder Conf File Configuration. Make sure you restart the SplunkForwarder service after changing the inputs.conf file.



The screenshot shows a text editor window titled "inputs.conf". The menu bar includes "File", "Edit", and "View". The main content area displays the configuration file with four sections for WinEventLog:

```
[WinEventLog://Application]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest
index = splunk-windows-site2

[WinEventLog://Security]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest
index = splunk-windows-site2

[WinEventLog://System]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest
index = splunk-windows-site2

[WinEventLog://ForwardedEvents]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest
index = splunk-windows-site3
```

Verification of Active Directory Logs

Following the same steps as listed under the Index Setup, create an index and call it "splunk-windows-site2" (site3 for Burnaby), and search the **index="splunk-windows-site2"**. You should be receiving logs from the domain controllers if configured properly.

Time	Event
5/23/25 11:45:10.959 -0700	collection="CPU Load" object="Processor" counter="% User Time" instance=_Total Show all 6 lines host = VANDC1 source = Perfmon:CPU Load sourcetype = Perfmon:CPU Load
5/23/25 11:45:10.959 -0700	collection="CPU Load" object="Processor" counter="% Processor Time" instance=_Total Show all 6 lines host = VANDC1 source = Perfmon:CPU Load sourcetype = Perfmon:CPU Load
5/23/25 11:45:10.959 -0700	collection="Available Memory"

Save the dashboard following the steps listed under the Verifications steps and save it to a new dashboard with a name of your choice. In Vancouver's Site case, we simply named it **Active Directory Logs**.

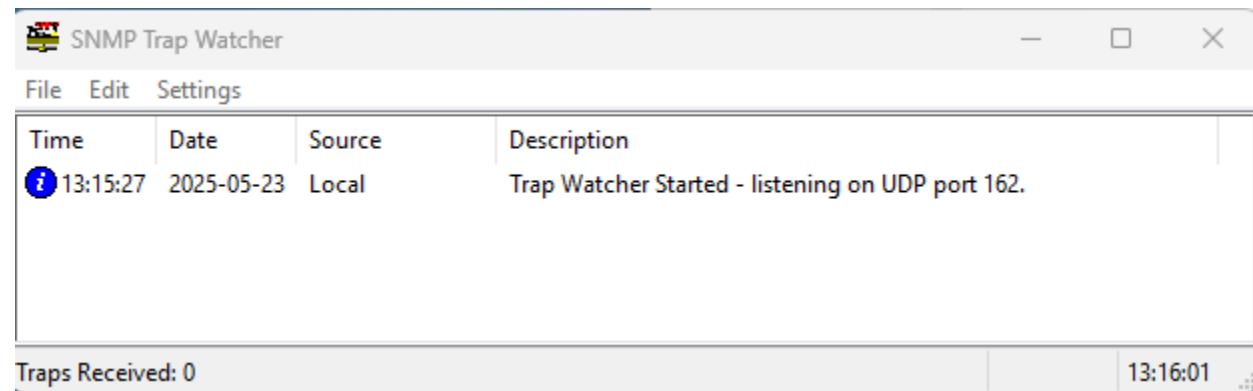
Title
Active Directory Log
cisco logs site2
fortigate-site2

SNMP Trap Configuration

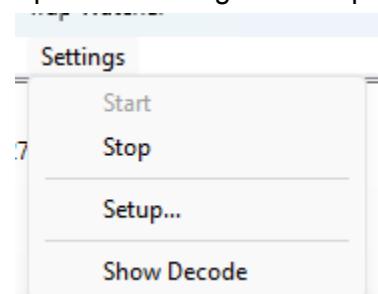
On the domain controllers, you will download a program called SNMP Trap Watcher and run it.



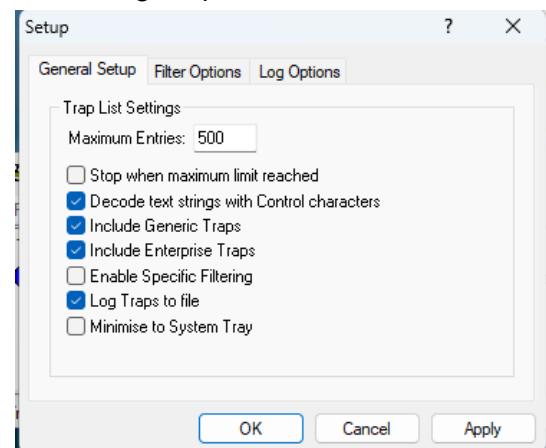
It will automatically start listening to UDP port 162. We will need to configure some settings to properly forward it.



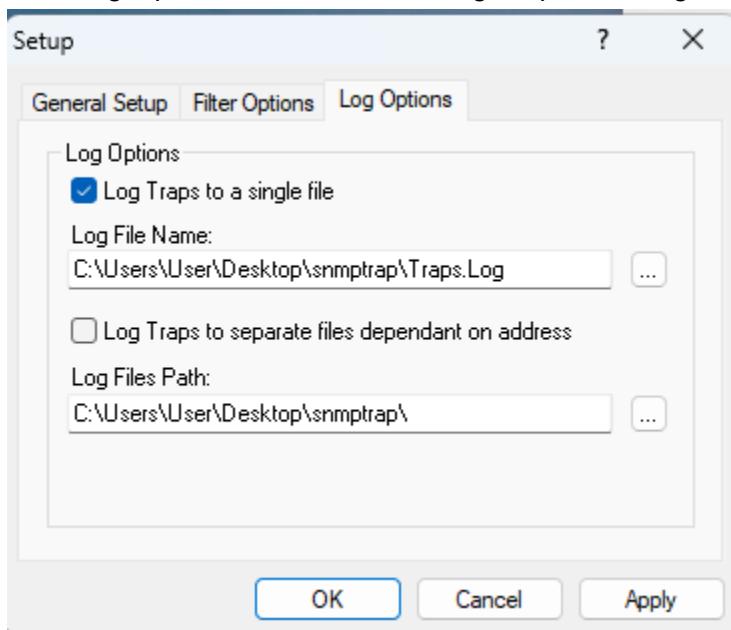
Open the Settings → Setup



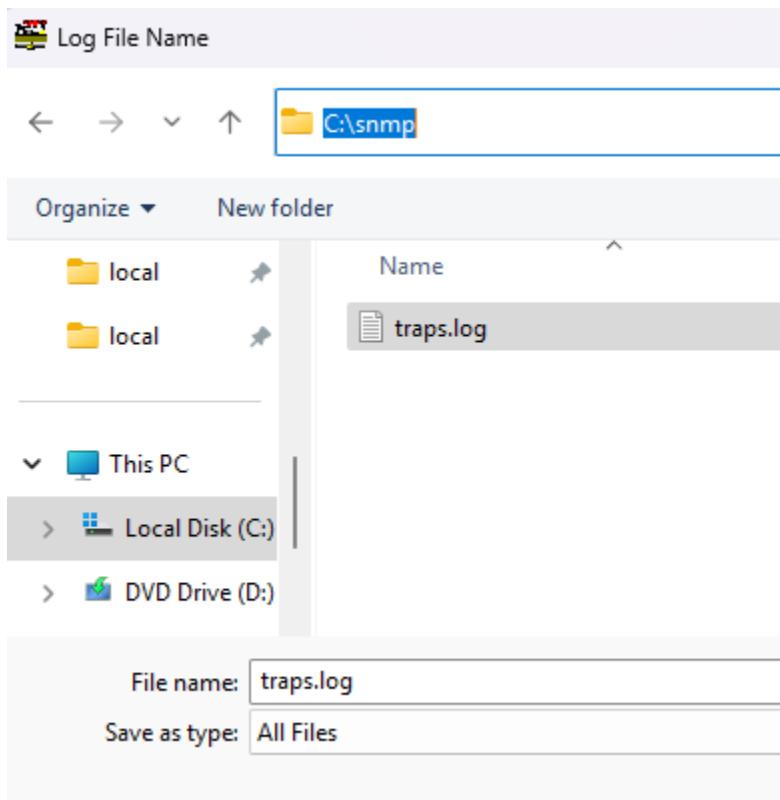
Check Log Traps to file

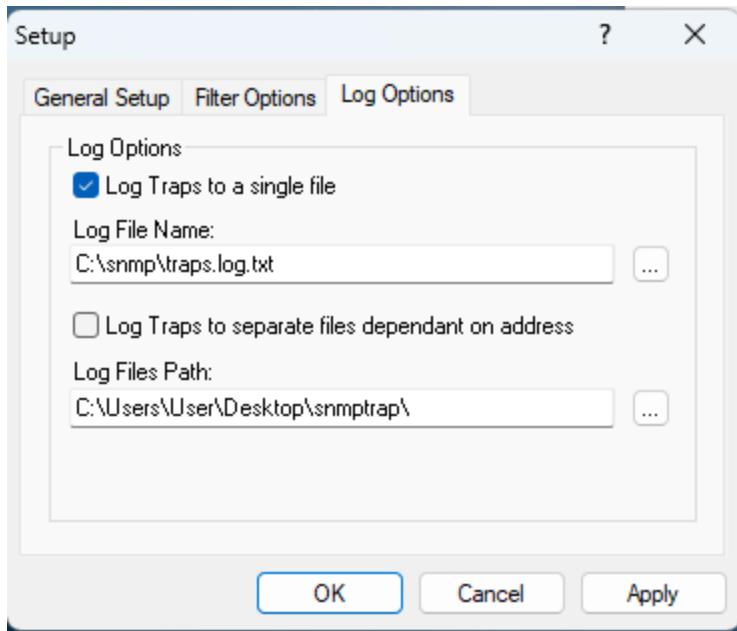


Click Log Options, and check the Log Traps to a single file.



Click the ... and point it a new file/folder location. In our case, I created a **snmp** folder located on C:\ and create a new text file called **traps.log**. Point to that and click Ok.





Apply it and OK.

On the Fortigate, we also need to configure a new DNAT rule so that the Cisco Router can route to Splunk Forwarder on UDP 162 (unchangeable)

Name	Details	Interfaces
IPv4 Virtual IP ②		
DNAT-WAN-TO-LAN	172.31.64.220 → 172.31.66.201 (UDP: 514 → 515)	To Router WAN (wan1)
SNMP DNAT-WAN-TO-LAN	172.31.64.220 → 172.31.66.201 (UDP: 162 → 162)	To Router WAN (wan1)

Then you need to add the SNMP NAT to the Syslog Service configured earlier. We renamed it for better naming.

Syslog-SNMP	all	DNAT-WAN-TO-LAN
		SNMP DNAT-WAN-TO-LAN

Syslog-SNMP

Interface	To Router WAN (wan1)
Interface	Internal LAN (internal)
	all
	+ <input type="button" value=""/>
	DNAT-WAN-TO-LAN
	SNMP DNAT-WAN-TO-LAN
	+ <input type="button" value=""/>
	always
	ALL
	+ <input type="button" value=""/>
<input checked="" type="button" value="ACCEPT"/> <input type="button" value="DENY"/>	

On the Cisco Router, configure the following:

snmp-server community public RO

snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart

snmp-server enable traps config

snmp-server enable traps memory bufferpeak

snmp-server enable traps cpu threshold

snmp-server enable traps syslog

snmp-server host 172.31.64.220 version 2c public

Then you can test using: **test snmp trap snmp linkup**

On the Forwarder VM, you can see that we successfully got the SNMP Test. Add this into the inputs.conf and restart SplunkForwarder service.

```
[monitor://C:\snmp\traps.log]
disabled = 0
sourcetype = snmp_trap
index = splunk-cisco-site2
```

Time	Date	Source	Description
13:47:16	2025-05-23	172.31.66.99	Trap contains no readable strings.
13:42:06	2025-05-23	172.31.66.99	GigabitEthernet0/0/0 Link Up Trap
13:42:05	2025-05-23	172.31.66.99	10.10.10.10
13:42:04	2025-05-23	172.31.66.99	GigabitEthernet0/0/0 Link Up Trap
13:42:04	2025-05-23	172.31.66.99	GigabitEthernet0/0/0 Link Up Trap
13:42:03	2025-05-23	172.31.66.99	GigabitEthernet0/0/0 Link Up Trap
13:40:19	2025-05-23	172.31.66.99	GigabitEthernet0/0/0 Link Up Trap
13:40:19	2025-05-23	172.31.66.99	GigabitEthernet0/0/0 Link Up Trap
13:40:19	2025-05-23	172.31.66.99	GigabitEthernet0/0/0 Link Up Trap
13:40:18	2025-05-23	172.31.66.99	GigabitEthernet0/0/0 Link Up Trap
13:40:18	2025-05-23	172.31.66.99	GigabitEthernet0/0/0 Link Up Trap
13:40:18	2025-05-23	172.31.66.99	GigabitEthernet0/0/0 Link Up Trap
13:40:17	2025-05-23	172.31.66.99	GigabitEthernet0/0/0 Link Up Trap
13:40:17	2025-05-23	172.31.66.99	GigabitEthernet0/0/0 Link Up Trap
13:40:14	2025-05-23	172.31.66.99	GigabitEthernet0/0/0 Link Up Trap
13:35:06	2025-05-23	172.31.66.99	10.10.10.10
13:35:06	2025-05-23	172.31.66.99	10.10.10.10
13:35:06	2025-05-23	172.31.66.99	10.10.10.10
13:35:05	2025-05-23	172.31.66.99	10.10.10.10
0090	06 0C 2B 06 01 04 01 09 02 02 01 01 14 01 04 0C		.+.....
00A0	4C 69 6E 6B 20 55 70 20 54 72 61 70		Link Up Trap
Frame Length:	172 bytes		
Version:	SNMPv2		
Community:	public		
PDU Type:	Trap v2		
Request ID:	17		
Error Status:	0		
Error Index:	0		
OID:	.1.3.6.1.2.1.1.3.0		
ASN.1 Type:	TimeTicks 0x43 (67)		
Value:	2 days, 01:42:15		
OID:	.1.3.6.1.6.3.1.1.4.1.0		
ASN.1 Type:	Object ID 0x06 (6)		
Value:	.1.3.6.1.6.3.1.1.5.4		
OID:	.1.3.6.1.2.1.2.2.1.1.1		
ASN.1 Type:	Integer32 0x02 (2)		
Value:	1		
OID:	.1.3.6.1.2.1.2.2.1.2.1		
ASN.1 Type:	Octet String 0x04 (4)		
Value:	GigabitEthernet0/0/0		
OID:	.1.3.6.1.2.1.2.2.1.3.1		
ASN.1 Type:	Integer32 0x02 (2)		
Value:	6		
OID:	.1.3.6.1.4.1.9.2.2.1.1.20.1		
ASN.1 Type:	Octet String 0x04 (4)		
Value:	Link Up Trap		
Traps Received:	22		

Verification of SNMP Trap Logging

Do a search on the **index="splunk-windows-site2" sourcetype="snmp_trap"** to filter to the SNMP logs under the index. Replace 'site2' with 'site3' for Burnaby.

New Search

index="splunk-cisco-site2" sourcetype="snmp_trap"

✓ 16 events (5/22/25 1:00:00.000 PM to 5/23/25 1:59:21.000 PM) No Event Sampling ▾

Events (16) Patterns Statistics Visualization

Timeline format ▾ — Zoom Out + Zoom to Selection × Deselect

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

Hide Fields	All Fields	i	Time	Event
SELECTED FIELDS		>	5/23/25 1:40:19.000 PM	2025-05-23 13:40:19 172.31.66.99 (v2)GigabitEthernet0/0/0 Link Up Trap host = SFORWARDER source = C:\snmp\traps.log sourcetype = snmp_trap
a host 1		>	5/23/25 1:40:19.000 PM	2025-05-23 13:40:19 172.31.66.99 (v2)GigabitEthernet0/0/0 Link Up Trap host = SFORWARDER source = C:\snmp\traps.log sourcetype = snmp_trap
a source 1		>	5/23/25 1:40:19.000 PM	2025-05-23 13:40:19 172.31.66.99 (v2)GigabitEthernet0/0/0 Link Up Trap host = SFORWARDER source = C:\snmp\traps.log sourcetype = snmp_trap
a sourcetype 1		>	5/23/25 1:40:19.000 PM	2025-05-23 13:40:19 172.31.66.99 (v2)GigabitEthernet0/0/0 Link Up Trap host = SFORWARDER source = C:\snmp\traps.log sourcetype = snmp_trap
INTERESTING FIELDS		>	5/23/25 1:40:19.000 PM	2025-05-23 13:40:19 172.31.66.99 (v2)GigabitEthernet0/0/0 Link Up Trap host = SFORWARDER source = C:\snmp\traps.log sourcetype = snmp_trap
# date_hour 1				
# date_mday 1				

Active Directory Log

VanDC1 AD Logging			VanDC2 AD Logging			SNMP Trap Logging		
i	Time	Event	i	Time	Event	i	Time	Event
>	5/23/25 12:30:33.000 PM	05/23/2025 12:30:33 PM LogName=Security EventCode=4634 EventType=0 ComputerName=VanDC1.TT17.org Show all 22 lines host = VANDC1 source = WinEventLog:Security sourcetype = WinEventLog:Security	>	5/23/25 12:30:30.000 PM	05/23/2025 12:30:30.116 -0700 collection="Available Memory" object="Memory" counter="Available Bytes" instance=0 Show all 6 lines host = VANDC2 source = Perfmon:Available Memory sourcetype = Perfmon:Available Memory	>	5/23/25 12:26:44.000 PM	12:26:44:05/23/25 0 172.31.65.100 2330966 1.3.6.1. host = VANDC1 source = C:\snmp\traps.log sourcetype = snmp_trap
>	5/23/25 12:30:33.000 PM	05/23/2025 12:30:33 PM LogName=Security EventCode=4624 EventType=0 ComputerName=VanDC1.TT17.org Show all 7 lines host = VANDC1 source = WinEventLog:Security sourcetype = WinEventLog:Security	>	5/23/25 12:30:30.000 PM	05/23/2025 12:30:30.116 -0700 collection="Network Interface" object="Network Interface" counter="Bytes Sent/sec" instance="Microsoft Hyper-V Network Adapter" Show all 6 lines host = VANDC2 source = Perfmon:Network Interface sourcetype = Perfmon:Network Interface	>	5/23/25 12:26:43.000 PM	12:26:43:05/23/25 0 172.31.65.100 2330953 1.3.6.1. host = VANDC1 source = C:\snmp\traps.log sourcetype = snmp_trap
>	5/23/25 12:30:30.000 PM	05/23/2025 12:30:30.214 -0700 collection="Available Memory" object="Memory" counter="Available Bytes" instance=0 Show all 6 lines host = VANDC1 source = Perfmon:Available Memory sourcetype = Perfmon:Available Memory	>	5/23/25 12:30:30.000 PM	05/23/2025 12:30:30.116 -0700 collection="Network Interface" object="Network Interface" counter="Bytes Received/sec" instance="Microsoft Hyper-V Network Adapter" Show all 6 lines host = VANDC2 source = Perfmon:Network Interface sourcetype = Perfmon:Network Interface	>	5/23/25 12:26:43.000 PM	12:26:43:05/23/25 0 172.31.65.100 2330941 1.3.6.1. host = VANDC1 source = C:\snmp\traps.log sourcetype = snmp_trap
>	5/23/25 12:30:30.000 PM	05/23/2025 12:30:30.214 -0700 collection="CPU Load"				>	5/23/25 12:26:43.000 PM	12:26:43:05/23/25 0 172.31.65.100 2330928 1.3.6.1. host = VANDC1 source = C:\snmp\traps.log sourcetype = snmp_trap
						>	5/23/25 12:26:43.000 PM	12:26:43:05/23/25 0 172.31.65.100 2330913 1.3.6.1. host = VANDC1 source = C:\snmp\traps.log sourcetype = snmp_trap
						>	5/23/25 12:26:43.000 PM	12:26:43:05/23/25 0 172.31.65.100 2330900 1.3.6.1. host = VANDC1 source = C:\snmp\traps.log sourcetype = snmp_trap
							E/23/25	12:26:43:05/23/25 0 172.31.65.100 2330907 1.3.6.1.

Cisco Site2 Logs

Cisco Syslog			Cisco SNMP Trap		
i	Time	Event	i	Time	Event
>	5/23/25 9:23:36.000 AM	May 23 09:23:36 172.31.66.201 1 2025-05-23T09:23:36-07:00 SFowarder EvntSLog -- Service stopped. host = 172.31.66.201 source = udp:515 sourcetype = ciscoios	>	5/23/25 1:40:19.000 PM	2025-05-23 13:40:19 172.31.66.99 (v2)GigabitEthernet0/0/0 Link Up Trap host = SFORWARDER source = C:\snmp\traps.log sourcetype = snmp_trap
>	5/23/25 9:23:13.000 AM	May 23 09:23:13 172.31.66.201 1 2025-05-23T09:23:12-07:00 SFowarder EvntSLog -- PowerSh ell console is ready for user input host = 172.31.66.201 source = udp:515 sourcetype = ciscoios	>	5/23/25 1:40:19.000 PM	2025-05-23 13:40:19 172.31.66.99 (v2)GigabitEthernet0/0/0 Link Up Trap host = SFORWARDER source = C:\snmp\traps.log sourcetype = snmp_trap
>	5/23/25 9:23:13.000 AM	May 23 09:23:13 172.31.66.201 1 2025-05-23T09:23:12-07:00 SFowarder EvntSLog -- Windows PowerShell has started an IPC listening thread on process: 8700 in AppDomain: DefaultAppDom ain. host = 172.31.66.201 source = udp:515 sourcetype = ciscoios	>	5/23/25 1:40:18.000 PM	2025-05-23 13:40:18 172.31.66.99 (v2)GigabitEthernet0/0/0 Link Up Trap host = SFORWARDER source = C:\snmp\traps.log sourcetype = snmp_trap
>	5/23/25 9:23:13.000 AM	May 23 09:23:13 172.31.66.201 1 2025-05-23T09:23:12-07:00 SFowarder EvntSLog -- PowerSh ell console is starting up host = 172.31.66.201 source = udp:515 sourcetype = ciscoios	>	5/23/25 1:40:18.000 PM	2025-05-23 13:40:18 172.31.66.99 (v2)GigabitEthernet0/0/0 Link Up Trap host = SFORWARDER source = C:\snmp\traps.log sourcetype = snmp_trap
>	5/23/25 9:23:12.000 AM	May 23 09:23:12 172.31.66.201 1 2025-05-23T09:23:12-07:00 SFowarder EvntSLog -- Engine state is changed from None to Available. Details: NewEngineState=Available PreviousEngineState=None SequenceNumber=13 HostName=ConsoleHost HostVersion=5.1.26100.1591 HostId=eb282c5e-0ac0-4973-9c9e-1e3ad62fe4d HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion=5.1.26100.1591 RunspaceId=40f58c8a-0e73-44e7-b932-8c1565b790ce Pid elined=CommandName= CommandType= ScriptName= CommandPath= Commandline= host = 172.31.66.201 source = udp:515 sourcetype = ciscoios	>	5/23/25 1:40:18.000 PM	2025-05-23 13:40:18 172.31.66.99 (v2)GigabitEthernet0/0/0 Link Up Trap host = SFORWARDER source = C:\snmp\traps.log sourcetype = snmp_trap
>	5/23/25	May 23 09:23:12 172.31.66.201 1 2025-05-23T09:23:12-07:00 SFowarder EvntSLog -- Provide	>	5/23/25 1:40:17.000 PM	2025-05-23 13:40:17 172.31.66.99 (v2)GigabitEthernet0/0/0 Link Up Trap host = SFORWARDER source = C:\snmp\traps.log sourcetype = snmp_trap
>	5/23/25	May 23 09:23:12 172.31.66.201 1 2025-05-23T09:23:12-07:00 SFowarder EvntSLog -- Provide	>	5/23/25 1:40:17.000 PM	2025-05-23 13:40:17 172.31.66.99 (v2)GigabitEthernet0/0/0 Link Up Trap host = SFORWARDER source = C:\snmp\traps.log sourcetype = snmp_trap