

Table of Content

1. Installation and Setting up of Window 11Pro.....	1
2. Installation and Configuration of Splunk SIEM on Windows 11 Pro.....	20
3. Installation and Configuration of Splunk Universal Forwarder.....	24
4. Detailed function of Splunk SIEM Service.....	30
5. Splunk SIEM: A Comprehensive Analysis of its Widespread Adoption.....	55
6. Critically Evaluation of Splunk SIEM Security Services	56
6.1 Splunk SIEM Strengths	56
6.2 Vulnerabilities and Attack Vectors against Splunk SIEM.....	57
6.3 Evaluating the Effectiveness of Splunk SIEM Service in Protecting Against Advanced Cyber-attacks.....	58

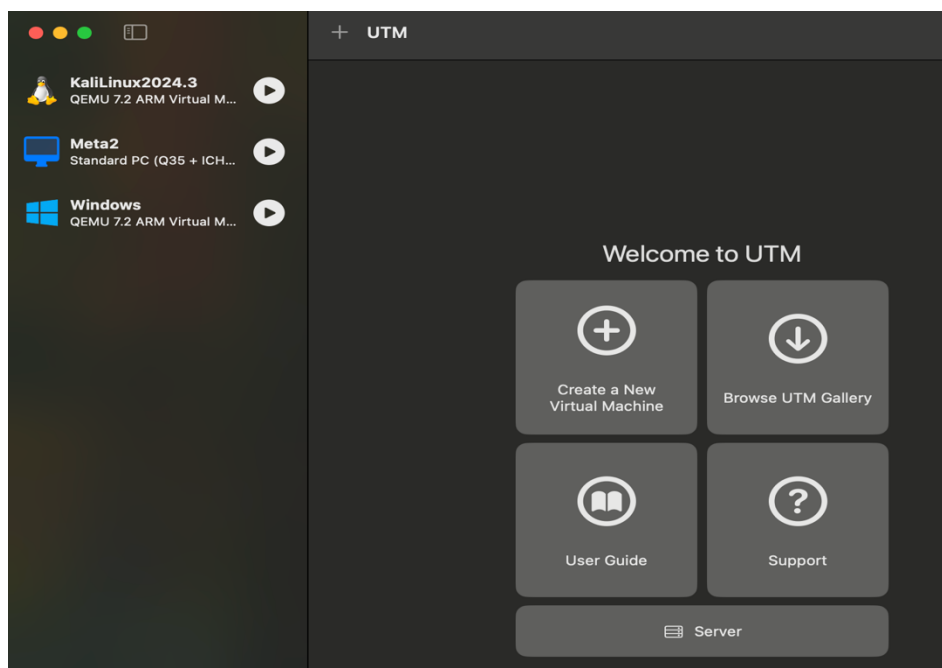
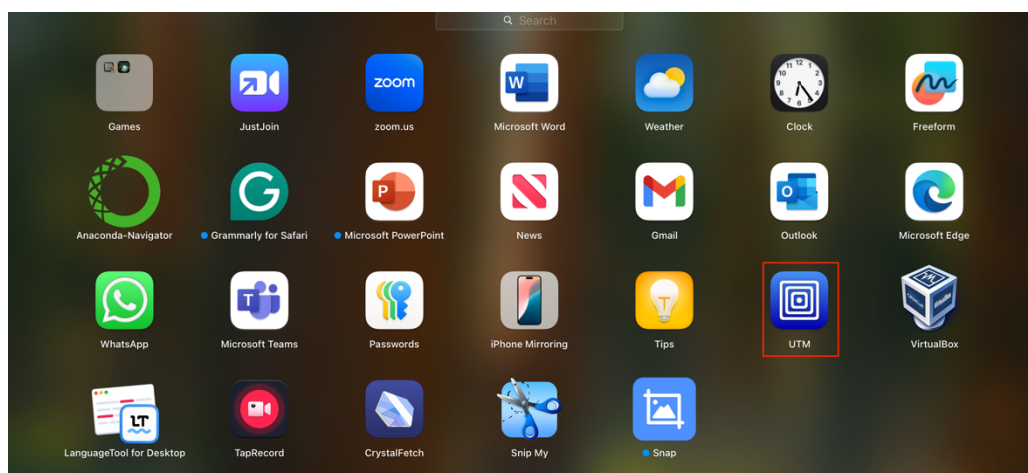
1. Installation and Setting up of Window 11Pro

Guide for installing and configuring Windows 11 Pro on your Mac with an M1 chip using UTM. Follow the steps below and refer to the images for visual assistance.

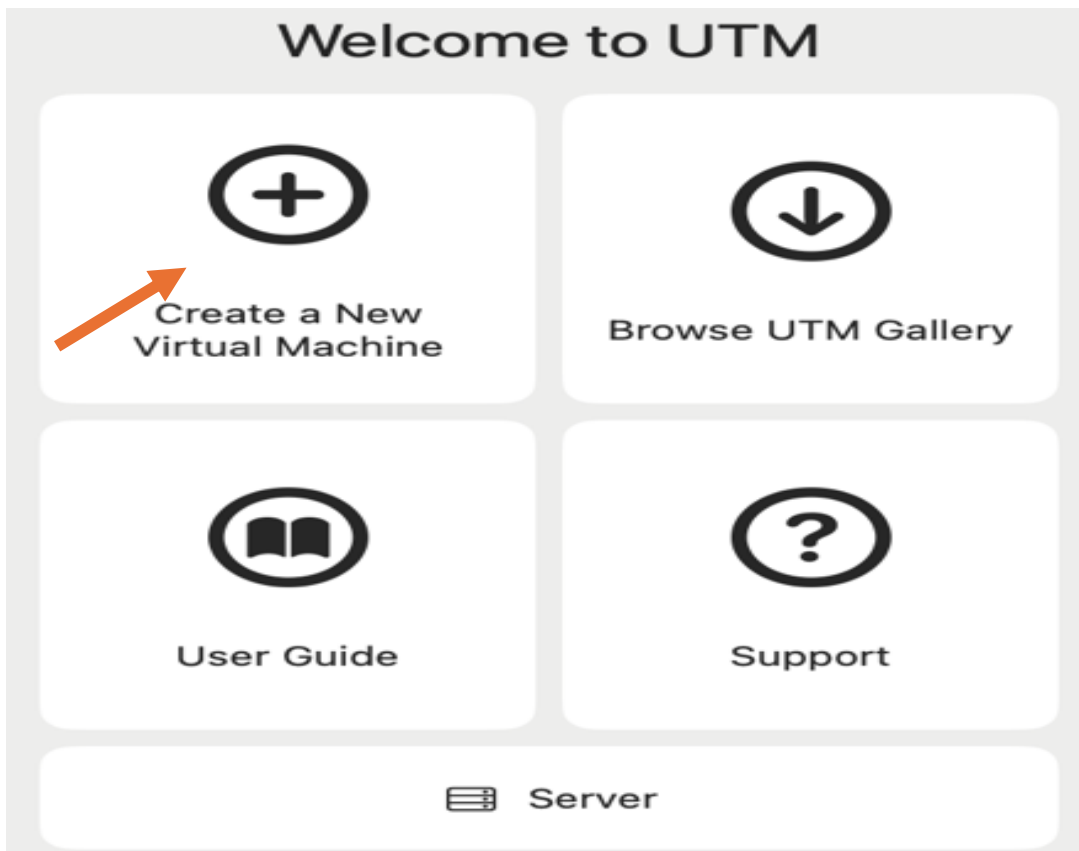
NOTE: If you don't have UTM already installed, visit the UTM Website <https://mac.getutm.app/> to download the latest version of UTM. Click the download button to get the application, once downloaded open the download file and move UTM to Application folder.

Step 1. Download Windows 11 pro ISO file and create a New Virtual Machine in UTM.

Open UTM: Launch the UTM app from your application folder.



Click on “+ New”: Create a new virtual machine



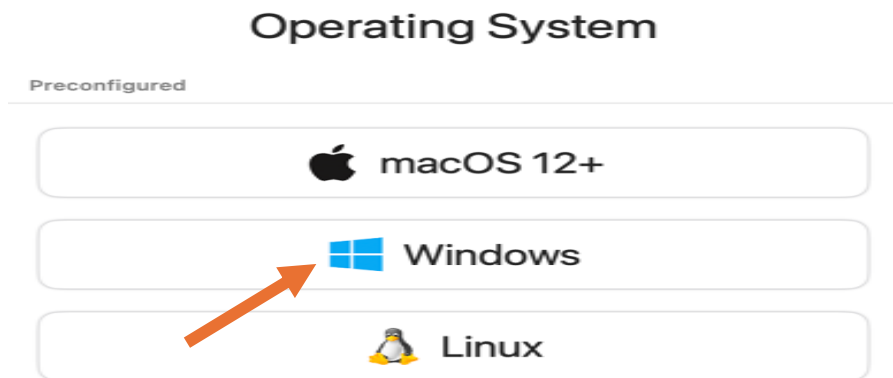
Select Virtualization: Choose the virtualization option for better performance on an M1 Mac.

Start

Custom



Click on Windows icon: Select Windows install Guide, it will automatically take you to website where you can download window 11 for Mac or via CrystalFetch ISO Downloader on App Store.



Windows

Image File Type

- ☒ Install Windows 10 or higher
- ☐ Import VHDX Image
- [Fetch latest Windows installer...](#)
- [Windows Install Guide](#)



Boot ISO Image

Path

Browse...

- ☒ Install drivers and SPICE tools

Download and mount the guest support package for Windows. This is required for some features including dynamic resolution and clipboard sharing.

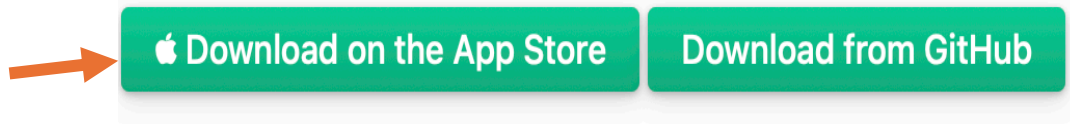
Cancel

Go Back

Continue

Obtain Windows

The easiest way to obtain a Windows installer ISO is with CrystalFetch, by legally obtaining the newest Windows builds from Microsoft.



Alternatively, you can also download an older ISO directly from Microsoft or Chrome to download as Microsoft's website sometimes does not

- [Download Windows 11 for Intel Macs](#)
- [Download Windows 11 for Apple Silicon Macs](#)

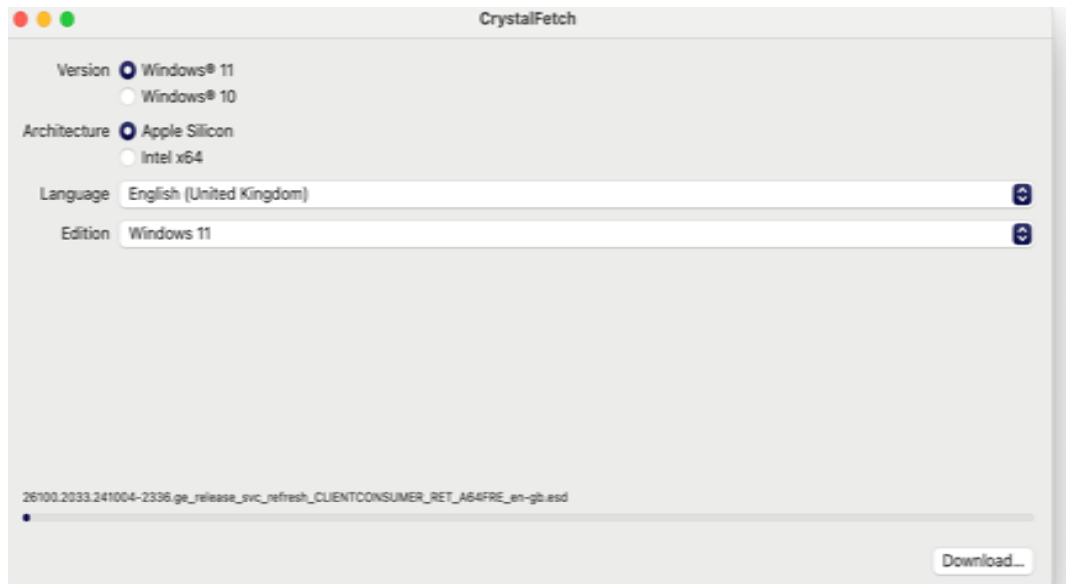


CrystalFetch ISO Downloader

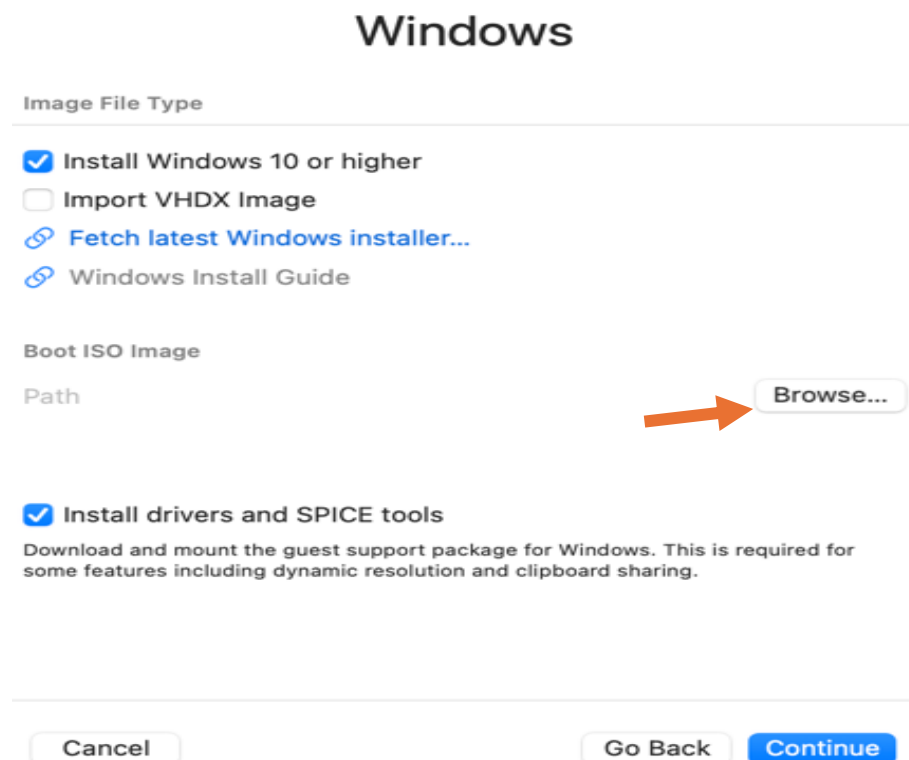
Installer for Windows® 11

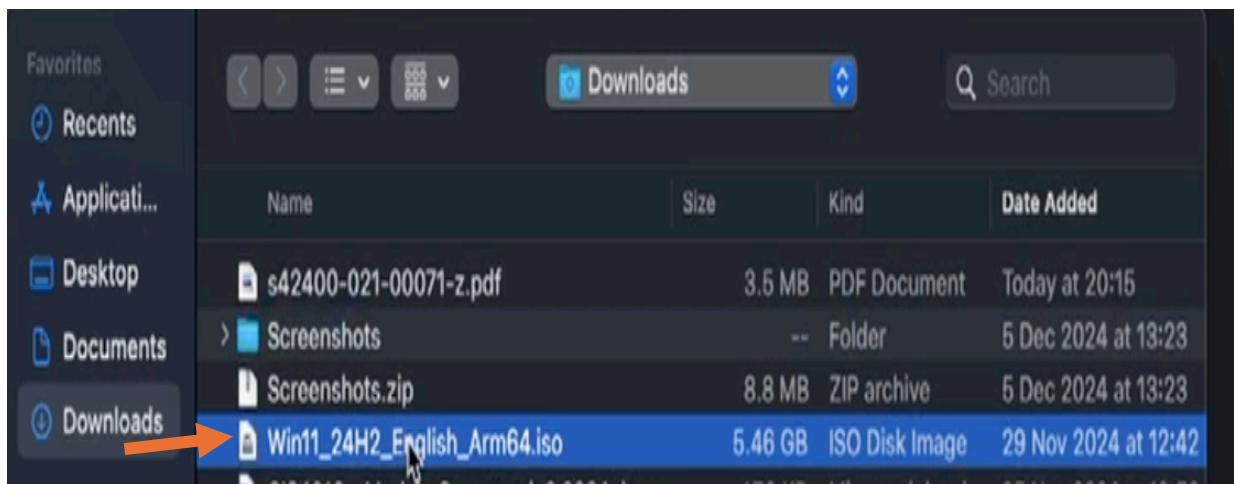
Open





Add the ISO File: Click on Browse to locate the downloaded Windows 11 pro ISO file and click open. Make sure you have Install Windows 10 or higher checked, do not check import VHDX image, make sure to check Install drivers and SPICE tools, its essential for fixing any internet problems and click continue.





Step 2: Configure the Virtual Machine

Set the Hardware Preferences: Configure the amount of memory (RAM) and CPU cores. Recommend: 4 GB RAM and 4 CPU cores for optimal performance, click continue to set the storage.

Hardware

Memory

4096 MB

CPU

CPU Cores 4

Cancel Go Back Continue



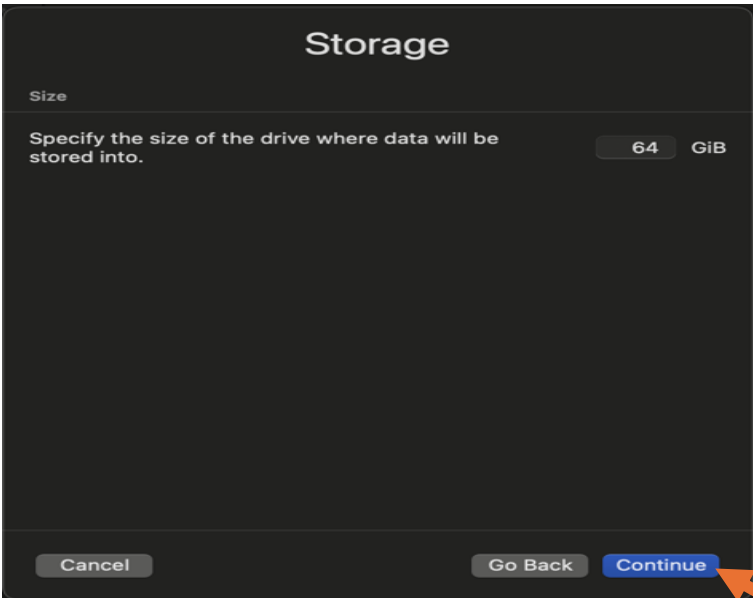
Storage

Size


Specify the size of the drive where data will be stored into.

64 GiB

Cancel Go Back Continue

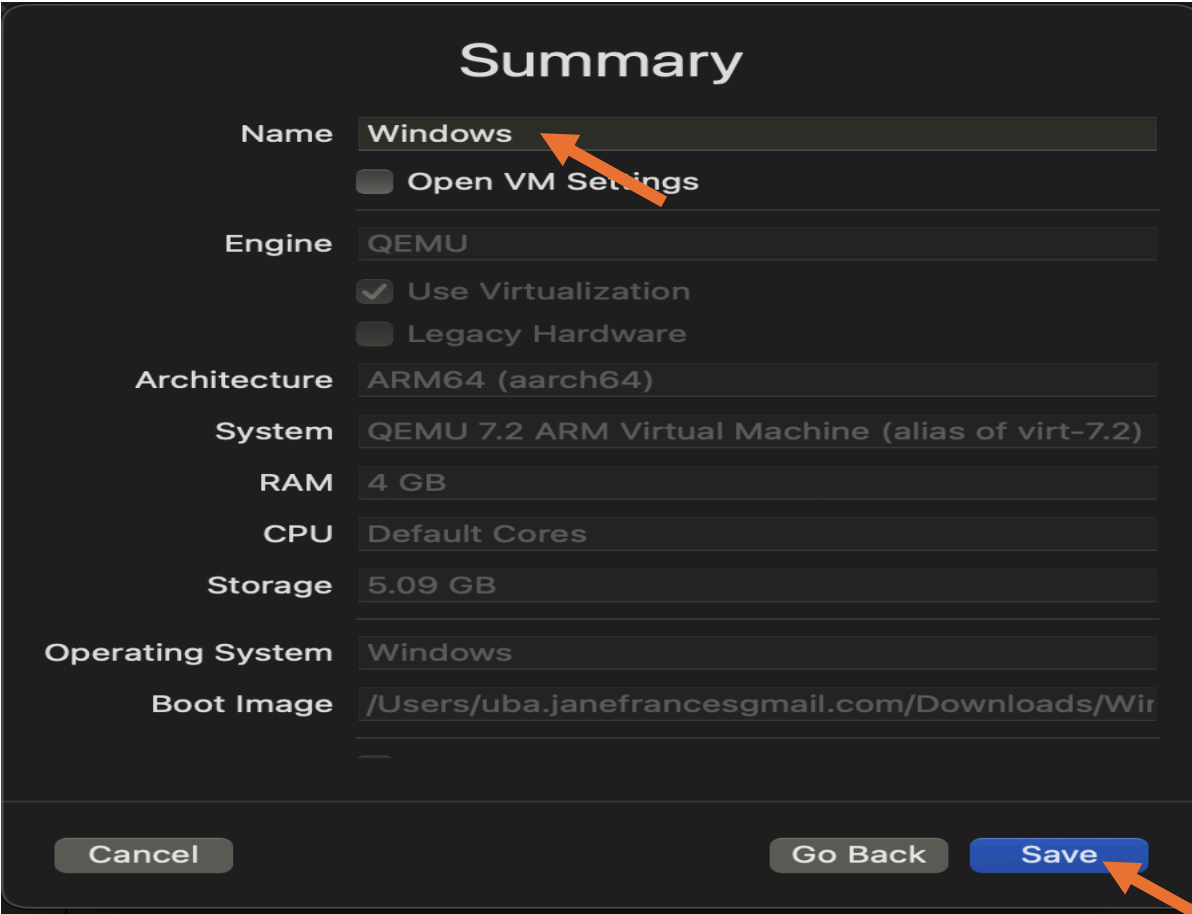


Do not check the Shared Directory, click continue



The 'Shared Directory' dialog box has a title bar 'Shared Directory'. Below it is a section 'Shared Directory Path' containing a 'Path' text field, a 'Clear' button, and a 'Browse...' button. A checkbox labeled 'Share is read only' is present. Below the checkbox is a paragraph of text: 'Optionally select a directory to make accessible inside the VM. Note that support for shared directories varies by the guest operating system and may require additional guest drivers to be installed. See UTM support pages for more details.' At the bottom are three buttons: 'Cancel', 'Go Back', and 'Continue'. An orange arrow points to the 'Continue' button.

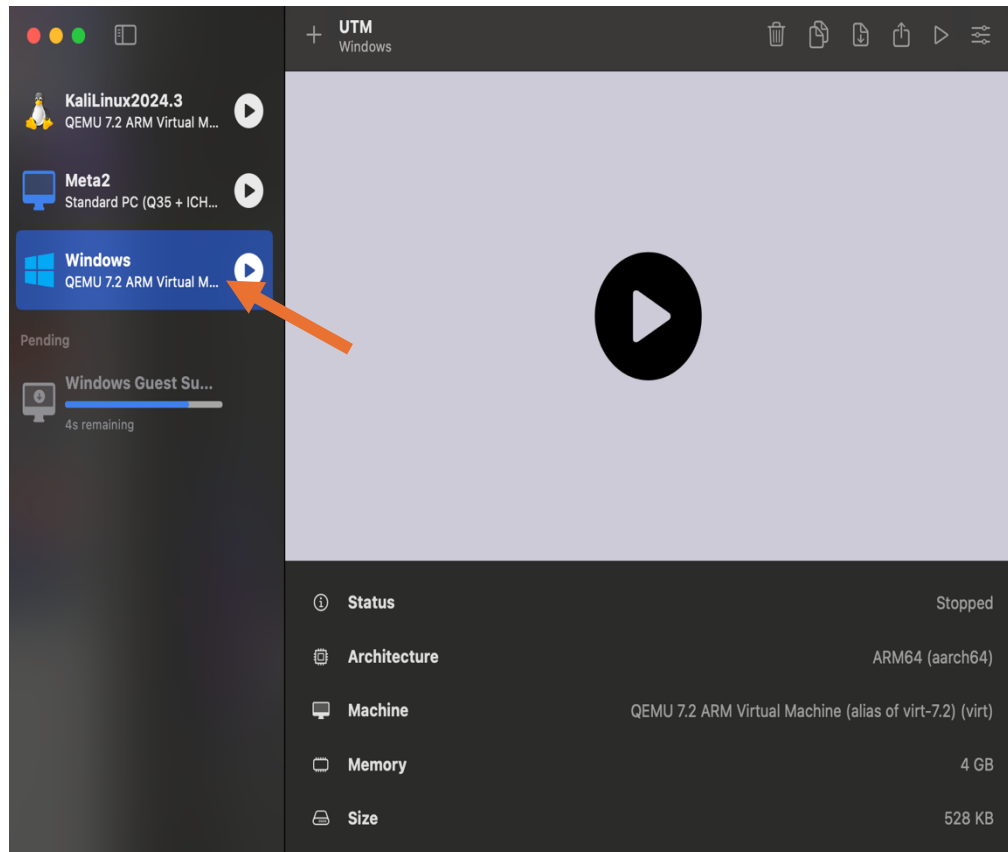
Enter a name for the VM, “Windows” and click Save



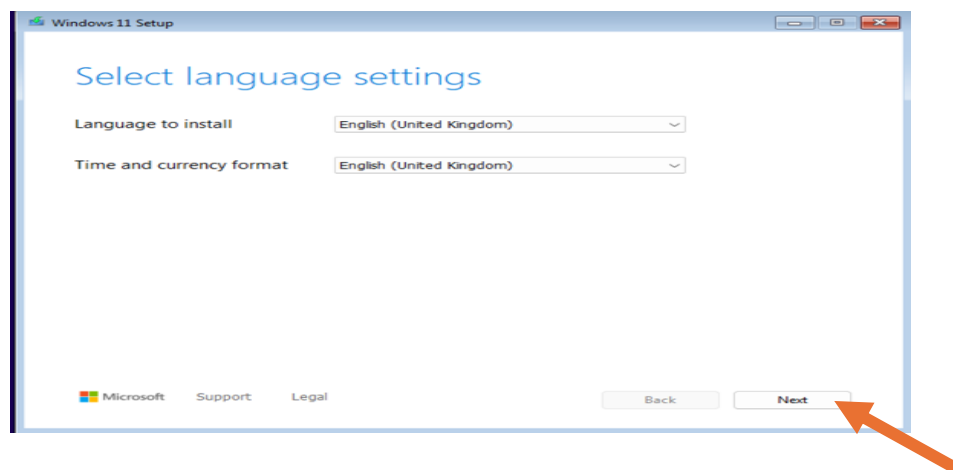
The 'Summary' dialog box displays various configuration options for a VM. The 'Name' field is set to 'Windows', with an orange arrow pointing to it. Below the name field is a checkbox for 'Open VM Settings'. The 'Engine' is set to 'QEMU', with checkboxes for 'Use Virtualization' (checked) and 'Legacy Hardware'. The 'Architecture' is set to 'ARM64 (aarch64)'. The 'System' is set to 'QEMU 7.2 ARM Virtual Machine (alias of virt-7.2)'. The 'RAM' is set to '4 GB', 'CPU' to 'Default Cores', and 'Storage' to '5.09 GB'. The 'Operating System' is set to 'Windows', and the 'Boot Image' is set to '/Users/uba.janefrancesgmail.com/Downloads/Wir'. At the bottom are three buttons: 'Cancel', 'Go Back', and 'Save'. An orange arrow points to the 'Save' button.

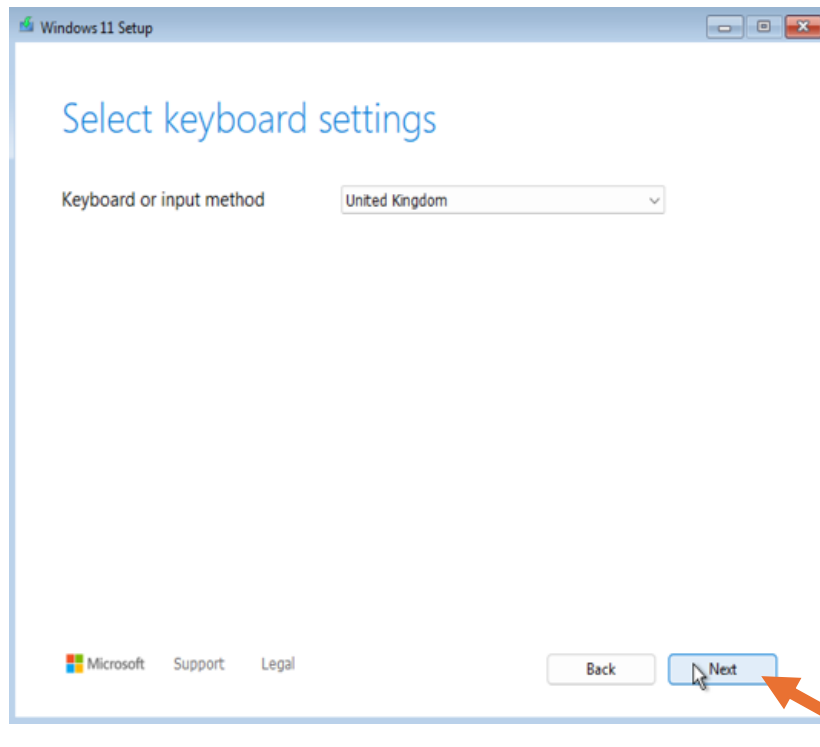
Step 3: Start the Installation

Click the “Play” button to start the virtual machine.

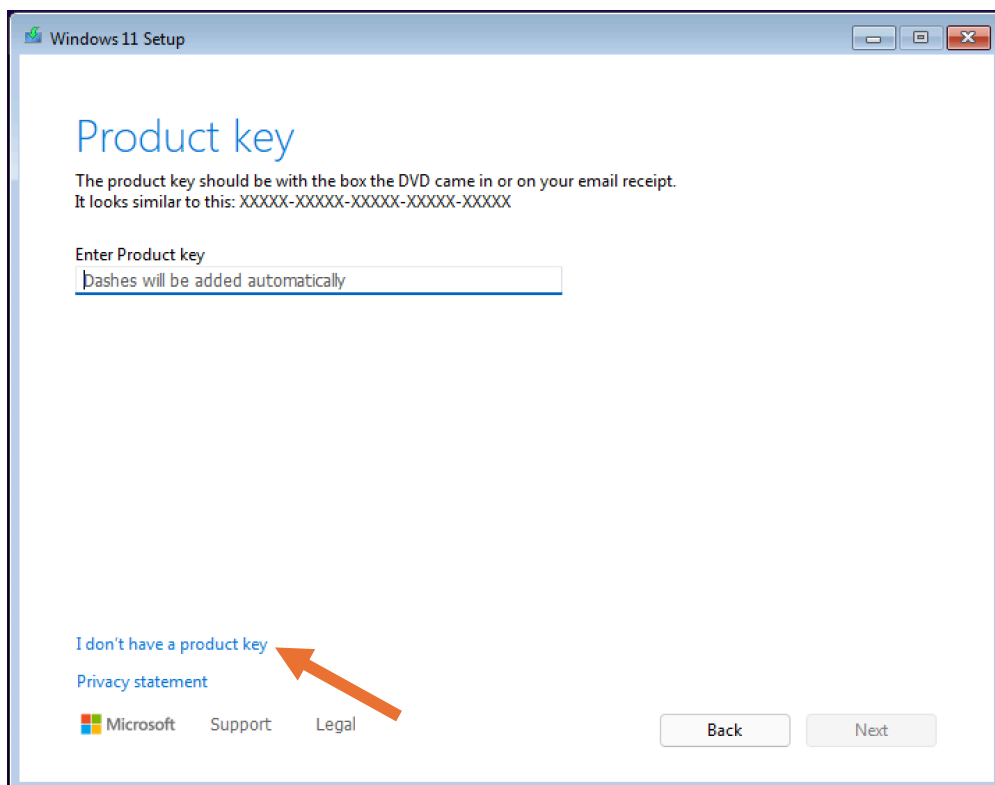


Follow Windows setup steps, the Windows 11 pro installer will launch kindly follow the on-screen instructions steps to complete the installation.

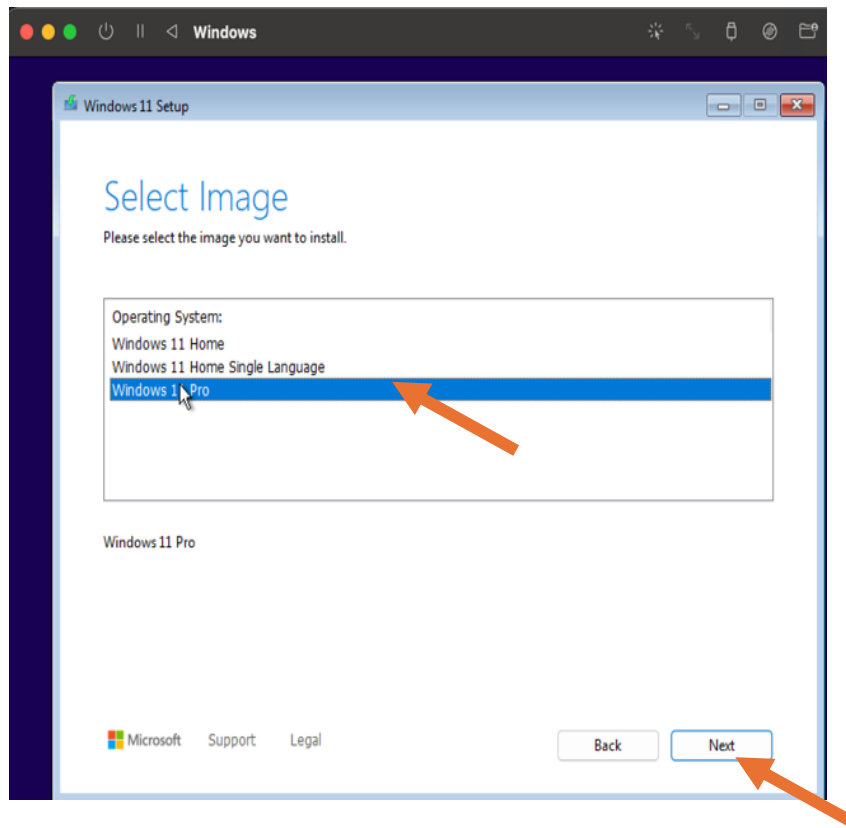




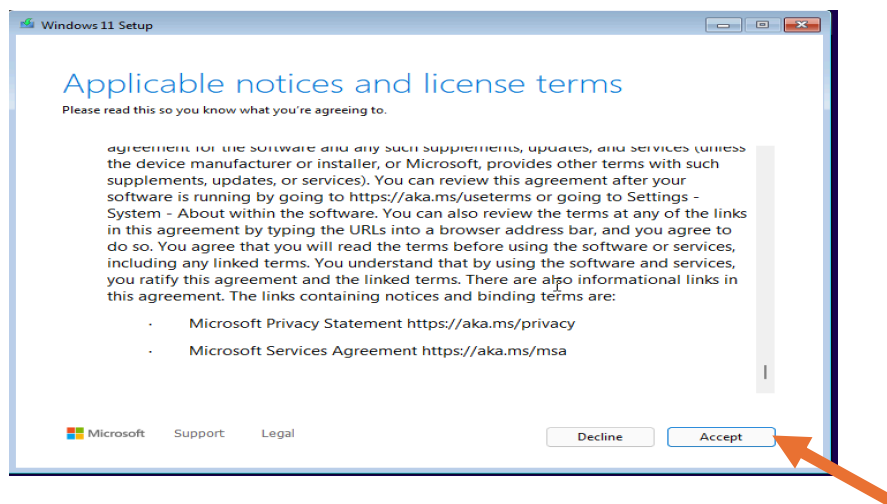
Product key: Add product key if you have, otherwise select I don't have product key.



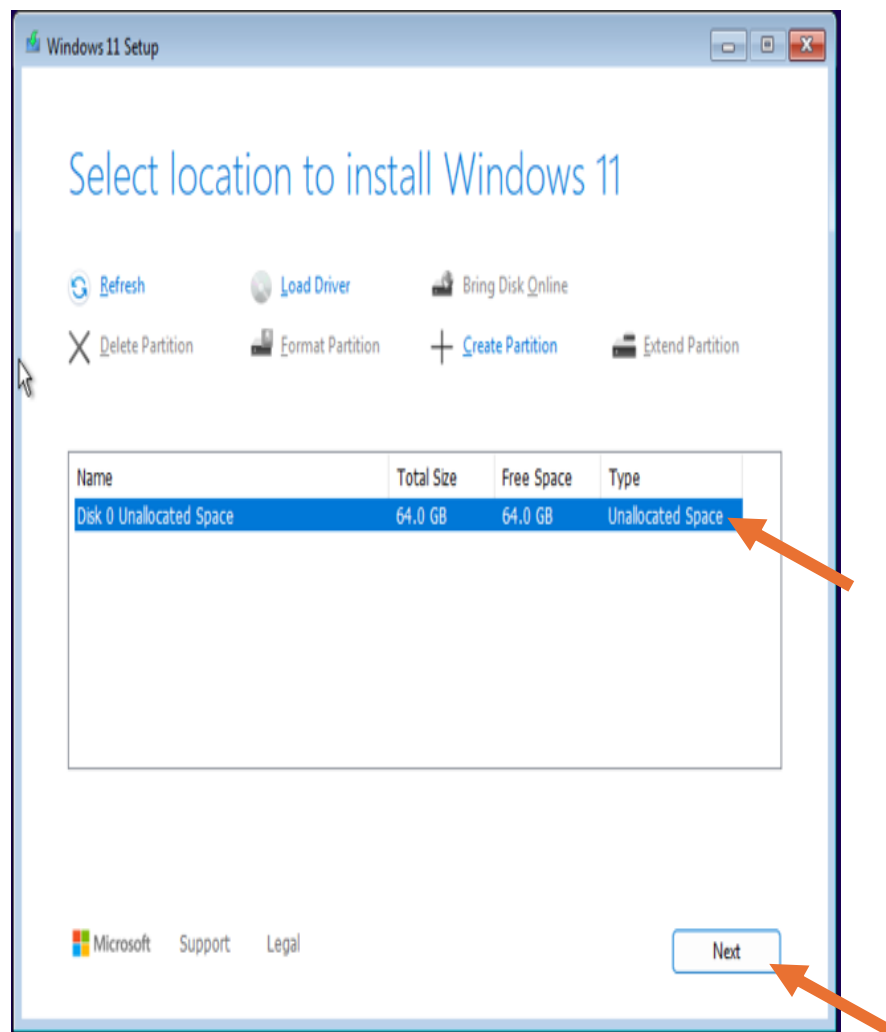
Select the version on the Windows and Click Next



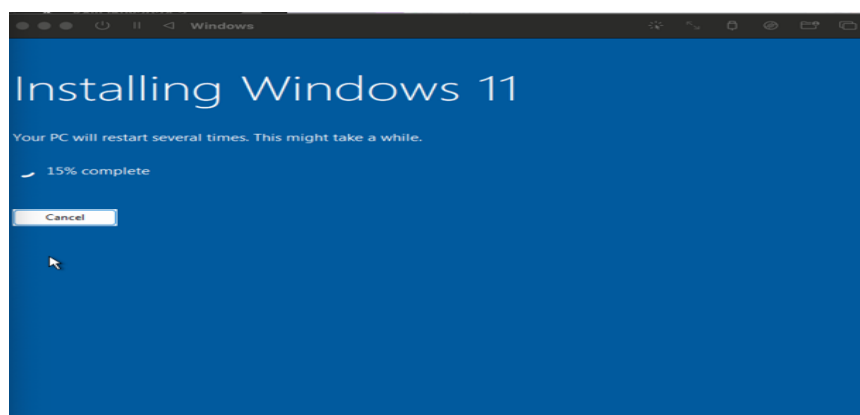
Accept the Licence



Select the Drive Space and click Next

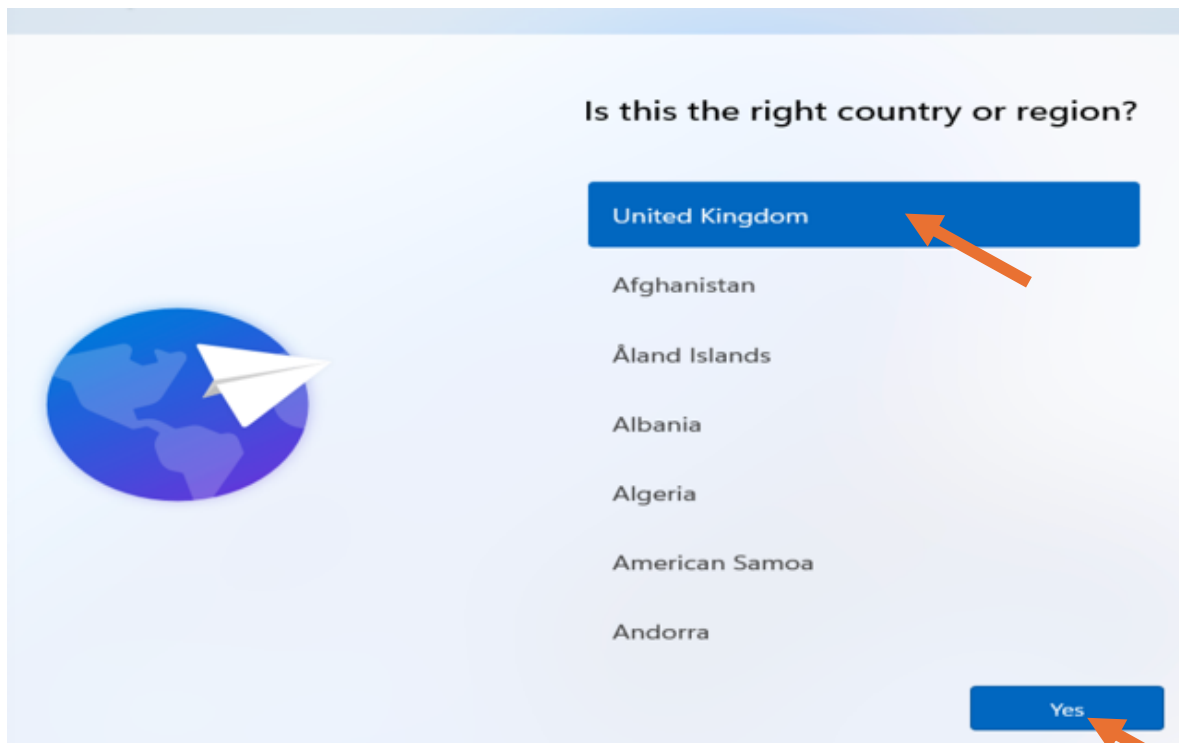


Wait for the Installation to complete

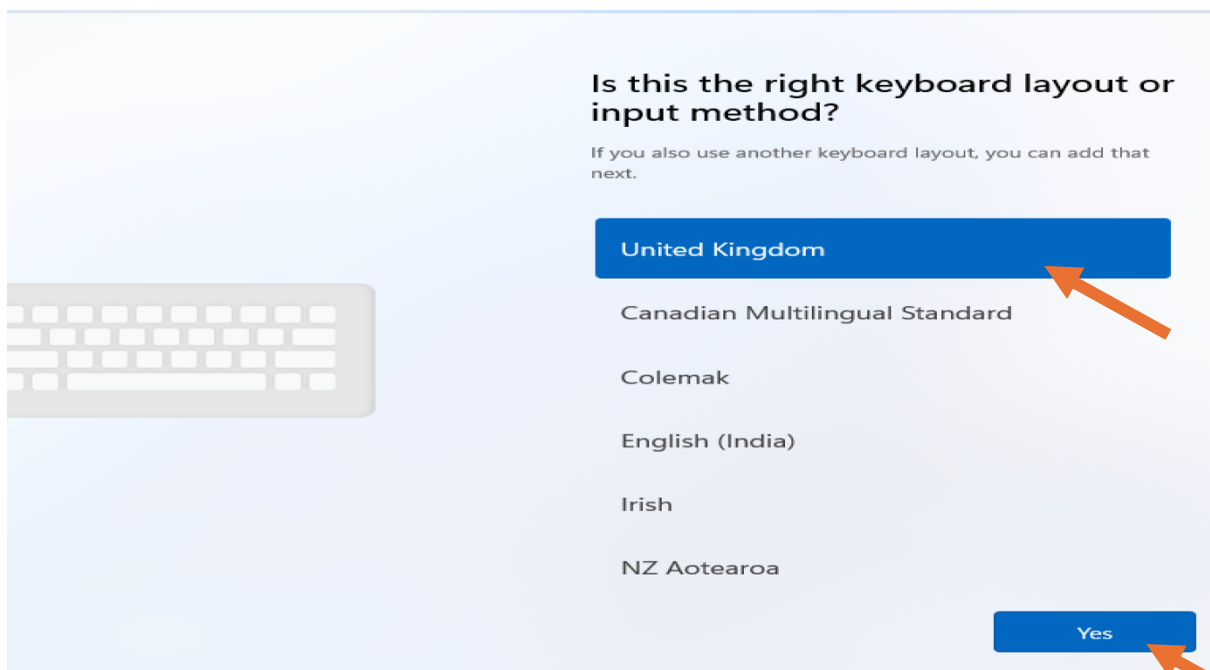


Once the Installation is complete it will restart the windows automatically if not you can click on restart button.

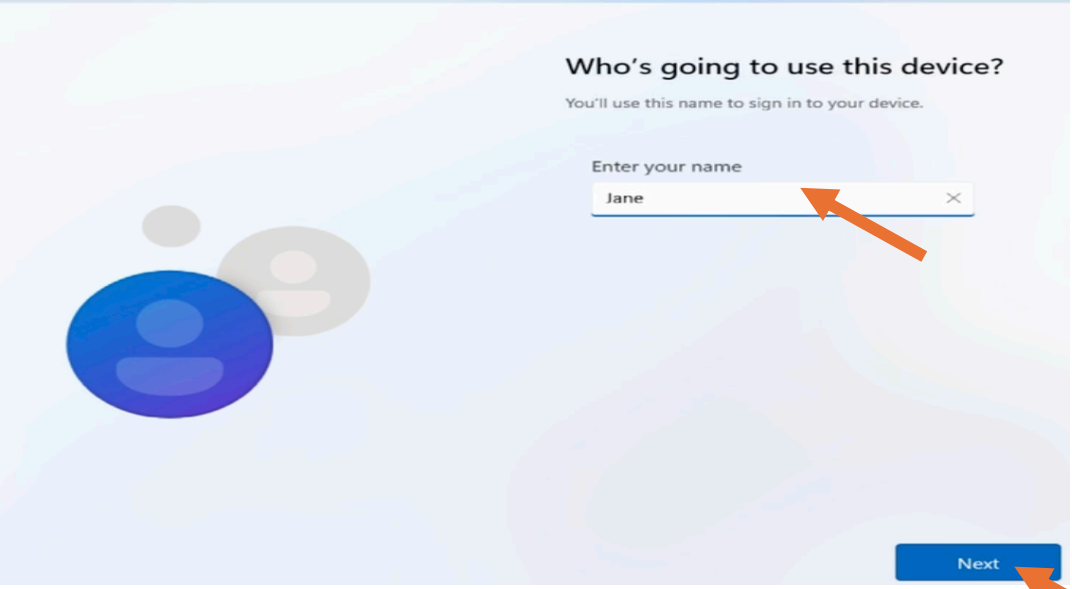
Select the Country



Select the Keyboard Layout



Create your login details “Name, Password and 3 security Questions and Answers”



Who's going to use this device?

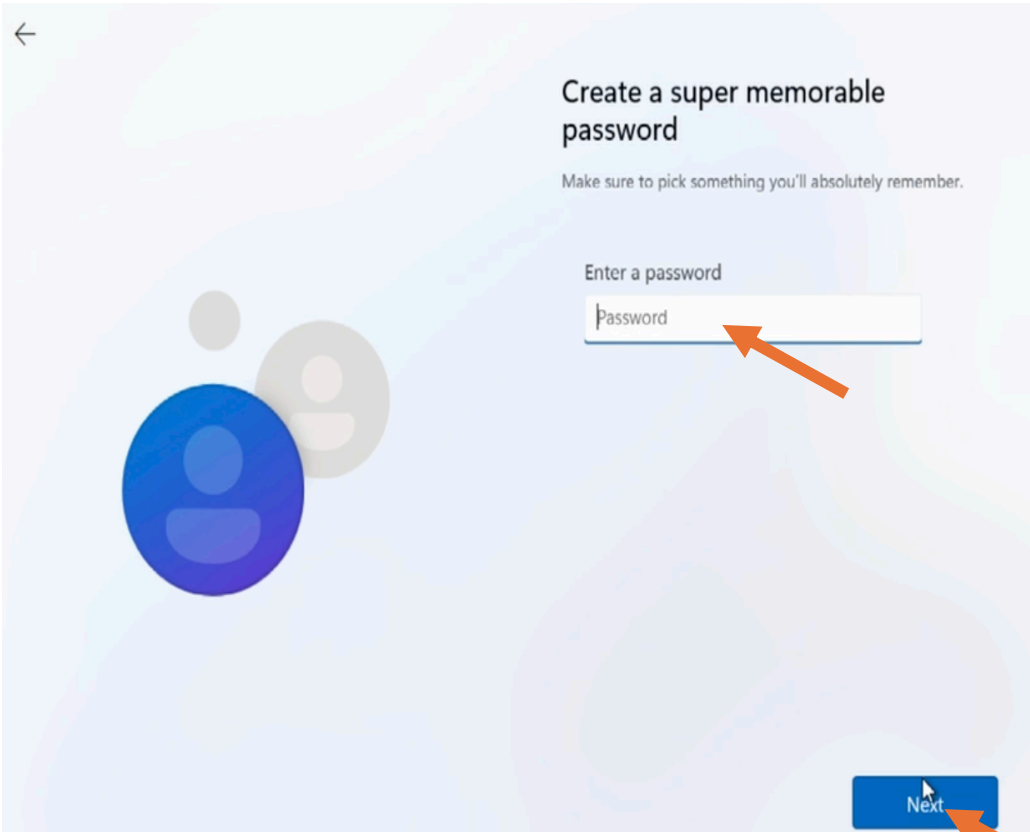
You'll use this name to sign in to your device.

Enter your name

Jane

Next

This screenshot shows the first step of the device setup process. On the left, there are three stylized user icons: a large blue one in the foreground and two smaller grey ones behind it. The main text asks 'Who's going to use this device?' and explains that the entered name will be used for sign-in. A text input field labeled 'Enter your name' contains the text 'Jane'. An orange arrow points to this input field. At the bottom right, there is a blue button labeled 'Next', with another orange arrow pointing to it.



Create a super memorable password

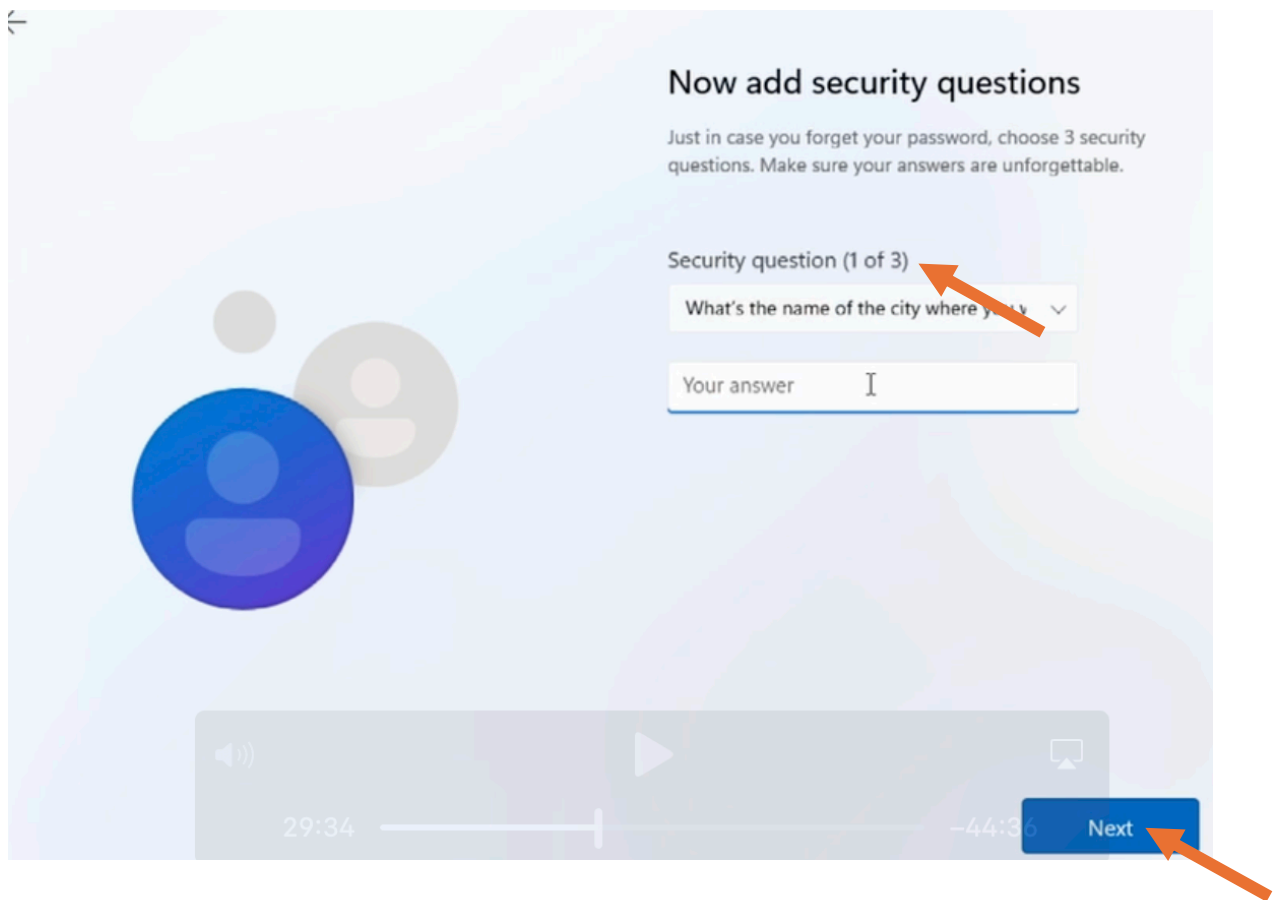
Make sure to pick something you'll absolutely remember.

Enter a password

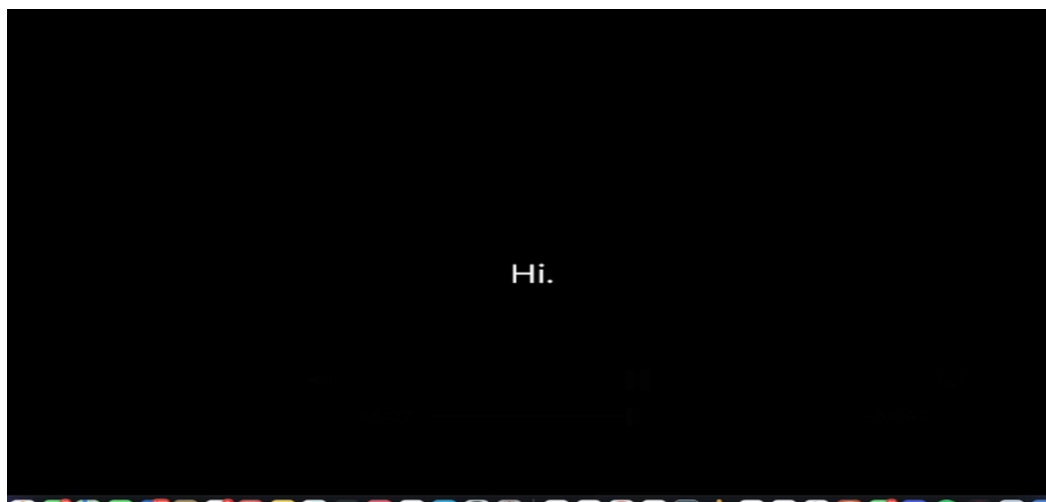
Password

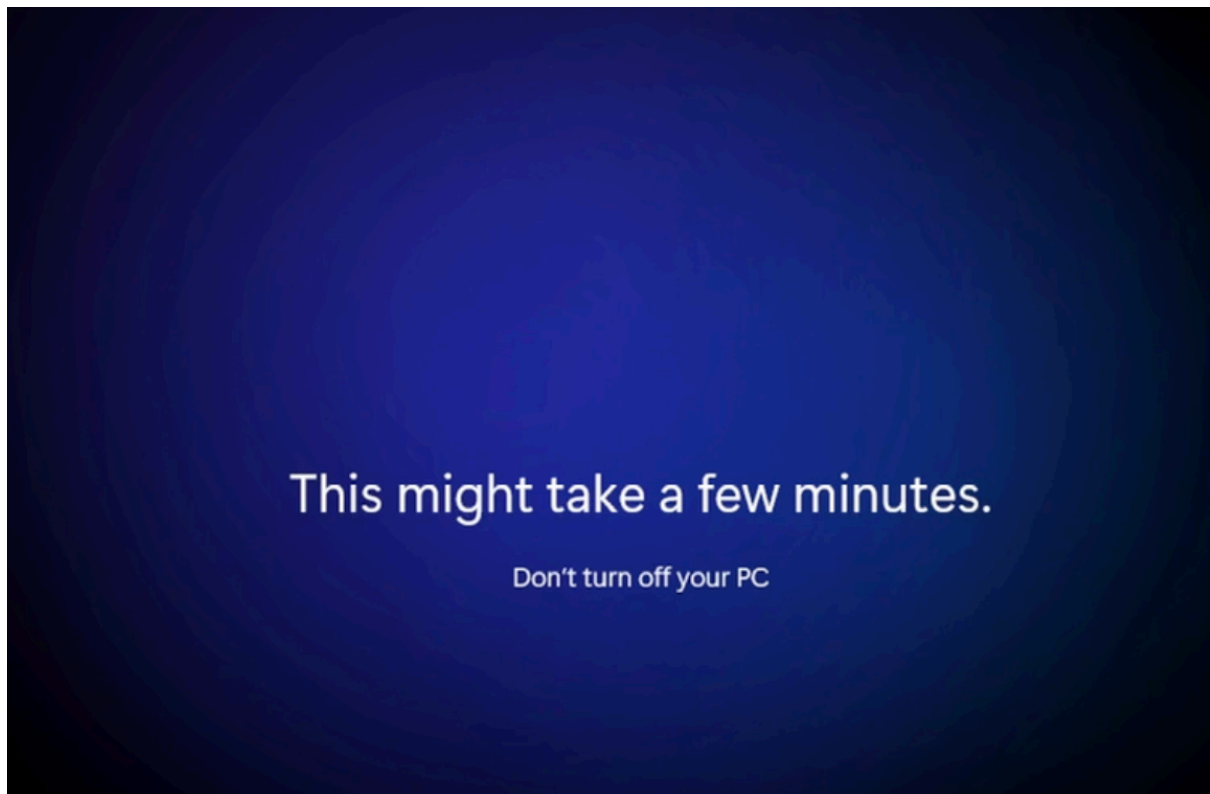
Next

This screenshot shows the second step of the device setup process. It features a back arrow in the top left corner. The main text asks 'Create a super memorable password' and advises the user to pick something they will remember. A text input field labeled 'Enter a password' contains the placeholder text 'Password'. An orange arrow points to this input field. At the bottom right, there is a blue button labeled 'Next', with another orange arrow pointing to it.

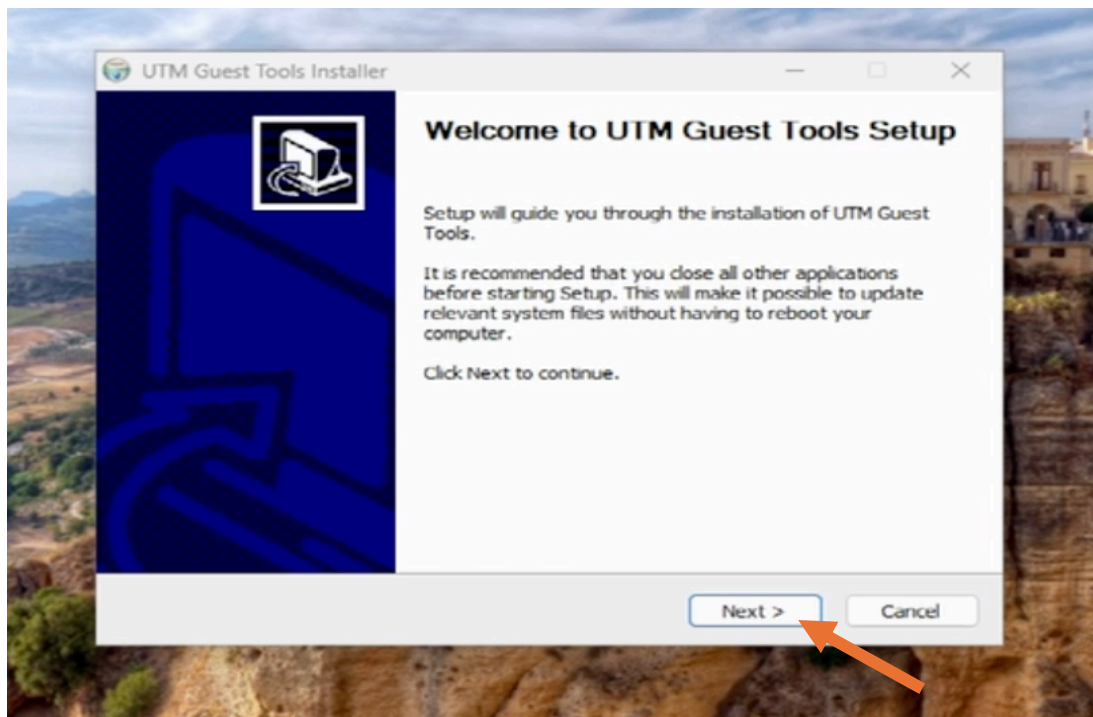


Congratulation you are now booting the windows it will take few minutes so be patient

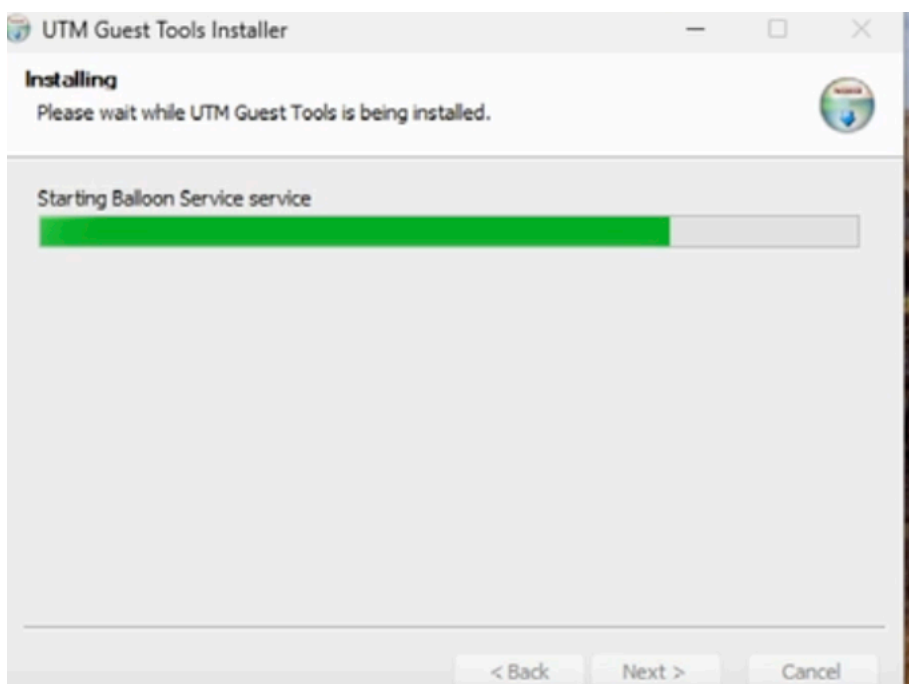
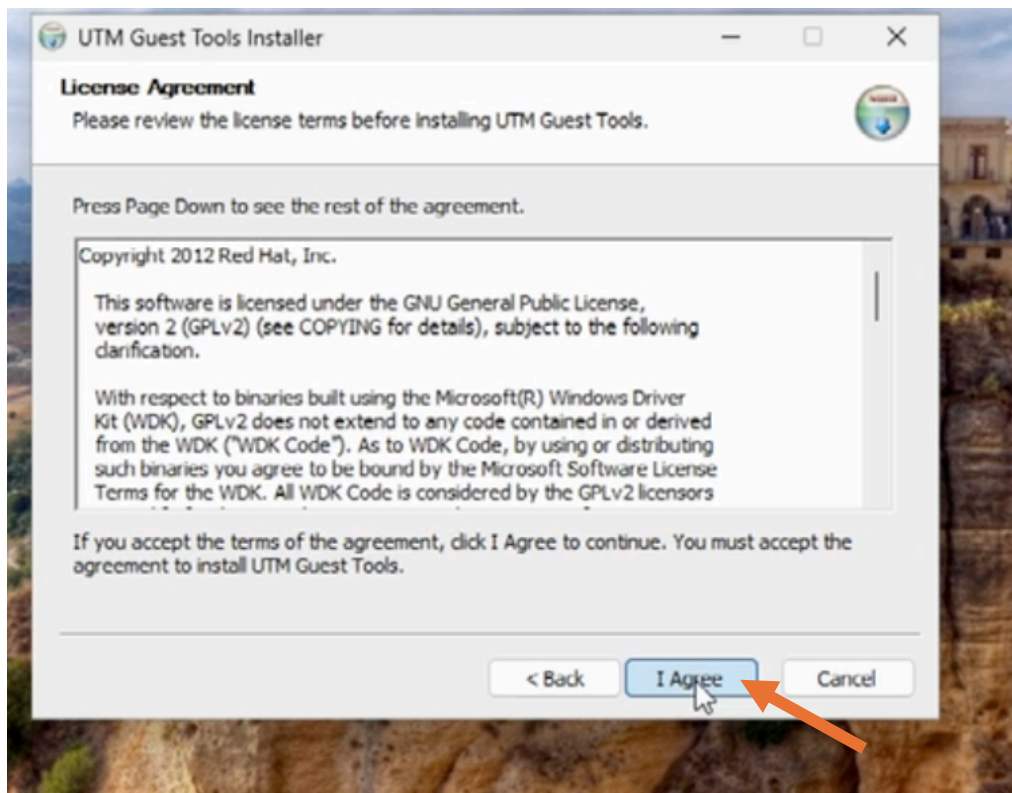


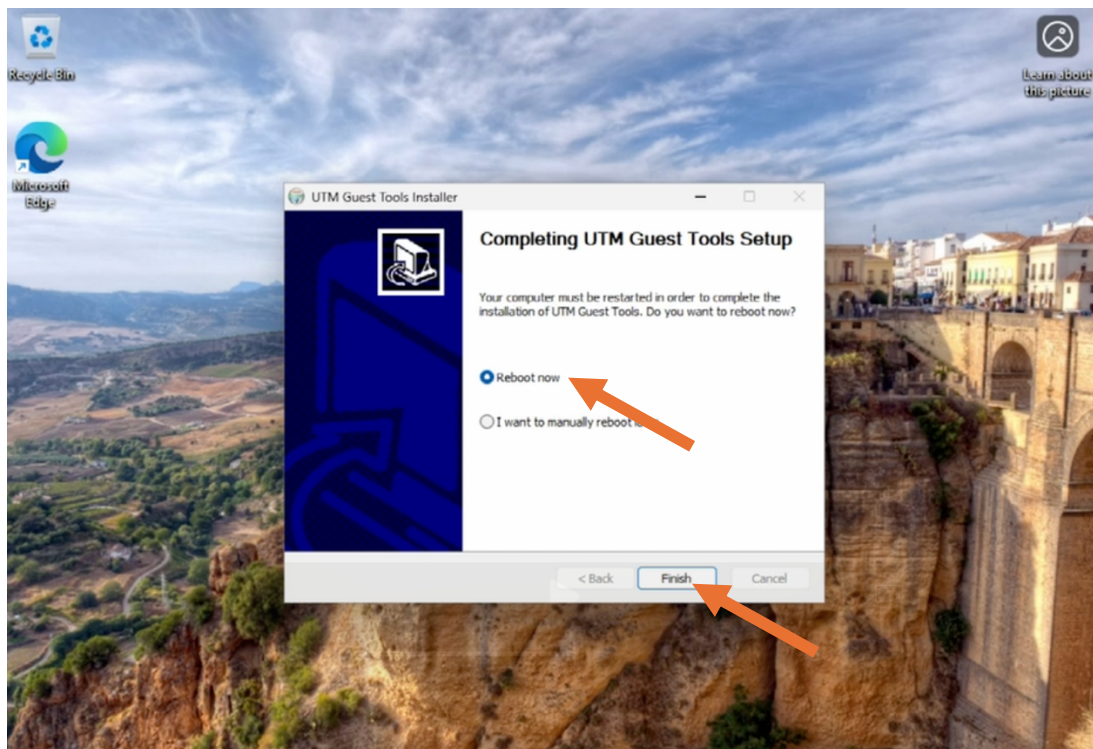


It will automatically launch the Guest Tools Installer. Click on “Next” to install the Guest Tools.



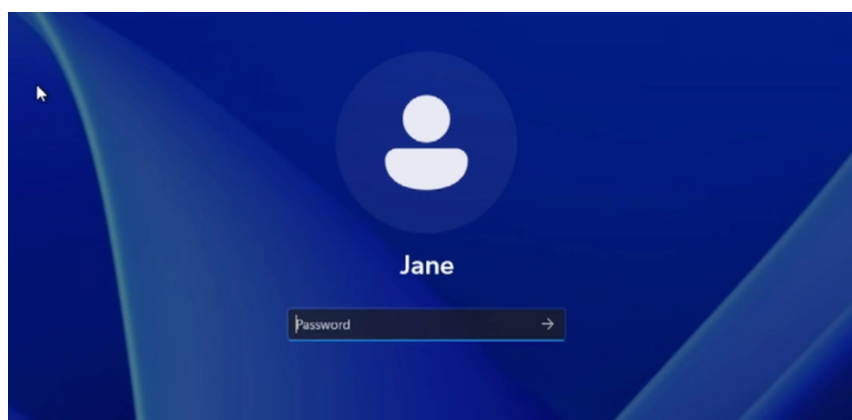
Licence Agreement: Click on “I Agree”, it will automatically be installed. Once done check “Reboot Now” and click on “Finish”.





Step 4: Install Guest Tools and Complete the Setup

- i. After windows is installed, open the UTM menu and install the UTM Guest Tools to enable better performance and additional features like clipboard sharing and resizing.
- ii. Restart the VM to apply the changes.
- iii. Adjust display resolution, keyboard preferences, and other system settings as needed.



2. Installation and Configuration of Splunk SIEM on Windows 11 Pro

Visit the Splunk website https://www.splunk.com/en_us/download/splunk-cloud.html click on Free Splunk button for 14 days trial if you don't want to be a paid customer.

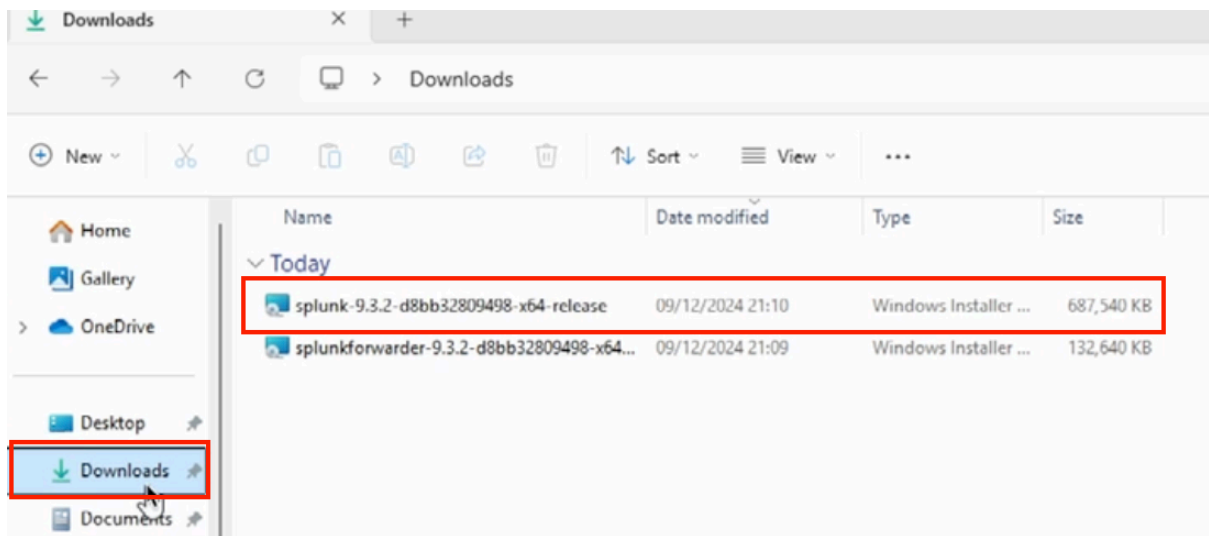
Create an account and login

The screenshot shows the Splunk Enterprise Free Trial sign-up page. The main heading is "FREE TRIAL Splunk Enterprise 9.3.2". Below it, it says "Try Splunk Enterprise free for 60 days. No credit card required." There are three bullet points describing the benefits: "Keep and manage your data in your on-premises environment with Splunk Enterprise.", "Start searching, analyzing and visualizing your data on powerful, easy-to-understand dashboards.", and "Install on Windows or Linux to get insights from all parts of your multicloud and hybrid environment." Below these, it says "Once you sign up for the Splunk Enterprise trial, you'll see how it helps you to:" followed by four bullet points: "Tackle your hardest security and observability use cases.", "Stream, collect and index any data at any scale.", "Set up real-time alerts so you can act fast.", and "Customize for your unique business needs with free, pre-built apps from Splunkbase." On the right side, there is a "Start Your Free Download" form with fields for "Business Email", "Password", "First Name", "Last Name", "Job Title", "Phone Number", and "Company". There is also a "Log In" link for existing users.

Download .msi installer

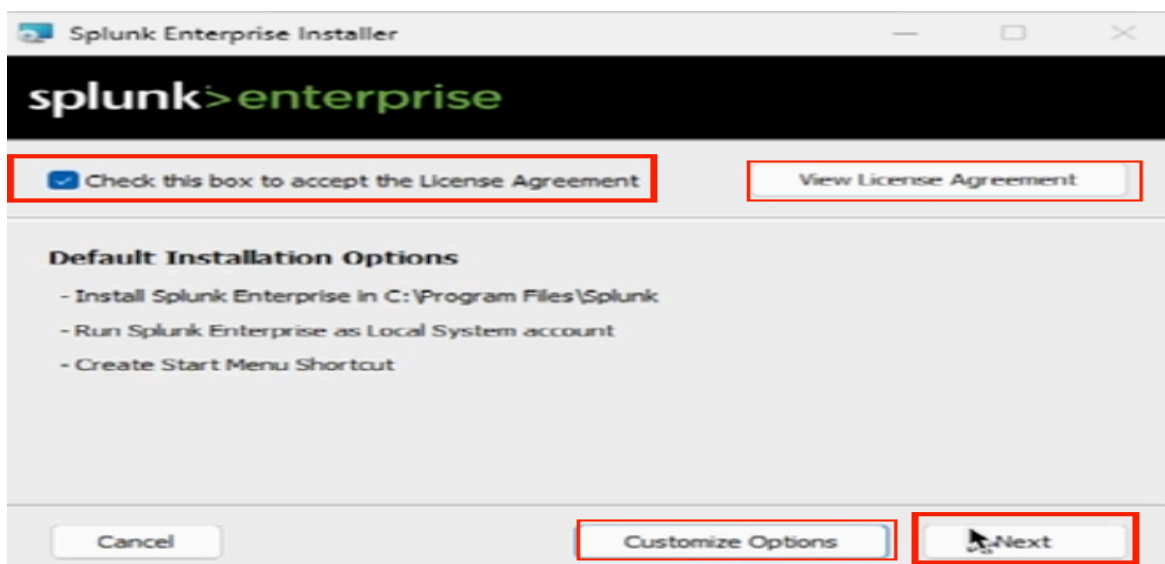
The screenshot shows the Splunk Enterprise 9.3.2 download page. The main heading is "GET STARTED Choose Your Download". Below it, it says "Splunk Enterprise 9.3.2" and "Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments." Below this, it says "Choose Your Installation Package" and there are three tabs: "Windows", "Linux", and "Mac OS". The "Windows" tab is selected. Below the tabs, there is a table of download links. The table has columns for "Architecture", "Operating System", "File Format", "File Size", "Download Now", "Copy wget link", and "More". The first row is highlighted with a red box and contains the following information: "64-bit", "Windows 10 Windows Server 2019, 2022", ".msi", "671.43 MB", "Download Now", "Copy wget link", and "More".

Architecture	Operating System	File Format	File Size	Download Now	Copy wget link	More
64-bit	Windows 10 Windows Server 2019, 2022	.msi	671.43 MB	Download Now	Copy wget link	More

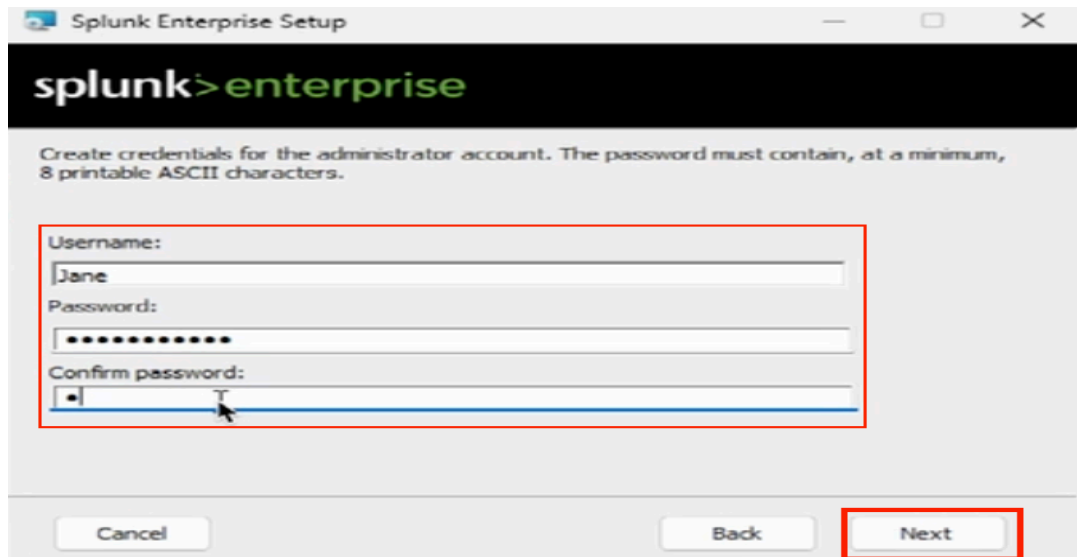


View and read the Licence Agreement for better understanding of how your data will be use.

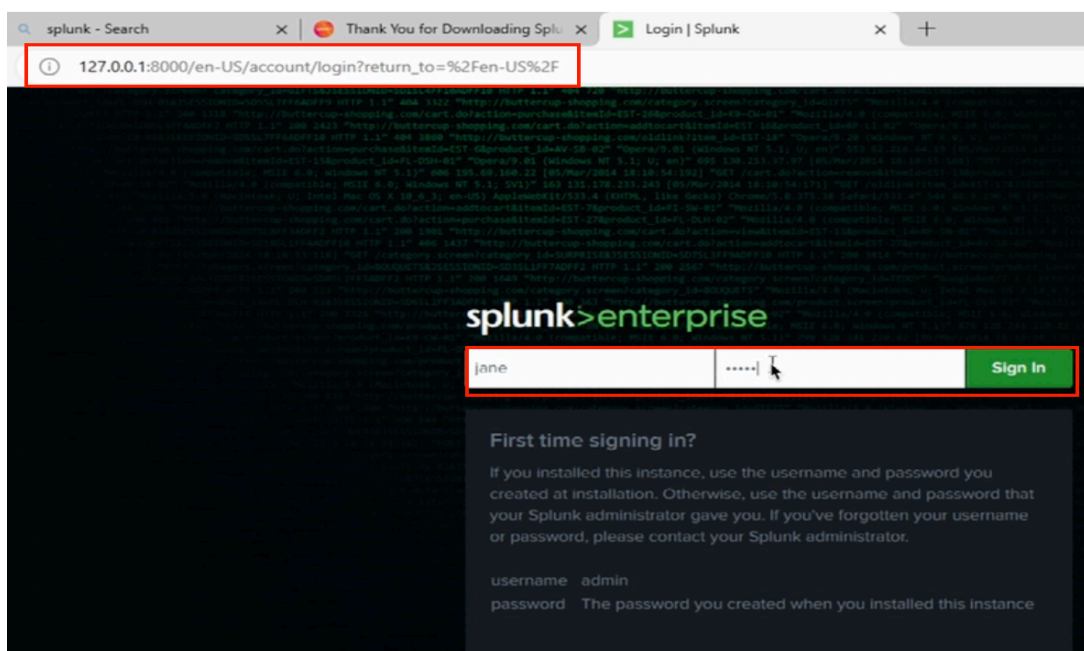
Check the box and accept the Licence Agreement, customize Options will be automatically selected but if not press the button, and click Next

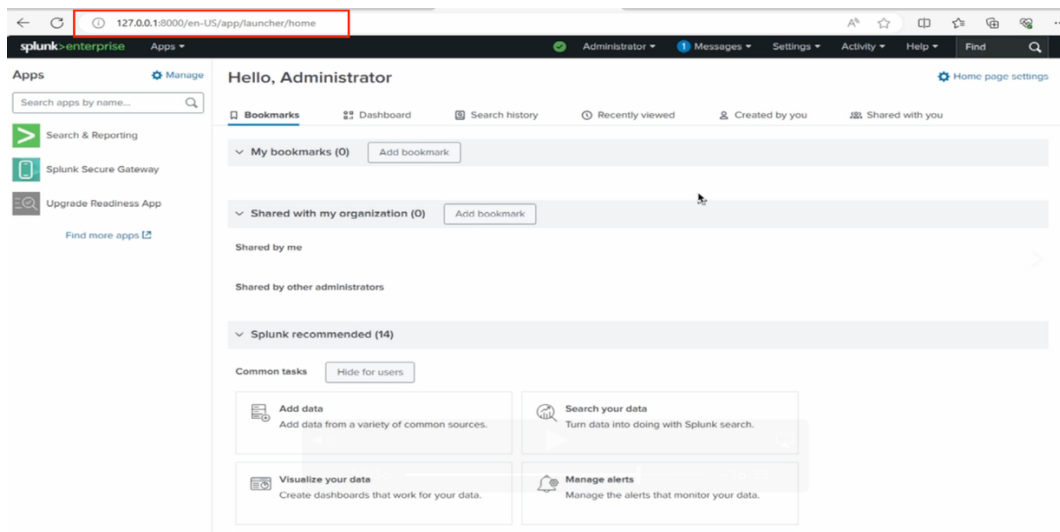


Select where you want to install Splunk
Install Splunk as local System
Set Username and Password and click Next

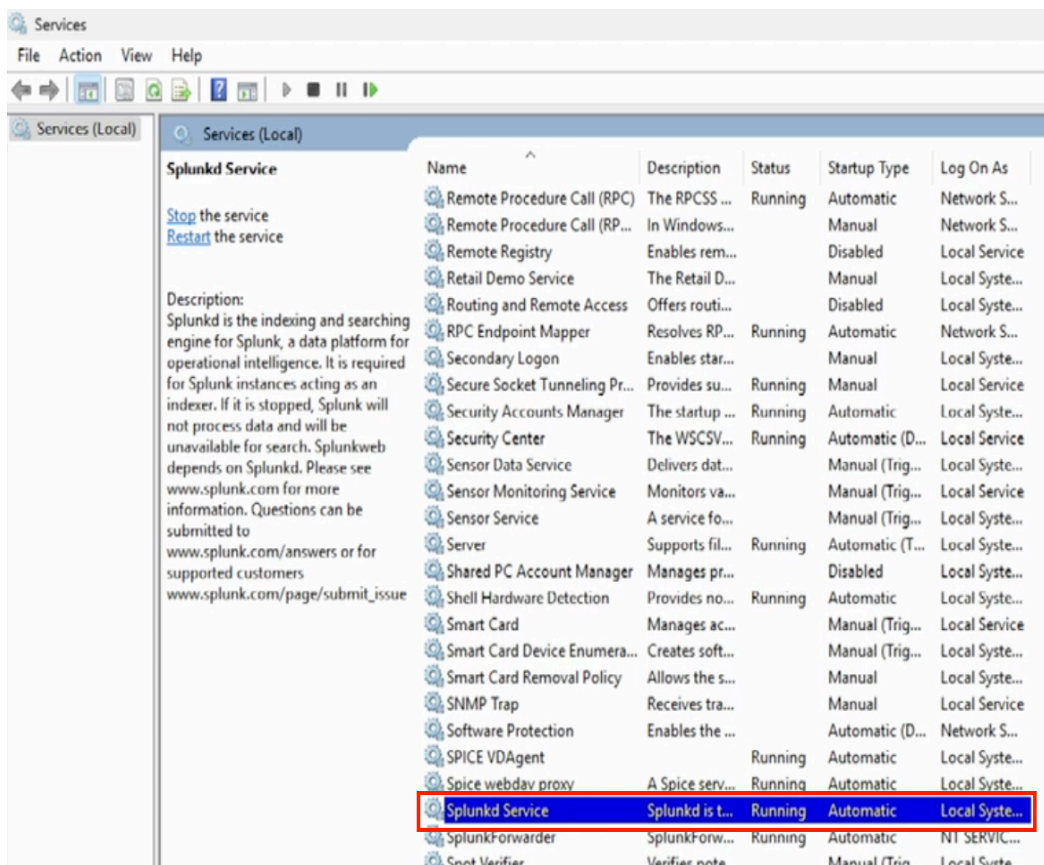


Launch the install and wait for the installation
Once done check the Splunk installation via <https://127.0.0.1:8000> if it didn't open automatically
Login with the Username and Password created





Check the Splunk Service Status. Type services on the Windows search to find Splunkd Service. Monitor the service, status and startup type, check the state of the Splunk it must be in running status.



3. Installation and Configuration of Splunk Universal Forwarder

Visit the Splunk website https://www.splunk.com/en_us/download/universal-forwarder.html

Download the windows 10, Windows 11 ... msi setup file

Splunk Universal Forwarder 9.3.2

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

Choose Your Installation Package

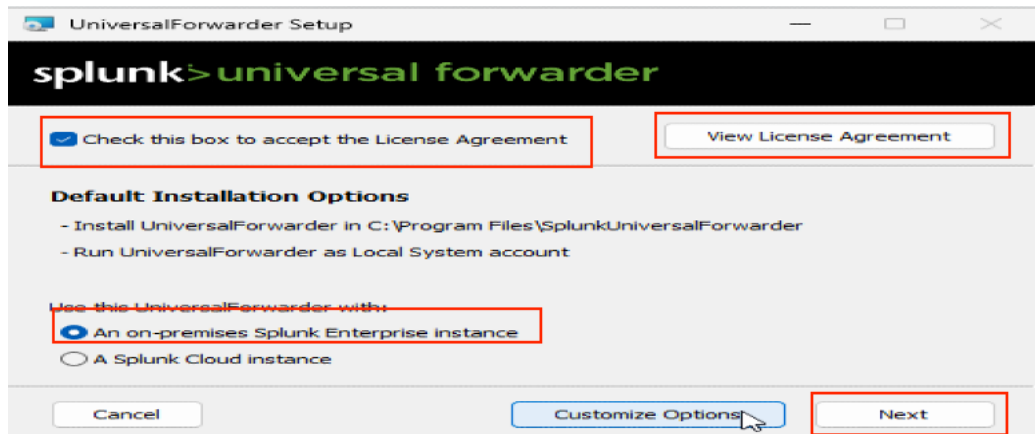
Windows Linux Mac OS Free BSD Solaris AIX

64-bit Windows 10, 11 Windows Server 2019, 2022 .msi 129.53 MB Download Now Copy wget link More

Launch the Splunk Universal Forwarder

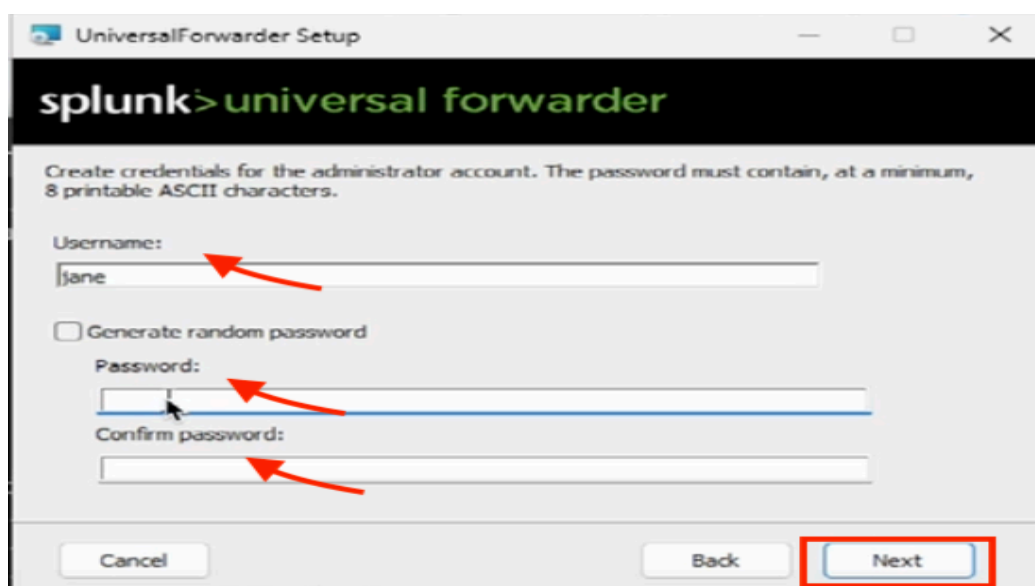
View and read the Licence Agreement for better understanding of how your data will be use.

Check the box and accept the Licence Agreement, select “an on-permises Splunk Enterprise instance” if you want to use op-permise server and click Next.

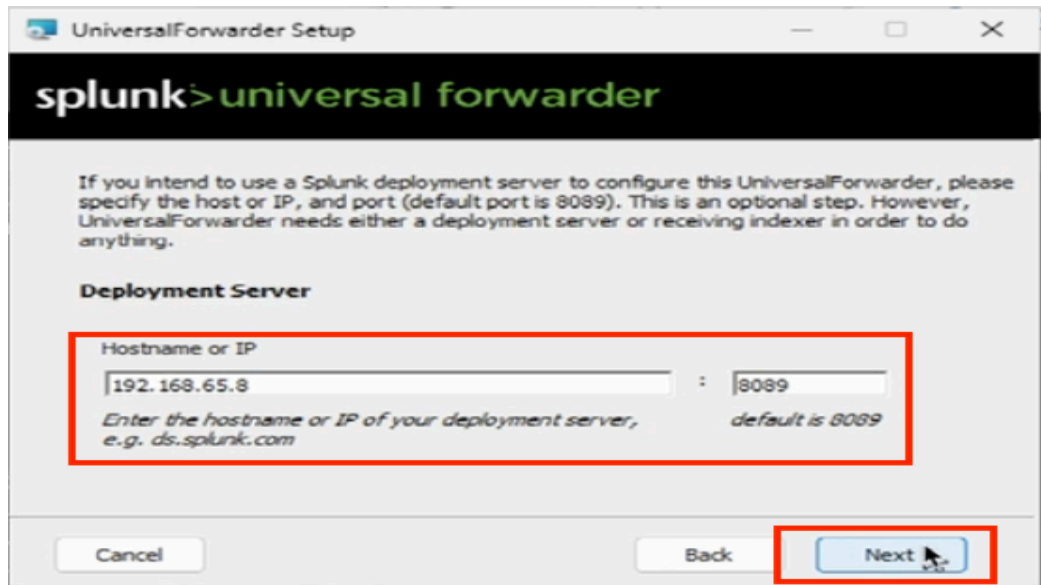


Set Username and Password to the Universal Forwarder and click Next

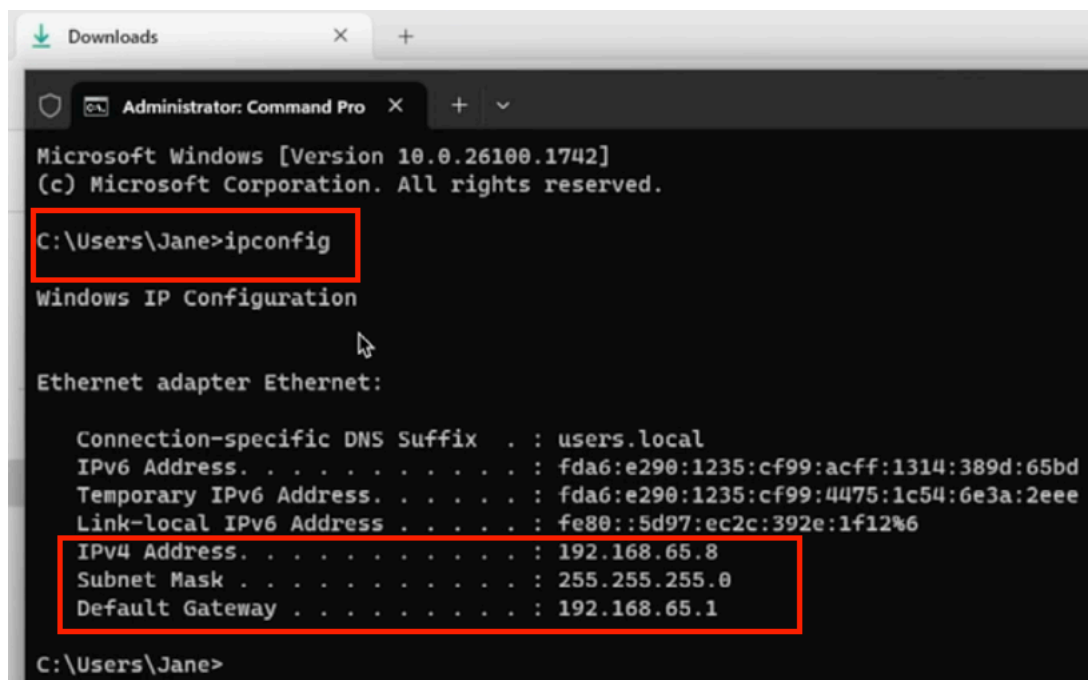
Note you can check Generate random password if you want randomized password



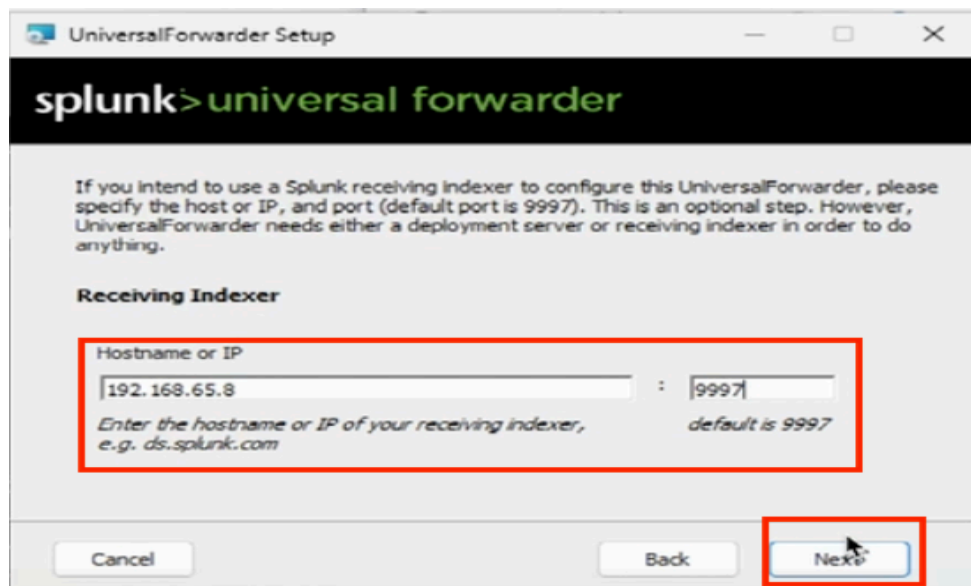
Write the server IP and the port to the Deployment Server and Click Next
Note: Splunk is installed on MacOS machine so the IP address of the machine is used



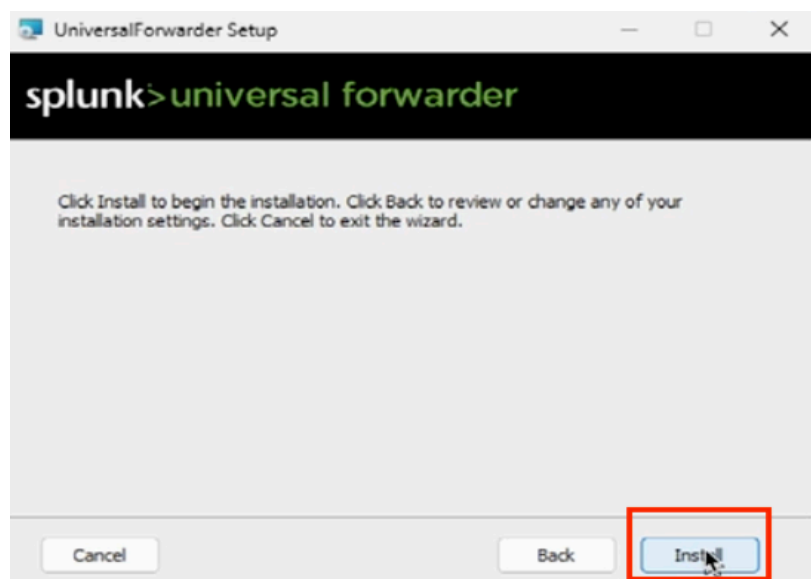
Type CMD on the Windows search bar to open the command prompt, run “ipconfig” as shown in the diagram to get the IP address of the machine.



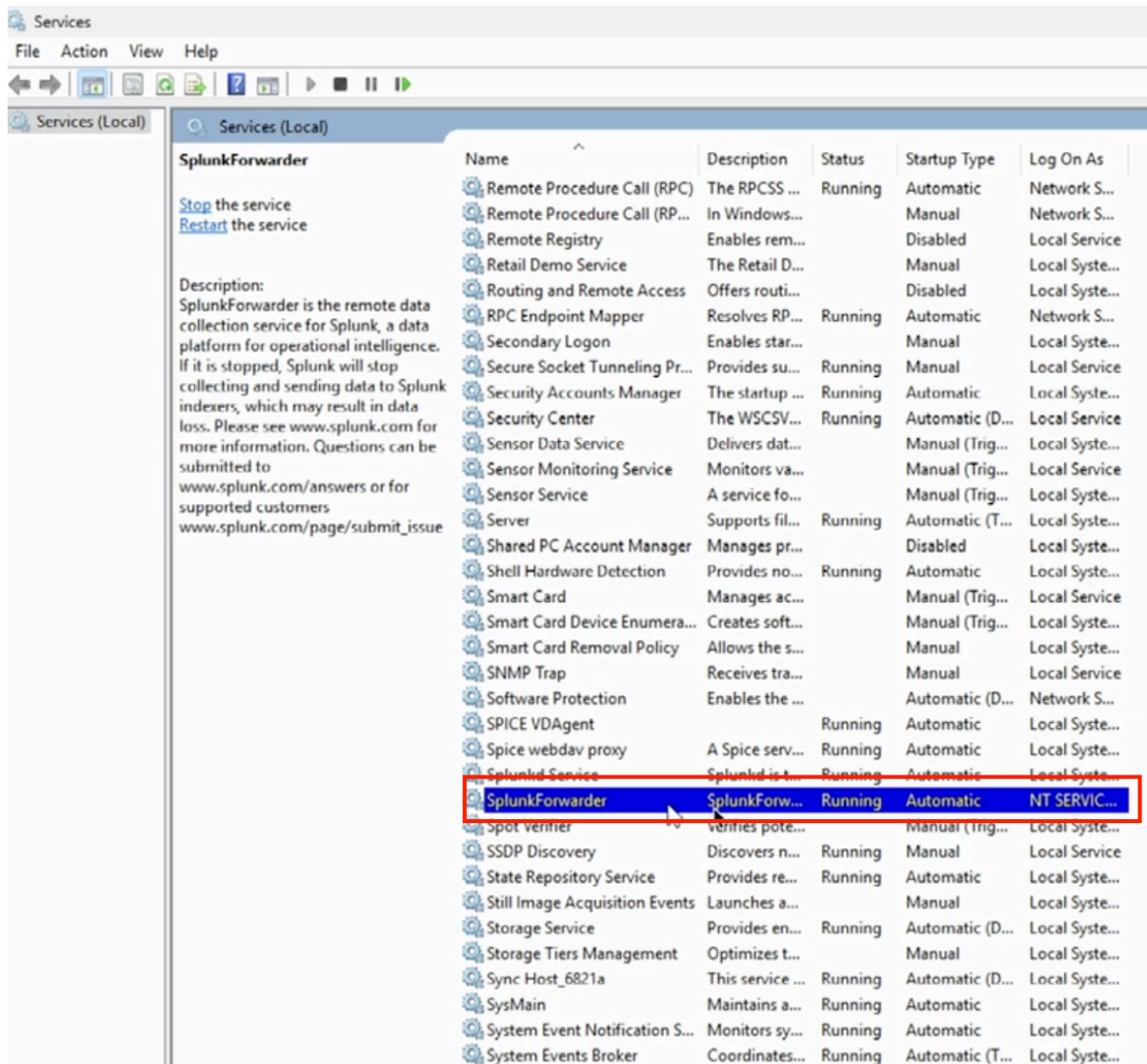
Write the server IP address which is the same as the Deployment server and port which is 9997 “Note: 9997 is a default port” to the Receiving Indexer and click Next



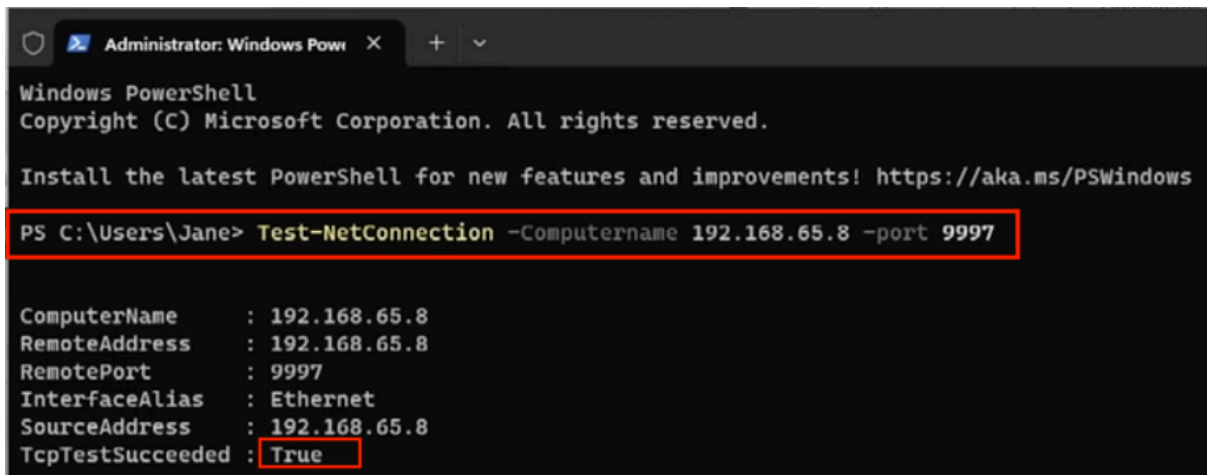
Launch the install



Check the Splunk Universal Forwarder Service Status. Type services on the Windows search to find Splunkforwarder Service. Monitor the service, status and startup type, check the state of the Splunk Universal Forwarder to see if it is up. The status must be running.



Use PowerShell command to Check if the communication is open type “Test-NetConnection -Computername 192.168.65.8 -port 9997”



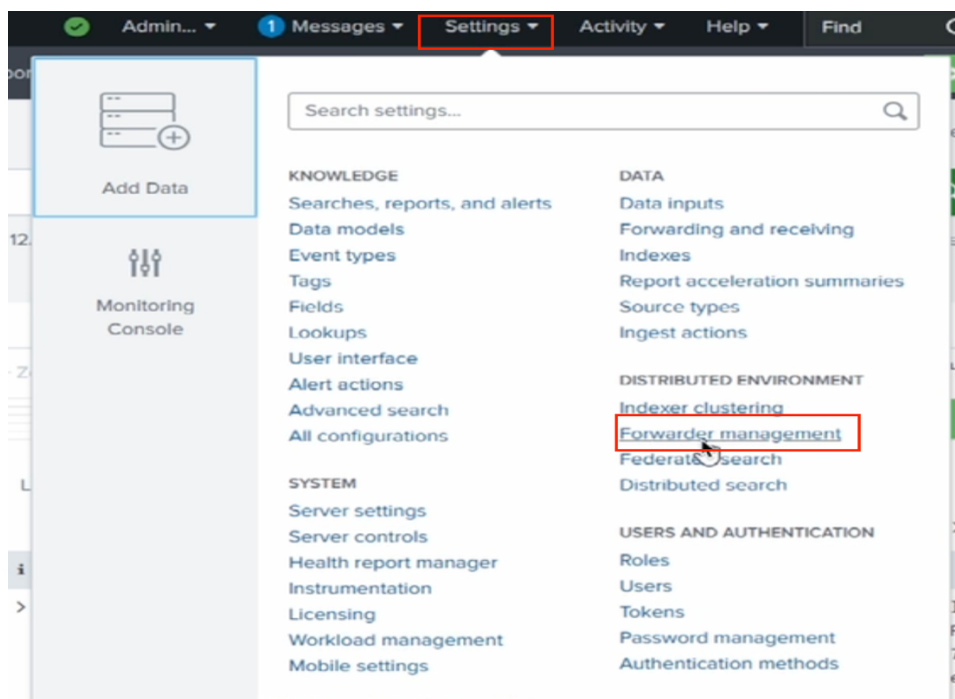
```
Administrator: Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

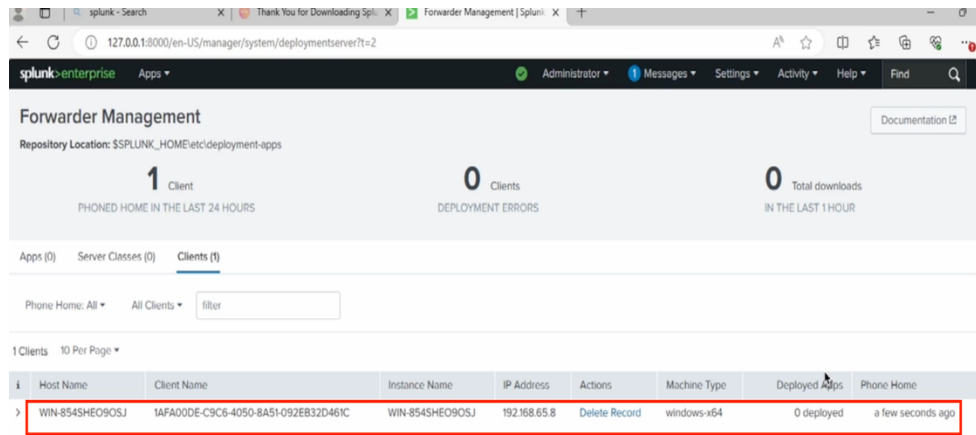
PS C:\Users\Jane> Test-NetConnection -Computername 192.168.65.8 -port 9997

ComputerName      : 192.168.65.8
RemoteAddress     : 192.168.65.8
RemotePort        : 9997
InterfaceAlias    : Ethernet
SourceAddress     : 192.168.65.8
TcpTestSucceeded  : True
```

Check the connection between client and server is okay, go to Splunk server, Setting then click on Forwarder management

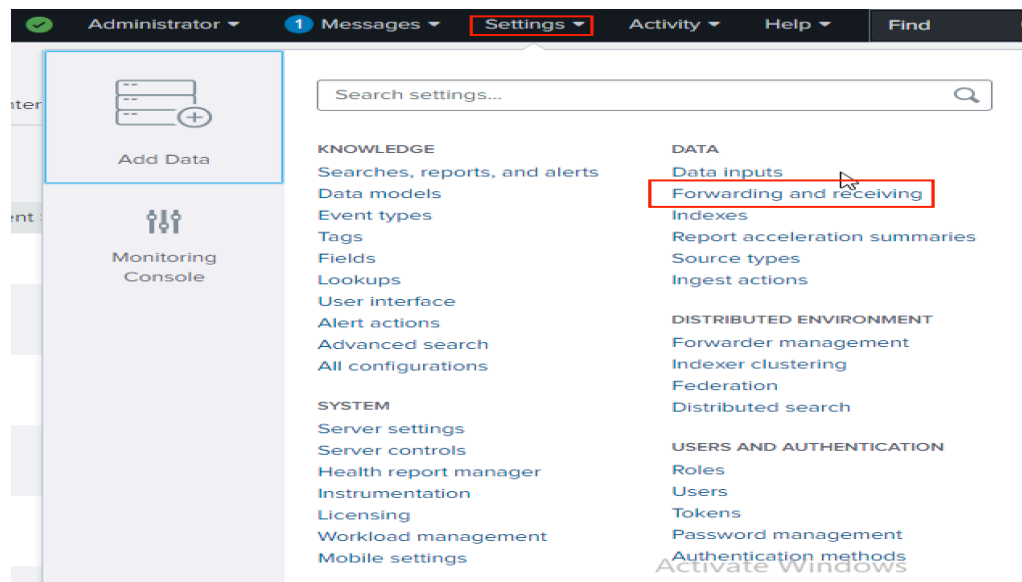


Forwarder Management: your Windows Computer must show on this page. If the computer didn't show after few minutes, restart Splunk Universal Forwarder service.

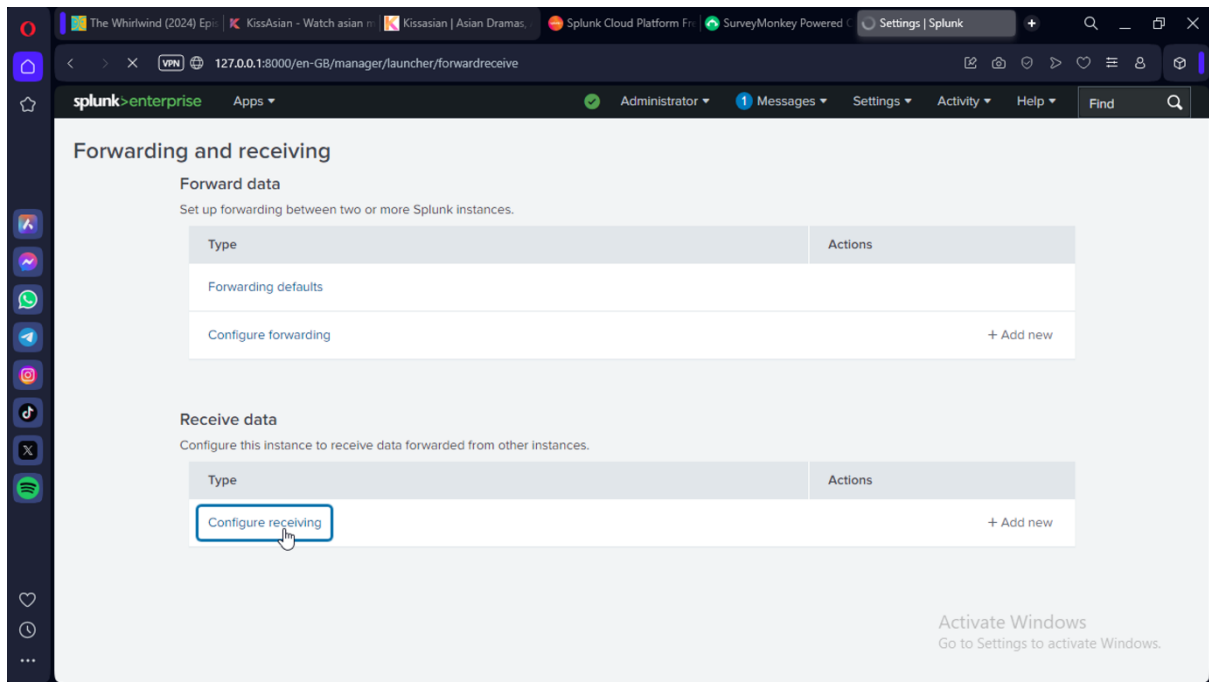


4. Detailed function of Splunk SIEM Service

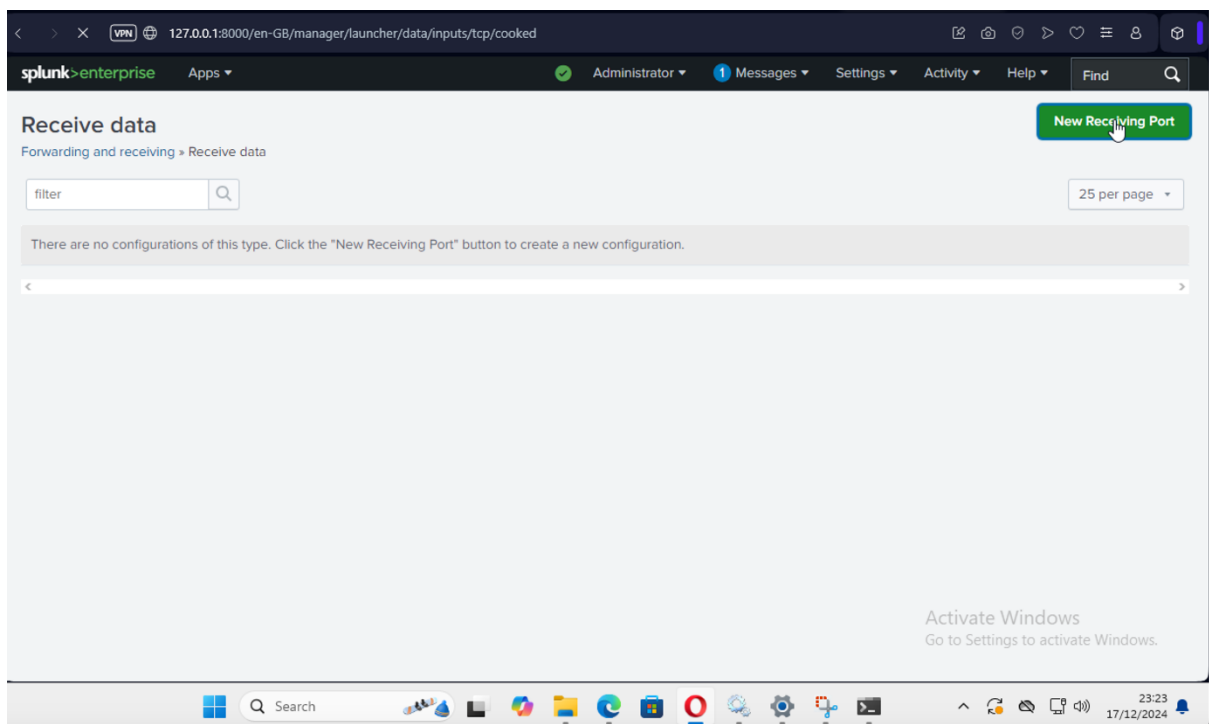
Receiving and Forwarding on Splunk Server: Click Settings> Forwarding and Receiving

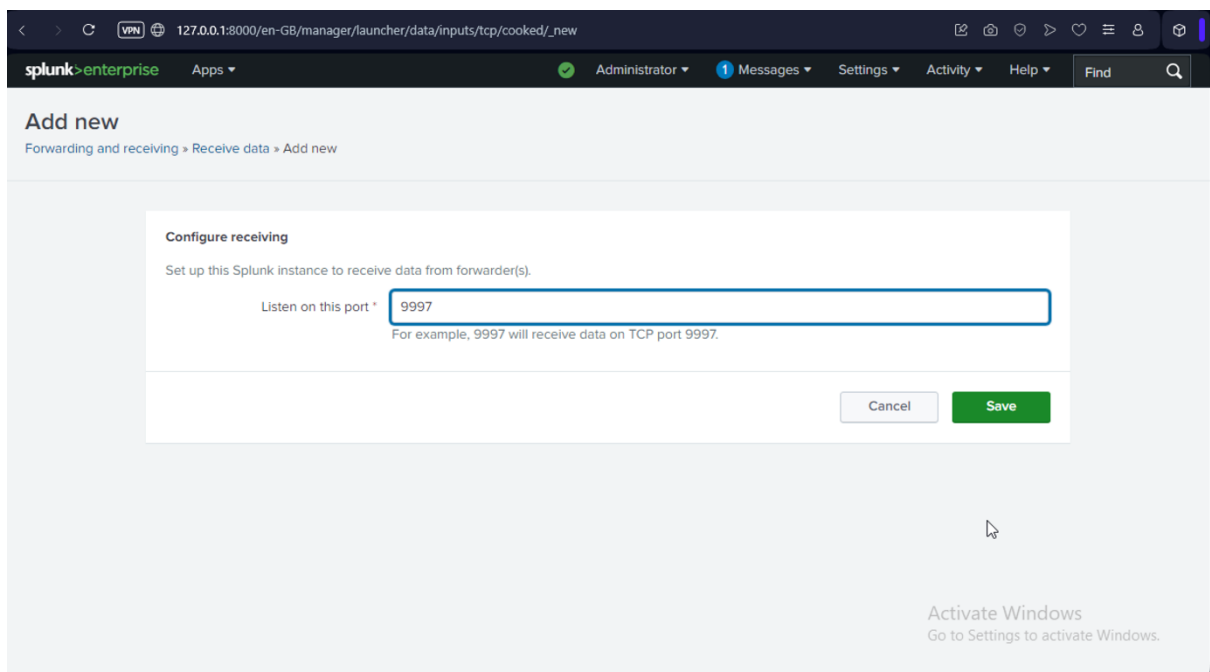
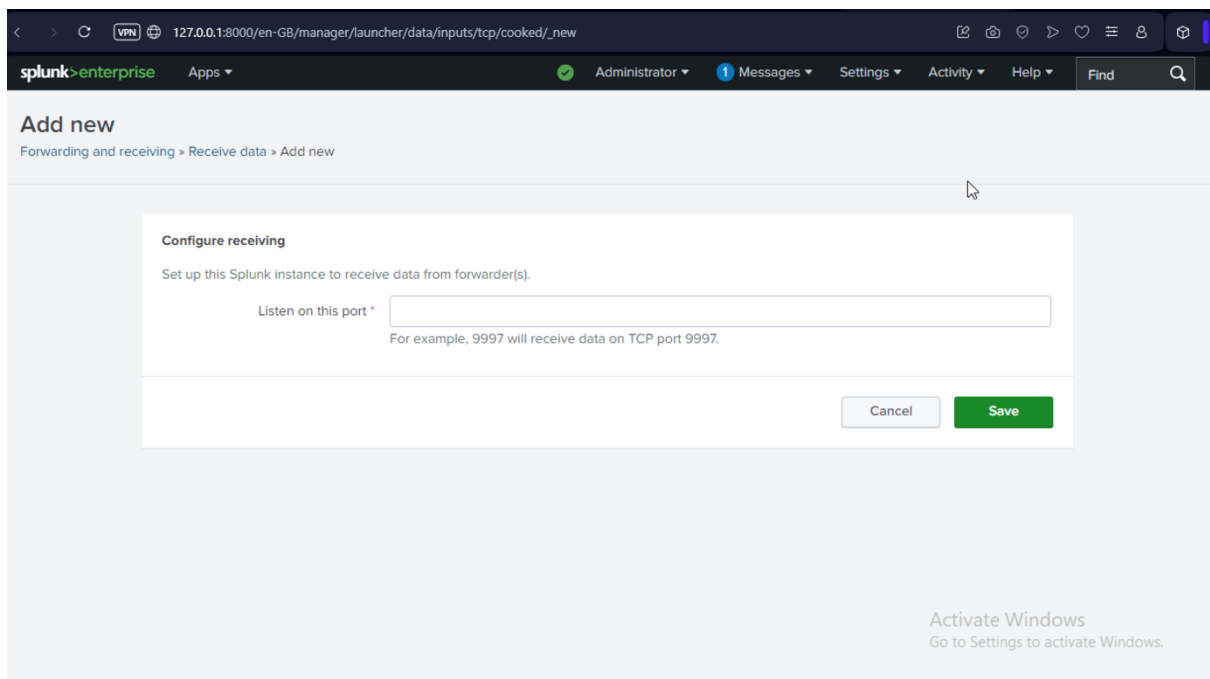


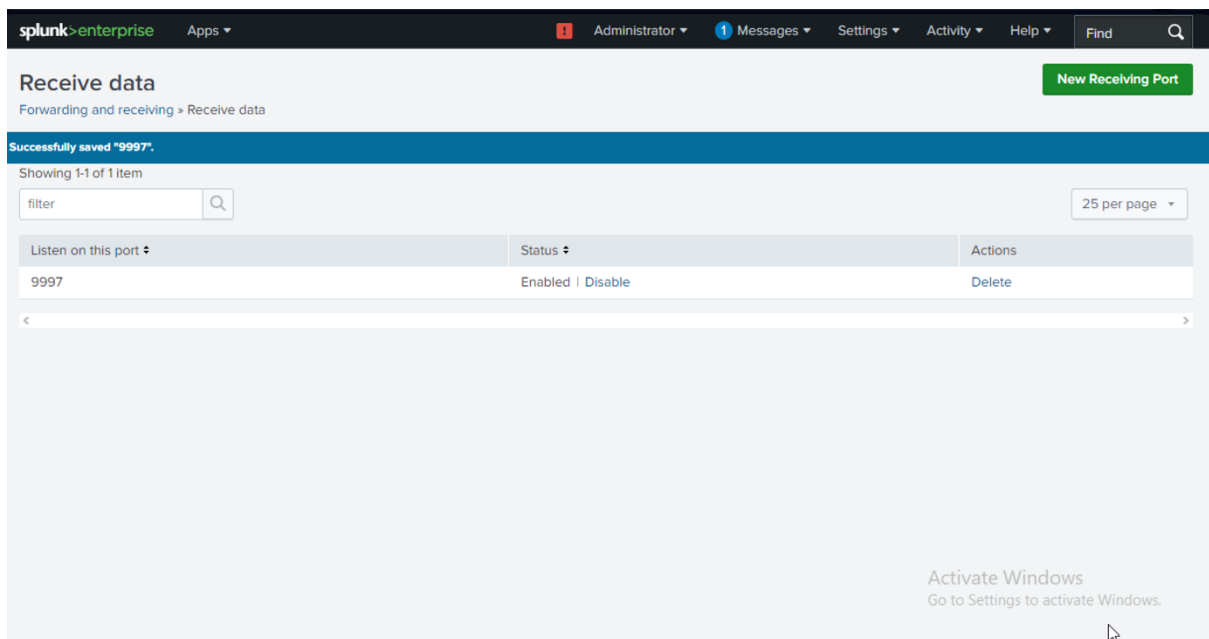
To view the available port for receiving data click on Configure receiving,



If no port shows click on New Receiving Port and add port 9997 which is the default port and click on Save. NOTE: for this tutorial we are using “default Port”.

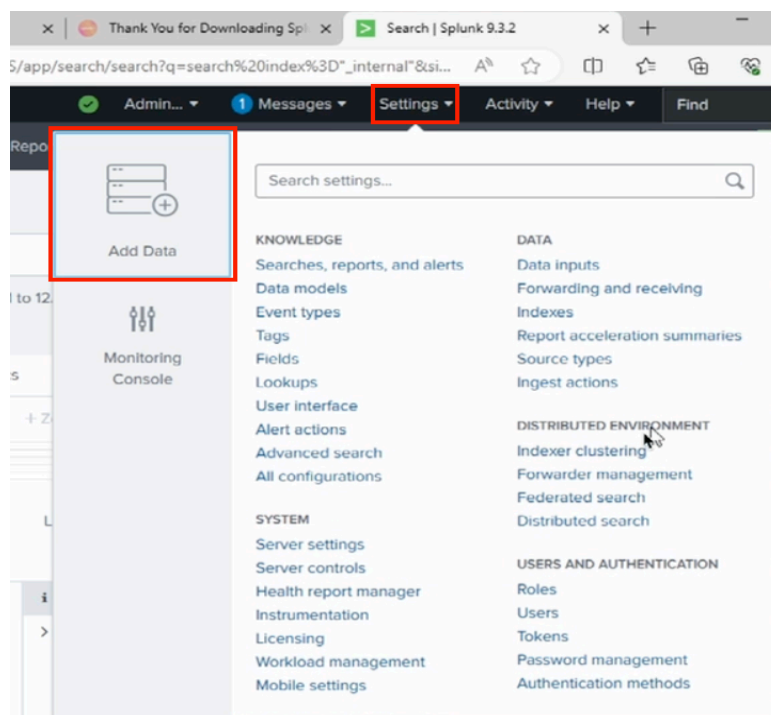


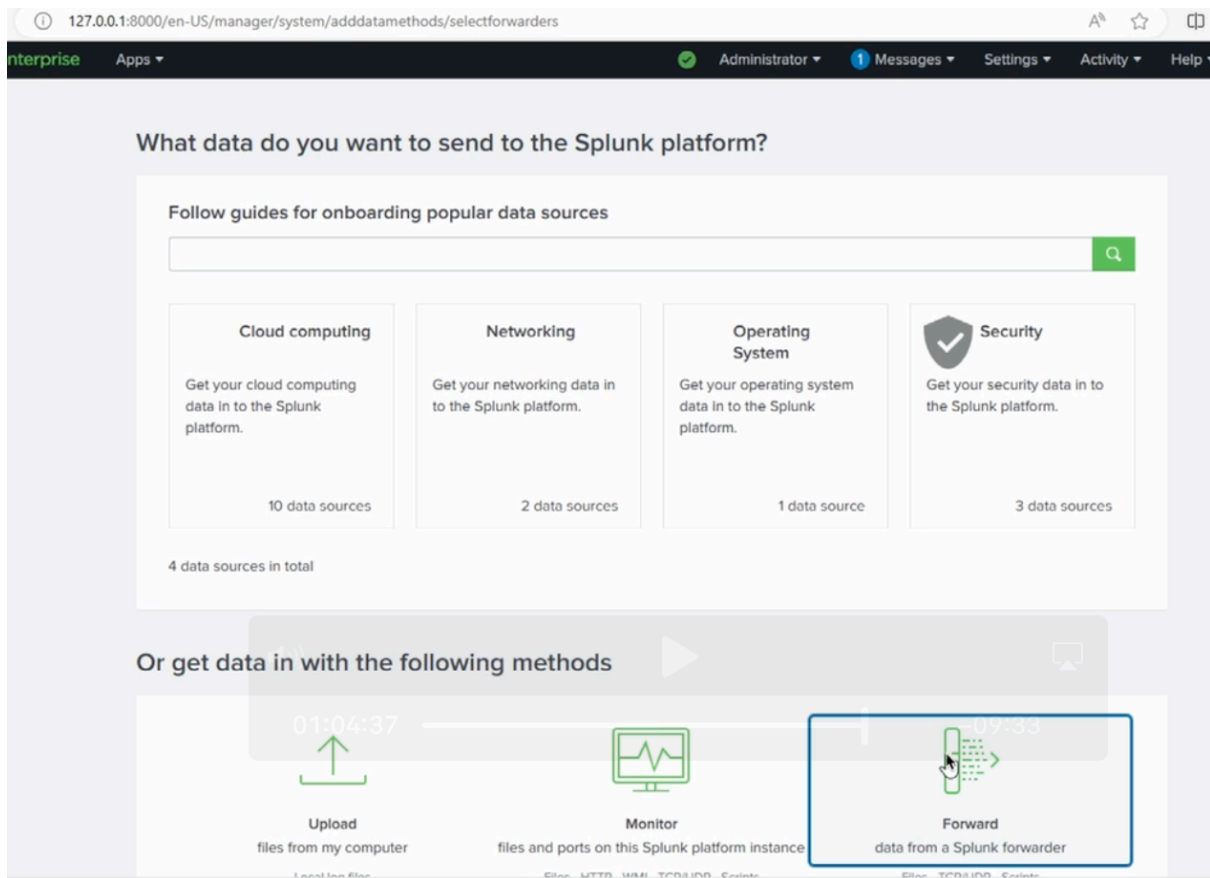




Add Data from Forwarder

Go to Settings click Add Data
Select Forward below





We added our computer to the selected host and gave it a New Server Class Name to do that Click on Add All to add the Available host to the Selected Host, then Click on Existing to select the Server Class create a New Server Class Name and click next

← 127.0.0.1:8000/en-US/manager/system/adddatamethods/selectforwarders

splunk>enterprise Apps Administrator 1 Messages Settings

Add Data Select Forwarders Select Source Input Settings Review Done < Back Next >

Select Forwarders

Create or select a server class for data inputs. Use this page only in a single-instance Splunk environment.

To enable forwarding of data from deployment clients to this instance, set the output configurations on your forwarders. [Learn More](#)

Select Server Class New Existing

Available host(s) add all Selected host(s) remove all

Available host(s)	Selected host(s)
WIN-854SHEO9OSJ WINDOWS	WIN-854SHEO9OSJ WINDOWS

New Server Class Name WIN-854SHEO9OSJ

Select Forwarders

Create or select a server class for data inputs. Use this page only in a single-instance Splunk environment.

To enable forwarding of data from deployment clients to this instance, set the output configurations on your forwarders. [Learn More](#)

Select Server Class New Existing

Server Class -- Select --

- ✓ -- Select --
- WIN-854SHEO9OSJ

FAQ

← 127.0.0.1:8000/en-US/manager/system/adddatamethods/selectforwarders

splunk>enterprise Apps Administrator 1 Messages Settings

Add Data Select Forwarders Select Source Input Settings Review Done < Back Next >

Select Forwarders

Create or select a server class for data inputs. Use this page only in a single-instance Splunk environment.

To enable forwarding of data from deployment clients to this instance, set the output configurations on your forwarders. [Learn More](#)

Select Server Class New Existing

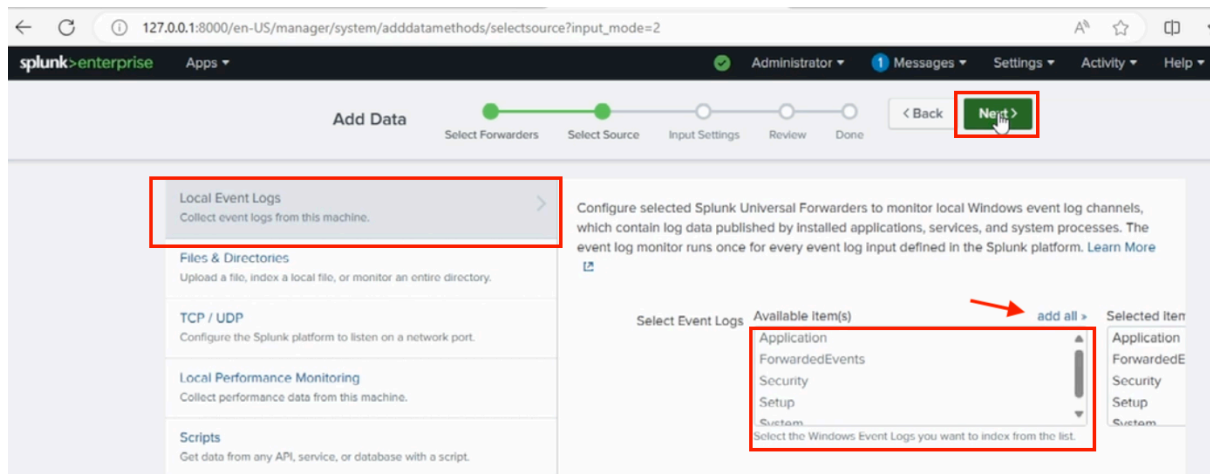
Server Class WIN-854SHEO9OSJ

List of Forwarders WINDOWS | WIN-854SHEO9OSJ

Monitoring:

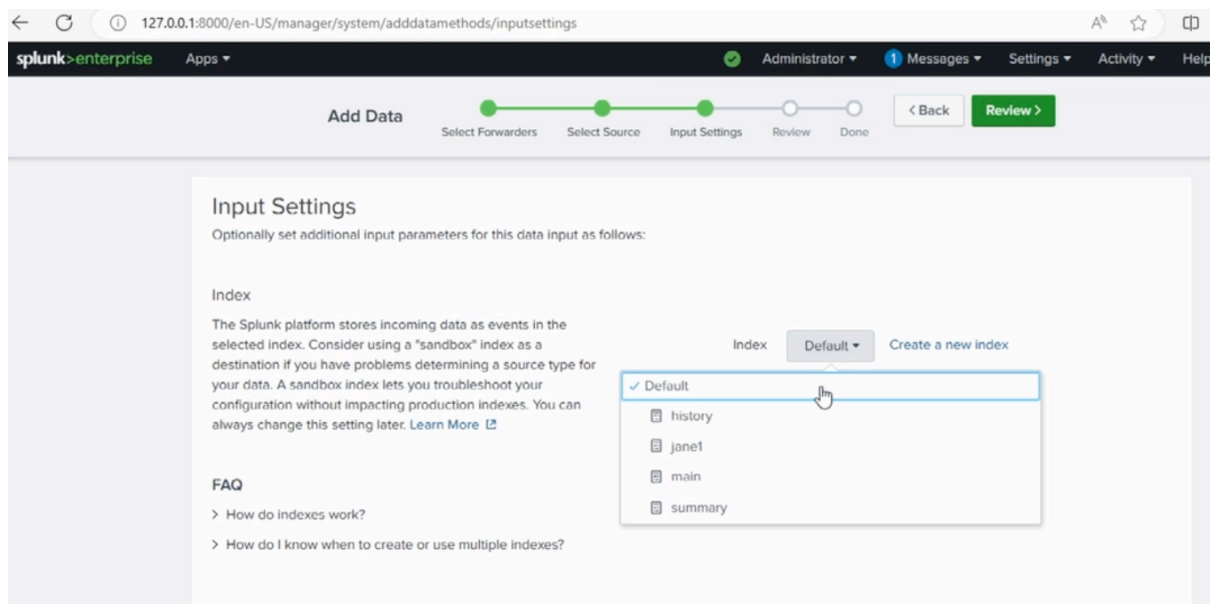
You can specify what you want to monitor but in this tutorial, we monitored local event logs from our computer as shown below.

Select Local Event Logs > Add All > Next



Select where the index will be allocated

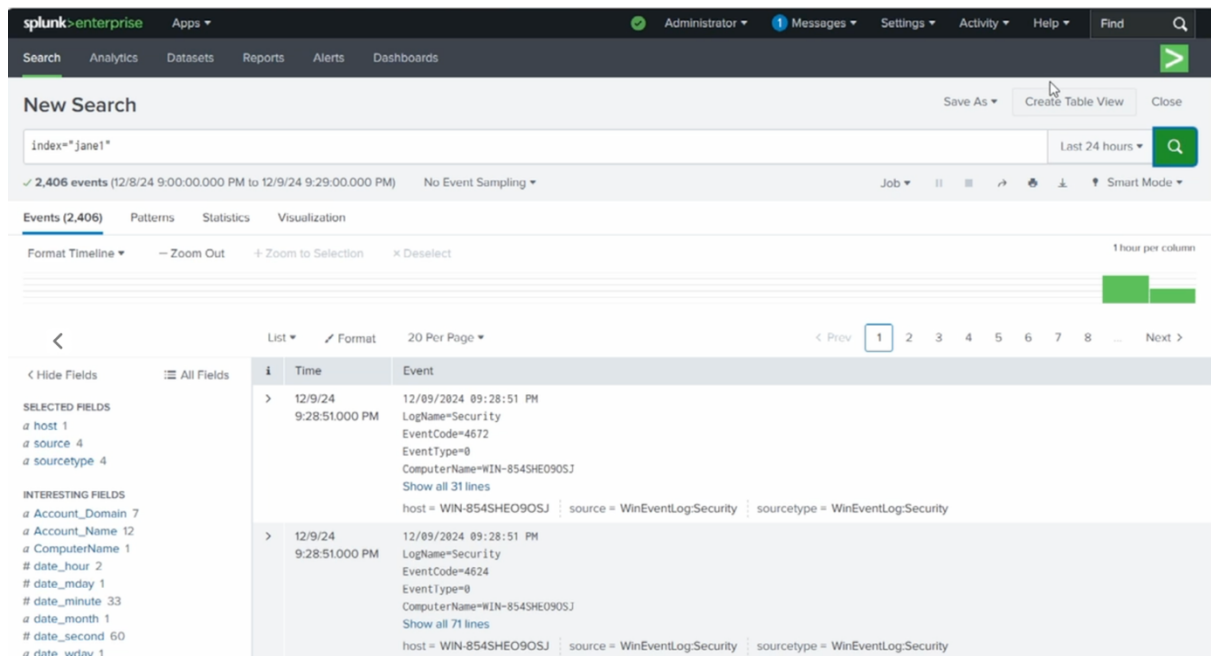
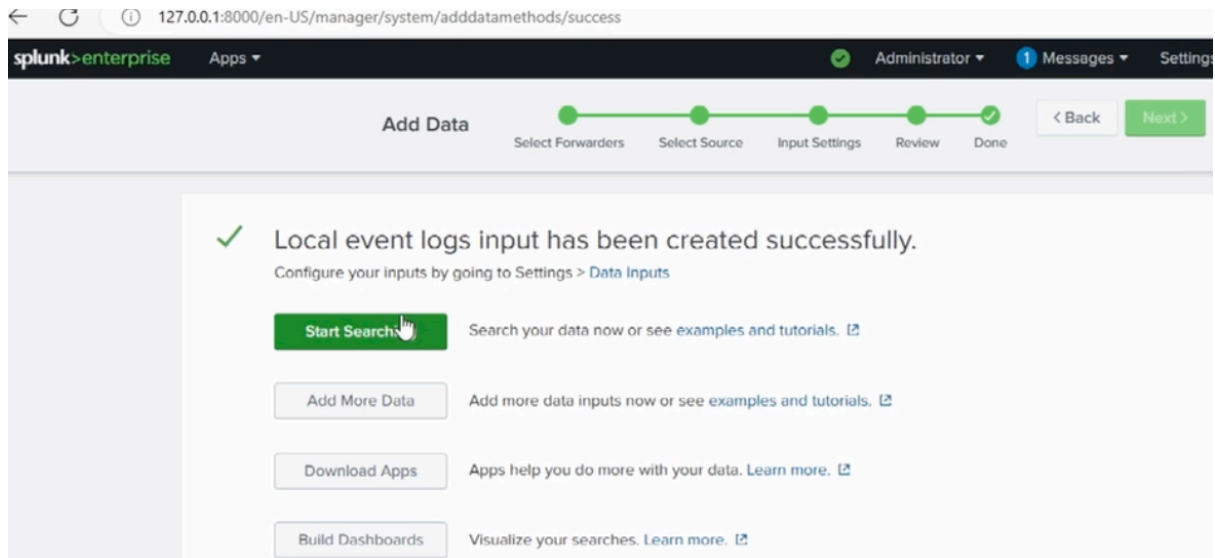
Click on Create a new index after you have created it click the Default drop down arrow to select the index you have created.



Click on Review button to check the logs you have created once viewed click on submit.
You can now click on “start searching” to find last connection on client’s computer

The screenshot shows the 'Add Data' wizard in Splunk Enterprise. The progress bar indicates the current step is 'Input Settings', with previous steps 'Select Forwarders' and 'Select Source' completed, and 'Review' and 'Done' remaining. A green 'Review >' button is highlighted. The main content area is titled 'Input Settings' and includes a description: 'Optionally set additional input parameters for this data input as follows:'. Under the 'Index' section, it explains that the Splunk platform stores incoming data as events in the selected index, and suggests using a 'sandbox' index for troubleshooting. An 'Index' dropdown menu is set to 'jane1', with a 'Create a new index' link next to it. Below this, an 'FAQ' section lists two questions: 'How do indexes work?' and 'How do I know when to create or use multiple indexes?'. The top navigation bar includes links for 'Apps', 'Administrator', 'Messages', 'Settings', and 'Activity'.

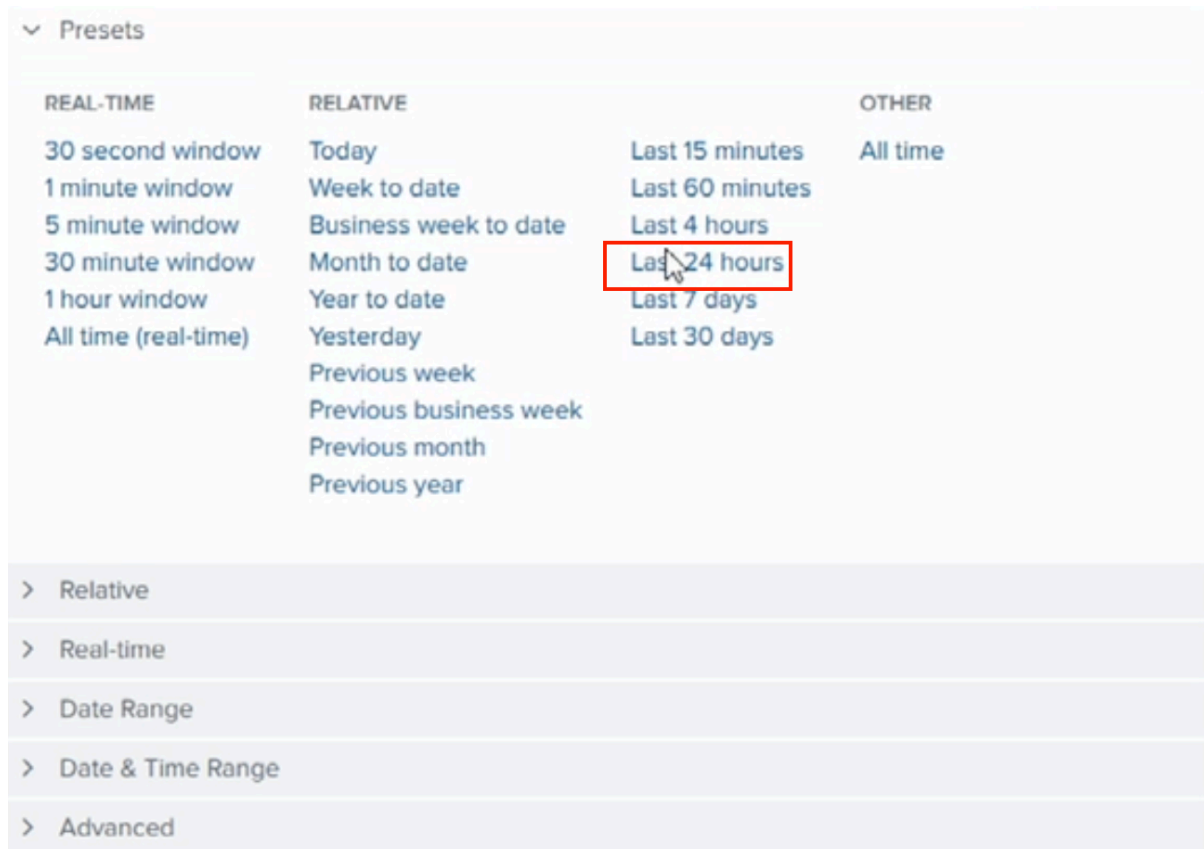
The screenshot shows the 'Review' step of the 'Add Data' wizard. The progress bar shows 'Review' as the current step, with 'Input Settings' completed. A green 'Submit >' button is highlighted. The main content area is titled 'Review' and displays a summary of the configuration: 'Server Class Name' is 'WIN-854SHEO9OSJ', 'List of Forwarders' is 'WINDOWS | WIN-854SHEO9OSJ', 'Collection Name' is 'localhost', 'Input Type' is 'Windows Event Logs', 'Event Logs' includes 'Application', 'ForwardedEvents', 'Security', 'Setup', and 'System', and 'Index' is 'jane1'. The top navigation bar is consistent with the previous screenshot.



NOTE: the field names are case-sensitive, but the field values are not case-sensitive, you can use operators such AND, OR NOT also wildcard is available (use *)

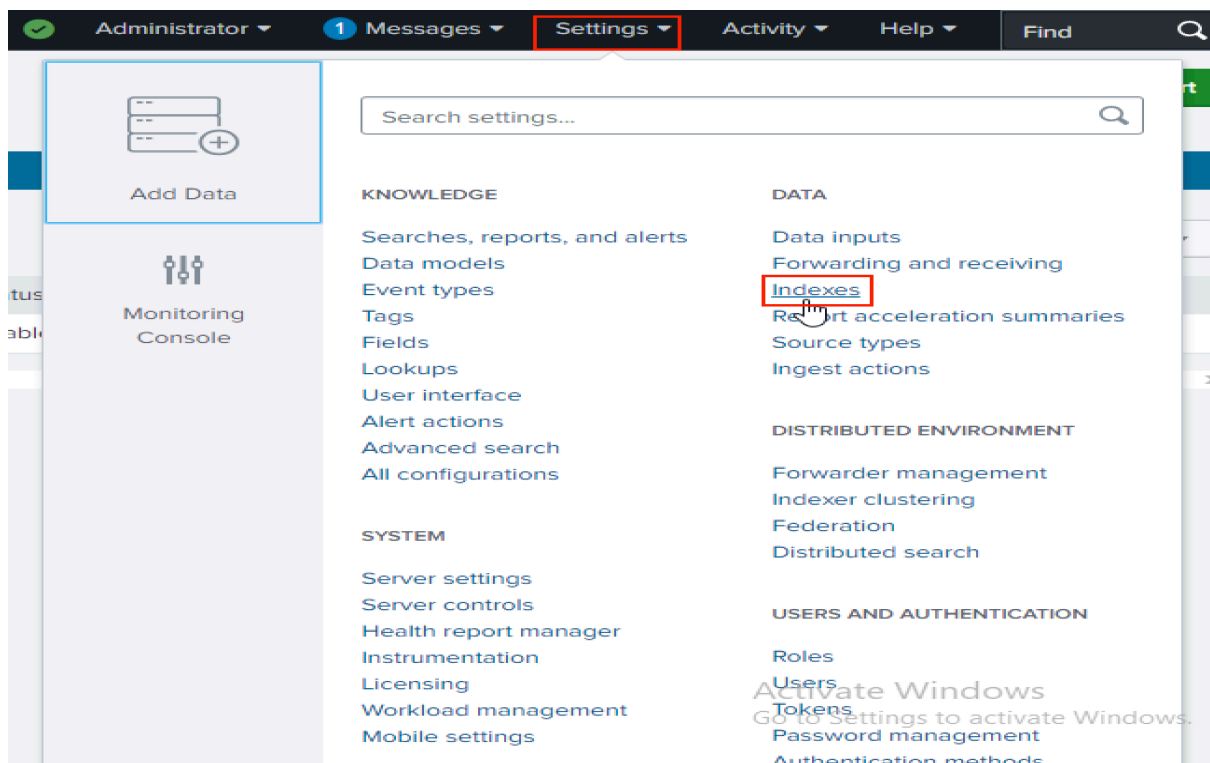
Date selection

First step it choosing the data range then choose if you want to search for Present, Relative, Real-time in our case we chose Present and select 24 hours

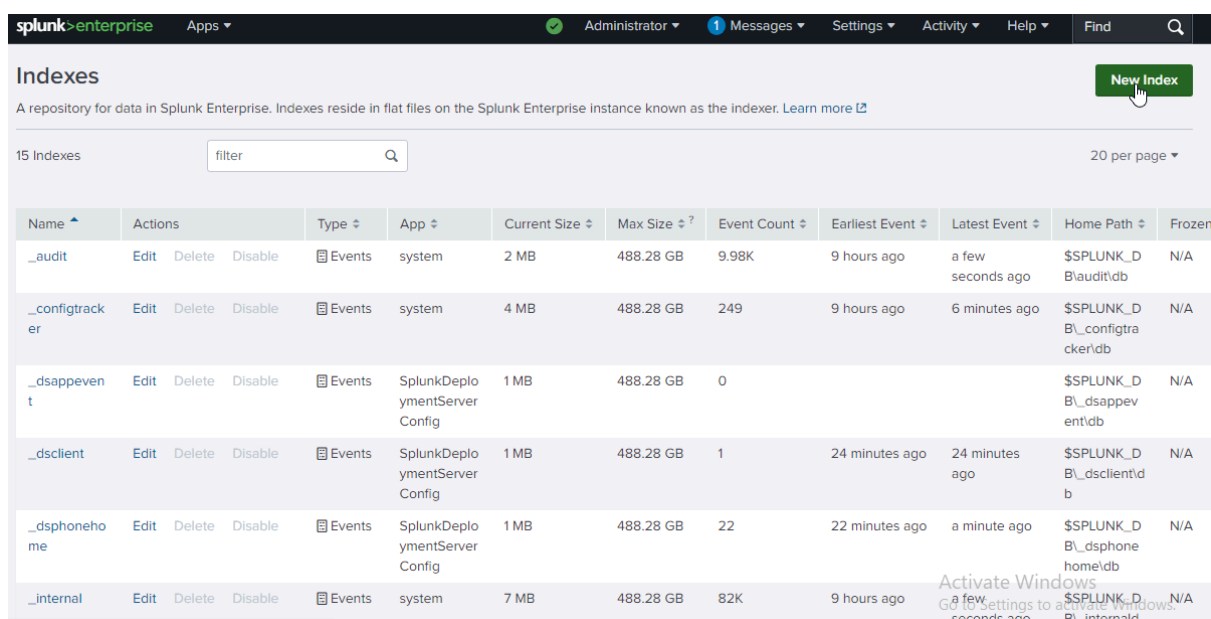


Check Indexes Settings

Click on Settings > Indexes



As seen that there is no incoming event, we are to create an event now click on “New Index”



									seconds ago	B_metrics/d b	
_metrics_roll up	Edit	Delete	Disable	Metrics	system	1 MB	488.28 GB	0		\$SPLUNK_D B_metrics_r ollup\db	N/A
_telemetry	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0		\$SPLUNK_D B_telemetry \db	N/A
_thefishbuck et	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0		\$SPLUNK_D B\fishbucket \db	N/A
history	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0		\$SPLUNK_D B\historydb \db	N/A
jane33	Edit	Delete	Disable	Events	search	1 MB	500 GB	0		\$SPLUNK_D B\jane33\db	N/A
main	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0		\$SPLUNK_D B\defaultdb \db	N/A
splunklogge r	Edit	Delete	Enable	Events	system	0 B	488.28 GB	0		\$SPLUNK_D B\splunklogg er\db	N/A
summary	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0		\$SPLUNK_D B\summaryd b\db	N/A

We named the new index “Jane1” then click on Save

New Index

General Settings

Index Name: Jane1
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).

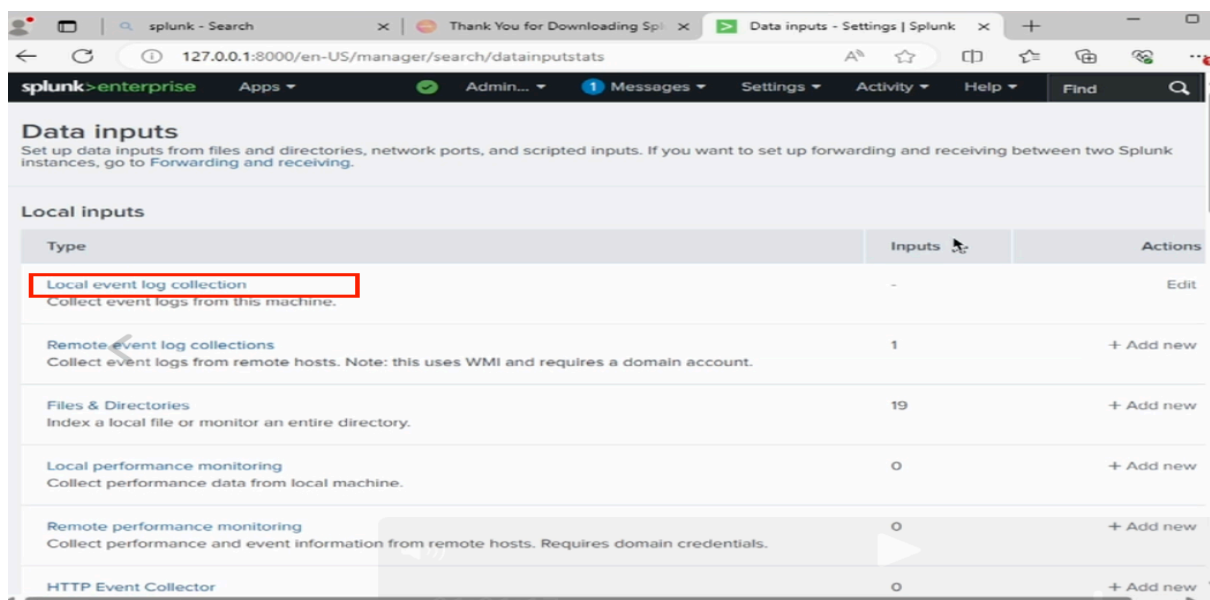
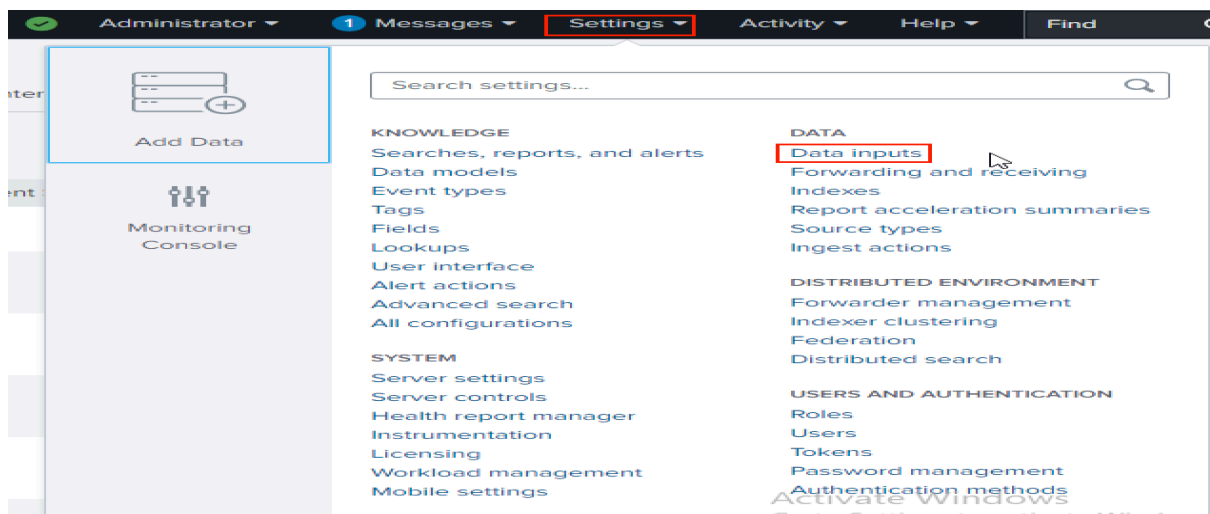
Cold Path: optional
Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).

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

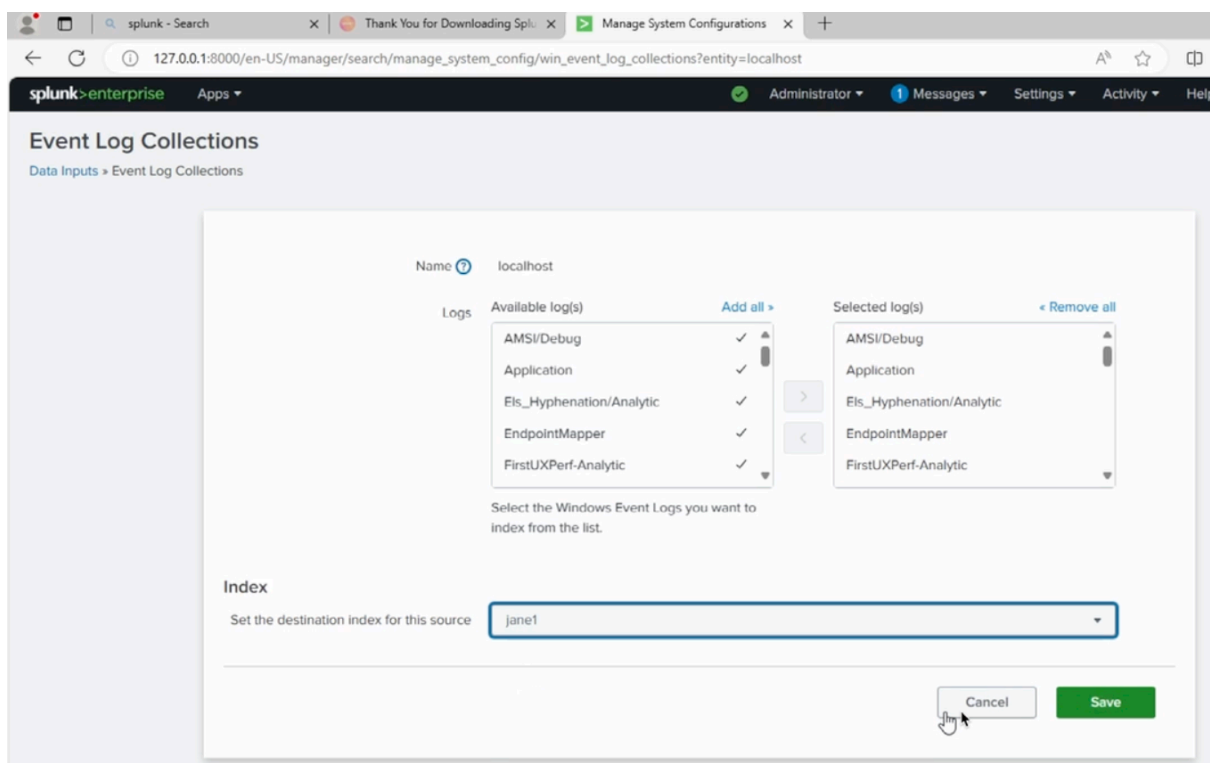
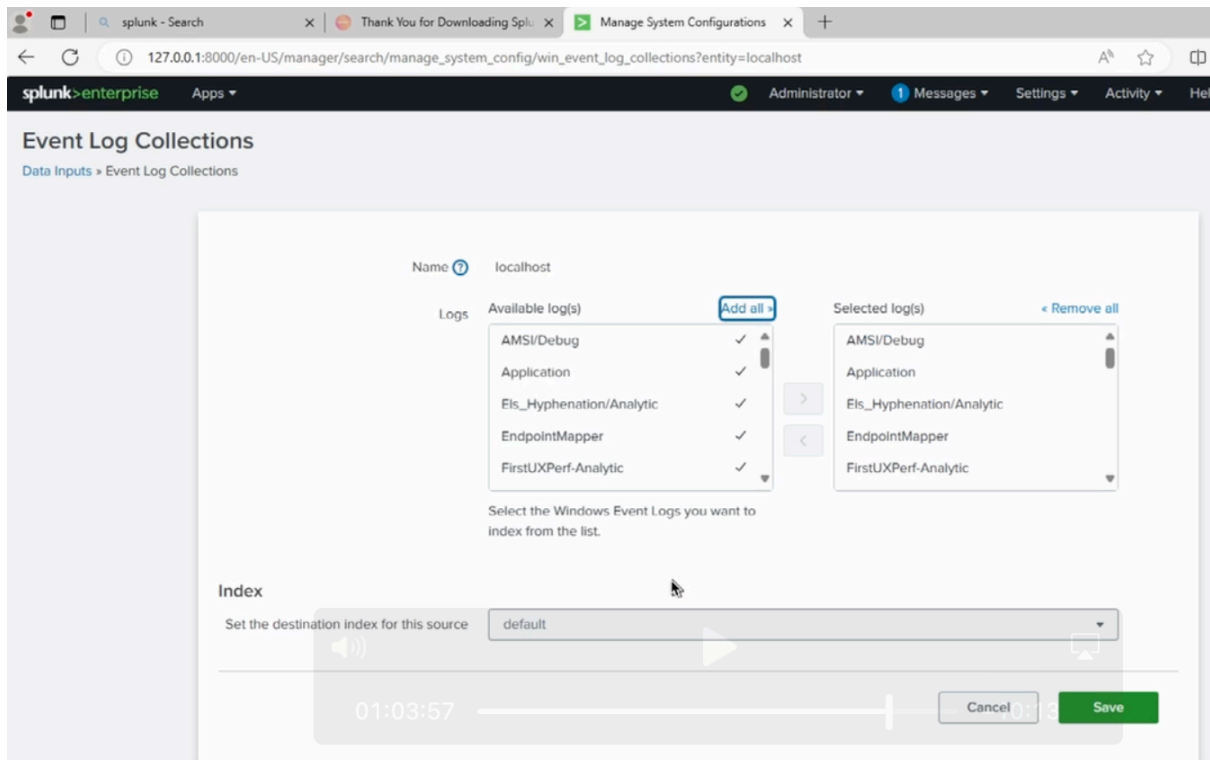
Data Integrity Check: ☐ Enable ☒ Disable
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Save **Cancel**

Go to settings> Data input > local events logs collection



The event logs are then added to newly created index “Jane1”



Go to settings > indexes the below image show that the events had updated “Jane1”

splunk - Search

Thank You for Downloading Splunk

Manage Indexes | Splunk 9.3.2

127.0.0.1:8000/en-US/manager/search/data/indexes

10 minutes ago

u few seconds ago

SSPLUNK_DB_internaldb

N/A

Enabled

_introspection	Edit Delete Disable	Events	system	3 MB	488.28 GB	1.04K	16 minutes ago	a few seconds ago	SSPLUNK_DB_introspectiondb	N/A	Enabled
_metrics	Edit Delete Disable	Metrics	system	5 MB	488.28 GB	6.45K	16 minutes ago	a few seconds ago	SSPLUNK_DB_metricsdb	N/A	Enabled
_metrics_rollup	Edit Delete Disable	Metrics	system	1 MB	488.28 GB	0			SSPLUNK_DB_metrics_rollupdb	N/A	Enabled
_telemetry	Edit Delete Disable	Events	system	1 MB	488.28 GB	1	6 minutes ago	6 minutes ago	SSPLUNK_DB_telemetrydb	N/A	Enabled
_thefishbucket	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			SSPLUNK_DB_thefishbucketdb	N/A	Enabled
history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			SSPLUNK_DB_historydb	N/A	Enabled
jane1	Edit Delete Disable	Events	search	1 MB	500 GB	4.77K	an hour ago	in 7 hours	SSPLUNK_DB_jane1db	N/A	Enabled
main	Edit Delete Disable	Events	system	1 MB	488.28 GB	0	4768 events		SSPLUNK_DB_defaultdb	N/A	Enabled
splunklogger	Edit Delete Enable	Events	system	0 B	488.28 GB	0			SSPLUNK_DB_splunkloggerdb	N/A	Disabled
summary	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			SSPLUNK_DB_summarydb	N/A	Enabled

6°C

Search

ENG

Splunk Reports

To save a report click on Save As > Report “title and Description”> Save > View

The screenshot displays the Splunk Enterprise web interface. At the top, the navigation bar includes 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The 'New Search' section shows the search query: `source=WinEventLog:* index=jane1 Account_Name=Jane`. Below the search bar, it indicates 54 events were found for the time range 12/8/24 9:00:00.000 PM to 12/9/24 9:27:22.000 PM. The 'Events (54)' tab is selected, showing a list of search results. The first event is expanded, revealing details such as `LogName=Security`, `EventCode=5379`, and `ComputerName=WIN-854SHE090SJ`. The interface also features a sidebar with 'SELECTED FIELDS' and 'INTERESTING FIELDS'.

i	Time	Event
>	12/9/24 9:21:08.000 PM	12/8/2024 09:21:08 PM LogName=Security EventCode=5379 EventType=0 ComputerName=WIN-854SHE090SJ host = WIN-854SHE090SJ source = WinEventLog:Security sourcetype = WinEventLog:Security
>	12/9/24 9:21:04.000 PM	12/8/2024 09:21:04 PM LogName=Security EventCode=5379 EventType=0 ComputerName=WIN-854SHE090SJ host = WIN-854SHE090SJ source = WinEventLog:Security sourcetype = WinEventLog:Security
>	12/9/24 9:21:05.000 PM	12/8/2024 09:21:05 PM LogName=Security EventCode=5379 EventType=0 ComputerName=WIN-854SHE090SJ host = WIN-854SHE090SJ source = WinEventLog:Security sourcetype = WinEventLog:Security

127.0.0.1:8000/en-US/app/search/search?q=search%20source%3D%20WinEventLog%3A%20index%3D%20jane1%20Account_Name%3DJane&earliest=-2...

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

New Search

source="WinEventLog:*" index="jane1" Account_Name=Jane

✓ 54 events (12/8/24 9:00:00.000 PM to 12/9/24 9:27:22.000 PM) No Event Sampling

Events (54) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

Save As Report

Report

Alert

Existing Dashboard

New Dashboard

Event Type

Last 24 hours

Smart Mode

1 hour per column

127.0.0.1:8000/en-US/app/search/search?q=search%20source%3D%20WinEventLog%3A%20index%3D%20jane1%20Account_Name%3DJane

splunk>enterprise Apps Administrator Messages

Search Analytics Datasets Reports Alerts

New Search

source="WinEventLog:*" index="jane1" Account_Name=Jane

events (12/8/24 9:00:00.000 PM to 12/9/24 9:27:22.000 PM)

Events (54) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection

List Format

Save As Report

Title Jane report

Description optional

Content Events

Time Range Picker Yes No

Cancel Save

Your Report Has Been Created

You may now view your report, add it to a dashboard, change additional settings, or continue editing it.

Additional Settings:

- Permissions
- Schedule
- Acceleration
- Embed

Continue EditingAdd to Dashboard ▾

View

←

↻

127.0.0.1:8000/en-US/app/search/report?ts=%2FservicesNS%2Fjane%2Fsearch%2Fsaved%2Fsearches%2Fjane%2520report&sid=1733779642.22&disp...

⌵

☆

📄

🔍

⋮

splunk>enterprise

Apps ▾

Administrator ▾

1 Messages ▾

Settings ▾

Activity ▾

Help ▾

Find 🔍

Search

Analytics

Datasets

Reports

Alerts

Dashboards

▶

Jane report

Edit ▾

More Info ▾

Add to Dashboard ▾

Last 24 hours ▾

✓ 54 events (12/8/24 9:00:00.000 PM to 12/9/24 9:27:22.000 PM)

Job ▾

⏏

⏏

⏏

⏏

⏏

⏏

20 per page ▾

< Prev

1

2

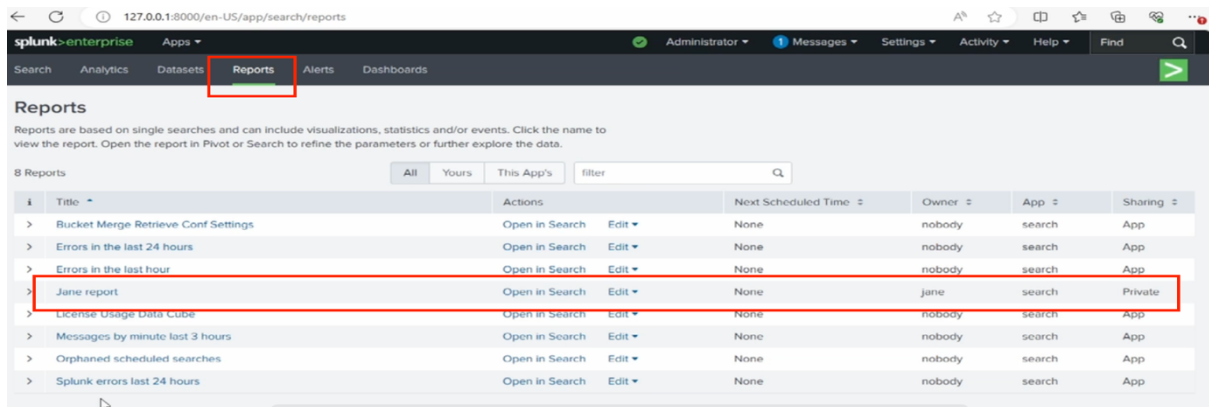
3

Next >

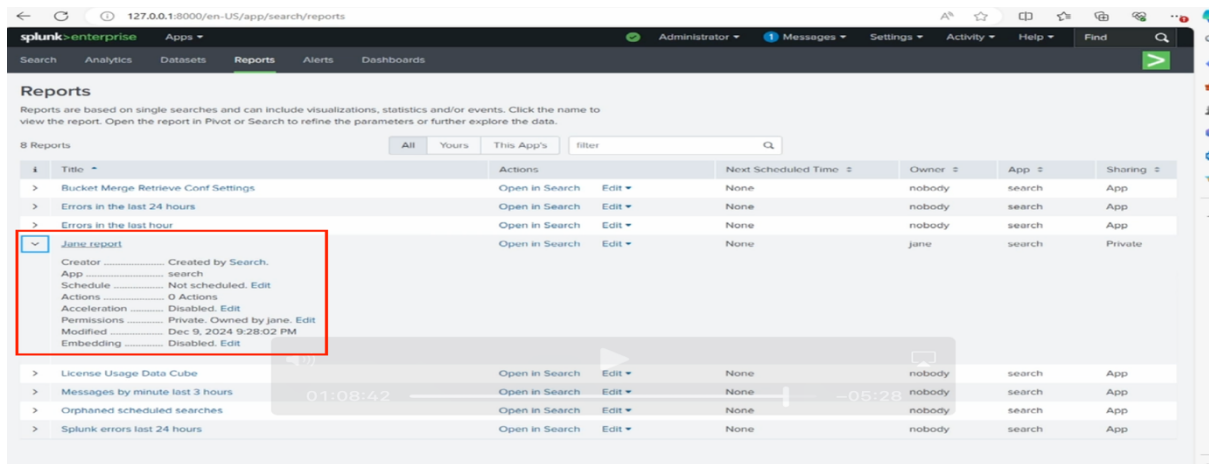
i	Time	Event
>	12/9/24 9:21:08.000 PM	12/09/2024 09:21:08 PM LogName=Security EventCode=5379 EventType=0 ComputerName=WIN-854SHE090SJ Show all 21 lines host = WIN-854SHE090SJ source = WinEventLog:Security sourcetype = WinEventLog:Security
>	12/9/24 9:21:04.000 PM	12/09/2024 09:21:04 PM LogName=Security EventCode=5379 EventType=0 ComputerName=WIN-854SHE090SJ Show all 21 lines host = WIN-854SHE090SJ source = WinEventLog:Security sourcetype = WinEventLog:Security
>	12/9/24 9:20:55.000 PM	12/09/2024 09:20:55 PM LogName=Security EventCode=5379 EventType=0 ComputerName=WIN-854SHE090SJ Show all 21 lines host = WIN-854SHE090SJ source = WinEventLog:Security sourcetype = WinEventLog:Security

To Edit an Existing Report

At the Search tap click on Report > Select the Report you created



Detailed information of the “Jane report”



Select Edit button to edit “Jane Report”



Set Alert

Click on Save As > Alert > “fill in the title, description e.t.c” > Save

Save As Alert

Settings

Title

Title

Description

Optional

Permissions

Private

Shared in App

Alert type

Scheduled

Real-time

Run every week ▾

On

Monday ▾

 at

6:00 ▾

Expires

24

hour(s) ▾

Trigger Conditions

Trigger alert when

Number of Results ▾

is greater than ▾

0

Trigger

Once

For each result

Throttle ?

☐

Trigger Actions

+ Add Actions ▾

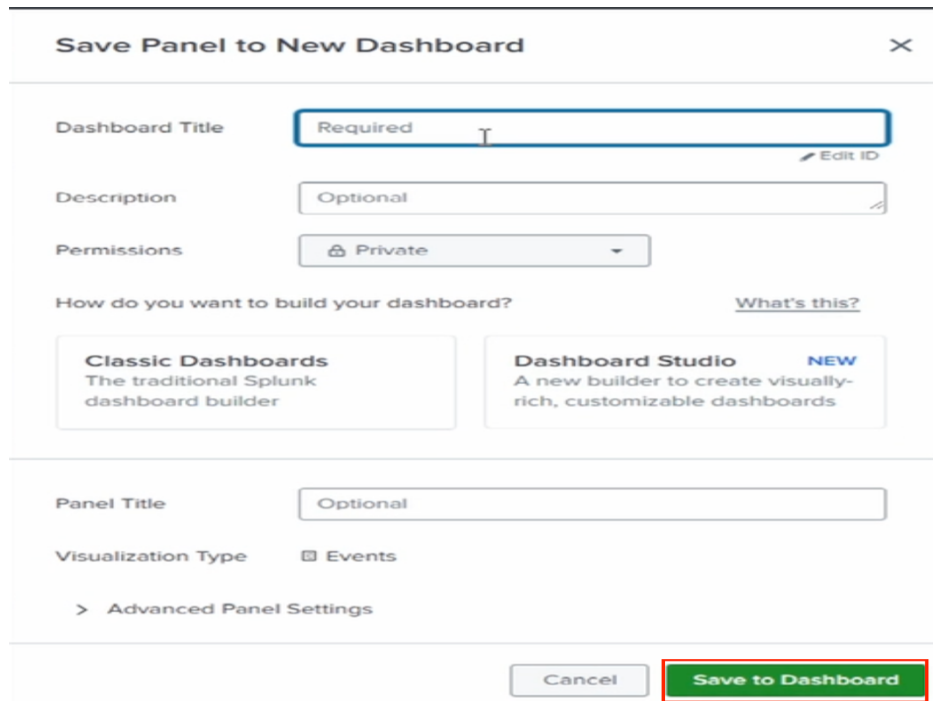
Cancel

Save

49

Save to Dashboard

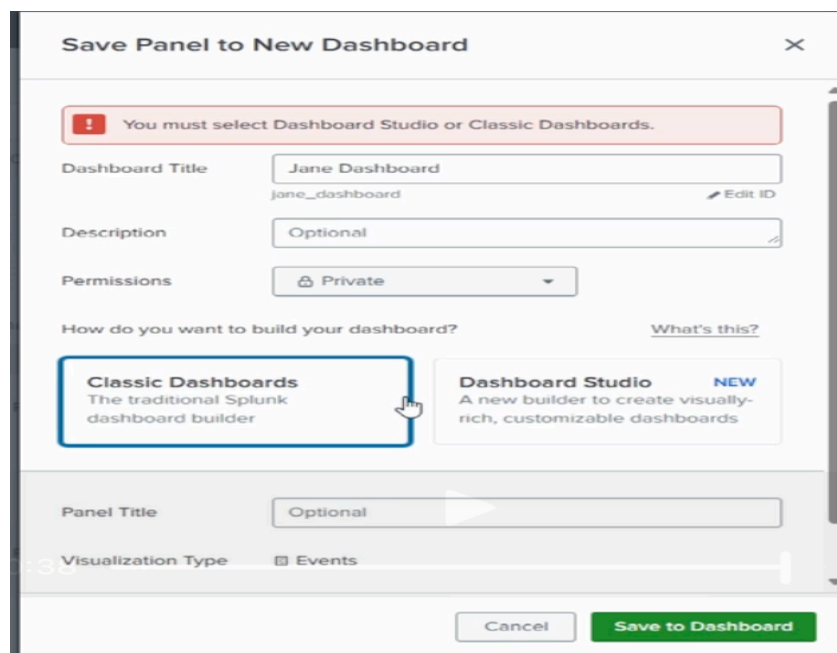
Click on Save As > New Dashboard > “fill in the dashboard title, description e.t.c” > Save to Dashboard



The screenshot shows the 'Save Panel to New Dashboard' dialog box. It has a title bar with a close button (X). The form contains the following fields and options:

- Dashboard Title:** A text input field with the placeholder 'Required' and an 'Edit ID' link.
- Description:** A text input field with the placeholder 'Optional'.
- Permissions:** A dropdown menu currently set to 'Private'.
- How do you want to build your dashboard?:** Two options are shown: 'Classic Dashboards' (The traditional Splunk dashboard builder) and 'Dashboard Studio' (A new builder to create visually-rich, customizable dashboards, marked as 'NEW').
- Panel Title:** A text input field with the placeholder 'Optional'.
- Visualization Type:** A dropdown menu currently set to 'Events'.
- Advanced Panel Settings:** A link to expand more options.
- Buttons:** 'Cancel' and 'Save to Dashboard' (highlighted with a red box).

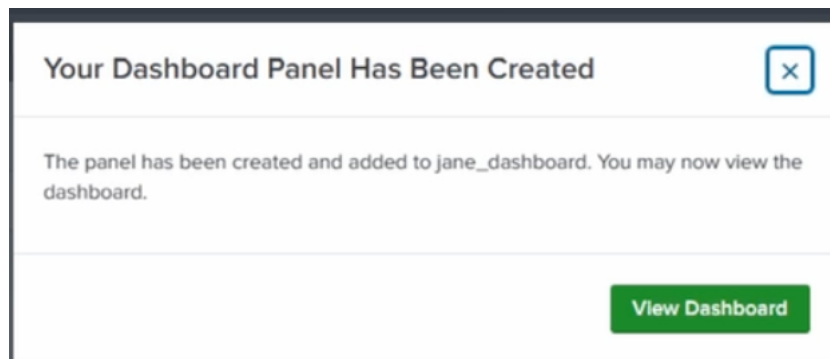
NOTE: You must select “Classic or Studio Dashboard



This screenshot shows the same dialog box but with an error message at the top: 'You must select Dashboard Studio or Classic Dashboards.' The 'Classic Dashboards' option is highlighted with a blue box and a mouse cursor. The 'Dashboard Studio' option is marked as 'NEW'. The 'Save to Dashboard' button is highlighted with a green box.

The form fields are filled with the following values:

- Dashboard Title:** 'Jane Dashboard' (ID: jane_dashboard)
- Description:** 'Optional'
- Permissions:** 'Private'
- Panel Title:** 'Optional'
- Visualization Type:** 'Events'



← 127.0.0.1:8000/en-US/app/search/dashboards

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts **Dashboards**

Dashboards

Create New Dashboard

Dashboards include searches, visualizations, and input controls that capture and present available data.

Latest Resources

- ☆ Examples for Dashboard Studio
Browse examples of dashboards & visualizations. [Visit Example Hub](#)
- Intro to Dashboard Studio
Learn how to build dashboards with Dashboard Studio. [Learn More](#)
- Intro to Classic Dashboards
Learn how to build traditional Simple XML dashboards. [Learn More](#)

6 Dashboards

All Yours This App's filter

i	Title	Actions	Owner	App	Sharing	Type
>	Integrity Check of Installed Files	Edit	nobody	search	App	Dashboard Studio
>	Jane Dashboard	Edit	jane	search	Private	Classic
>	Job Details Dashboard	Edit	nobody	search	App	Dashboard Studio
>	jQuery Upgrade	Edit	nobody	search	App	Classic
>	Orphaned Scheduled Searches, Reports, and Alerts	Edit	nobody	search	App	Dashboard Studio
>	Scheduled export is now available for Dashboard Studio	Edit	nobody	search	Global	Dashboard Studio

Detailed information of the “Jane Dashboard”

←↻127.0.0.1:8000/en-US/app/search/jane_dashboard

splunk>enterpriseApps

Administrator1M

SearchAnalyticsDatasetsReportsAlertsDashboards

Jane Dashboard

i	Time	Event
>	12/9/24 9:30:17.000 PM	12/09/2024 09:30:17 PM LogName=Application EventCode=16394 EventType=4 ComputerName=WIN-854SHE090SJ <a>Show all 12 lines host = WIN-854SHE090SJ source = WinEventLog:Application sourcetype = WinEventLog:Application
>	12/9/24 9:30:17.000 PM	12/09/2024 09:30:17 PM LogName=Application EventCode=16394 EventType=4 ComputerName=WIN-854SHE090SJ <a>Show all 12 lines host = WIN-854SHE090SJ source = WinEventLog:Application sourcetype = WinEventLog:Application
>	12/9/24 9:29:49.000 PM	12/09/2024 09:29:49 PM LogName=Application EventCode=1001 EventType=4 ComputerName=WIN-854SHE090SJ <a>Show all 47 lines host = WIN-854SHE090SJ source = WinEventLog:Application sourcetype = WinEventLog:Application
>	12/9/24 9:29:49.000 PM	12/09/2024 09:29:49 PM LogName=Application EventCode=1001 EventType=4 ComputerName=WIN-854SHE090SJ <a>Show all 47 lines host = WIN-854SHE090SJ source = WinEventLog:Application sourcetype = WinEventLog:Application

Select Edit button to edit “Jane Dashboard”

←↻127.0.0.1:8000/en-US/app/search/dashboards

splunk>enterpriseApps

AdministratorMessagesSettingsActivityHelpFind

SearchAnalyticsDatasetsReportsAlertsDashboards

Dashboards

Create New Dashboard

Dashboards include searches, visualizations, and input controls that capture and present available data.

Latest Resources

☆ Examples for Dashboard Studio
Browse examples of dashboards & visualizations. [Visit Example Hub](#)

📖 Intro to Dashboard Studio
Learn how to build dashboards with Dashboard Studio. [Learn More](#)

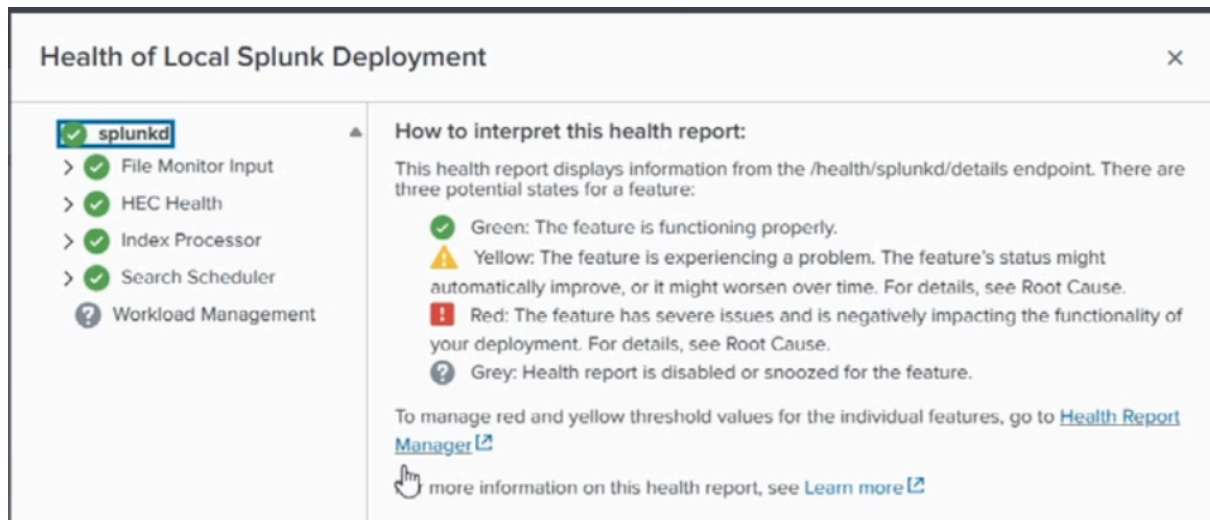
📖 Intro to Classic Dashboards
Learn how to build traditional Simple XML dashboards. [Learn More](#)

6 Dashboards

AllYoursThis App'sfilter

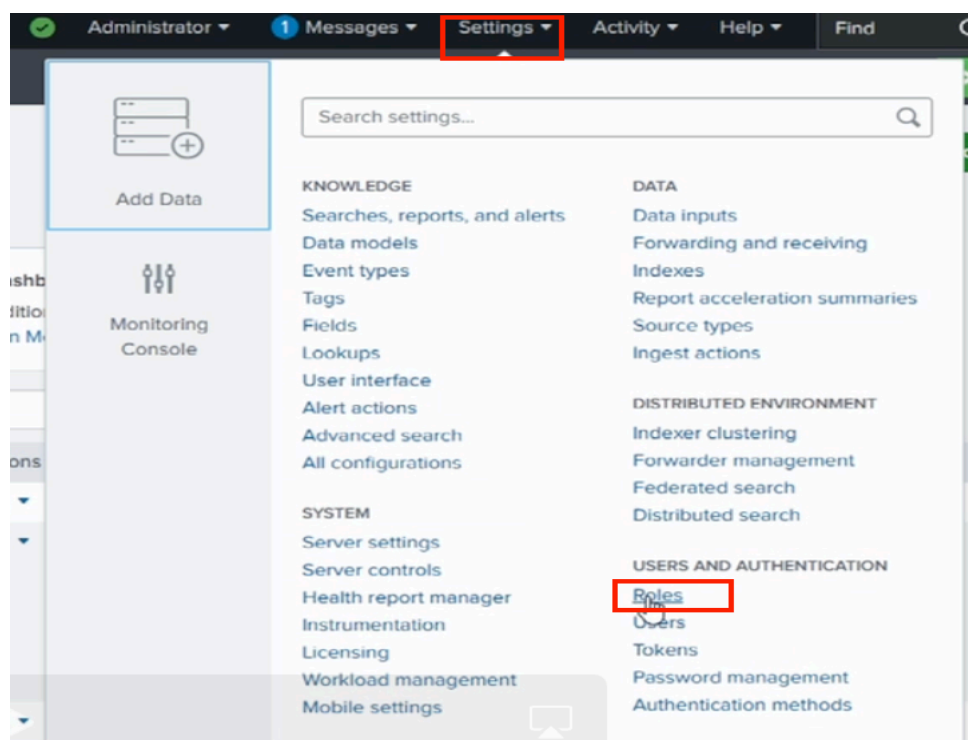
i	Title	Actions	Owner	App	Sharing	Type
>	Integrity Check of Installed Files	Edit	nobody	search	App	Dashboard Studio
▼	Jane Dashboard App: search Schedule: Not scheduled. Edit Permissions: Private. Owned by Jane. Edit Modified: Dec 9, 2024 9:30:24 PM	Edit	jane	search	Private	Classic
>	Job Details Dashboard	Edit	nobody	search	App	Dashboard Studio
>	jQuery Upgrade	Edit	nobody	search	App	Classic
>	Orphaned Scheduled Searches, Reports, and Alerts	Edit	nobody	search	App	Dashboard Studio
>	Scheduled export is now available for Dashboard Studio	Edit	nobody	search	Global	Dashboard Studio

Splunk Health Status Check

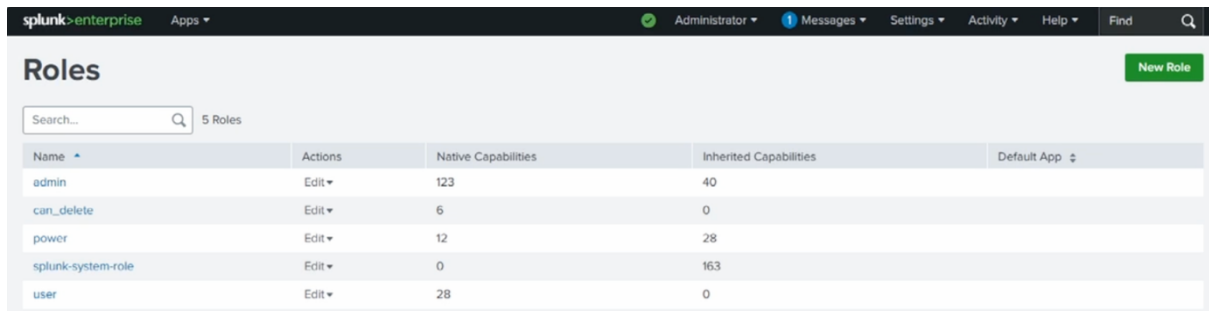


User management on Splunk

To find and Create a new Role click on Settings > Roles



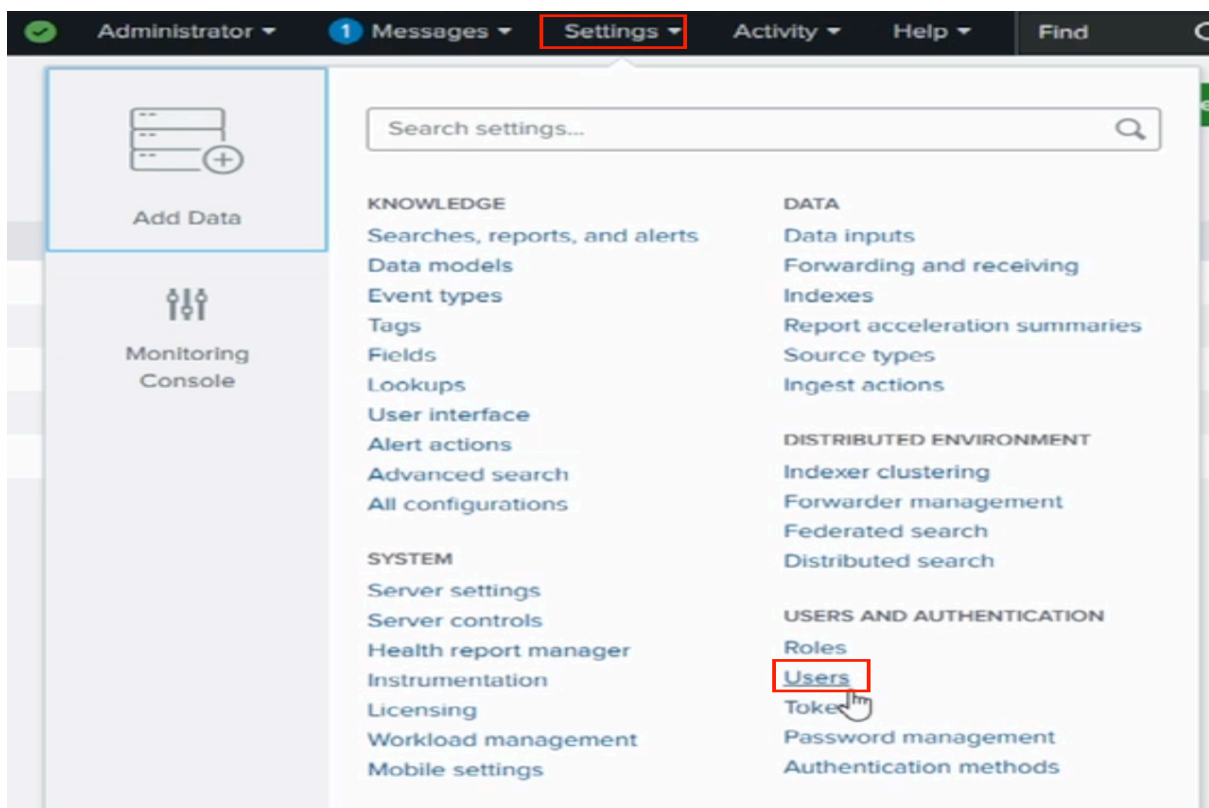
Here you can “Edit or Add New Role”



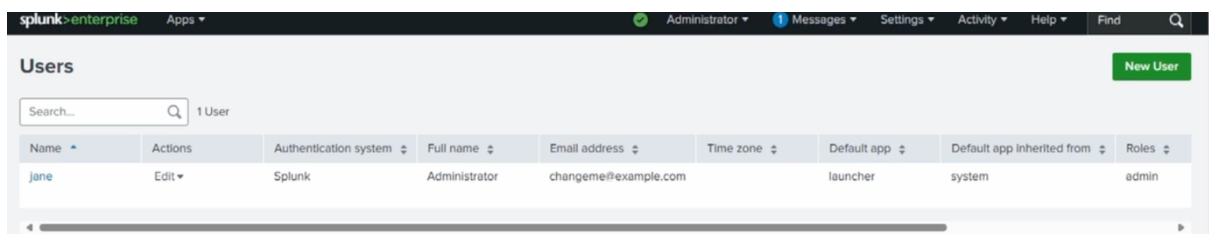
The screenshot shows the 'Roles' page in the Splunk Enterprise interface. At the top, there's a navigation bar with 'splunk>enterprise' and various menu items. Below the navigation bar, the 'Roles' title is followed by a 'New Role' button. A search bar indicates '5 Roles'. The main content is a table with columns: Name, Actions, Native Capabilities, Inherited Capabilities, and Default App. The table lists five roles: admin, can_delete, power, splunk-system-role, and user.

Name	Actions	Native Capabilities	Inherited Capabilities	Default App
admin	Edit	123	40	
can_delete	Edit	6	0	
power	Edit	12	28	
splunk-system-role	Edit	0	163	
user	Edit	28	0	

To Create a New User click on Settings > Users



Here you can “Edit or Add New User”



The screenshot shows the 'Users' page in the Splunk Enterprise interface. At the top, there's a navigation bar with 'splunk>enterprise' and various menu items. Below the navigation bar, the 'Users' title is followed by a 'New User' button. A search bar indicates '1 User'. The main content is a table with columns: Name, Actions, Authentication system, Full name, Email address, Time zone, Default app, Default app inherited from, and Roles. The table lists one user: jane.

Name	Actions	Authentication system	Full name	Email address	Time zone	Default app	Default app inherited from	Roles
jane	Edit	Splunk	Administrator	changeme@example.com		launcher	system	admin

5. Splunk SIEM: A Comprehensive Analysis of its Widespread Adoption

Splunk, a leading enterprise software provider, has redefined security information and event management (SIEM) with its innovative Splunk SIEM solution. Renowned for its versatility and efficiency, the platform is widely adopted across industries to effectively address modern security challenges (Conran, 2022).

Harisuthan (2021) highlights that the core strength of Splunk SIEM lies in its ability to collect and analyze vast amounts of data from diverse sources, including security devices, networks, systems, and applications. By standardizing and correlating this data, the platform provides security teams with a unified view of their IT environment, enabling faster and more accurate threat detection and anomaly identification.

A key feature of Splunk SIEM, according to Caccia et al. (2021), is its capacity to process various data formats, including log data—critical for security operations. This comprehensive data handling makes Splunk SIEM an indispensable tool for incident response, user activity monitoring, and compliance reporting, serving organizations of all sizes (Caccia et al., 2021).

What sets Splunk SIEM apart further is its adaptability and customization. The platform can be tailored to meet the unique security requirements of different industries and use cases, ensuring it aligns with each organization's specific needs (González-Granadillo et al., 2021).

Cooper (2024) emphasizes that, unlike traditional SIEM solutions, Splunk SIEM offers advanced functionality, such as the ability to process and analyze both unstructured and structured data. This feature enables security teams to gain a more comprehensive understanding of their IT environments, helping them detect and mitigate sophisticated threats that older systems might miss.

Splunk SIEM's popularity is also due to its ability to adapt to the rapidly evolving threat landscape. As cybercriminals develop increasingly advanced tactics, the platform equips organizations with powerful tools to anticipate and counter emerging threats (Hristov et al., 2021).

By aggregating and analyzing data from multiple sources, Splunk SIEM enables security teams to respond to incidents more efficiently. This timely threat detection and mitigation enhance the organization's overall security posture, strengthening defences in a dynamic and complex cybersecurity environment (Pan, 2024).

In summary, Splunk SIEM has become a top choice for organizations worldwide due to its robust data collection and analysis capabilities, customization options, and ability to adapt to the ever-changing security landscape.

6. Critically evaluation of Splunk SIEM security services

6.1 Splunk SIEM Strengths

Splunk, a prominent provider of security information and event management solutions, is well-recognized as a strong and versatile security service. The platform has a compelling combination of capabilities, making it a popular choice for businesses looking to improve their security posture (Pan, 2024).

According to Simko (2024), one of Splunk SIEM's main advantages is its capacity to gather, compile, and centralize data from a variety of sources. The platform offers a thorough understanding of the security environment of the company by ingesting and analyzing data from several logs, network traffic, security sensors, and other disparate systems. Security teams can access and correlate pertinent information from a single, unified platform thanks to data consolidation, which speeds up the process of identifying and responding to possible threats. (Wopat, 2024).

The comprehensive search and analysis features of Splunk SIEM are also excellent. With the help of the platform's sophisticated search engine and query language, security experts can easily find trends, spot anomalies, and discover any security problems by swiftly sorting through enormous volumes of data (Sheeraz et al., 2023). In addition, security teams may create thorough dashboards and perceptive visualizations with Splunk's powerful analytics and reporting capabilities, which aid in their comprehension and dissemination of the security posture status of their company (Roche and Dowling, 2023).

Sinha (2024) points out that another significant strength of Splunk SIEM is its adaptability and scalability. The platform supports deployment on-premises, in the cloud, or within a hybrid environment, enabling organizations to tailor their security solutions to fit their specific needs and infrastructure. Its modular architecture and a broad ecosystem of third-party integrations allow seamless compatibility with various security tools, enhancing the platform's functionality and fostering a comprehensive security approach (Khaveen, 2021).

Furthermore, Iribhogbe (2024) Splunk SIEM is widely recognized for its intuitive and user-friendly interface, which simplifies the navigation and analysis of large volumes of security data. This design empowers security teams, including those without advanced technical expertise, to effectively utilize the platform's features and make well-informed decisions based on its insights (Kenny, 2023).

Lastly, Splunk SIEM's advanced threat intelligence capabilities stand out as a notable strength (Adeyanju, 2024). Its ability to ingest and correlate threat data from diverse sources, including both open-source and commercial threat feeds, equips security teams to anticipate and counter emerging threats proactively (Kenny, 2023).

In summary, Splunk SIEM combines a comprehensive set of features that cater to organizations of all sizes. Its strengths include data aggregation, search and analysis, adaptability, user-friendliness, and advanced threat intelligence. These capabilities make it a reliable and effective tool for strengthening security operations and managing incidents efficiently (Pan, 2024).

6.2 Vulnerabilities and Attack Vectors against Splunk SIEM

Splunk, a widely recognized Security Information and Event Management (SIEM) solution, has established itself as a key player in the cybersecurity domain (Conran, 2022). Despite its robust features and capabilities, it is crucial to evaluate its potential weaknesses to make informed decisions and address risks effectively.

Mehta (2021) highlights that one notable vulnerability of Splunk is its substantial resource demands, particularly in terms of CPU, RAM, and storage. As a platform heavily reliant on data processing, Splunk requires considerable computing power and storage capacity to manage and analyze large volumes of security data. This poses a significant challenge for organizations with constrained IT infrastructure, especially small and medium-sized enterprises (Mehta, 2021).

Additionally, according to Subramanian (2020), Splunk is often associated with a steep learning curve, which can create challenges for beginners or security teams with limited SIEM experience. The complexity involved in configuring, customizing, and fully utilizing Splunk's features can be overwhelming, especially for organizations that lack dedicated cybersecurity personnel or specialized training.

Another notable vulnerability highlighted by Piotrowski (2024) is Splunk's reliance on well-structured data inputs. The platform's performance is heavily dependent on the quality and completeness of the data it processes, which can be a challenge in heterogeneous environments with varying data sources and formats. Incomplete or poorly structured data may impair Splunk's ability to provide comprehensive security insights and effectively detect potential threats (Piotrowski, 2024).

The cost of Splunk's enterprise licensing is another significant limitation, particularly for smaller organizations operating with tight budgets (Manzoor et al., 2024). The financial burden of these licensing fees can make it difficult for such organizations to adopt and maintain the platform.

Finally, Splunk's ability to detect zero-day threats out-of-the-box is somewhat limited, as it relies on predefined rules and patterns to identify potential threats (Riversafe, 2024). This can reduce its effectiveness in detecting previously unknown vulnerabilities.

Organizations considering the adoption of Splunk SIEM should carefully assess these potential vulnerabilities and weigh them against their specific security needs and available resources.

6.3 Evaluating the Effectiveness of Splunk SIEM in Protecting Against Advanced Cyber Threats

As cyber threats rapidly evolve, organizations are increasingly adopting Security Information and Event Management (SIEM) solutions to bolster their defences against sophisticated attacks (Hristov et al., 2021). Splunk, a robust platform offering comprehensive visibility and actionable security intelligence, is one such solution gaining significant attention.

This paper provides a critical analysis of Splunk SIEM's effectiveness in protecting against complex cyber threats, focusing on five key areas: data ingestion and normalization, threat detection and correlation, incident response and investigation, reporting and compliance, and scalability and performance.

Data Ingestion and Normalization

Splunk's strength is its ability to collect and standardize data from a wide range of sources, such as network devices, security tools, applications, and cloud services (Conran, 2022). This consolidated view of an organization's security environment is essential for detecting and addressing intricate, multi-faceted attacks. Additionally, Splunk's flexible data modelling features empower users to design custom data inputs and transformations, allowing them to swiftly respond to new threats and integrate emerging data sources (Oyedele, 2024).

Threat Detection and Correlation

Splunk's advanced analytics engine combines machine learning and rule-based detection to identify suspicious behaviours and potential indicators of compromise. Simko (2024) discusses that by linking events from different sources Splunk can detect subtle patterns and anomalies that might be overlooked, helping security teams recognize and investigate advanced persistent threats, insider threats, and other complex attack strategies.

Incident Response and Investigation

According to Oyedele (2024), Splunk's comprehensive search and investigation features allow security teams to quickly identify the underlying causes of incidents and implement effective mitigation strategies. The platform's user-friendly interface and integrated dashboards offer a centralized overview of security events, enabling analysts to rapidly assess the scope and impact of an attack (Subrosa, 2023).

Reporting and Compliance

Organizations may show the efficacy of their security policies and comply with regulatory obligations by utilizing Splunk's comprehensive reporting and compliance tools. Sinha (2024) discusses that while automated log management and preservation features guarantee adherence to legal requirements and industry standards, the platform's configurable dashboards and visualizations enable security teams to produce comprehensive reports and communicate actionable findings with stakeholders.

Scalability and Performance

As businesses struggle with the rapidly increasing volume of security data, Splunk's scalable infrastructure and efficient indexing capabilities become increasingly crucial (Warner, 2023). Its distributed system and flexible indexing allow Splunk to process large datasets, ensuring that security teams can adapt to the constantly evolving threat landscape (Sheeraz et al., 2023).

In summary, Splunk's comprehensive SIEM service has proven its effectiveness in defending against advanced cyberattacks. With its robust features for data ingestion, threat detection, incident response, reporting, and scalability, Splunk enables organizations to swiftly identify, analyze, and counteract complex threats efficiently (Simko, 2024).