Table of Content

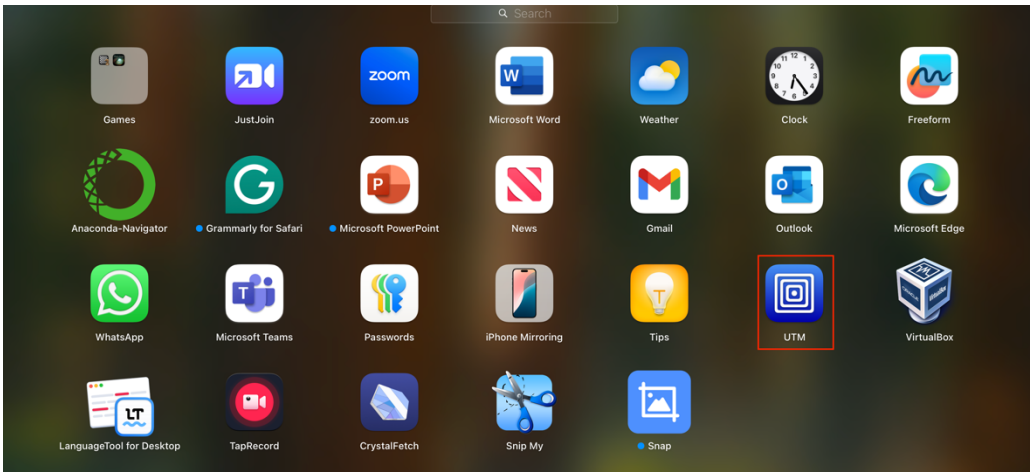
1. Installation and Setting up of Window 11Pro

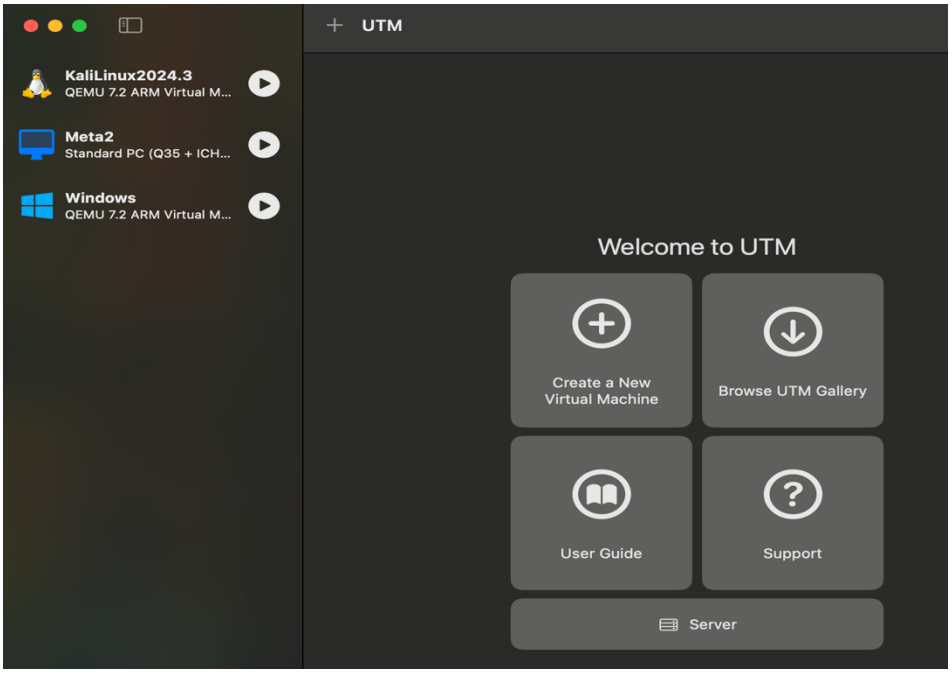
Guide for installing and configuring Windows 11 Pro on your Mac with an M1 chip using UTM. Follow the steps below and refer to the images for visual assistance.

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.

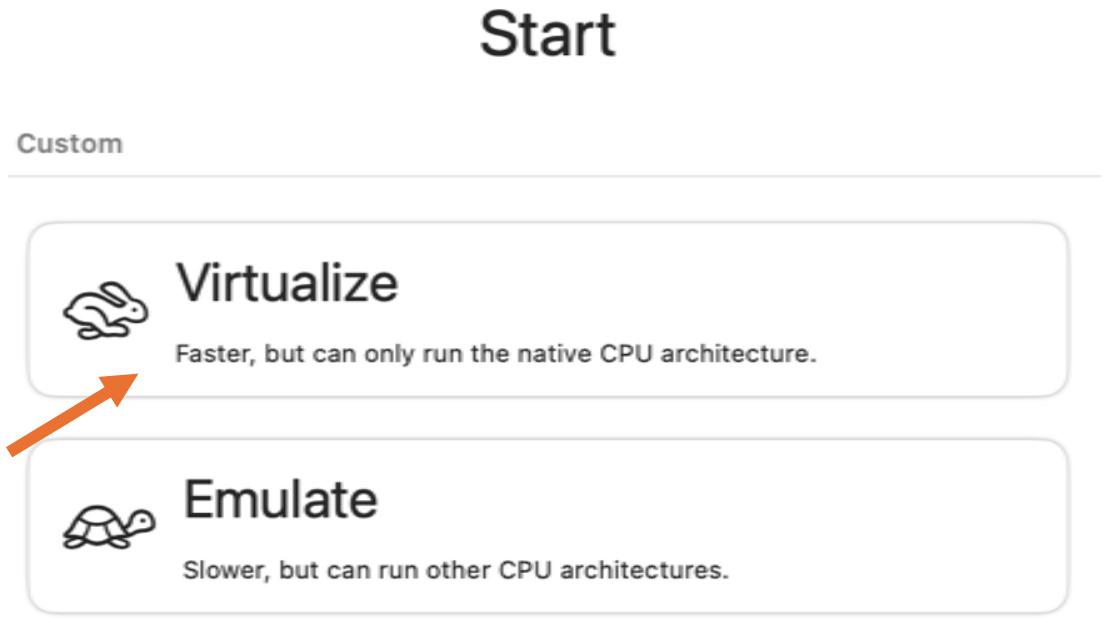
Open UTM: Launch the UTM app from your application folder.



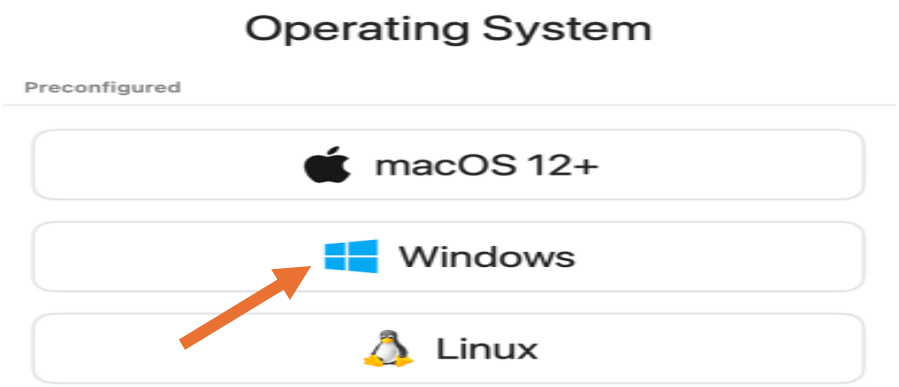


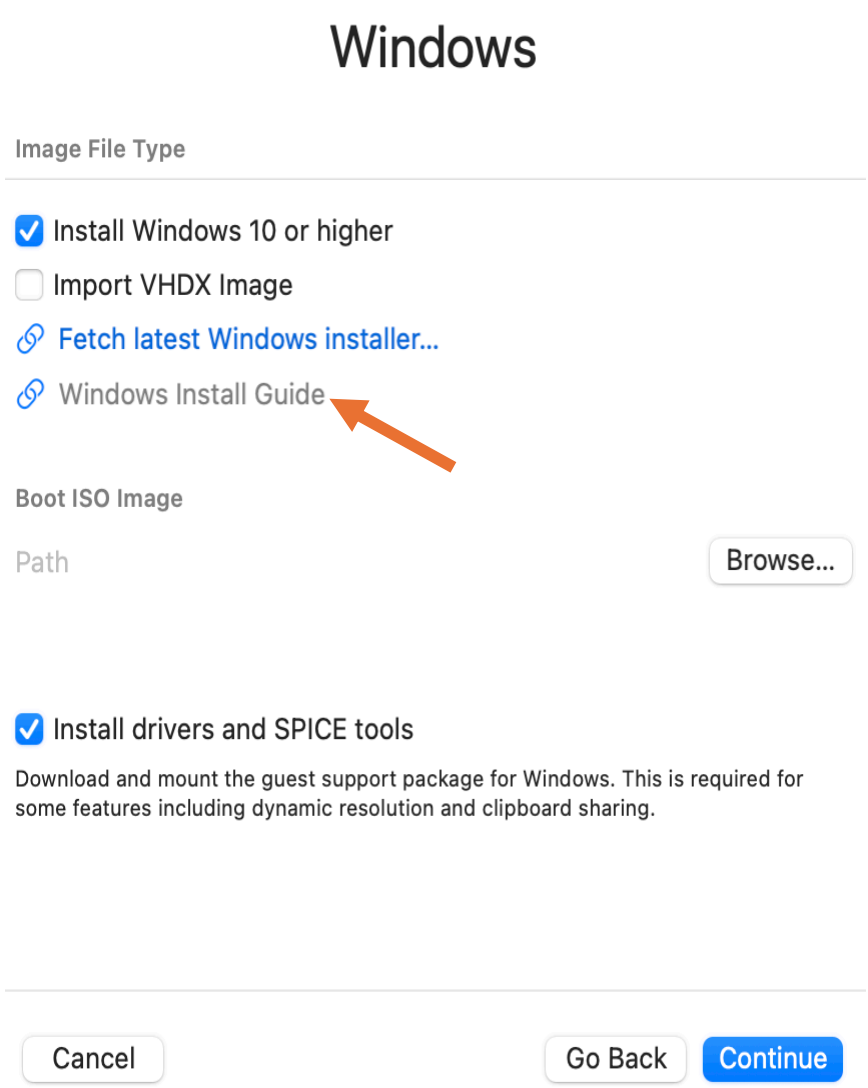
Click on “+ New”: Create a new virtual machine

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



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

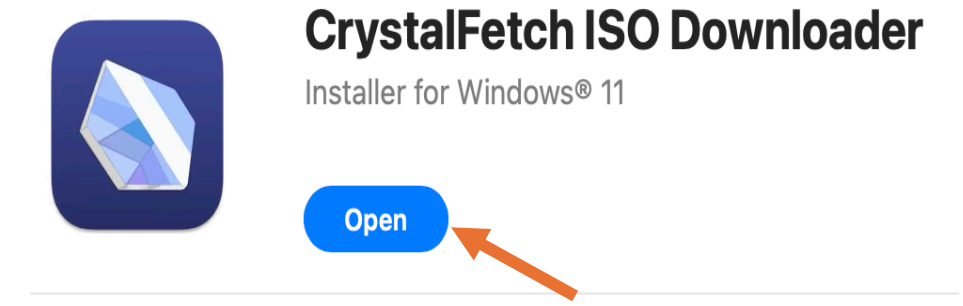
Obtain Windows

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

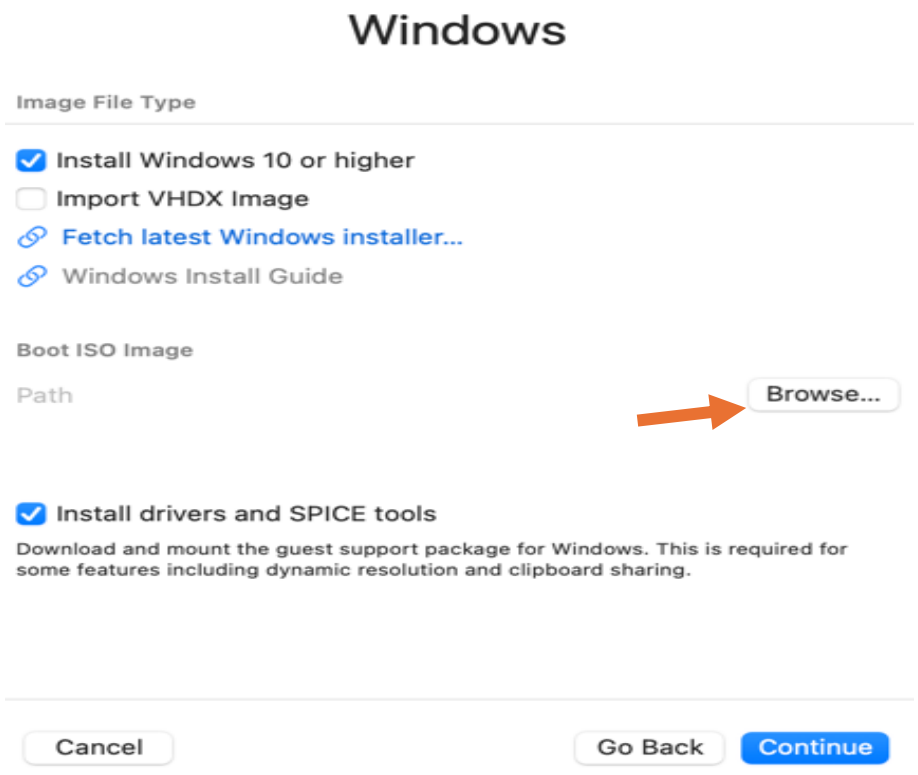
Download on the App Store | Download from GitHub

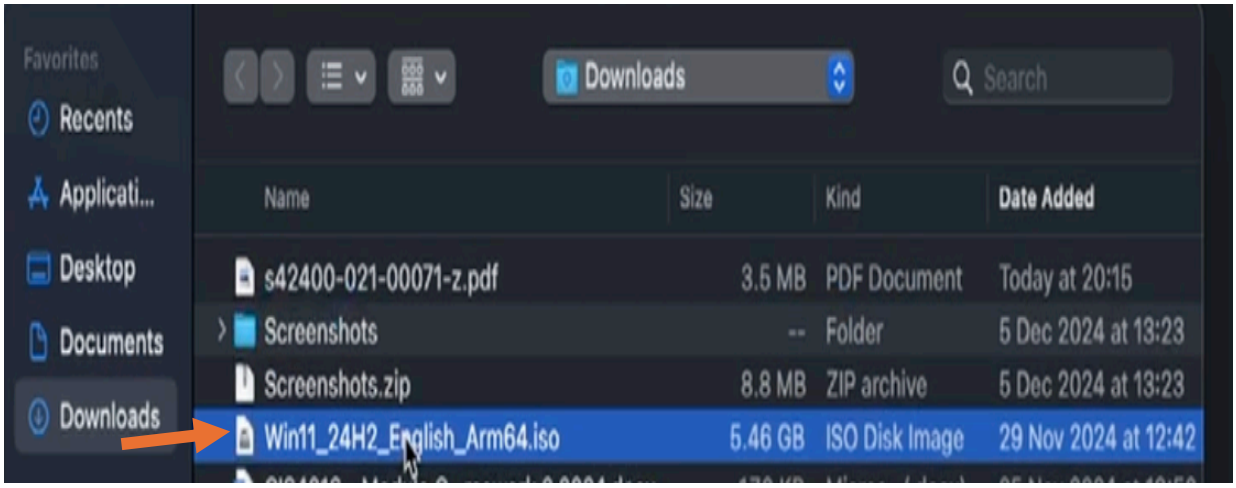
Alternatively, you can also download an older ISO directly from Mi
or Chrome to download as Microsoft's website sometimes does n

- Download Windows 11 for Intel Macs
- Download Windows 11 for Apple Silicon Macs



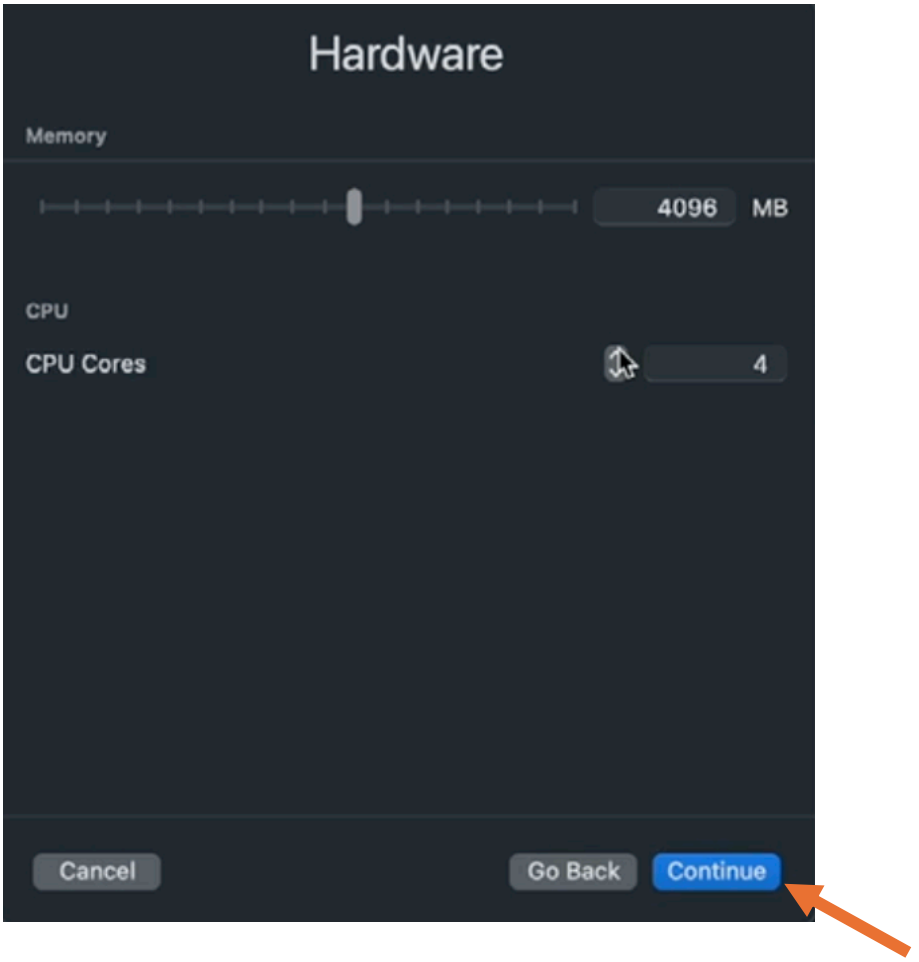
Add the ISO File: Click on Browse to locate the downloaded Windows 11 pro ISO file and click open. Make sure you have Install Windows 10 or higher checked, do not check import VHDX image, make sure to check Install drivers and SPICE tools, its essential for fixing any internet problems and click continue.

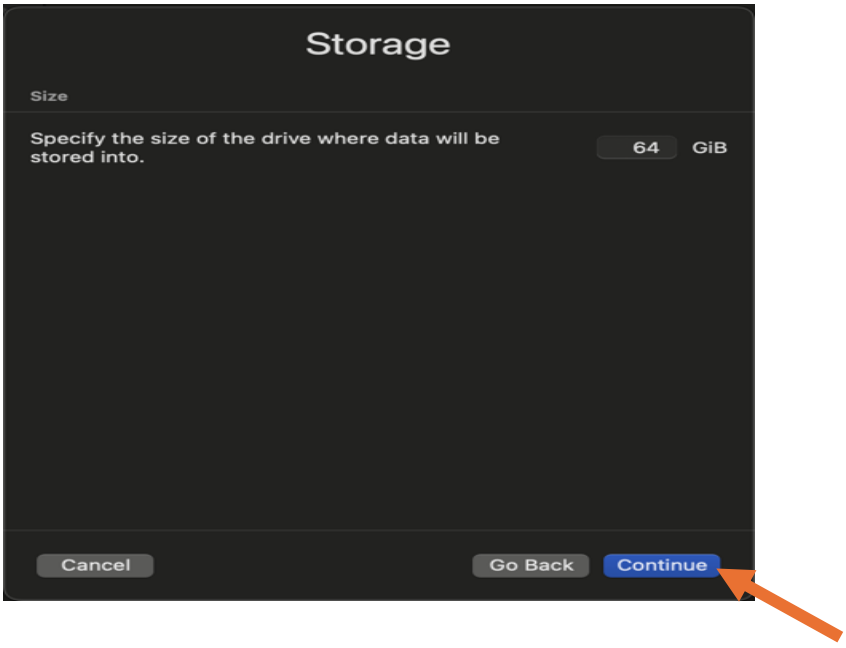




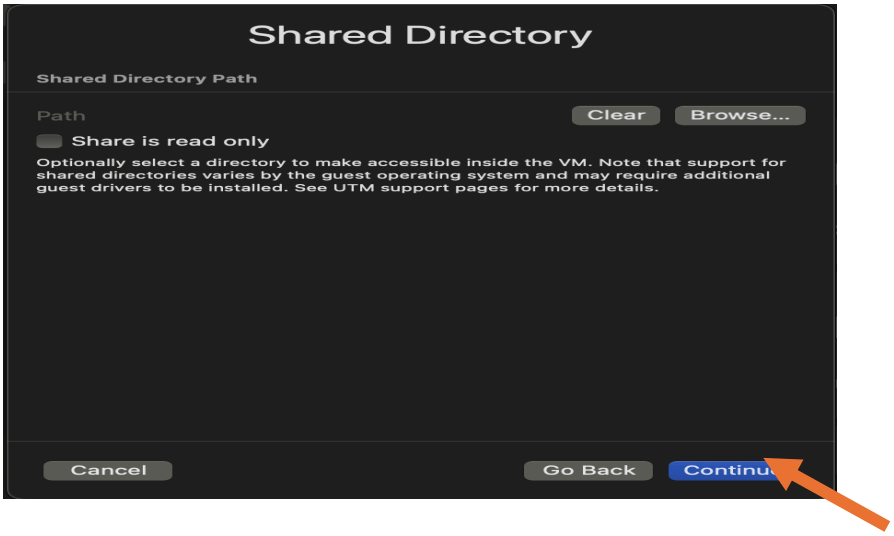
Step 2: Configure the Virtual Machine

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.

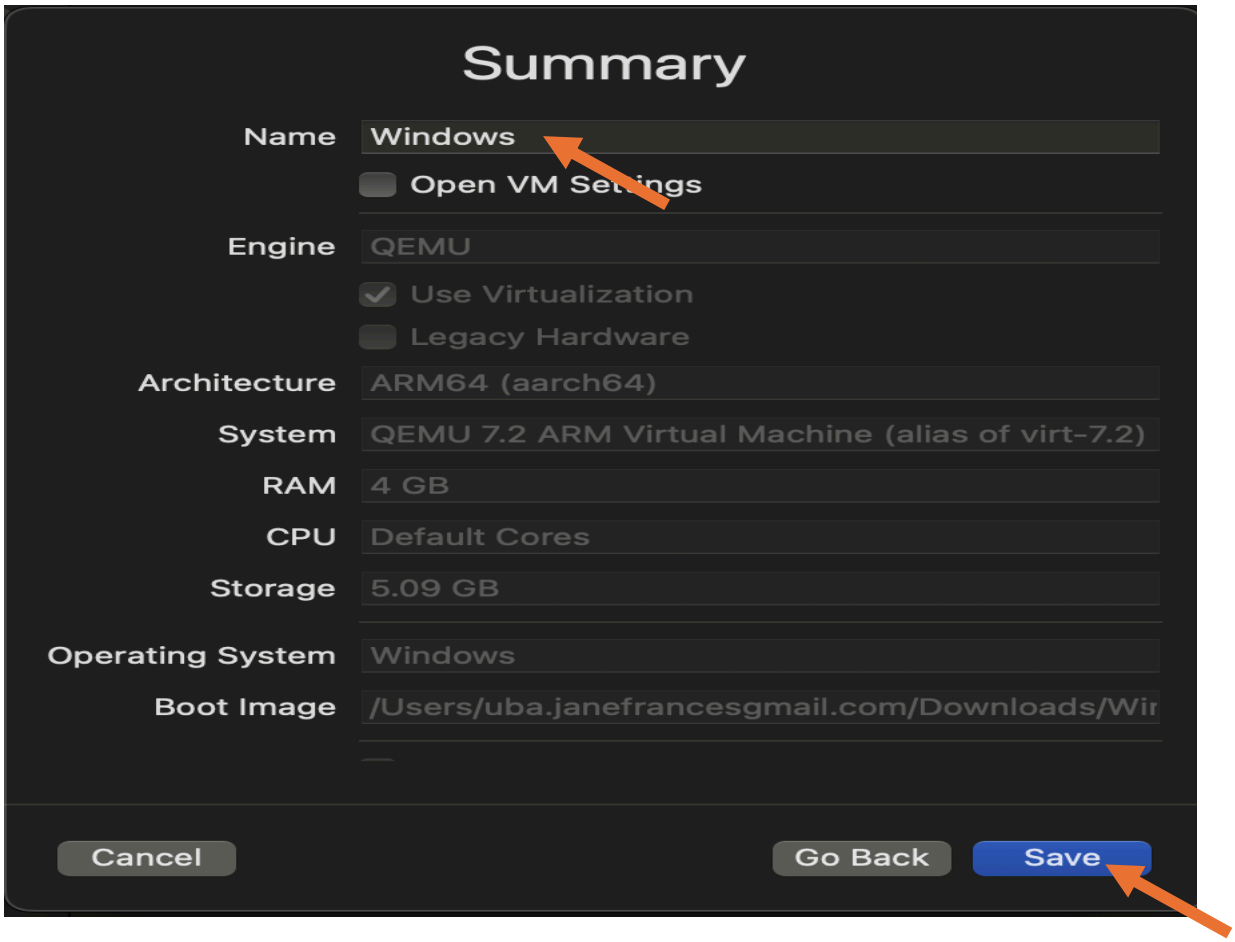

Hardware
Memory
4096
MB
CPU
CPU Cores
4
Cancel
Go Back
Continue


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

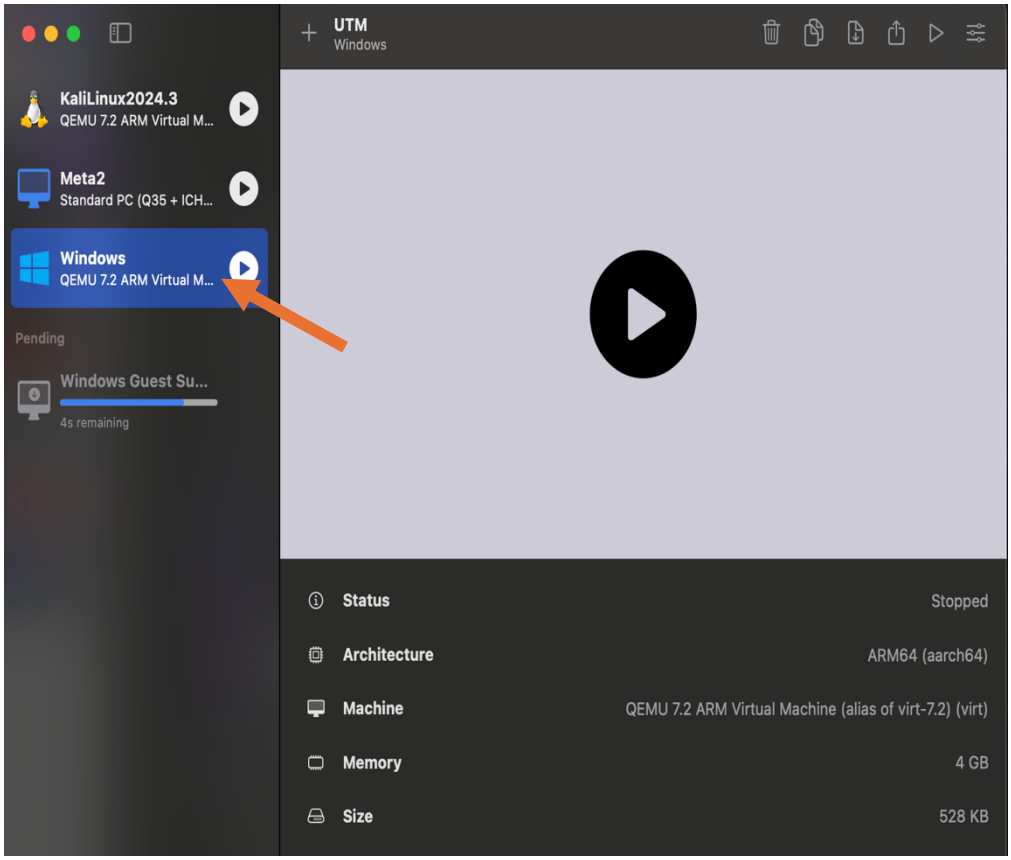


Enter a name for the VM, “Windows” and click Save

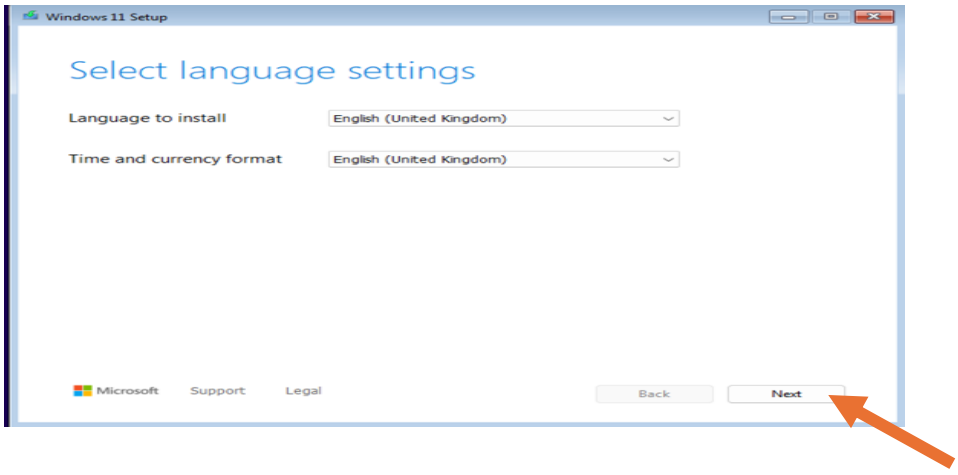


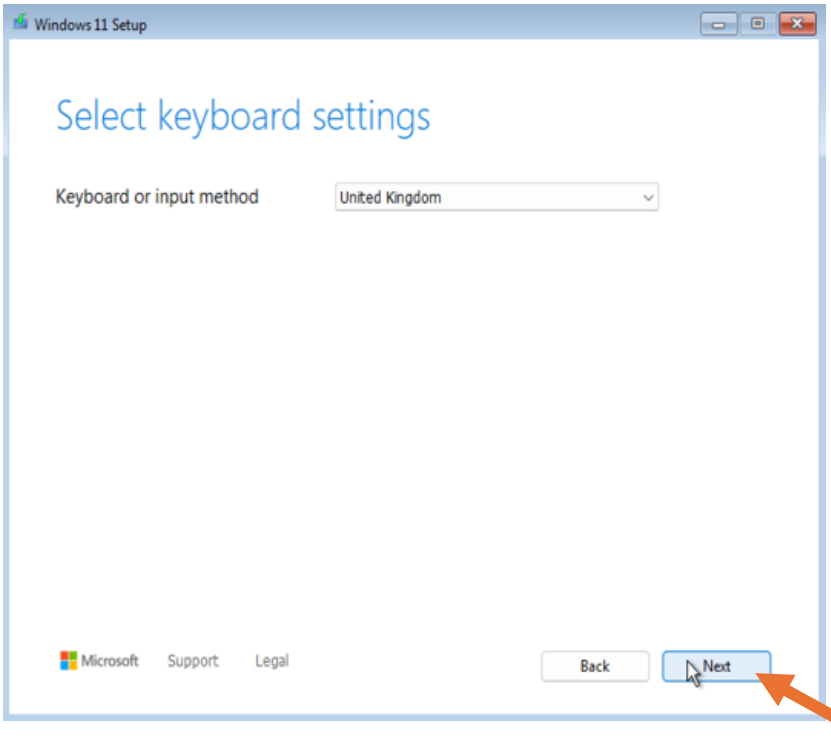
Step 3: Start the Installation

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

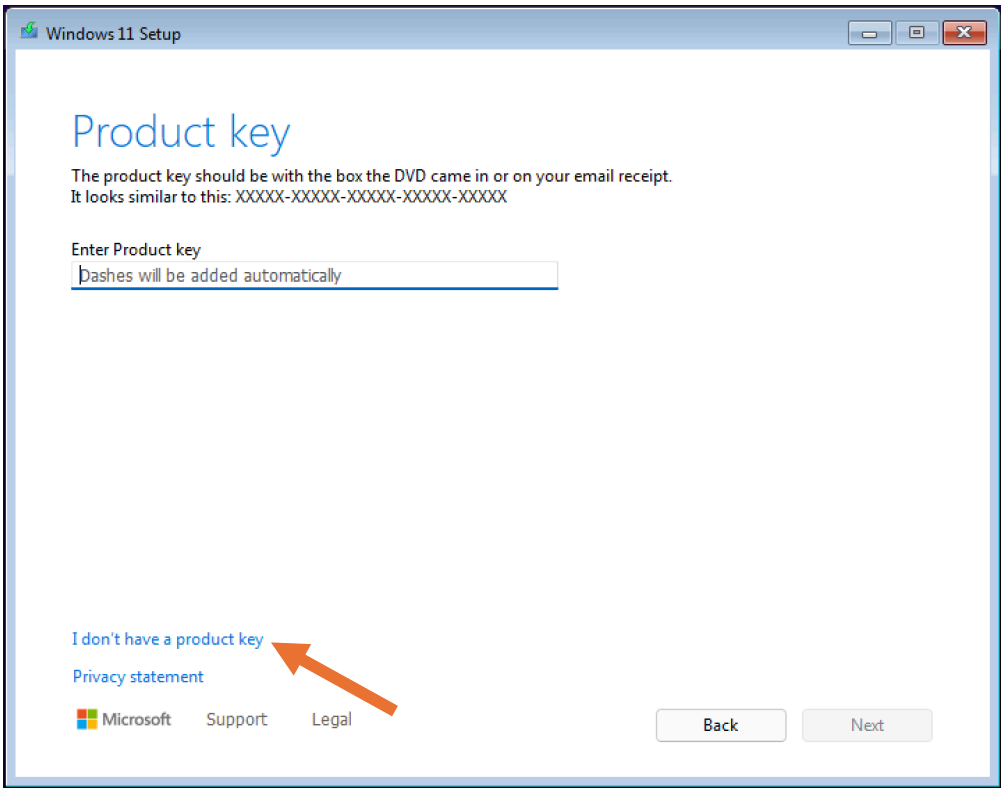


Follow Windows setup steps, the Windows 11 pro installer will launch kindly follow the on-screen instructions steps to complete the installation.

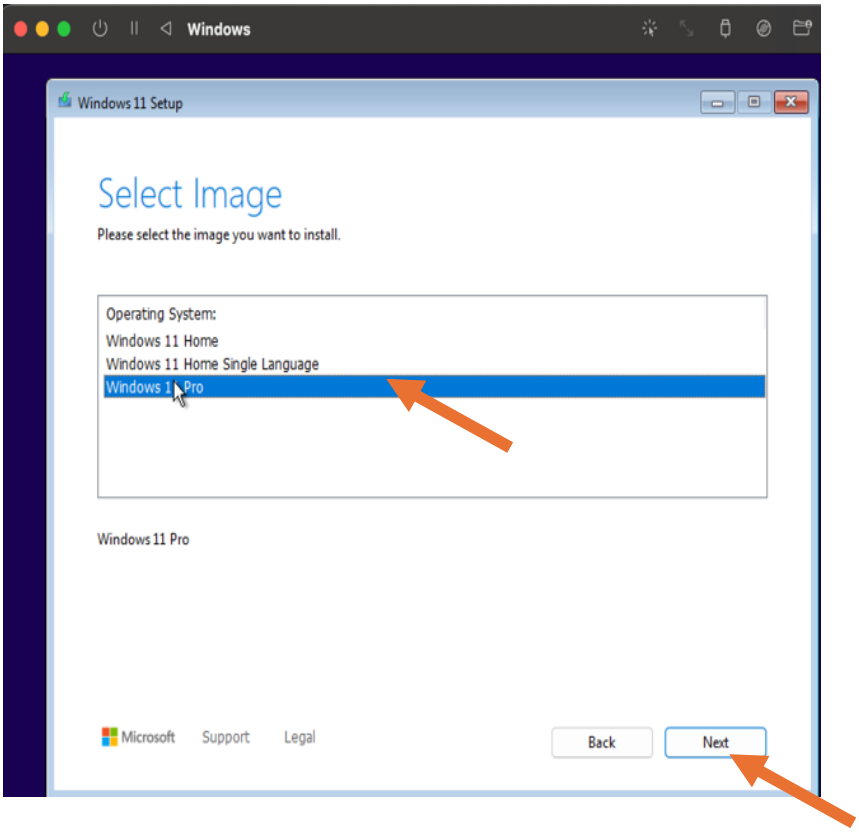




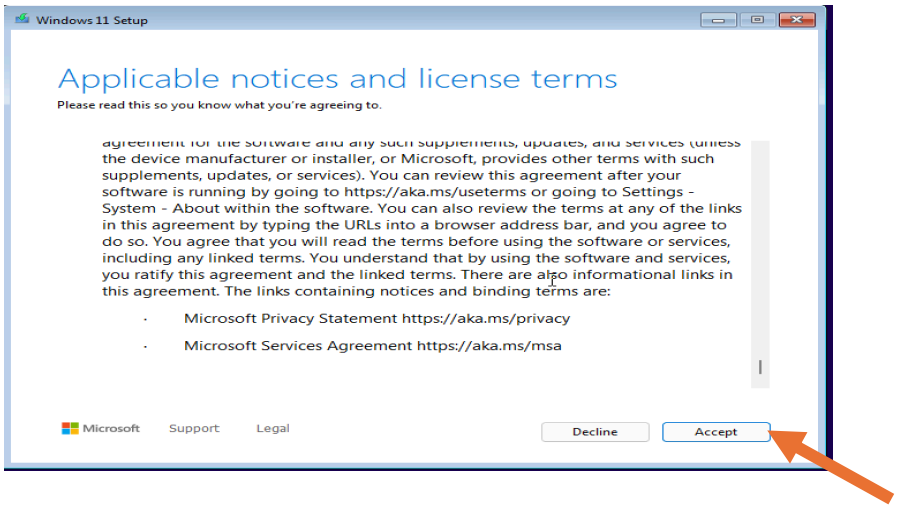
Product key: Add product key if you have, otherwise select I don't have product key.



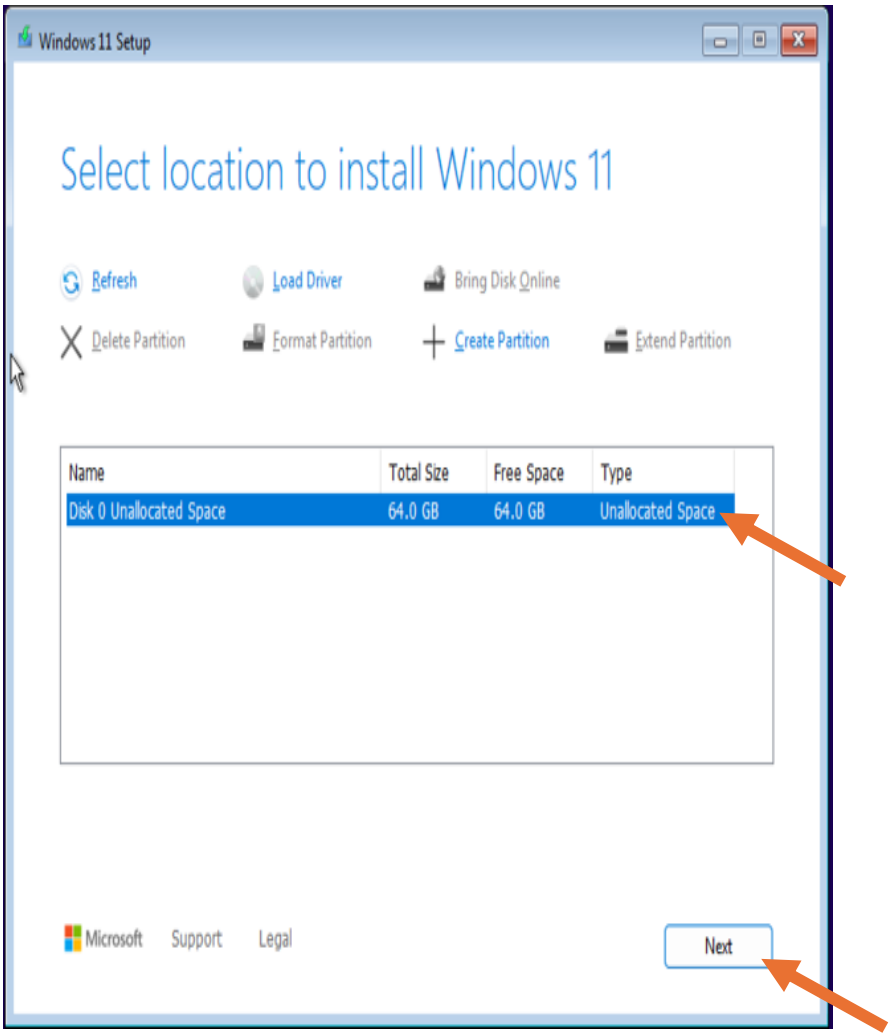
Select the version on the Windows and Click Next



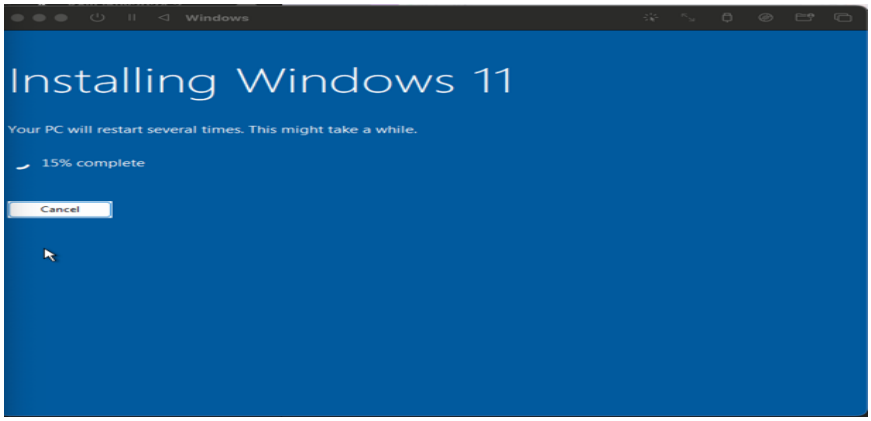
Accept the Licence



Select the Drive Space and click Next

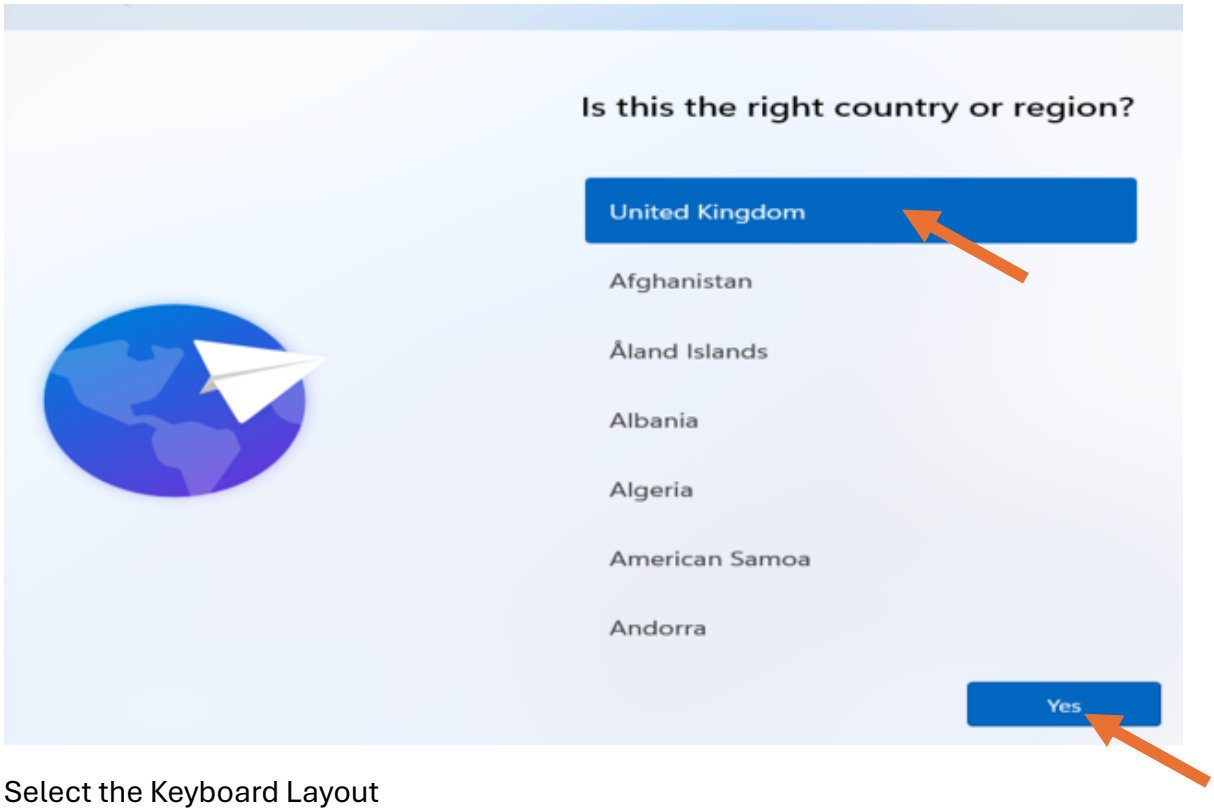


Wait for the Installation to complete

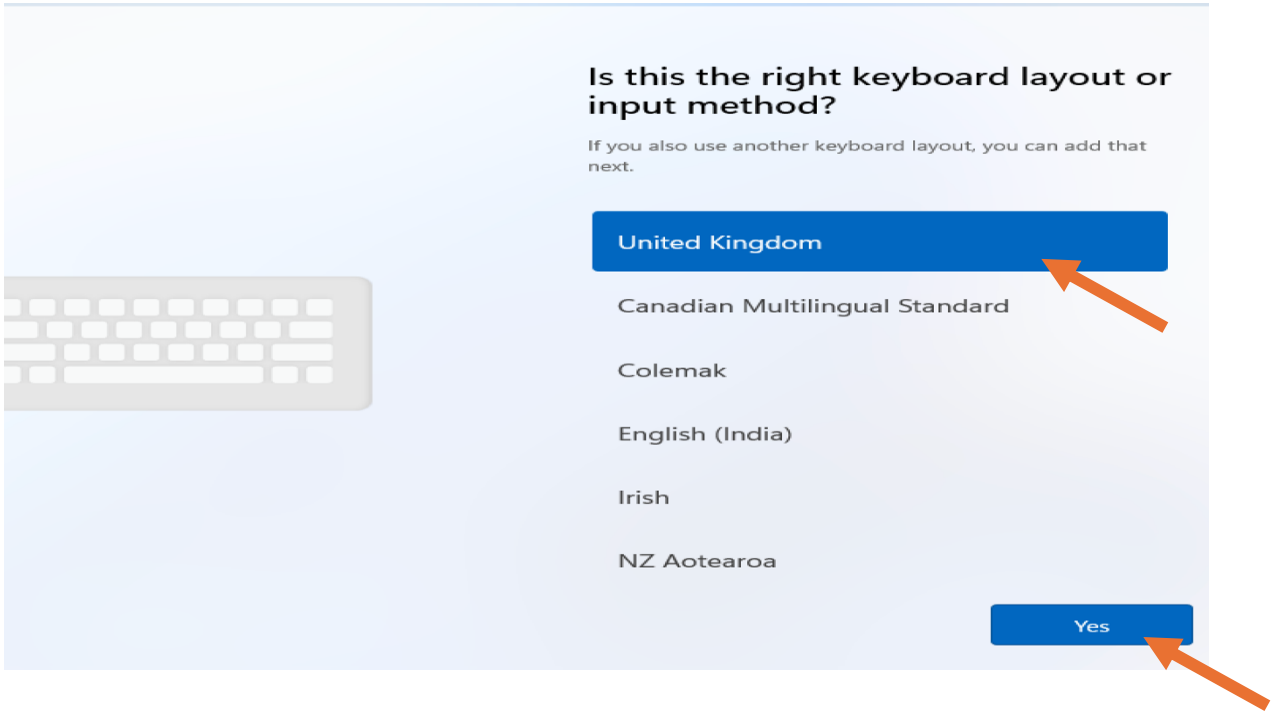


Once the Installation is complete it will restart the windows automatically if not you can click on restart button.

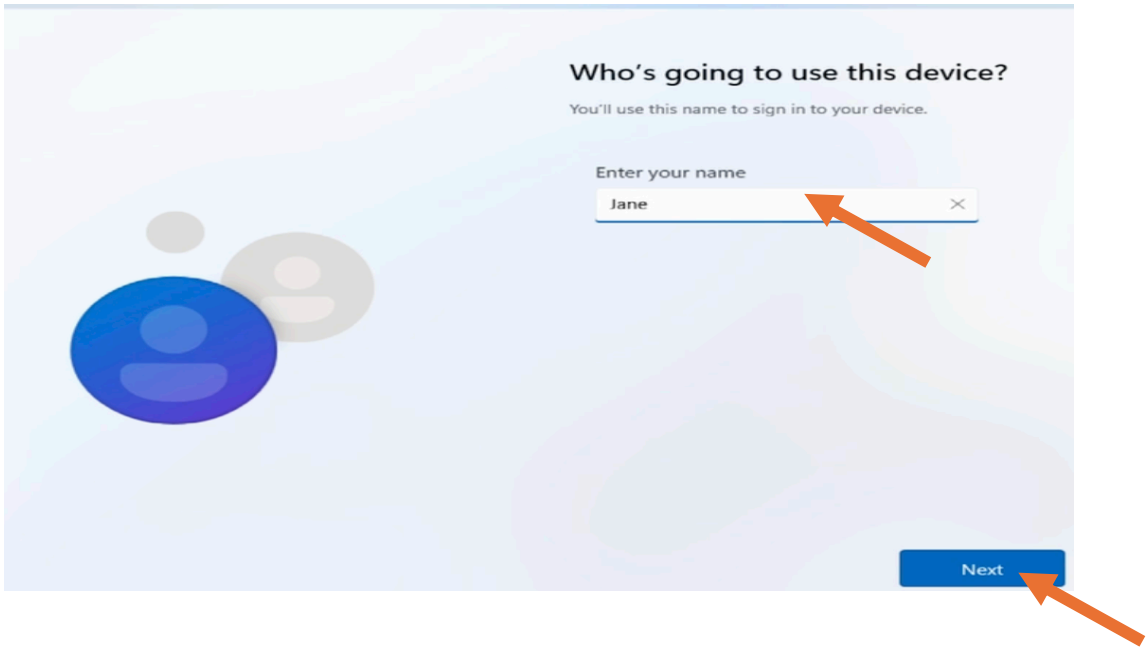
Select the Country

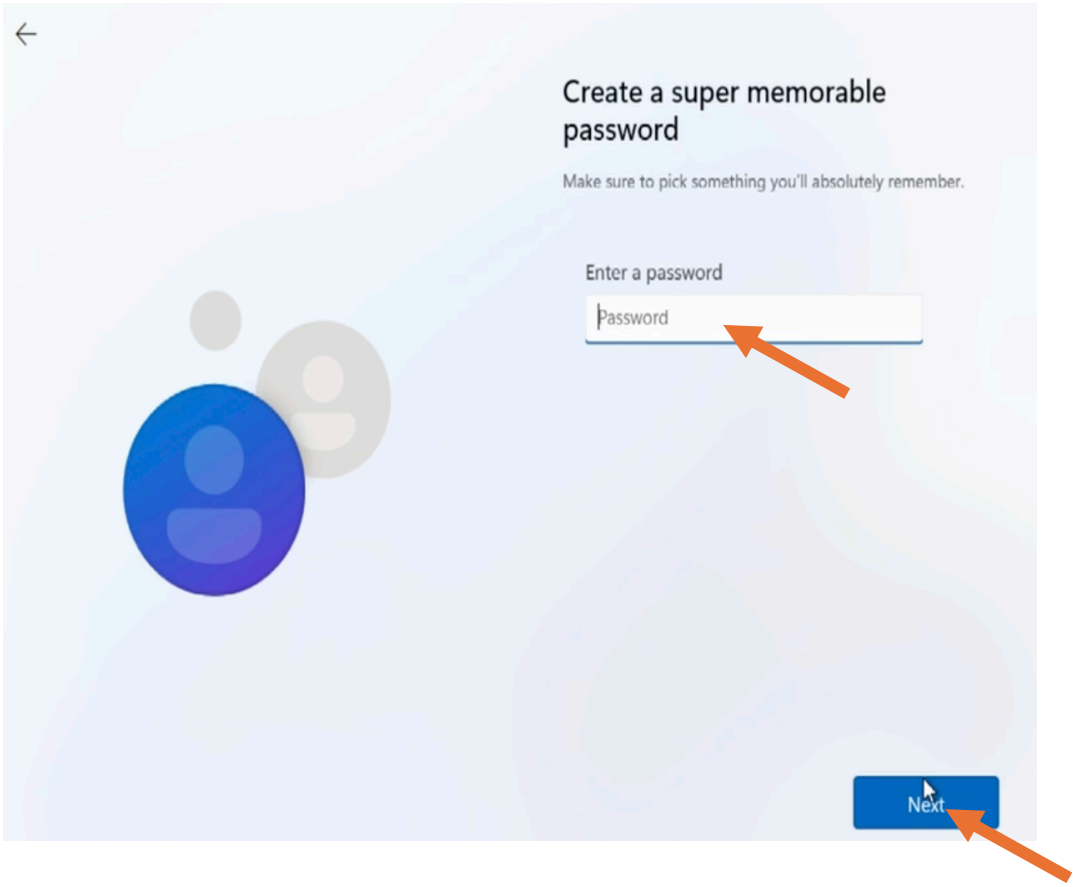


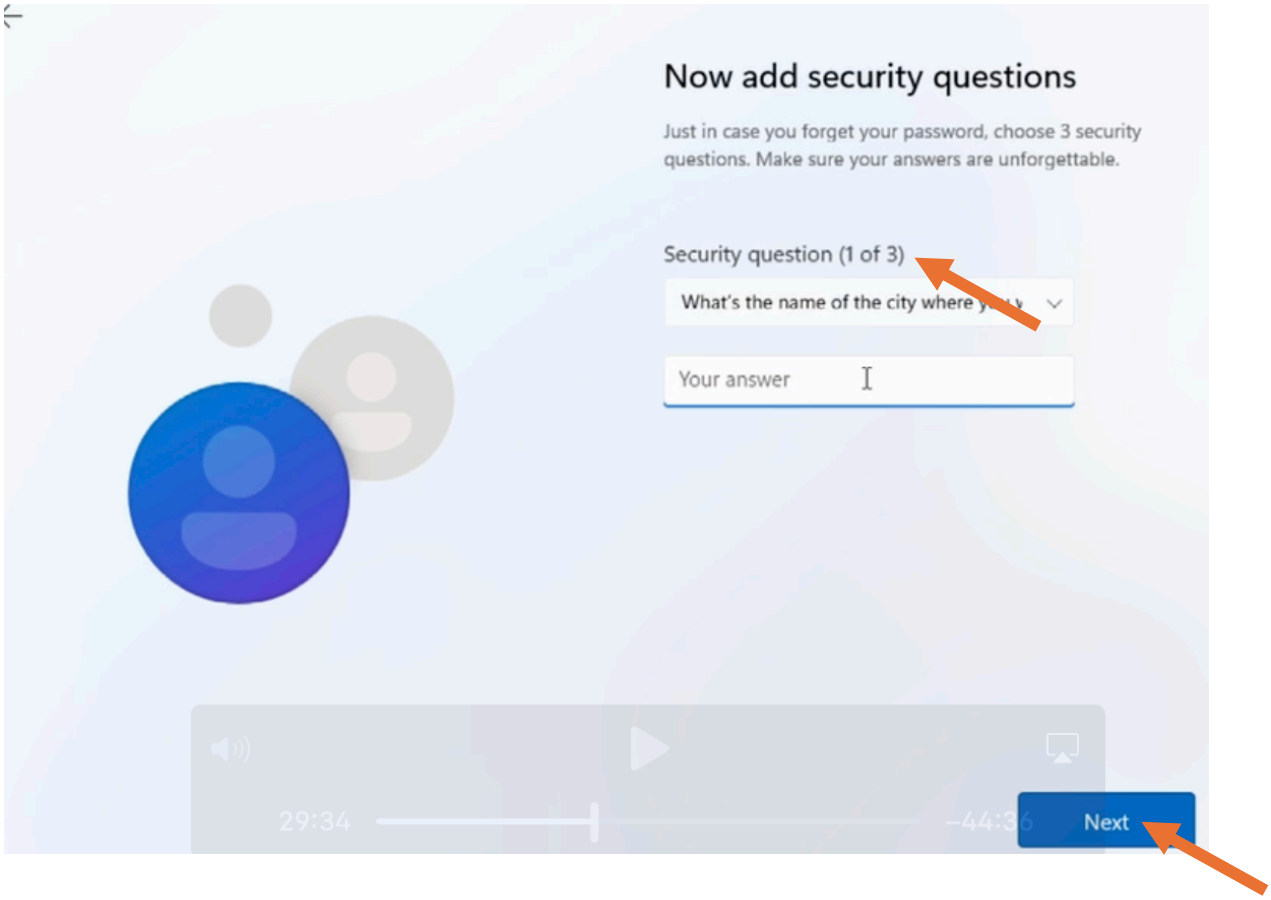
Select the Keyboard Layout



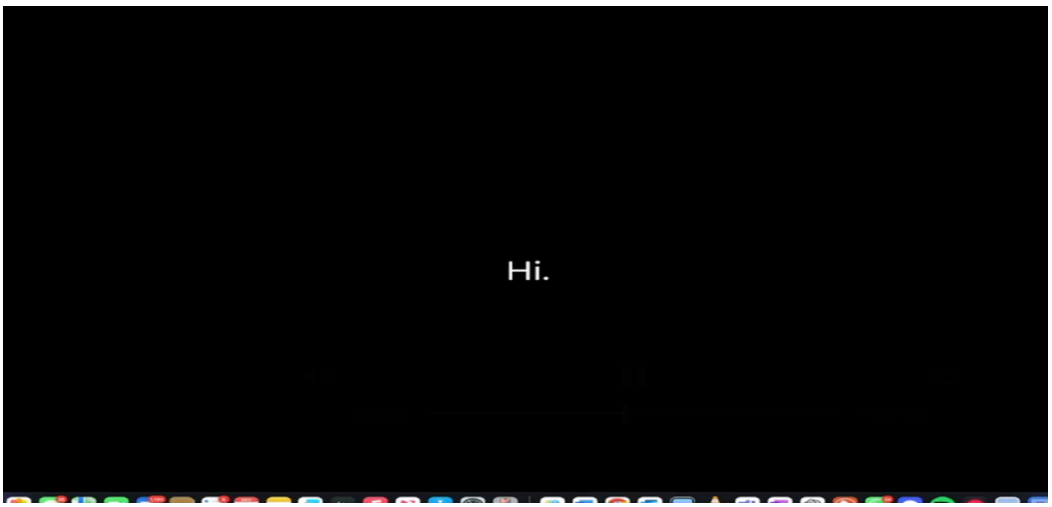
Create your login details “Name, Password and 3 security Questions and Answers”

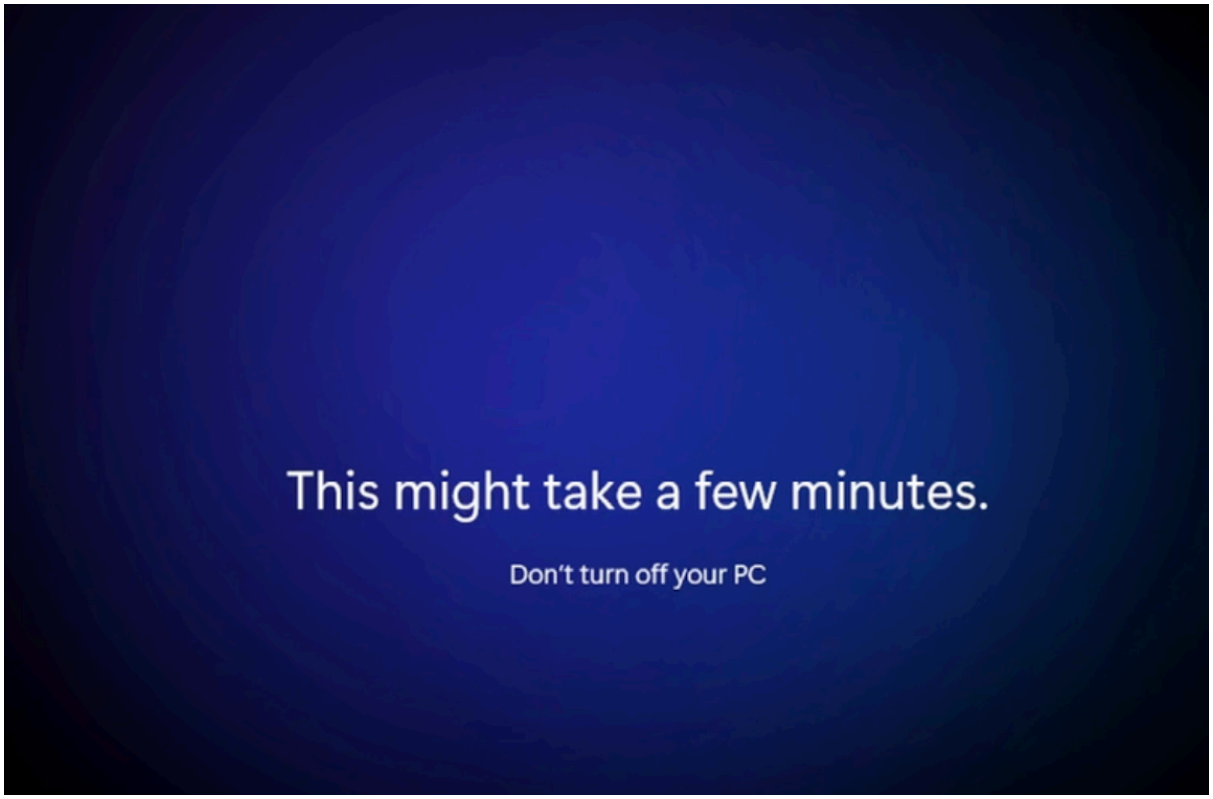




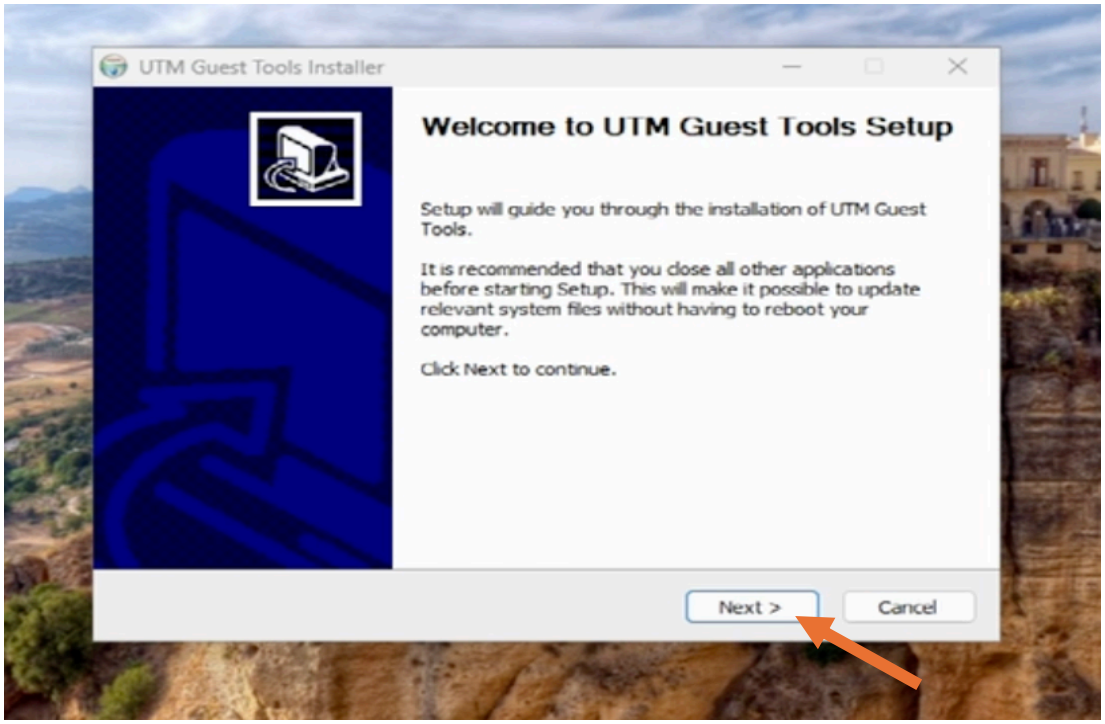


Congratulation you are now booting the windows it will take few minutes so be patient

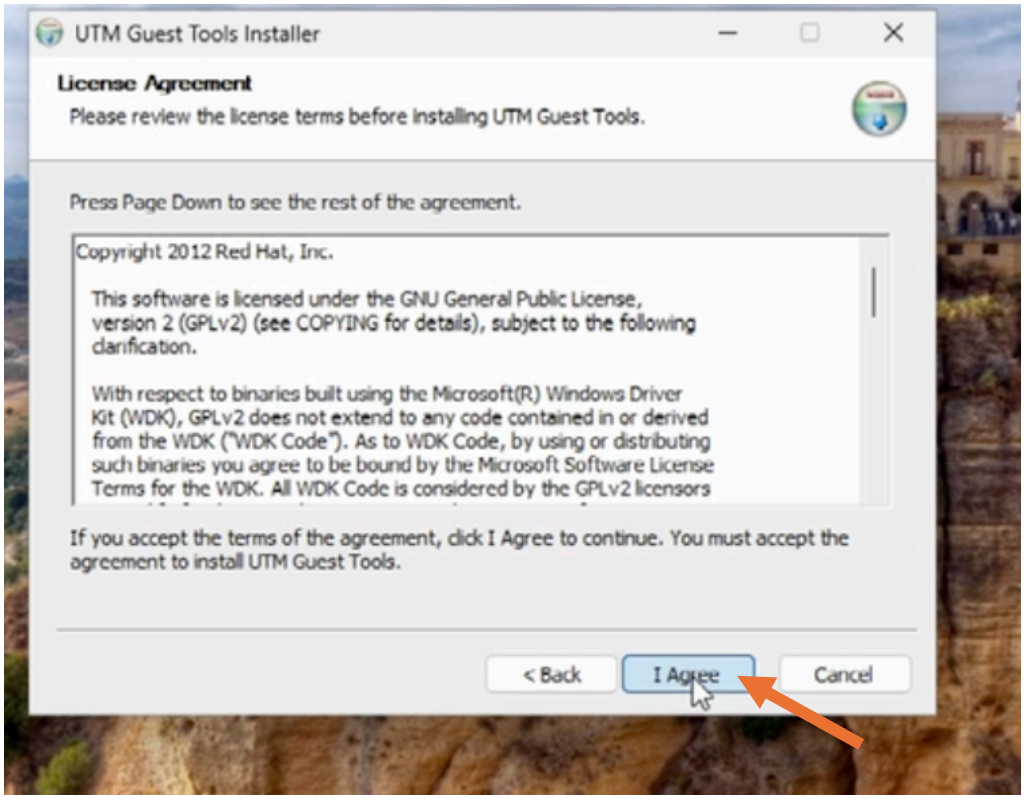


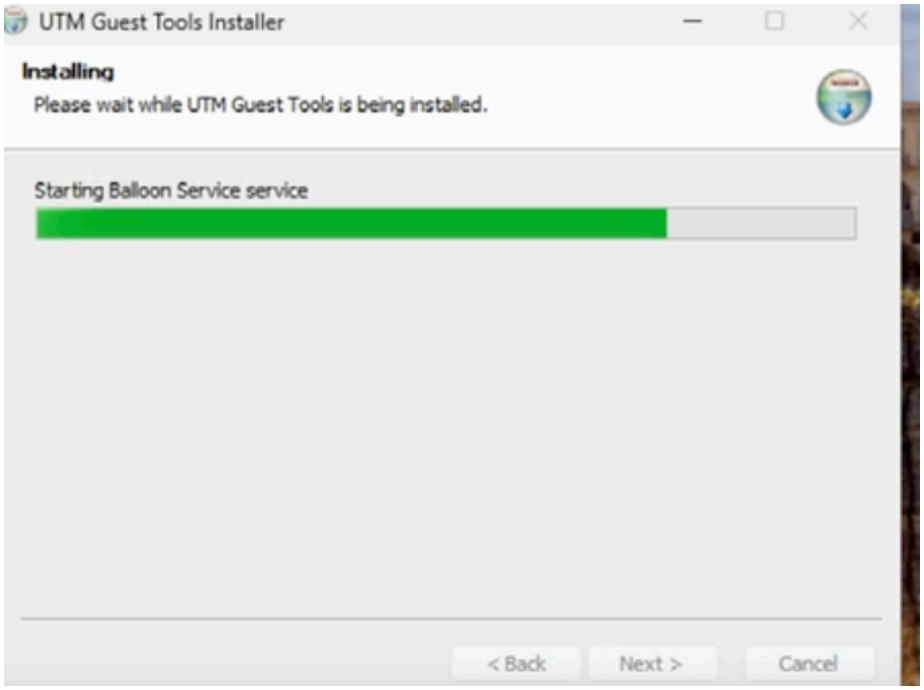


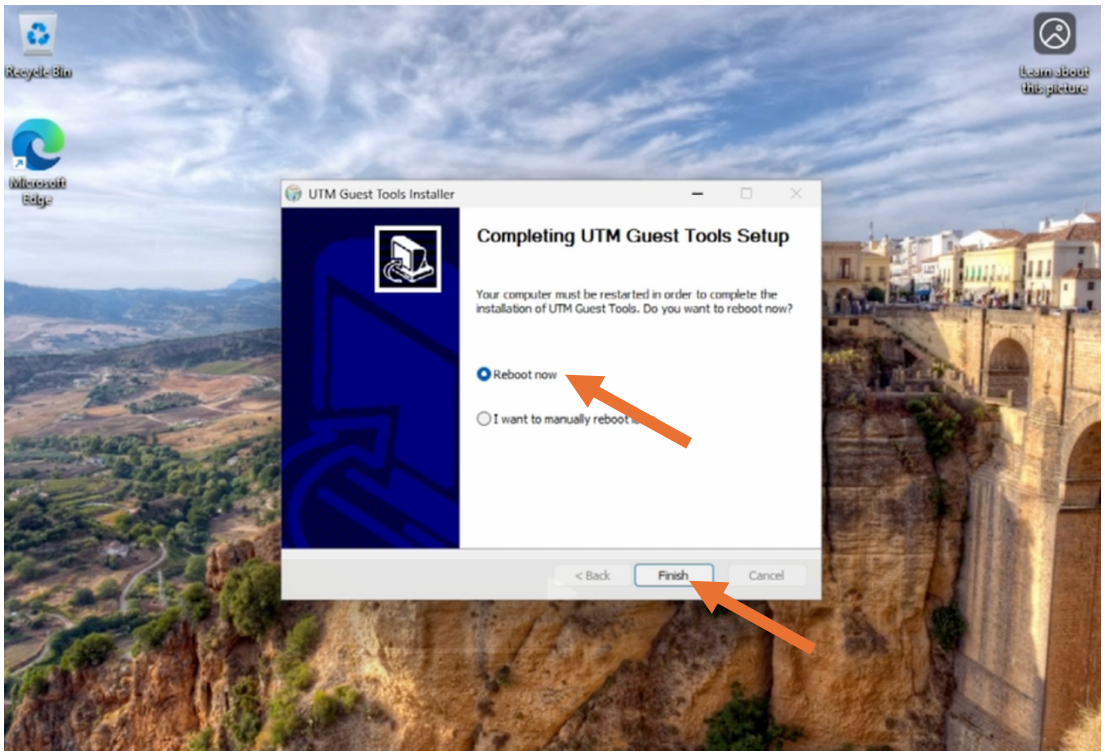
It will automatically lunch the Guest Tools Installer. Click on “Next” to install the Guest Tools.



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

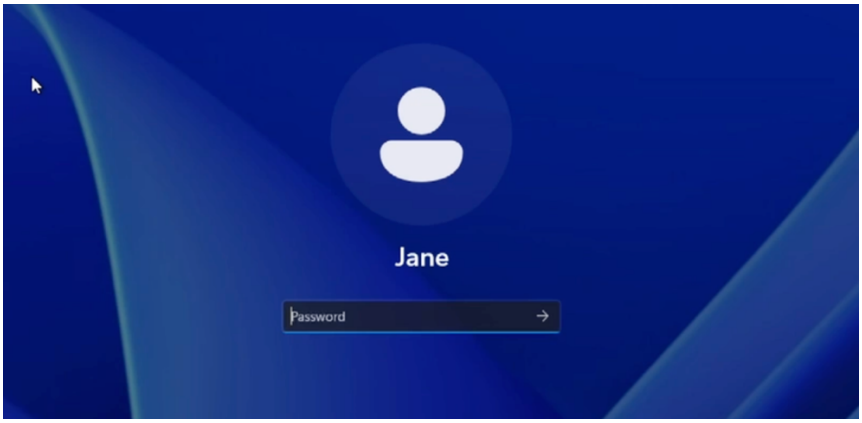






Step 4: Install Guest Tools and Complete the Setup

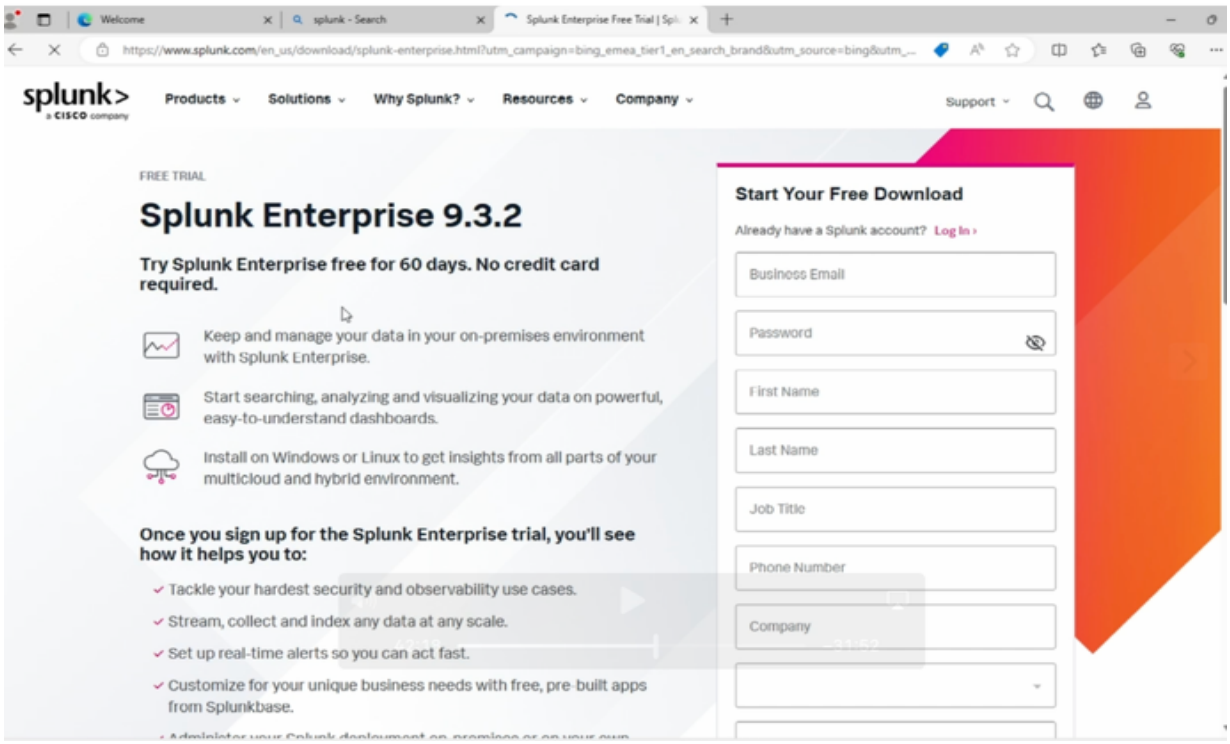
i. After windows in installed, open the UTM menu and install the UTM Guest Tools to enable better performance and additional features like clipboard sharing and resizing.
ii. Restart the VM to apply the changes.
iii. Adjust display resolution, keyboard preferences, and other system settings as needed.



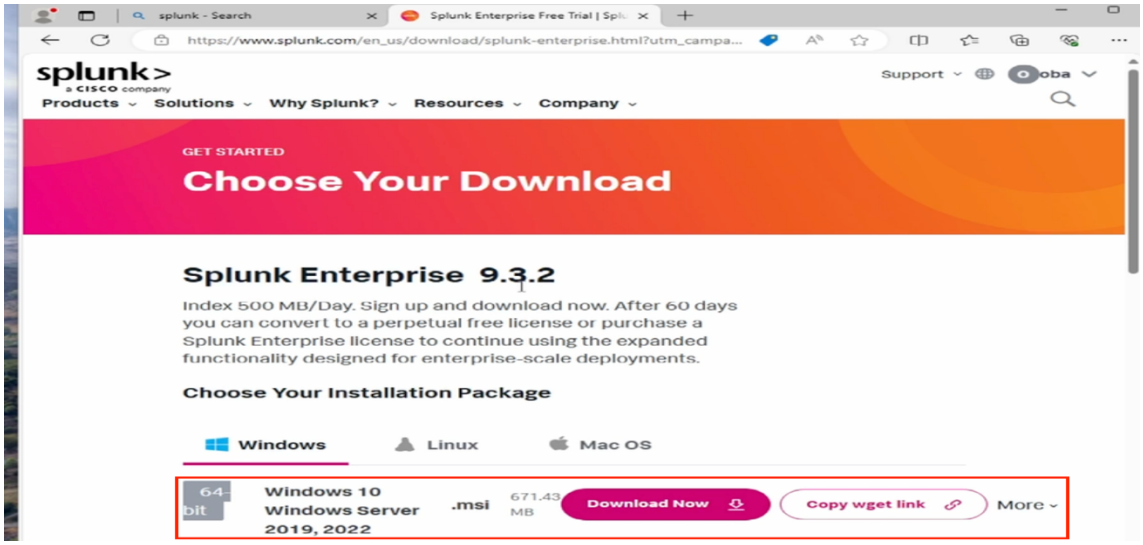
2. **Installation and Configuration of Splunk SIEM on Windows 11 Pro**

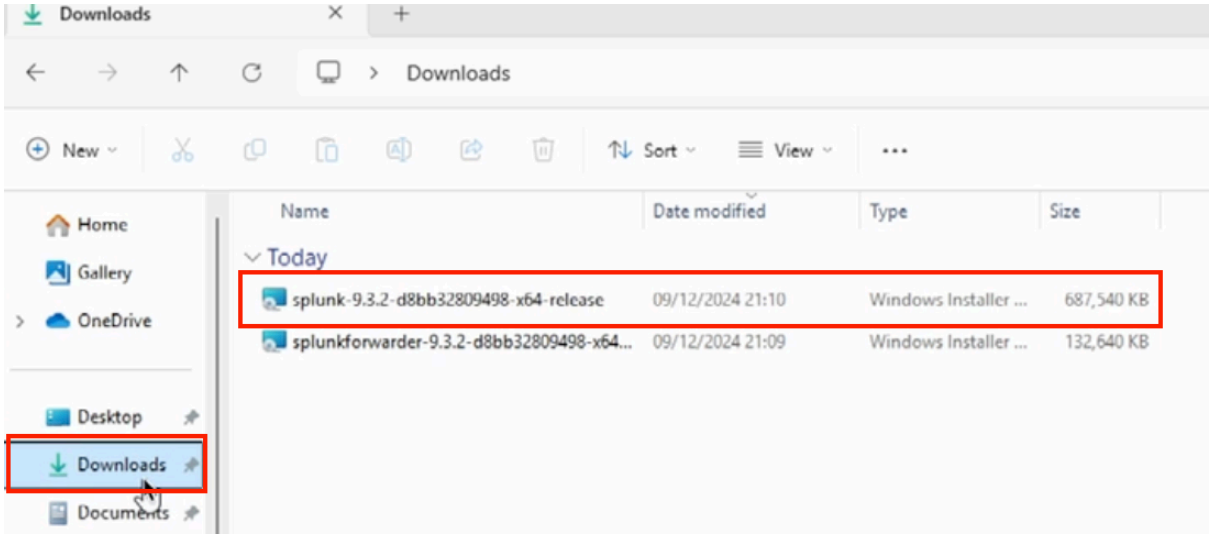
Visit the Splunk website https://www.splunk.com/en_us/download/splunk-cloud.html click on Free Splunk button for 14 days trial if you don't want to be a paid customer.

Create an account and login

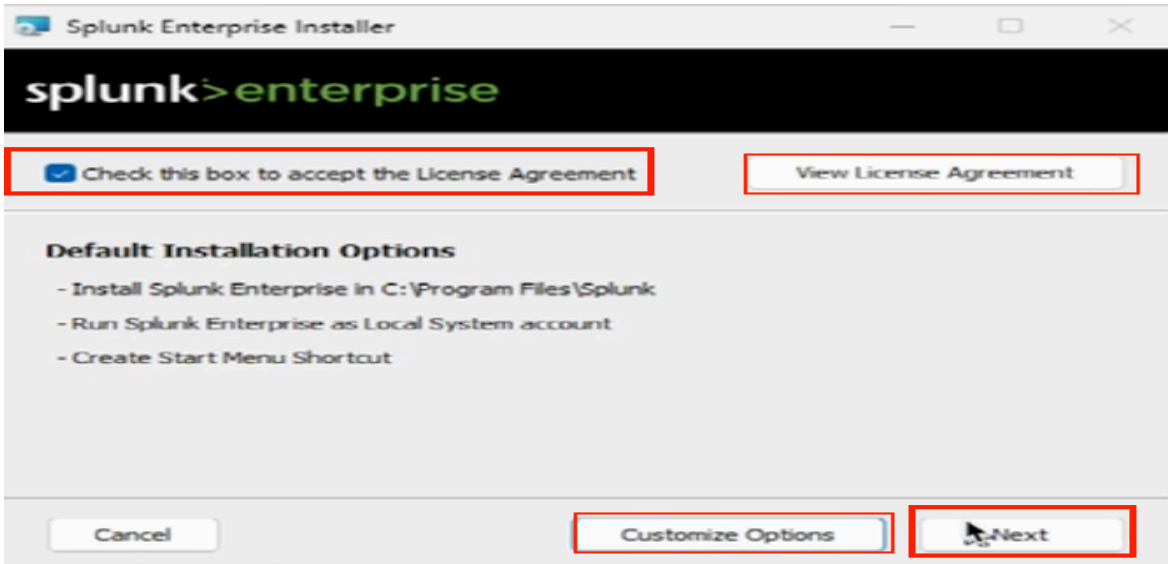


Download .msi installer

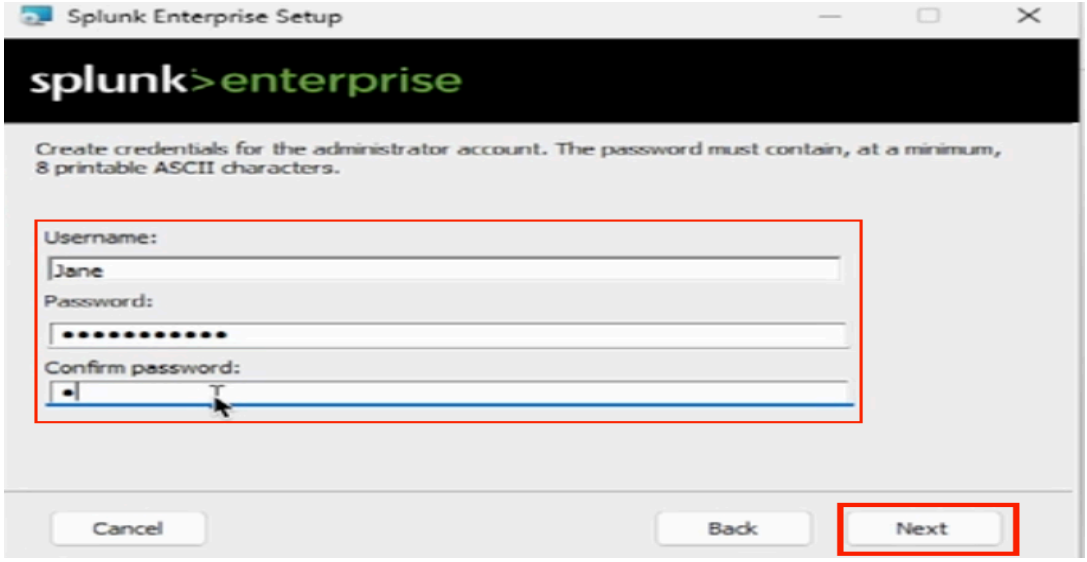




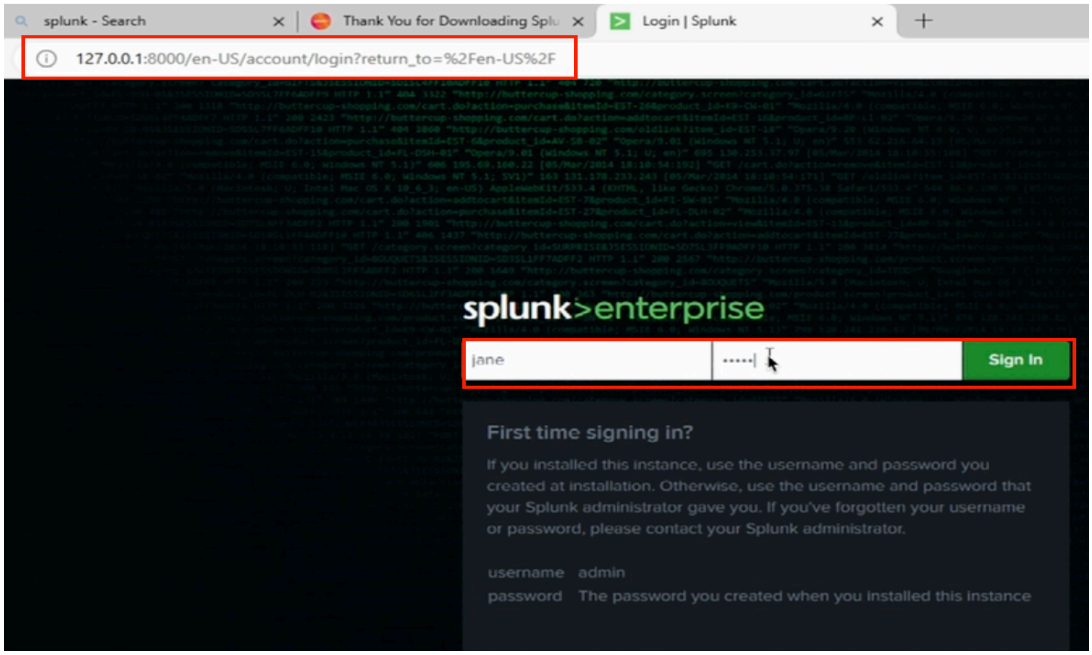
View and read the Licence Agreement for better understanding of how your data will be use.
Check the box and accept the Licence Agreement, customize Options will be automatically selected but if not press the button, and click Next

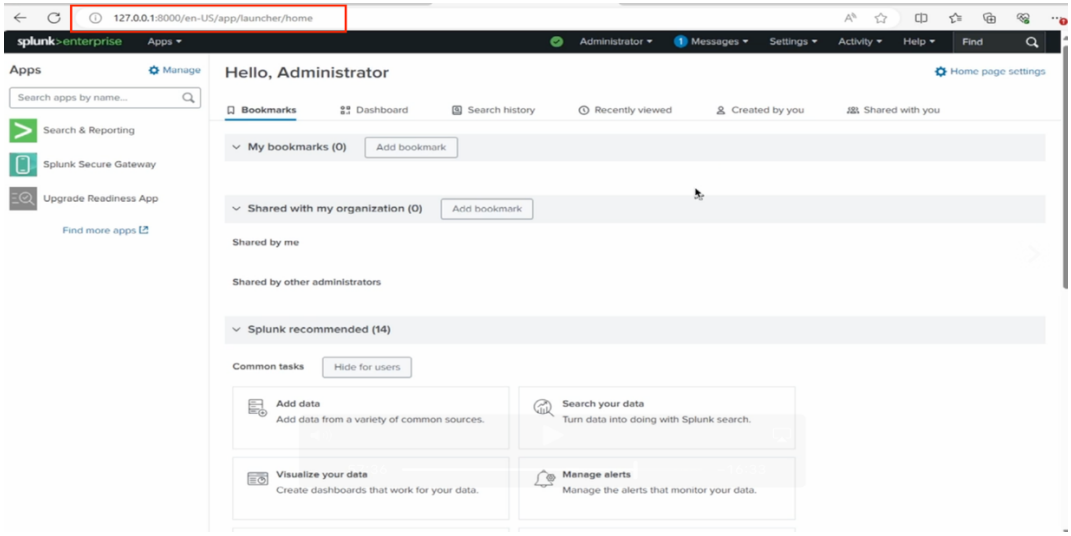


Select where you want to install Splunk
Install Splunk as local System
Set Username and Password and click Next

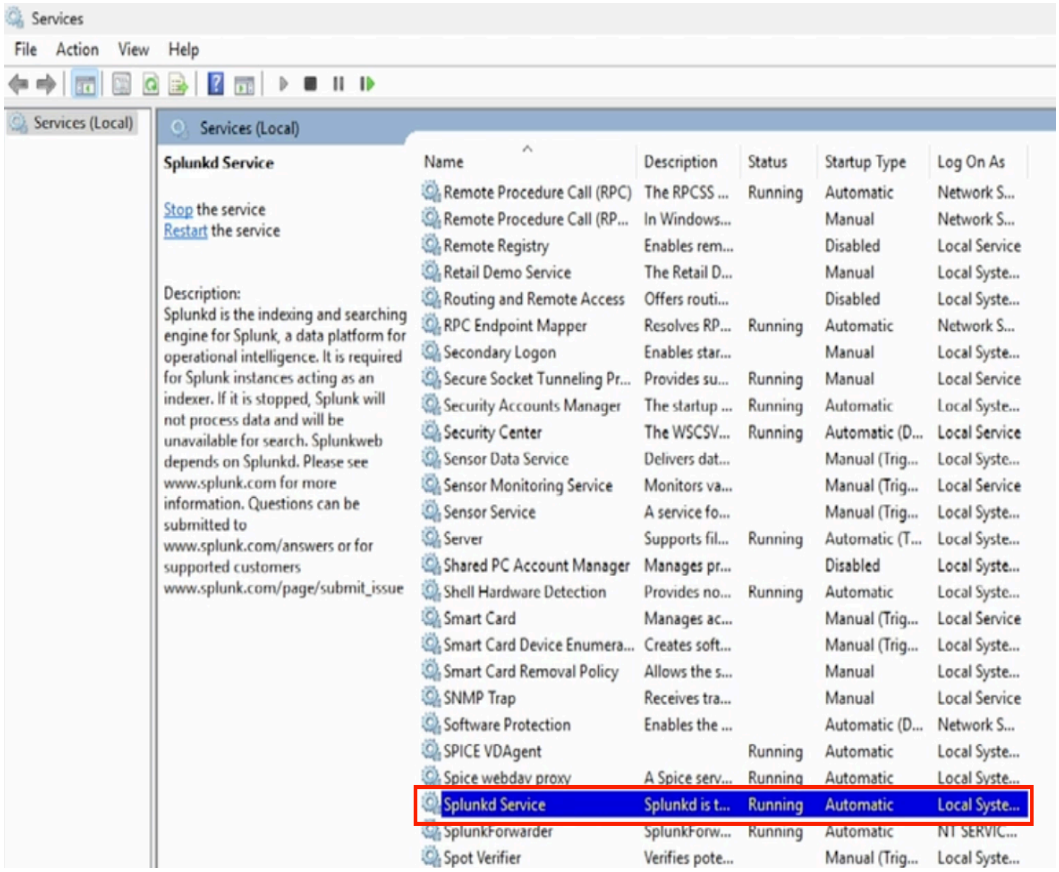


Launch the install and wait for the installation
Once done check the Splunk installation via https://127.0.0.1:8000 if it didn't open automatically
Login with the Username and Password created



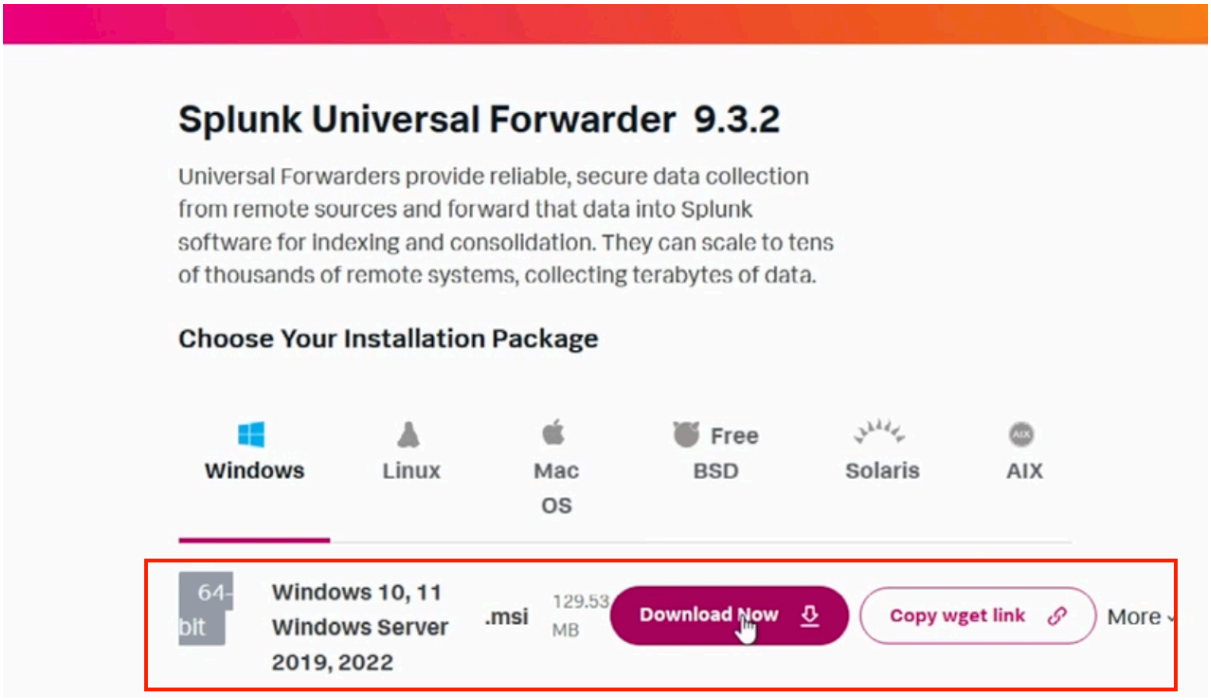


Check the Splunk Service Status. Type services on the Windows search to find Splunkd Service. Monitor the service, status and startup type, check the state of the Splunk it must be in running status.



3. Installation and Configuration of Splunk Universal Forwarder

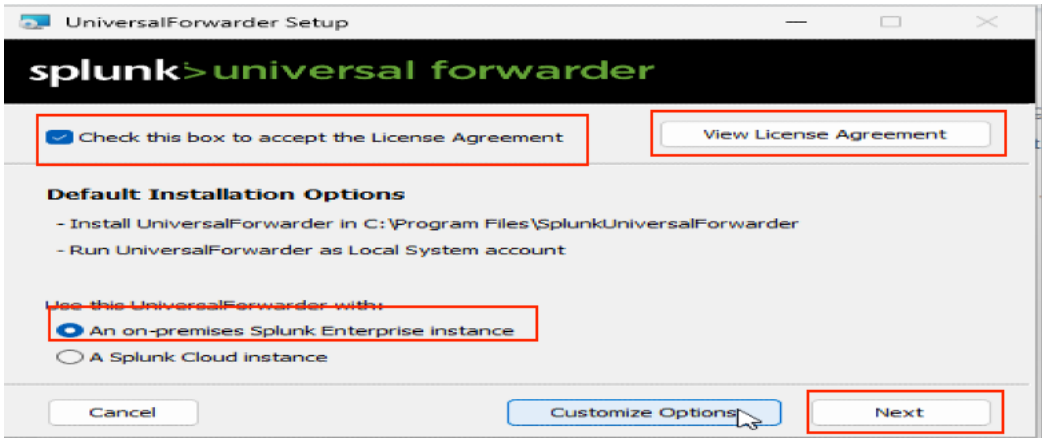
Visit the Splunk website https://www.splunk.com/en_us/download/universal-forwarder.html
Download the windows 10, Windows 11 … msi setup file



Launch the Splunk Universal Forwarder

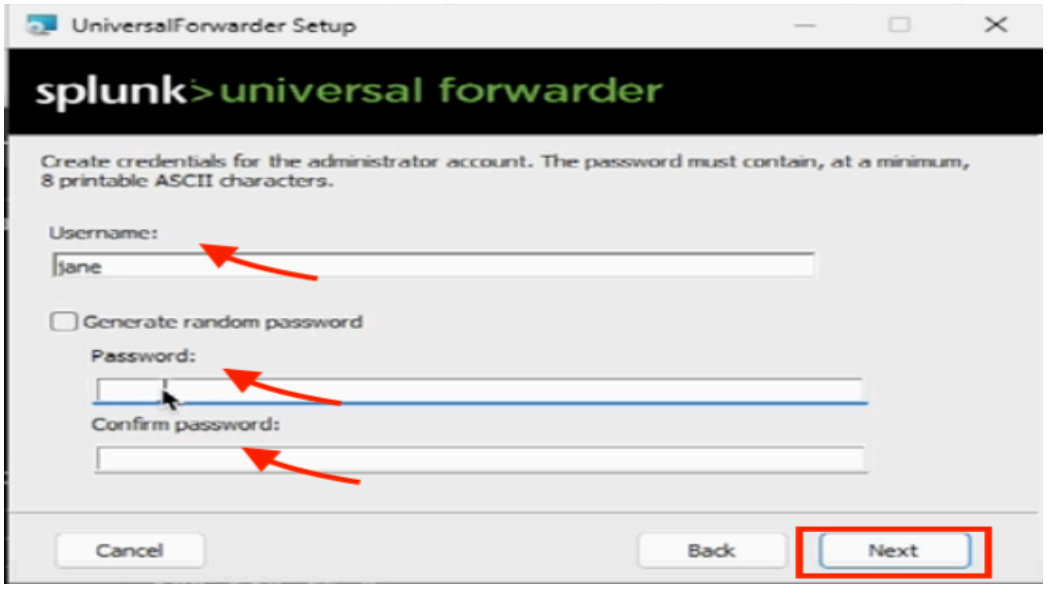
View and read the Licence Agreement for better understanding of how your data will be use.

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.

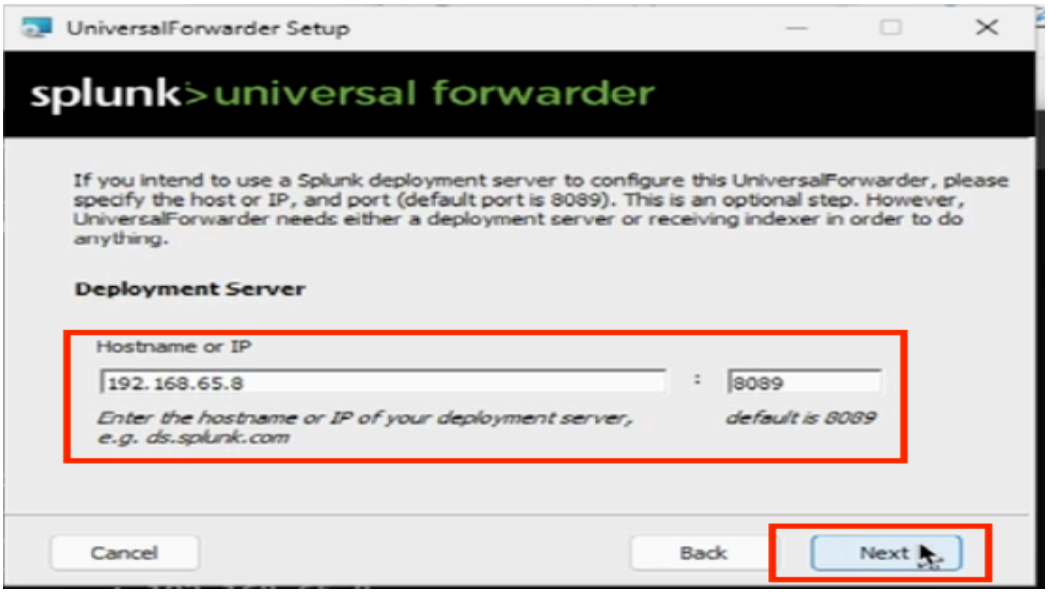


Set Username and Password to the Universal Forwarder and click Next

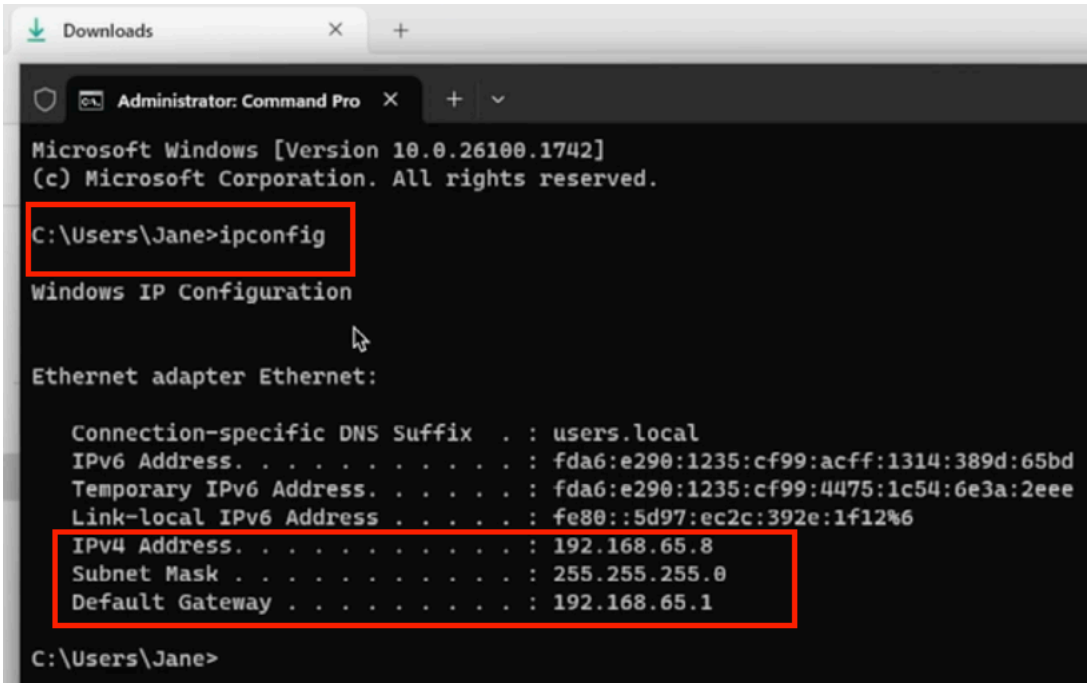
Note you can check Generate random password if you want randomized password



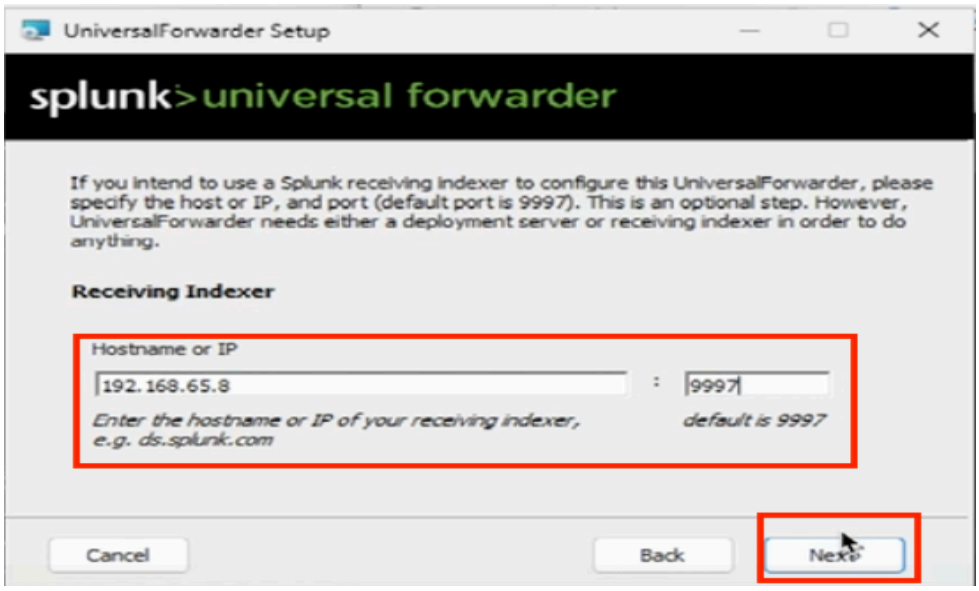
Write the server IP and the port to the Deployment Server and Click Next
Note: Splunk is installed on MacOS machine so the IP address of the machine is used



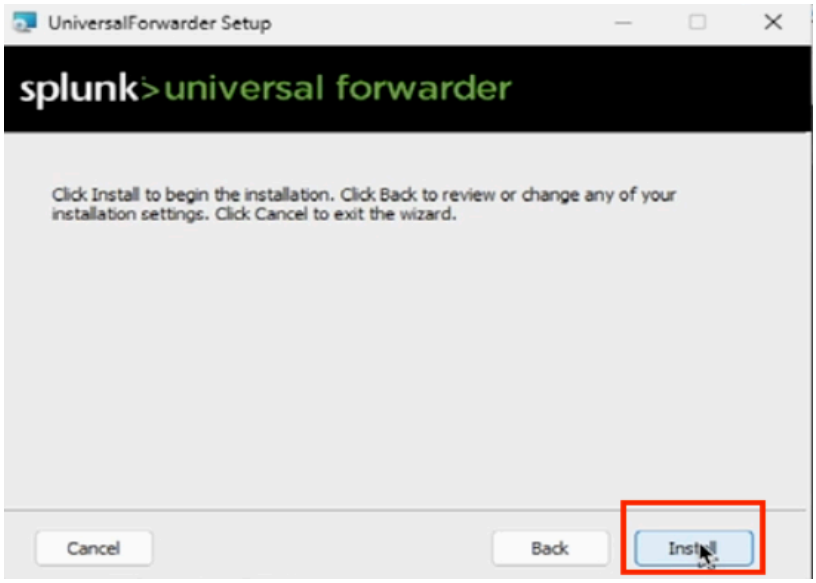
Type CMD on the Windows search bar to open the command prompt, run "ipconfig" as shown in the diagram to get the IP address of the machine.



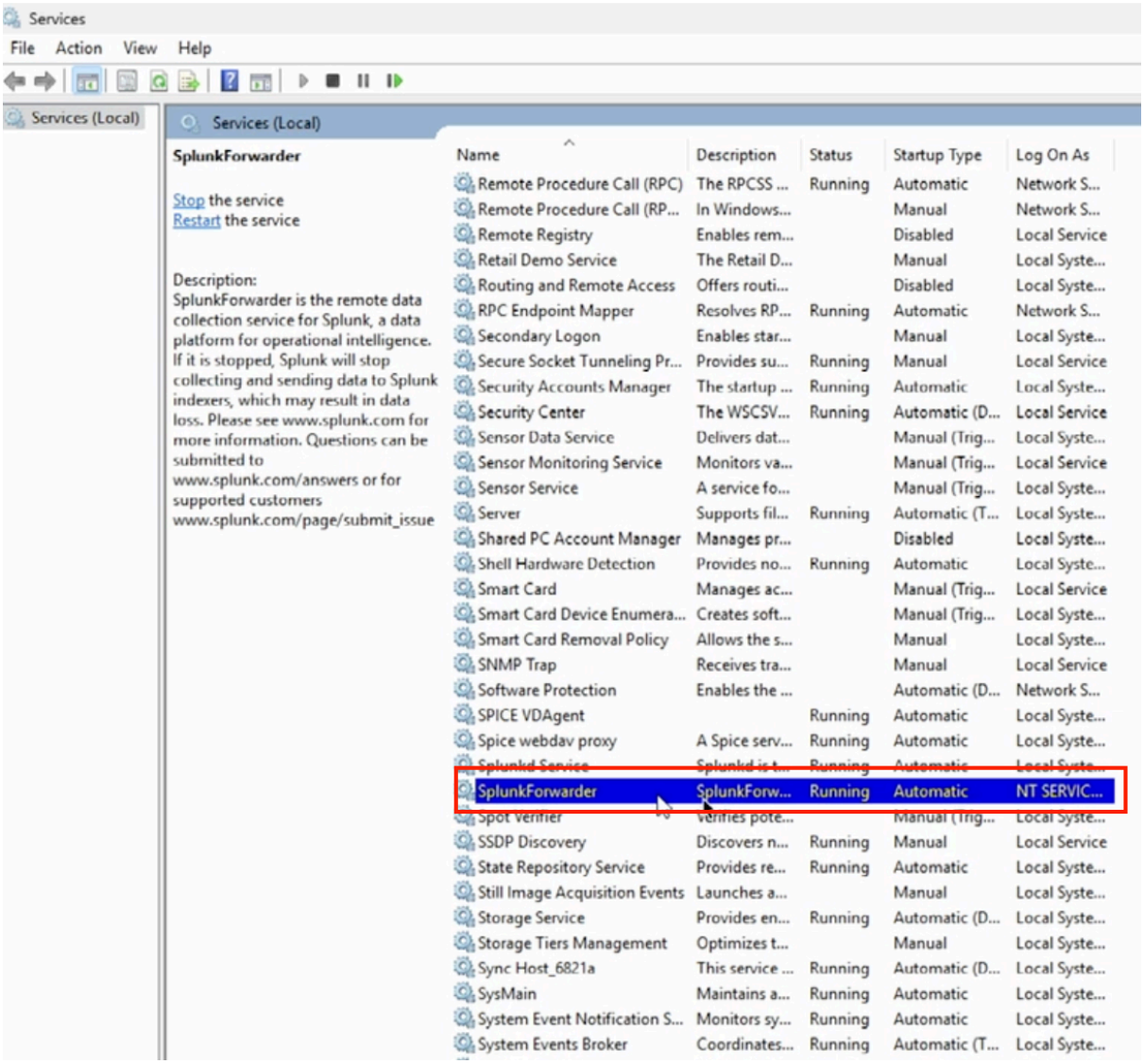
Write the server IP address which is the same as the Deployment server and port which is 9997 “Note: 9997nis a default port” to the Receiving Indexer and click Next



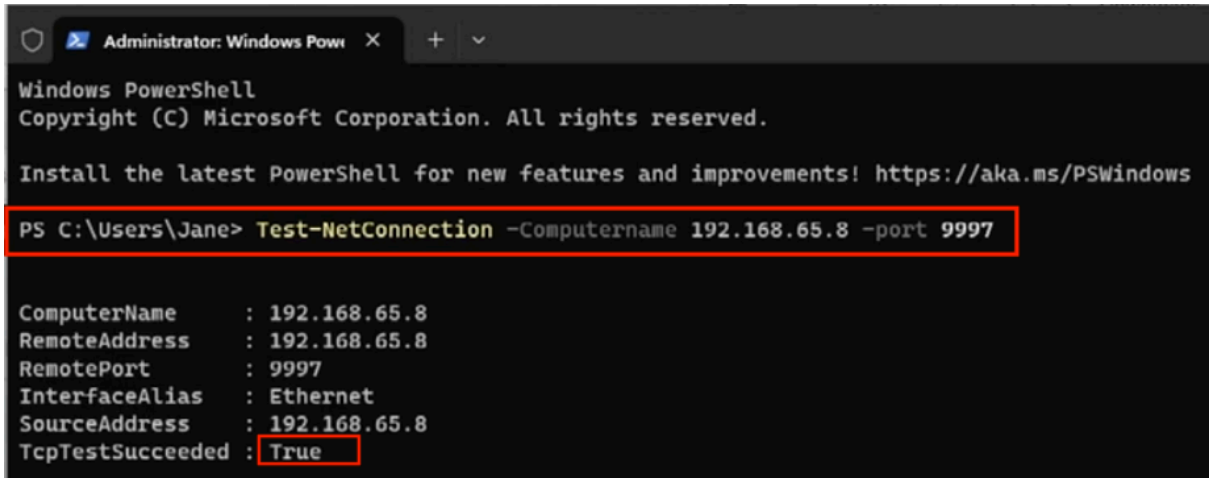
Launch the install



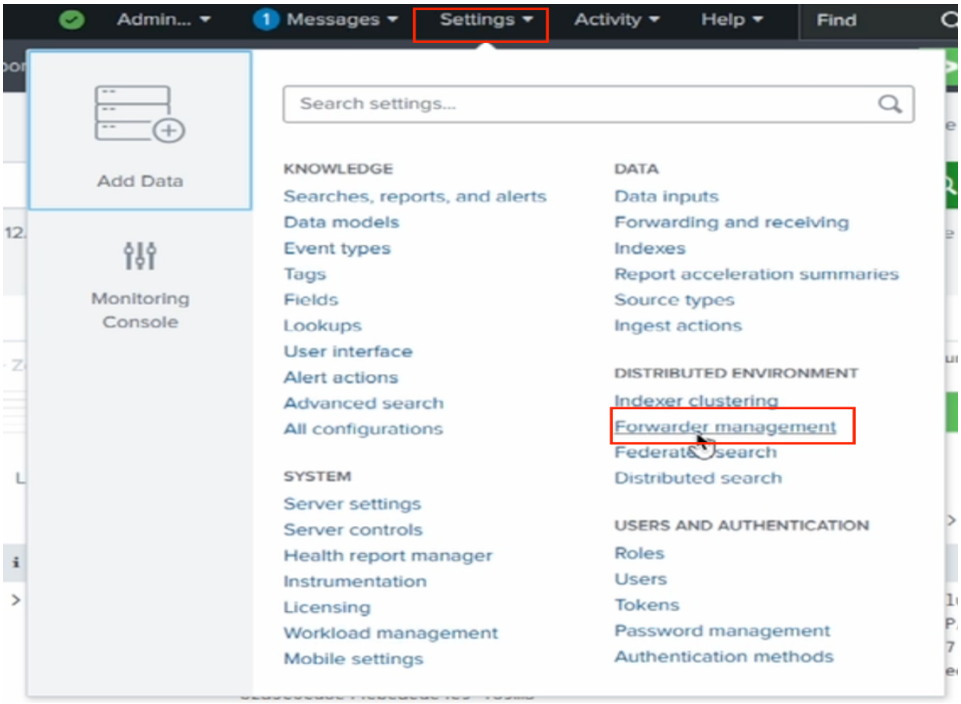
Check the Splunk Universal Forwarder Service Status. Type services on the Windows search to find Splunkforwarder Service. Monitor the service, status and startup type, check the state of the Splunk Universal Forwarder to see if is up. The status must be running.



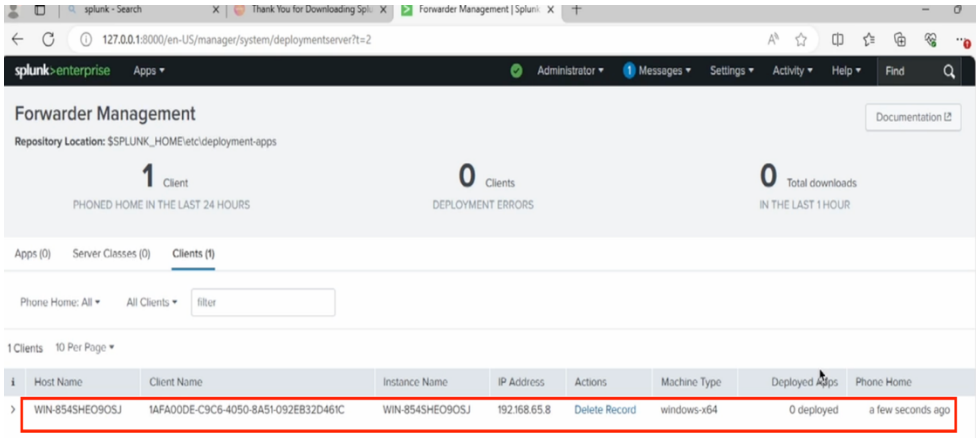
Use PowerShell command to Check if the communication is open type “Test-NetConnection -Computername 192.168.65.8 -port 9997”



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

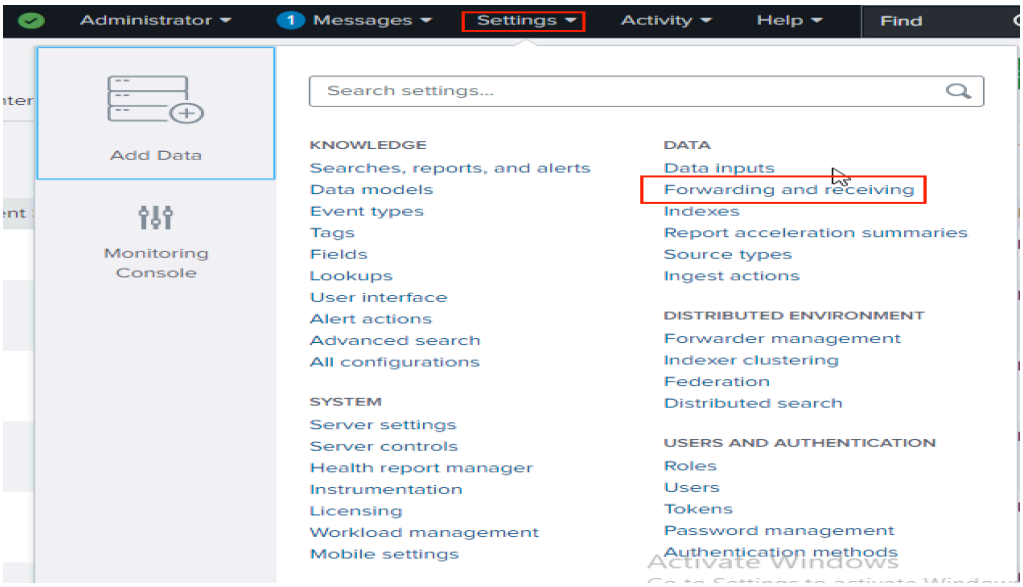


Forwarder Management: your Windows Computer must show on this page. If the computer didn't show after few minutes, restart Splunk Universal Forwarder service.

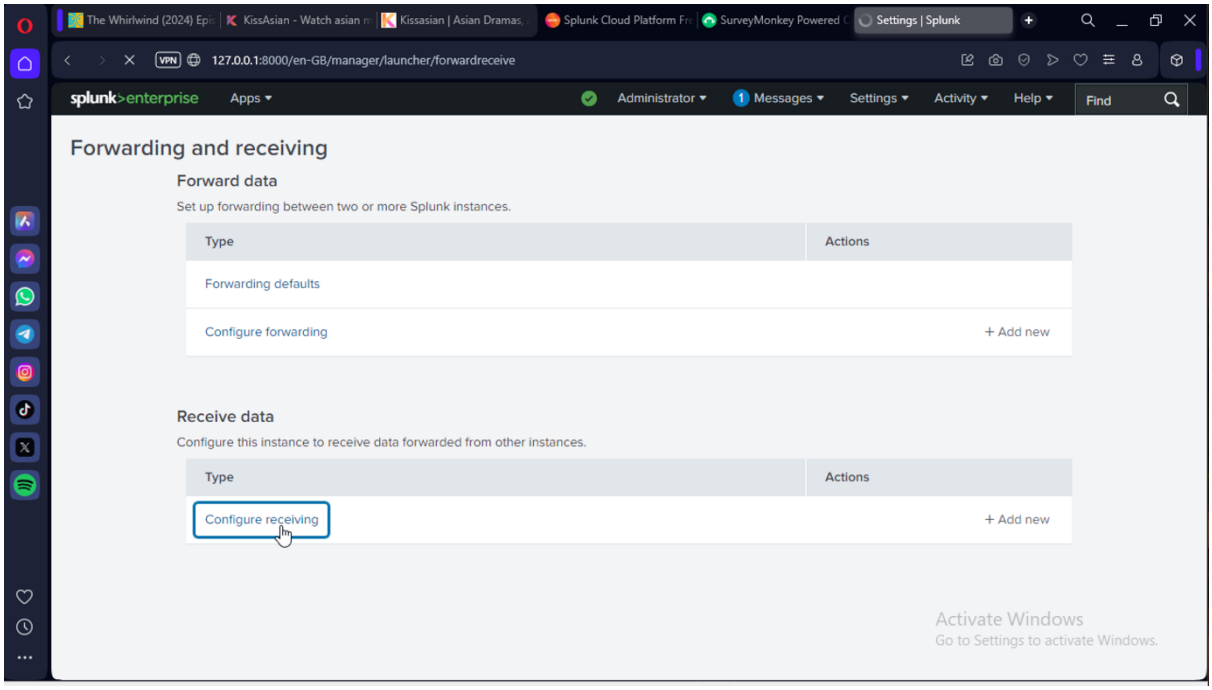


4. Detailed function of Splunk SIEM Service

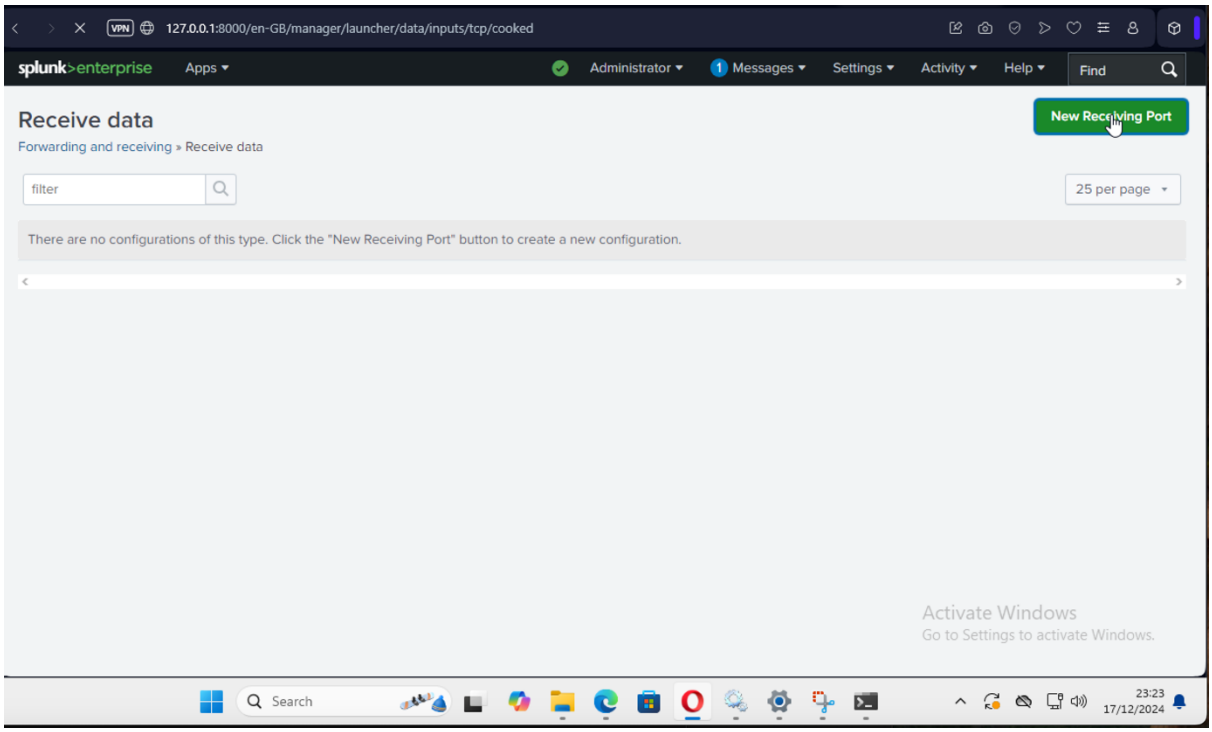
Receiving and Forwarding on Splunk Server: Click Settings> Forwarding and Receiving

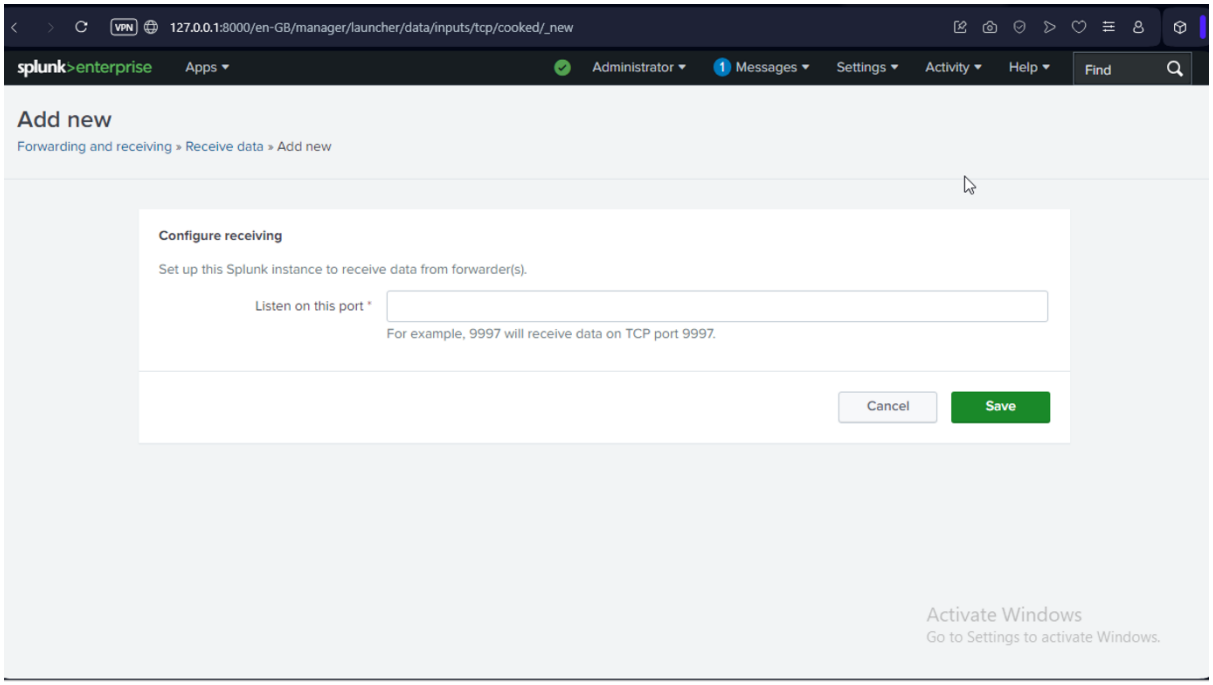


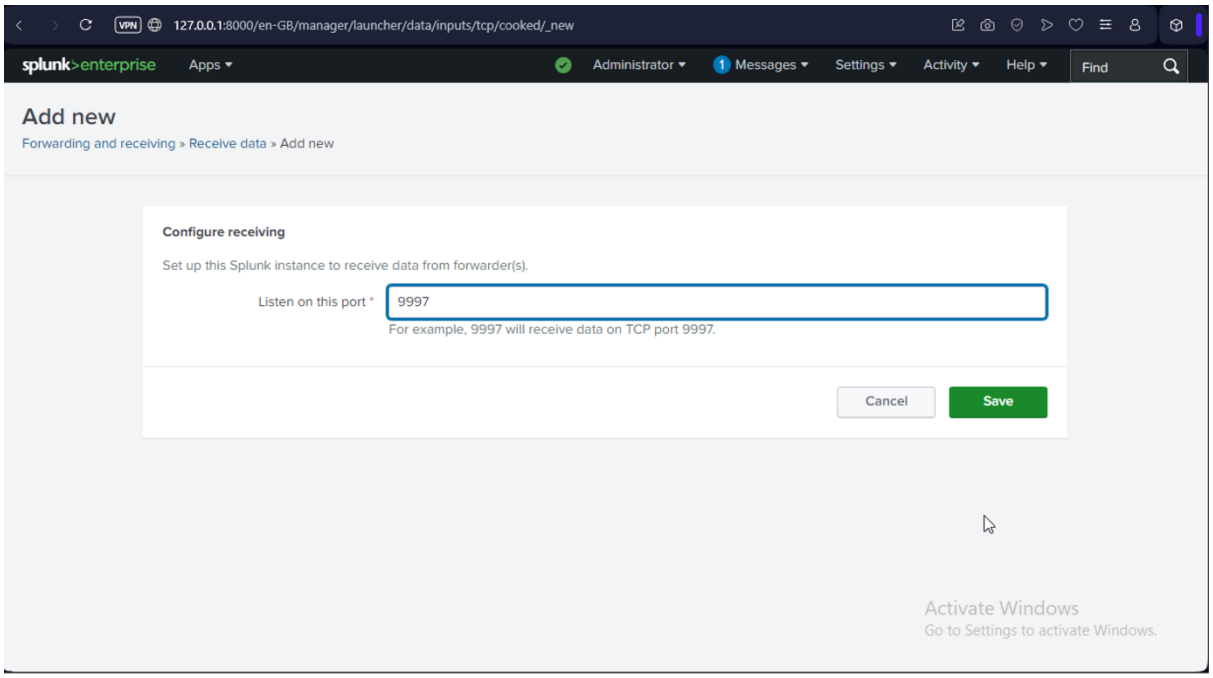
To view the available port for receiving data click on Configure receiving,

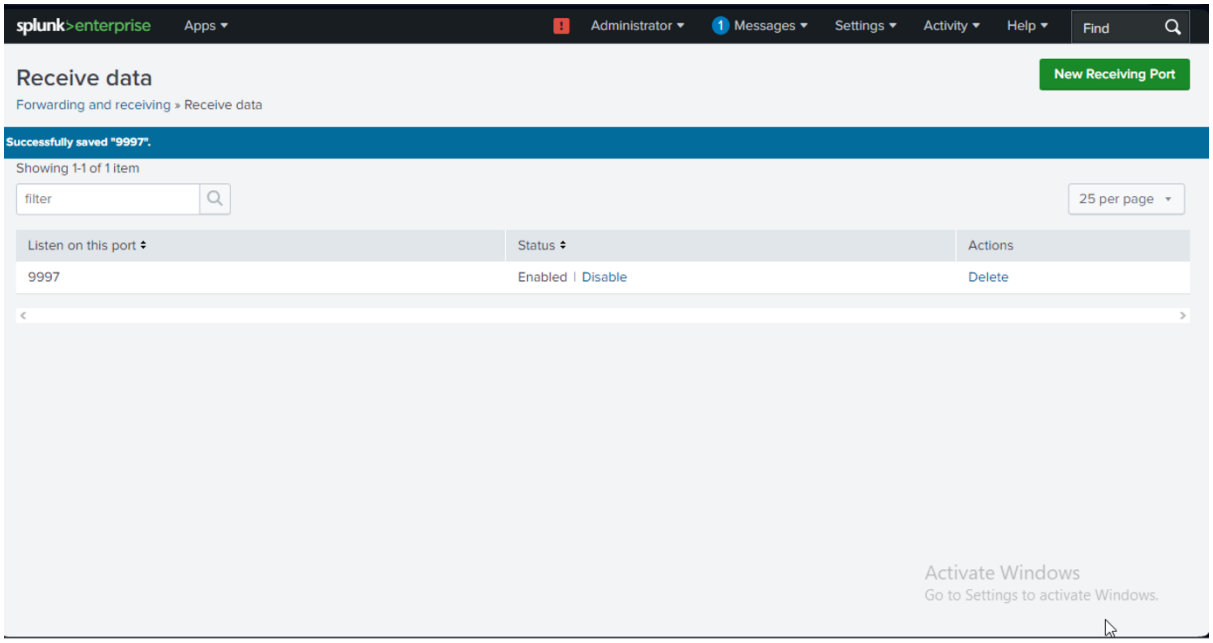


If no port shows click on New Receiving Port and add port 9997 which is the default port and click on Save. NOTE: for this tutorial we are using “default Port”.



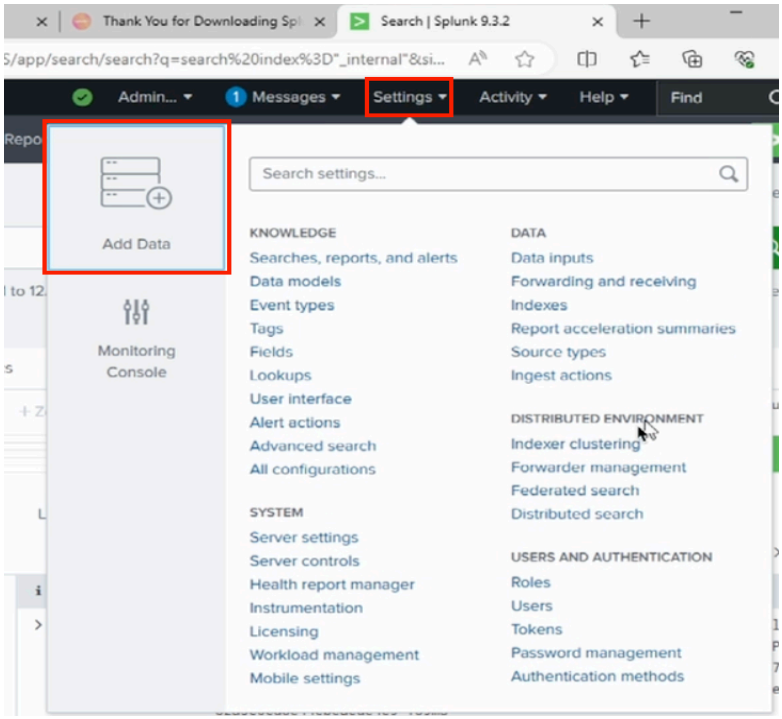

127.0.0.1:8000/en-GB/manager/launcher/data/inputs/tcp/cooked/_new
splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Add new
Forwarding and receiving » Receive data » Add new
Configure receiving
Set up this Splunk instance to receive data from forwarder(s).
Listen on this port *
For example, 9997 will receive data on TCP port 9997.
Cancel
Save
Activate Windows
Go to Settings to activate Windows.

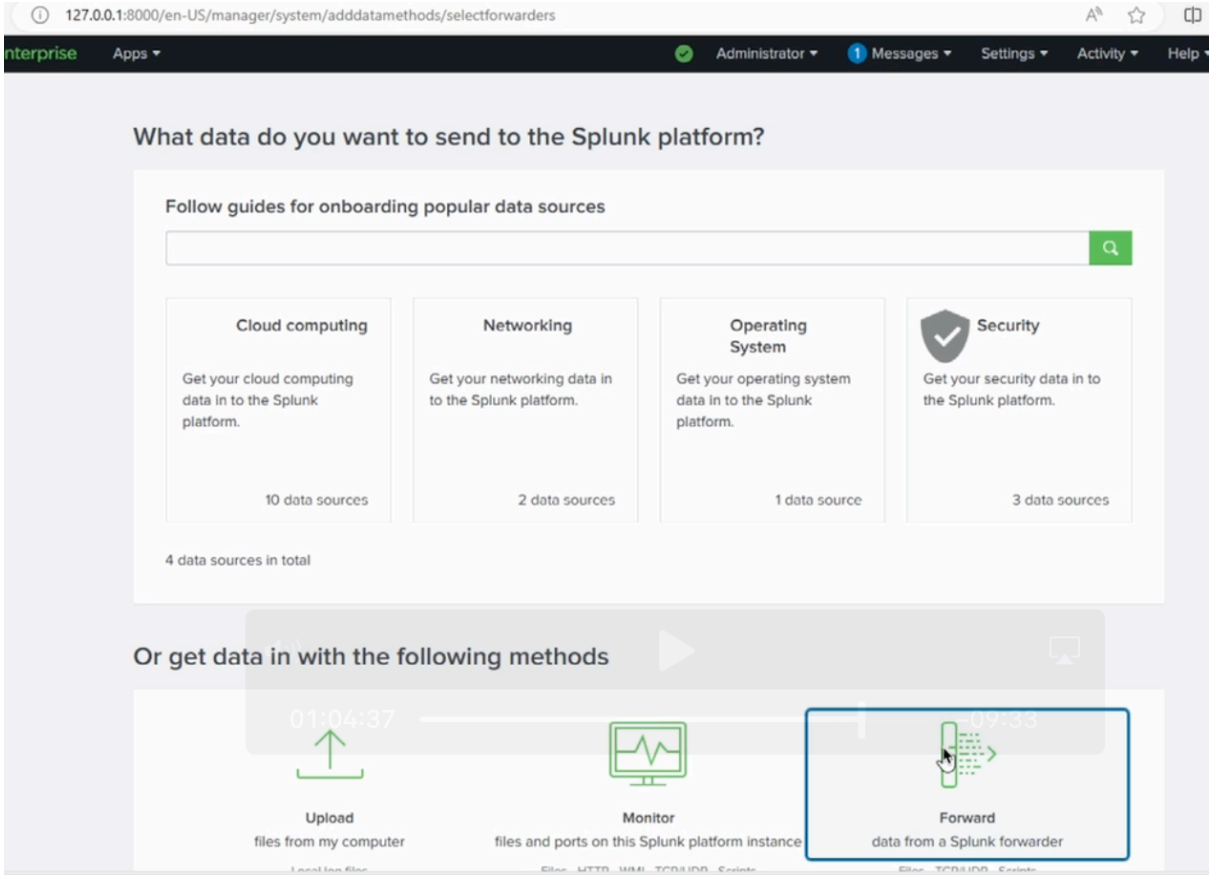

127.0.0.1:8000/en-GB/manager/launcher/data/inputs/tcp/cooked/_new
splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Add new
Forwarding and receiving » Receive data » Add new
Configure receiving
Set up this Splunk instance to receive data from forwarder(s).
Listen on this port *
9997
For example, 9997 will receive data on TCP port 9997.
Cancel
Save
Activate Windows
Go to Settings to activate Windows.



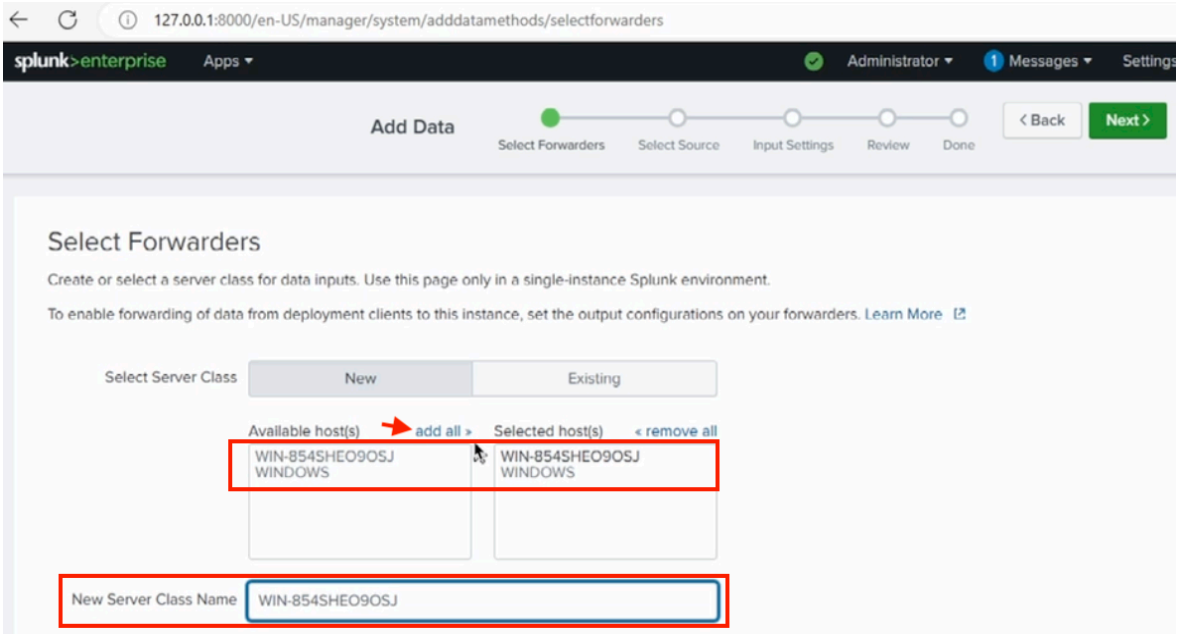
Add Data from Forwarder

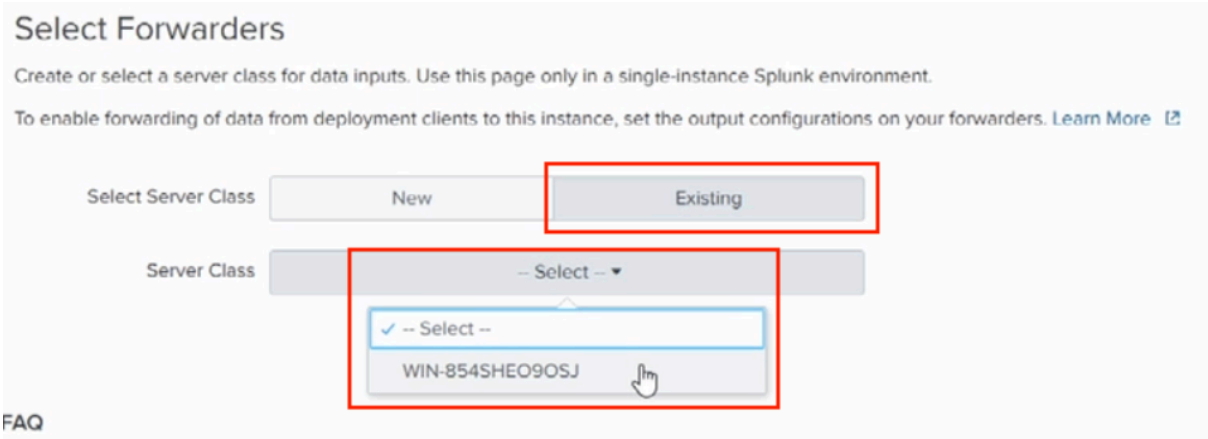
Go to Settings click Add Data
Select Forward below

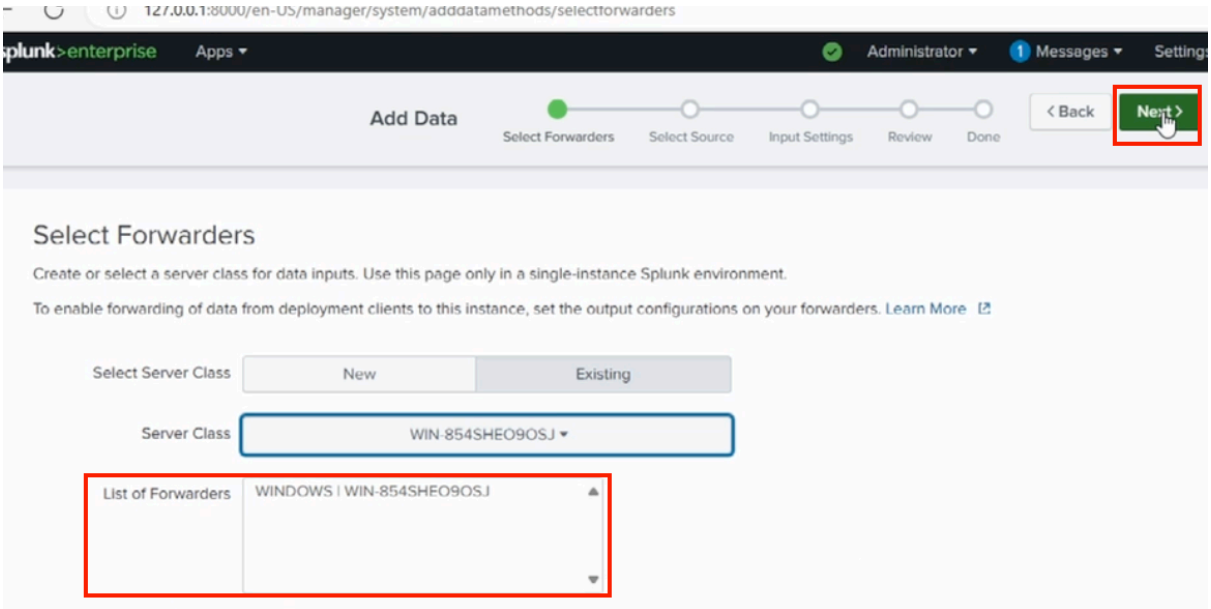




We added our computer to the selected host and gave it a New Server Class Name to do that Click on Add All to add the Available host to the Selected Host, then Click on Existing to select the Server Class
create a New Server Class Name and click next


127.0.0.1:8000/en-US/manager/system/adddatamethods/selectforwarders
splunk>enterprise
Apps
Administrator
Messages
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
WIN-854SHEO9OSJ
WINDOWS
New Server Class Name
WIN-854SHEO9OSJ

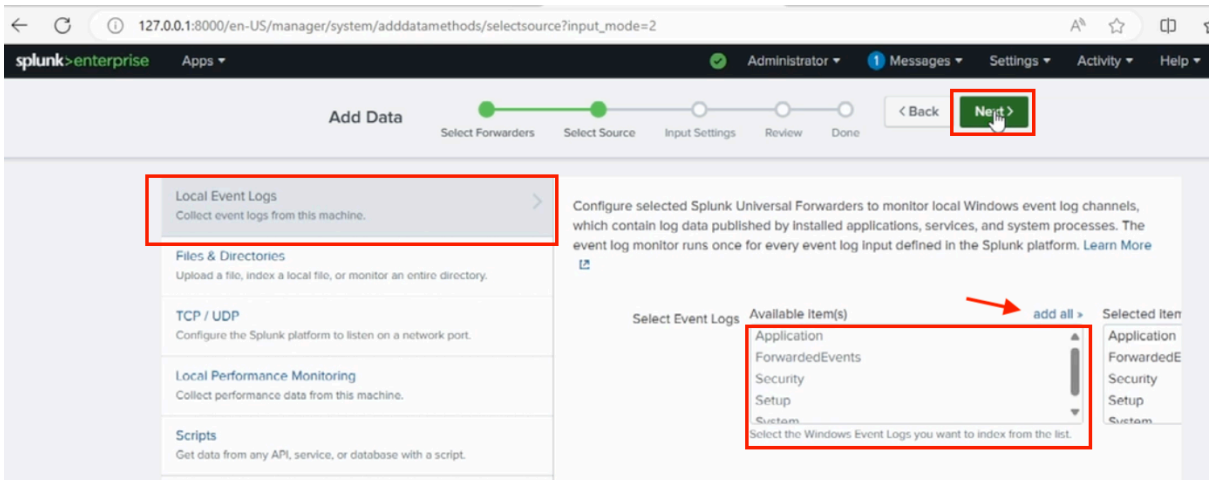

Select Forwarders
Create or select a server class for data inputs. Use this page only in a single-instance Splunk environment.
To enable forwarding of data from deployment clients to this instance, set the output configurations on your forwarders. Learn More
Select Server Class
New
Existing
Server Class
-- Select --
WIN-854SHEO9OSJ
FAQ


splunk>enterprise
Apps
Administrator
Messages
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:

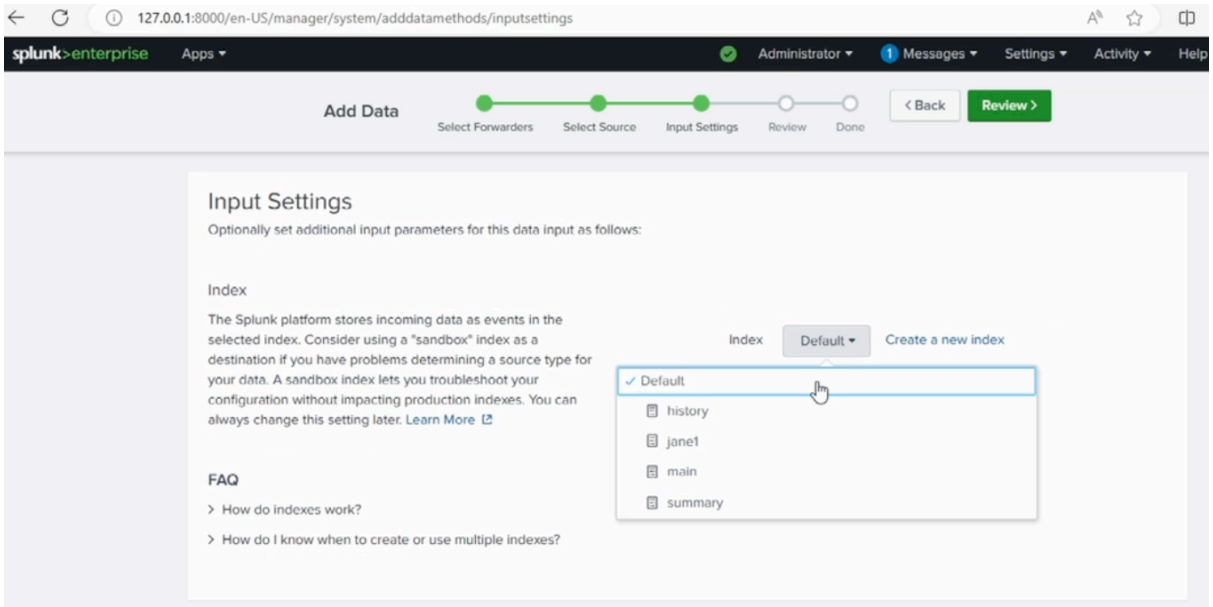
You can specify what you want to monitor but in this tutorial, we monitored local event logs from our computer as shown below.

Select Local Event Logs > Add All > Next

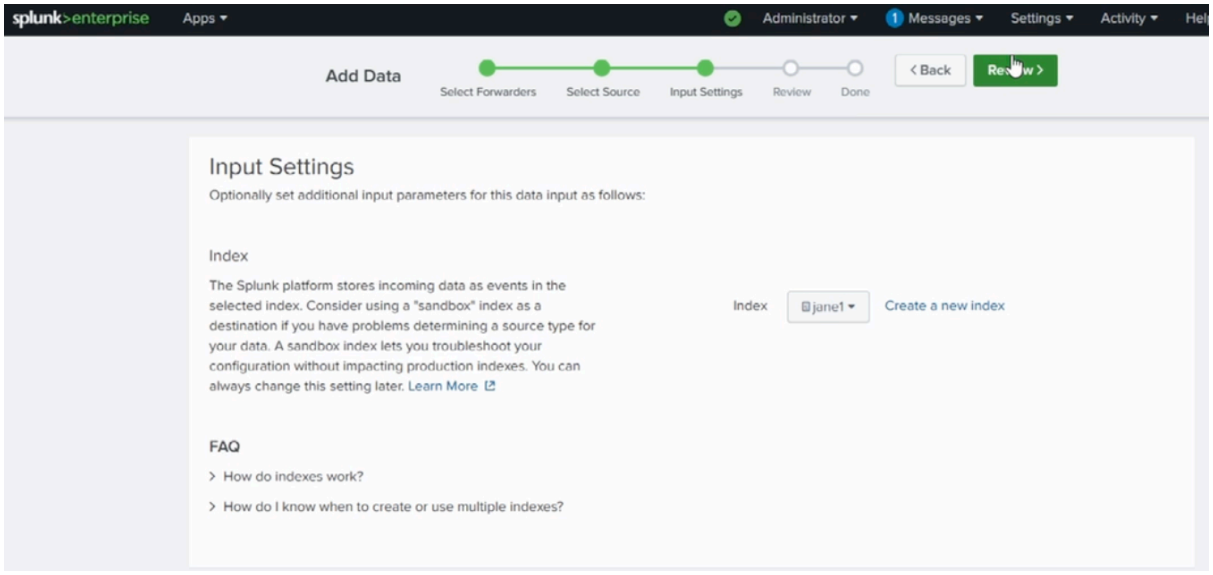


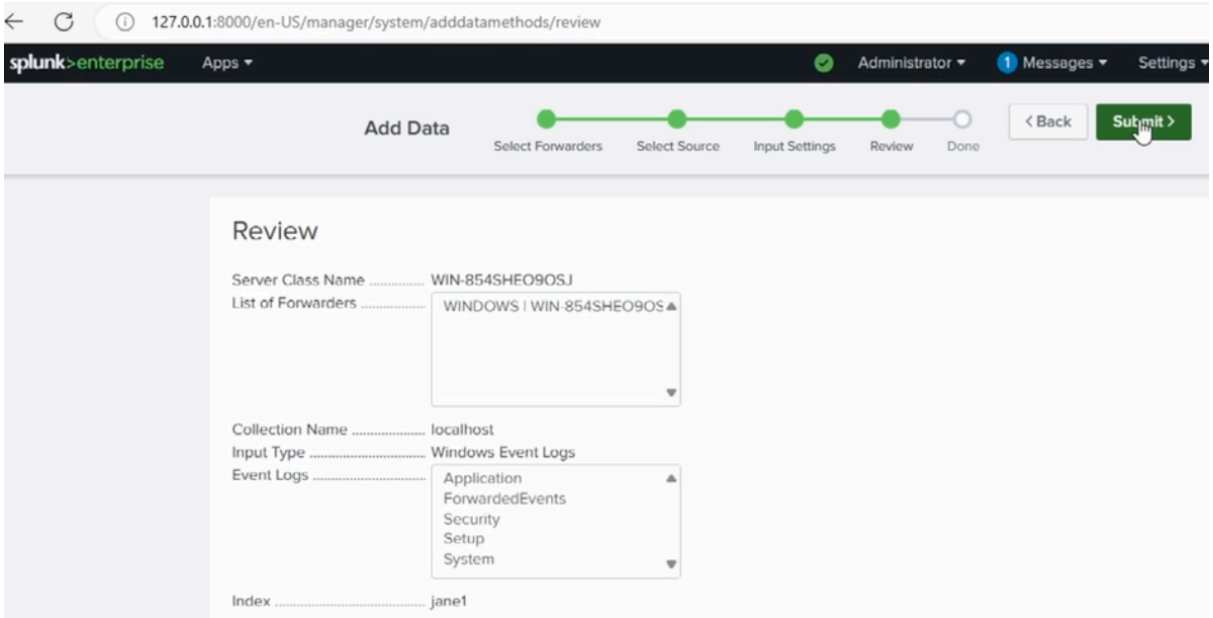
Select where the index will be allocated

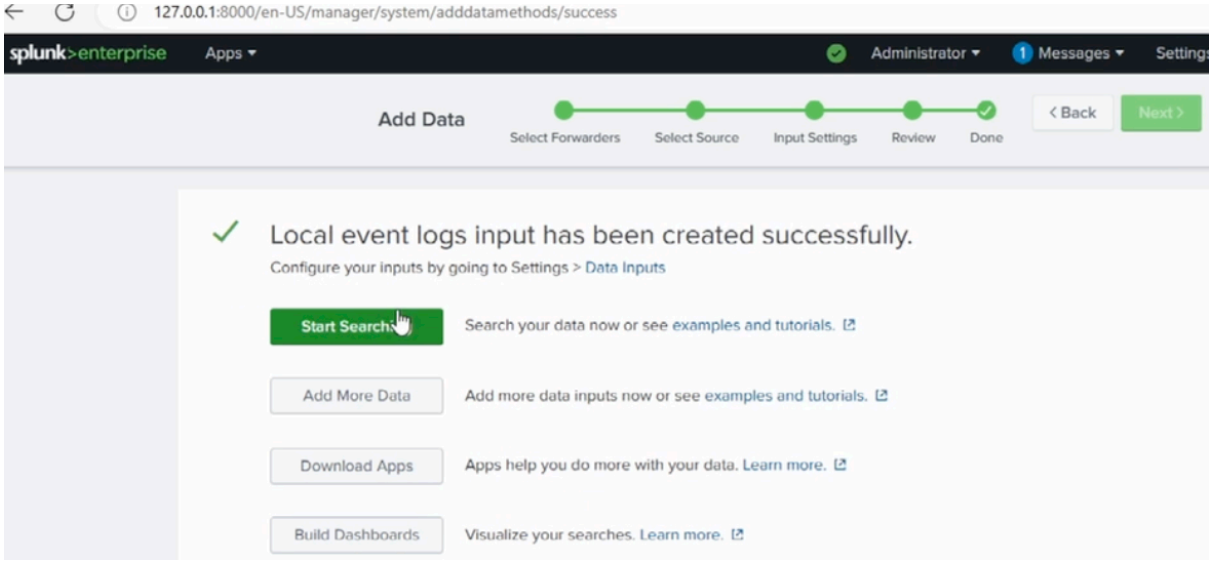
Click on Create a new index after you have created it click the Default drop down arrow to select the index you have created.

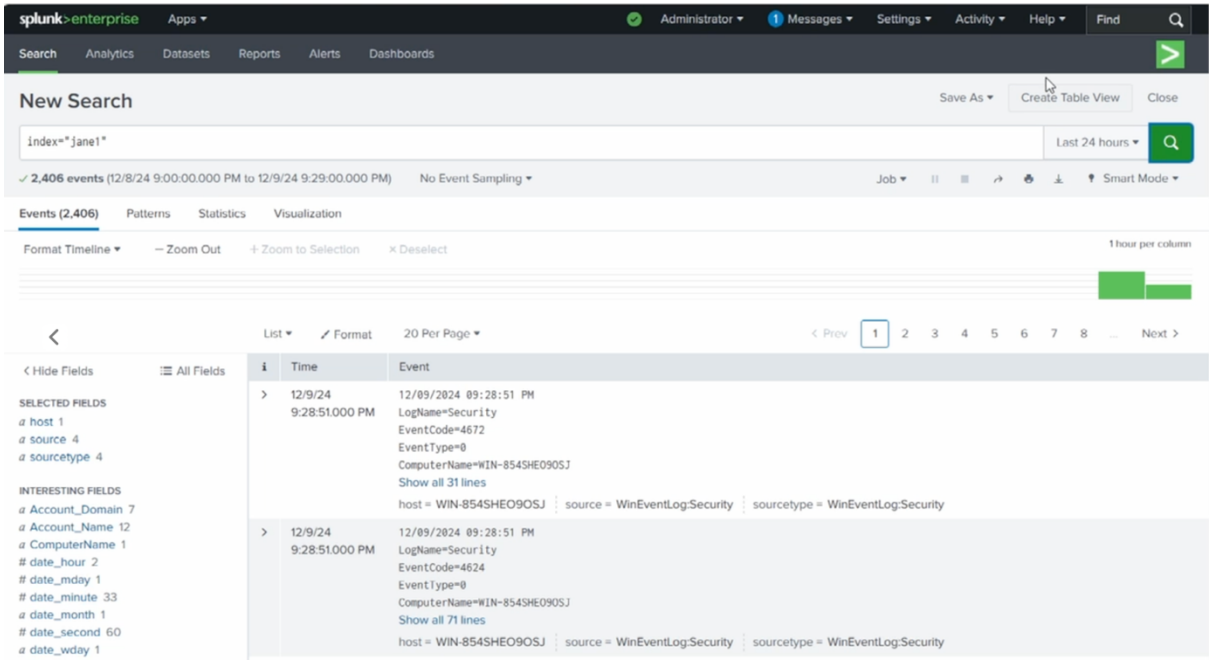


Click on Review button to check the logs you have created once viewed click on submit. You can now click on “start searching” to find last connection on client’s computer





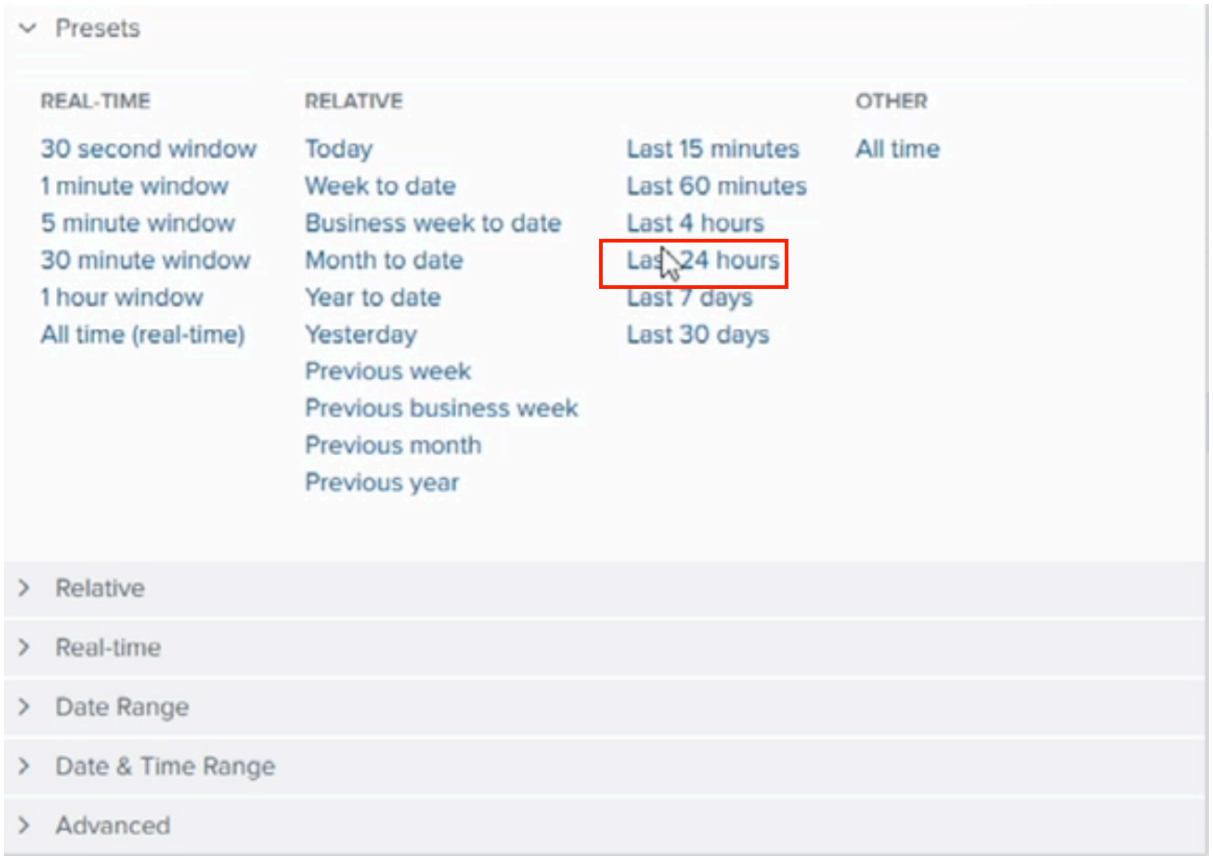




NOTE: the field names are case-sensitive, but the field values are not case-sensitive, you can use operators such AND, OR NOT also wildcard is available (use *)

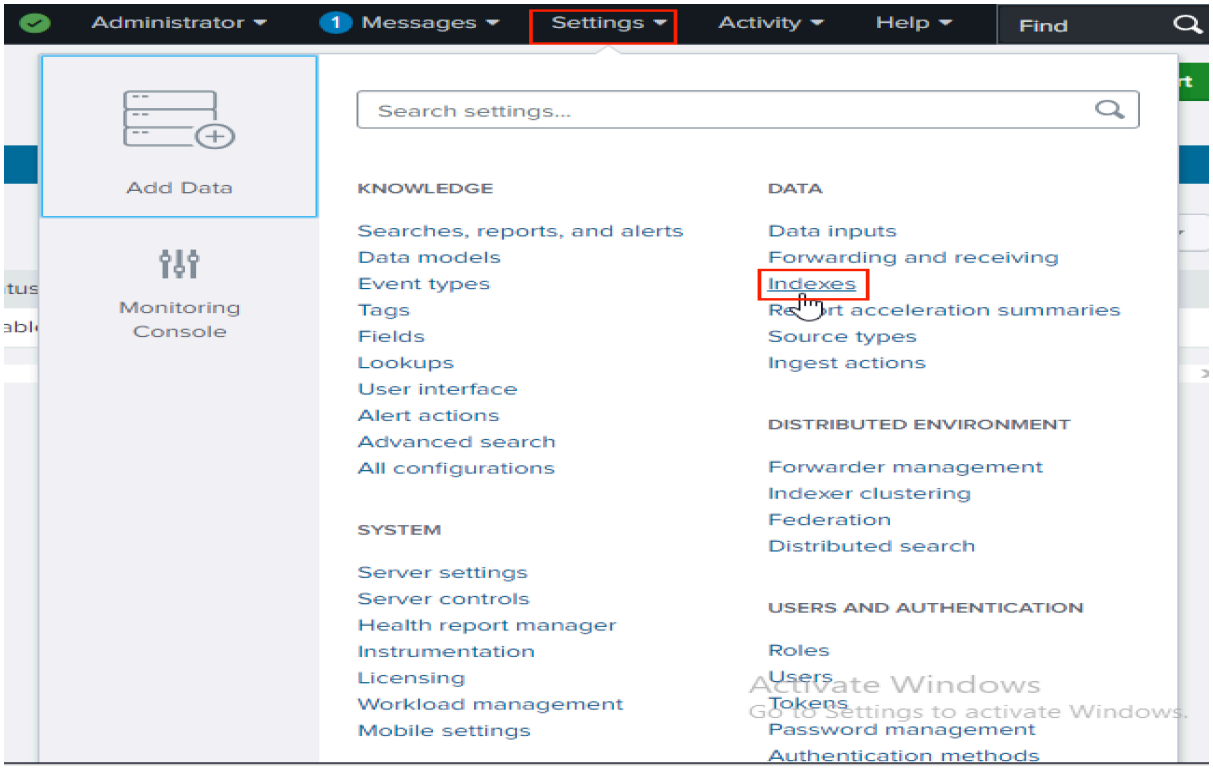
Date selection

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

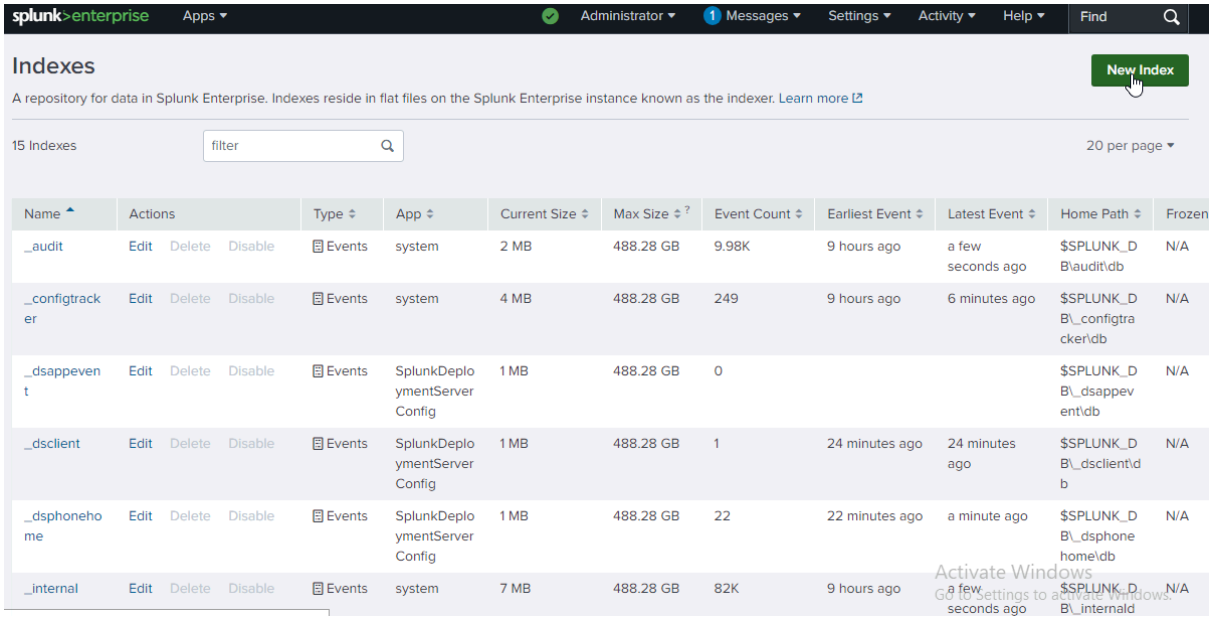


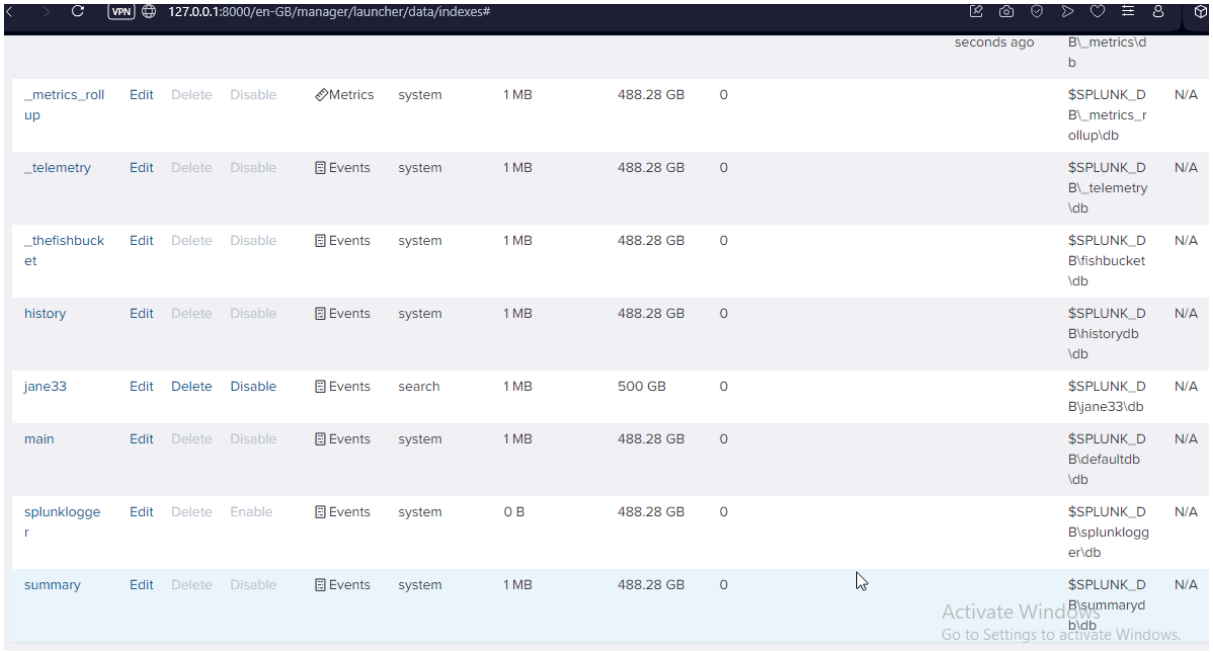
Check Indexes Settings

Click on Settings > Indexes



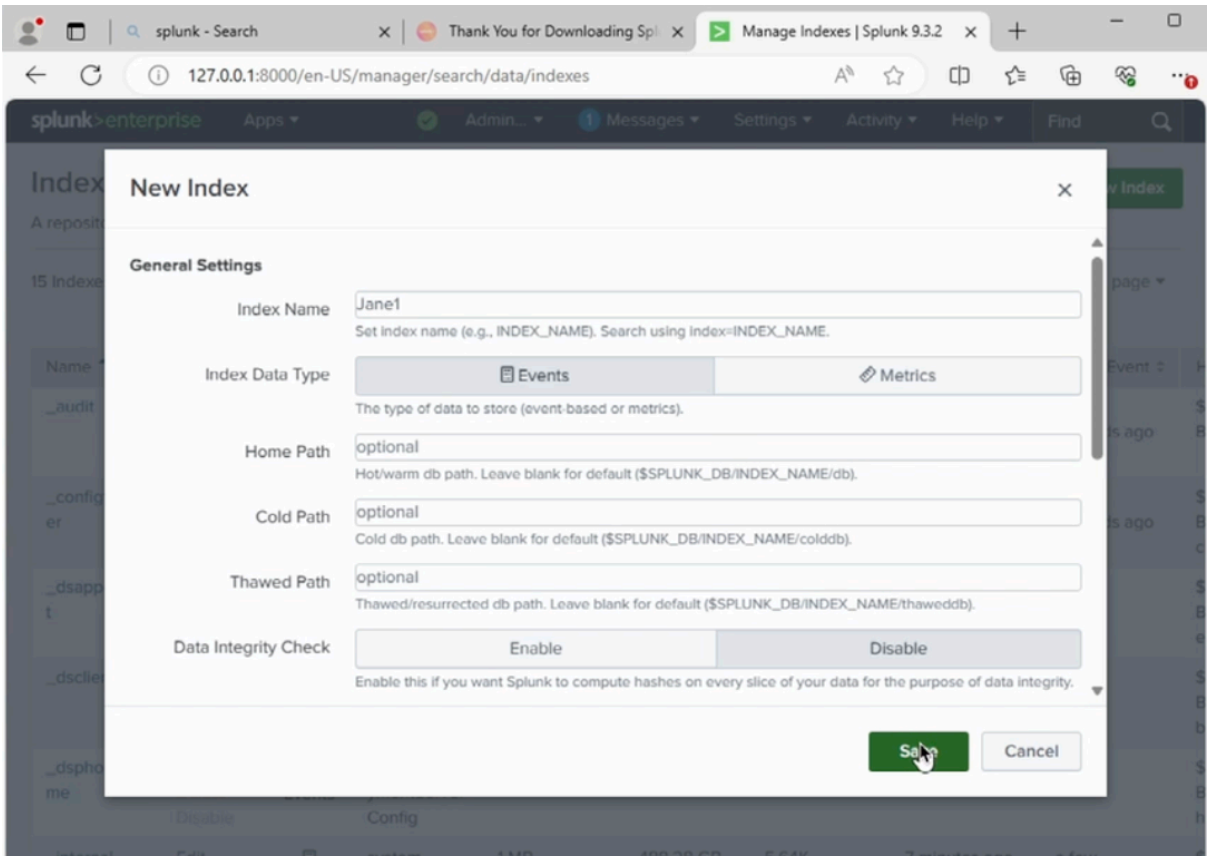
As seen that there is no incoming event, we are to create an event now click on “New Index”



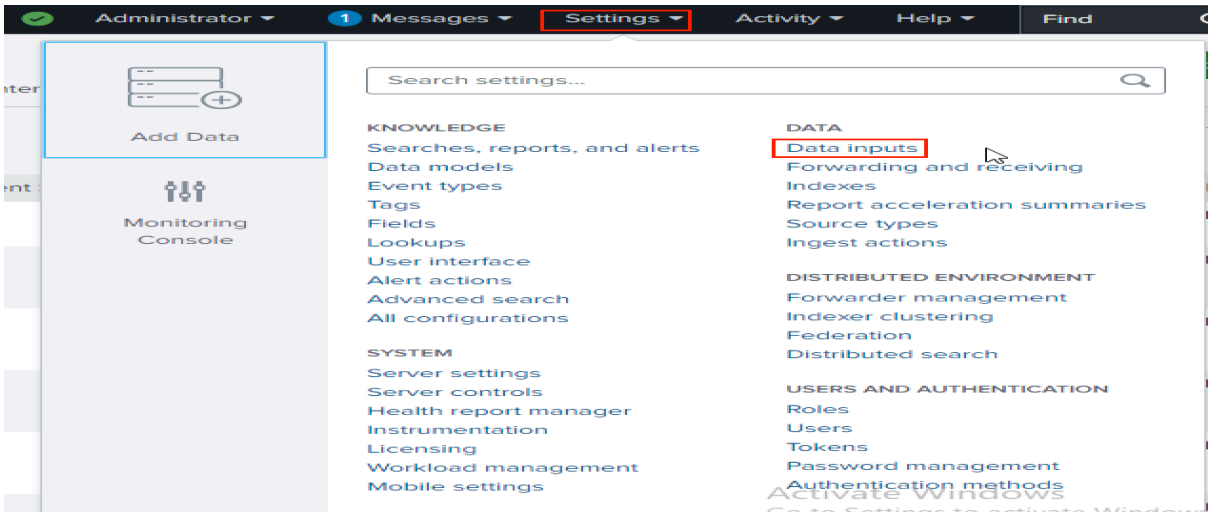


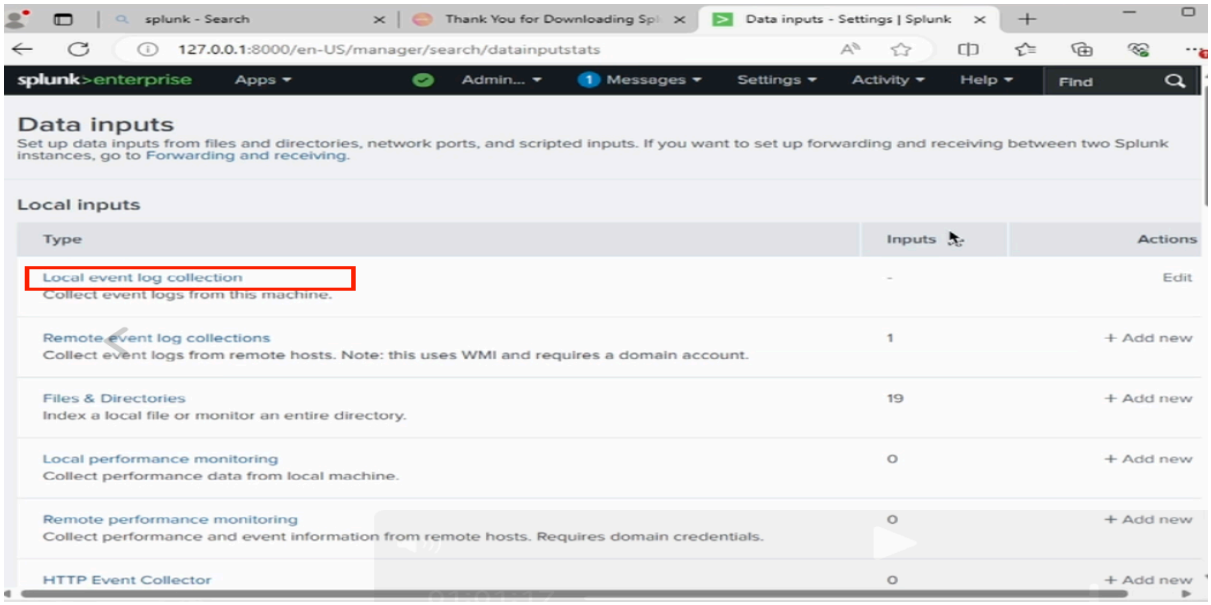
									seconds ago	B_metrics\db
_metrics_rollup	Edit	Delete	Disable	Metrics	system	1 MB	488.28 GB	0		$SPLUNK_DB_metrics_rollup\db	N/A
_telemetry	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0		$SPLUNK_DB_telemetry\db	N/A
_thefishbucket	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0		$SPLUNK_DB\fishbucket\db	N/A
history	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0		$SPLUNK_DB\historydb\db	N/A
jane33	Edit	Delete	Disable	Events	search	1 MB	500 GB	0		$SPLUNK_DB\jane33\db	N/A
main	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0		$SPLUNK_DB\defaultdb\db	N/A
splunklogger	Edit	Delete	Enable	Events	system	0 B	488.28 GB	0		$SPLUNK_DB\splunklogger\db	N/A
summary	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0		$SPLUNK_DB\summarydb\db	N/A

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

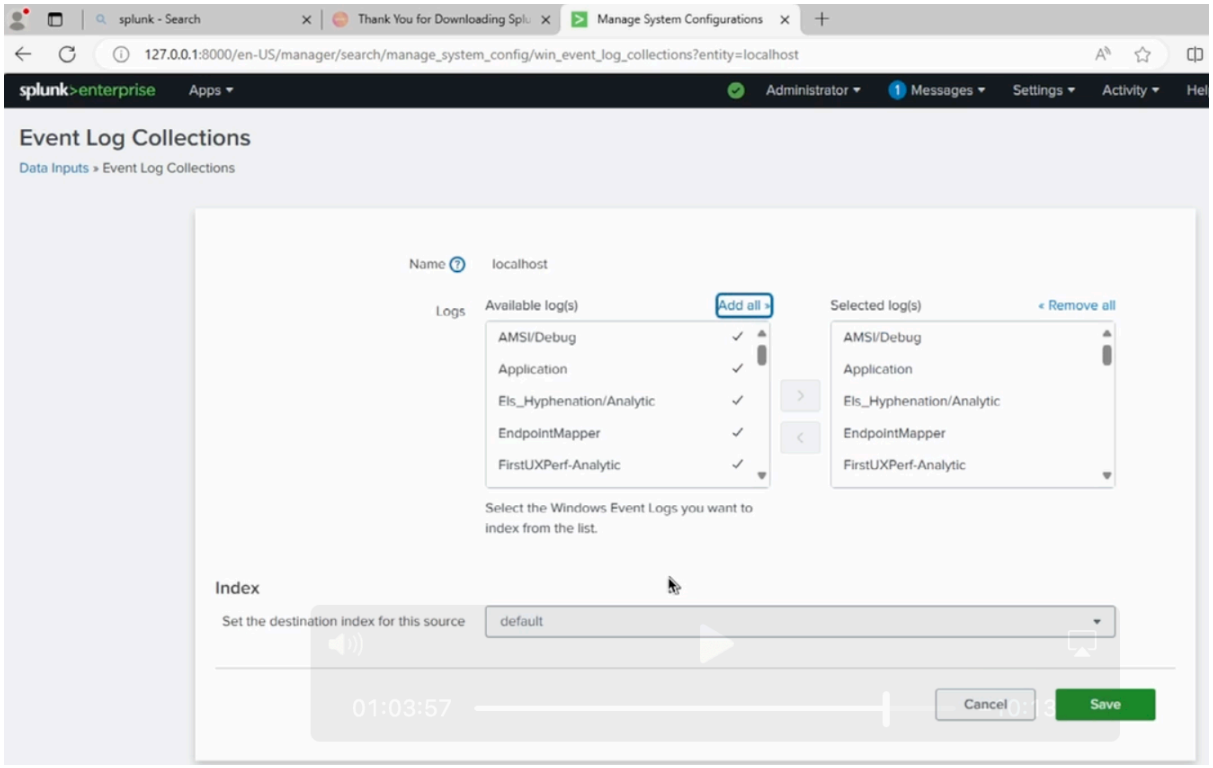


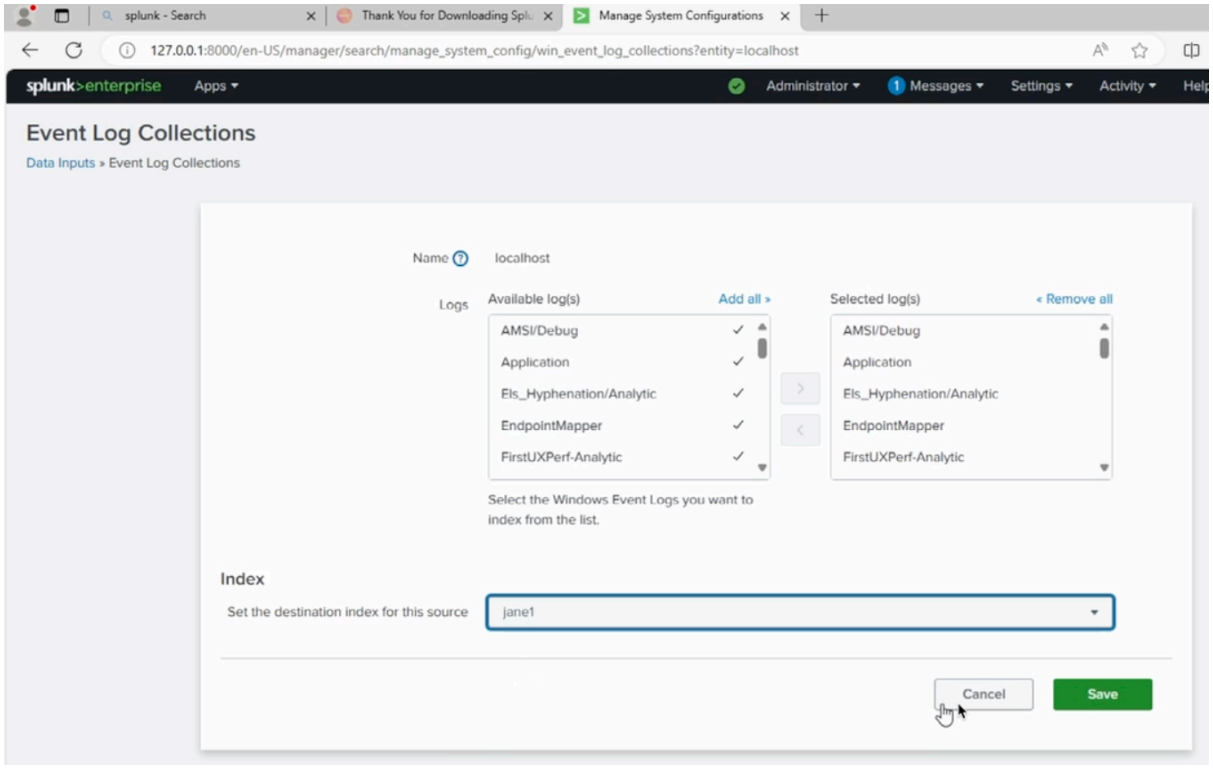
Go to settings> Data input > local events logs collection



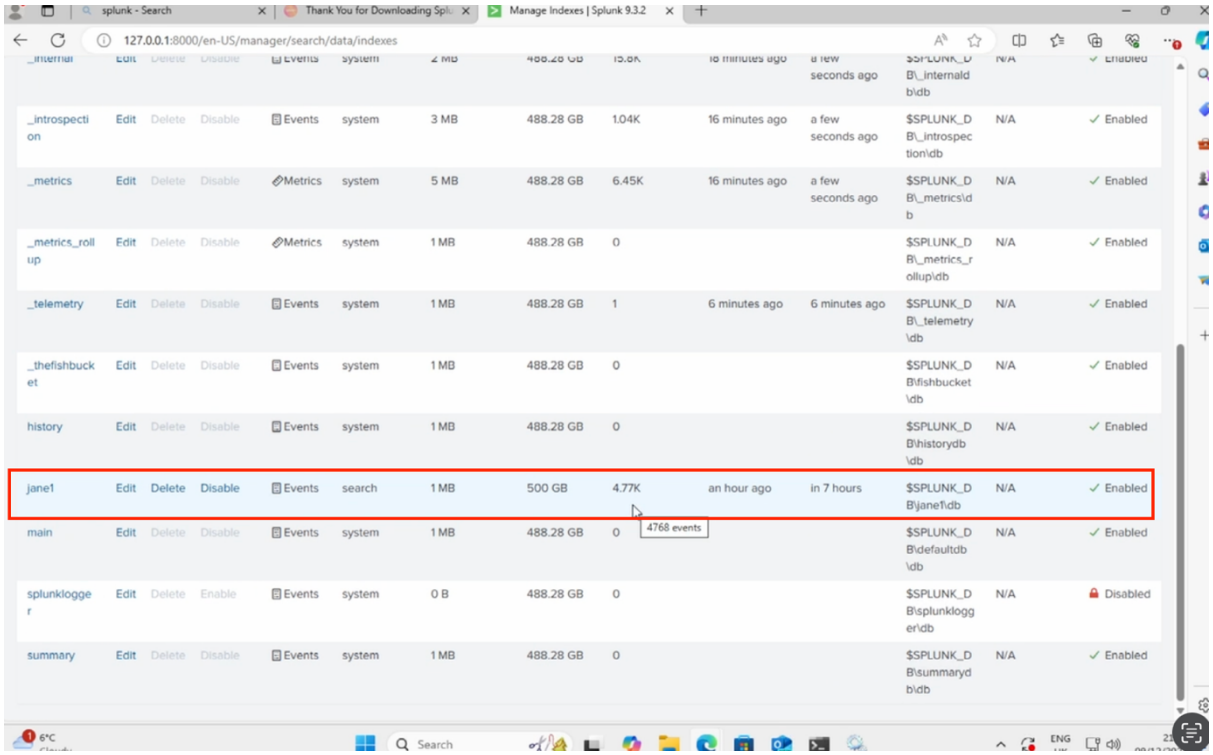


The event logs are then added to newly created index “Jane1”



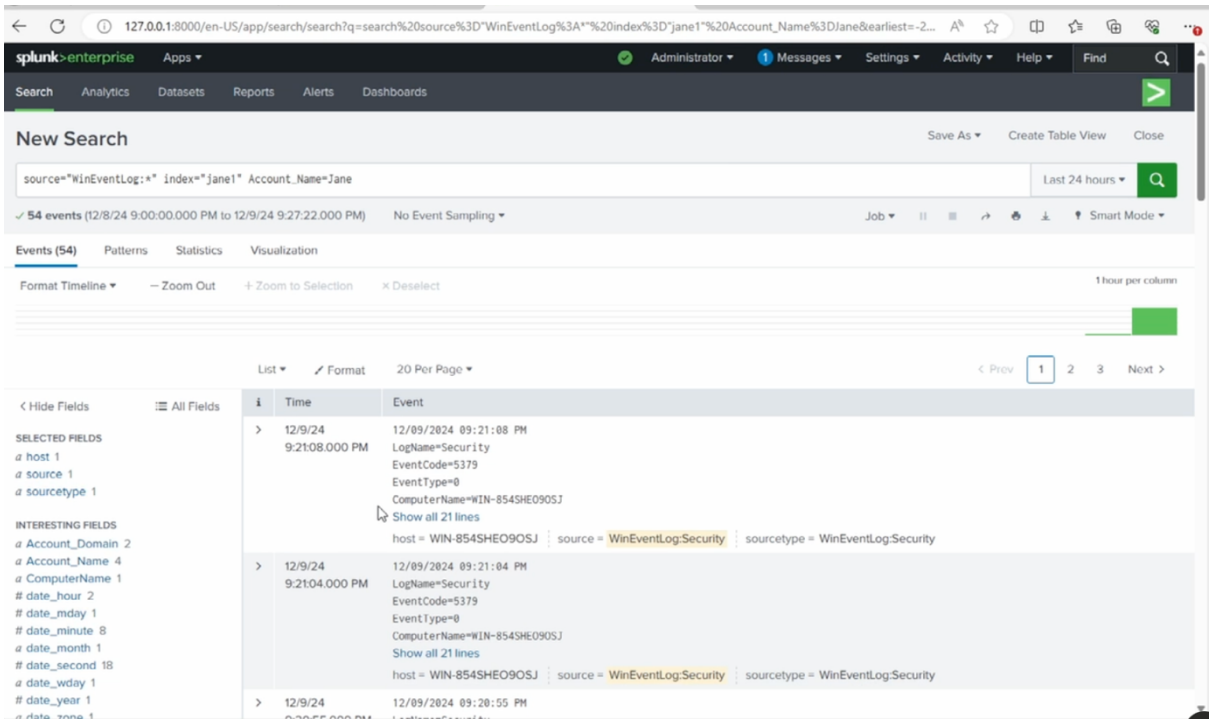


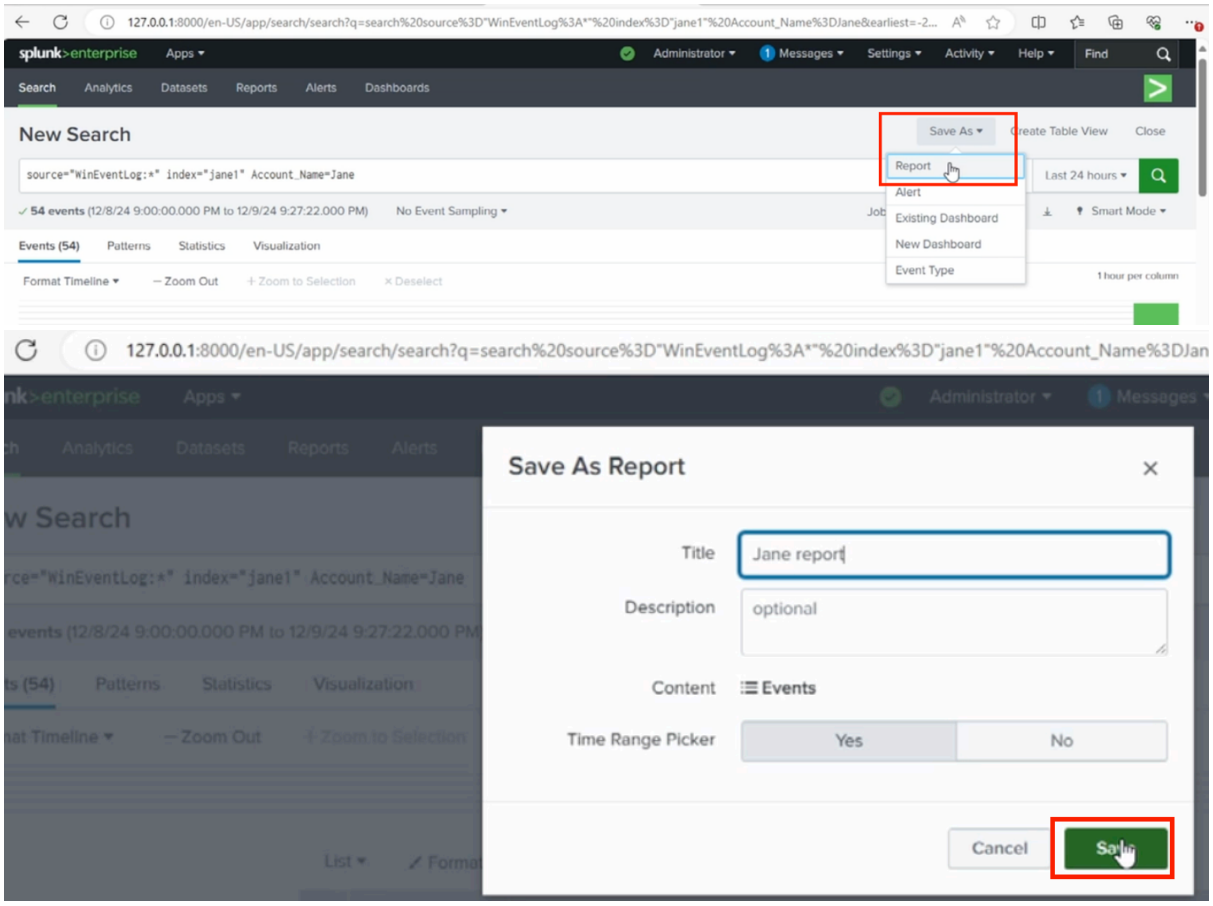
Go to settings > indexes the below image show that the events had updated “Jane1”

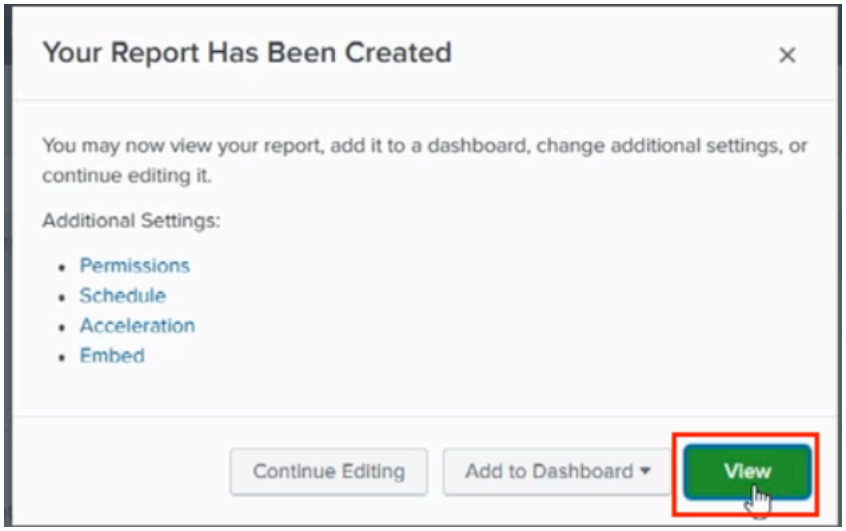


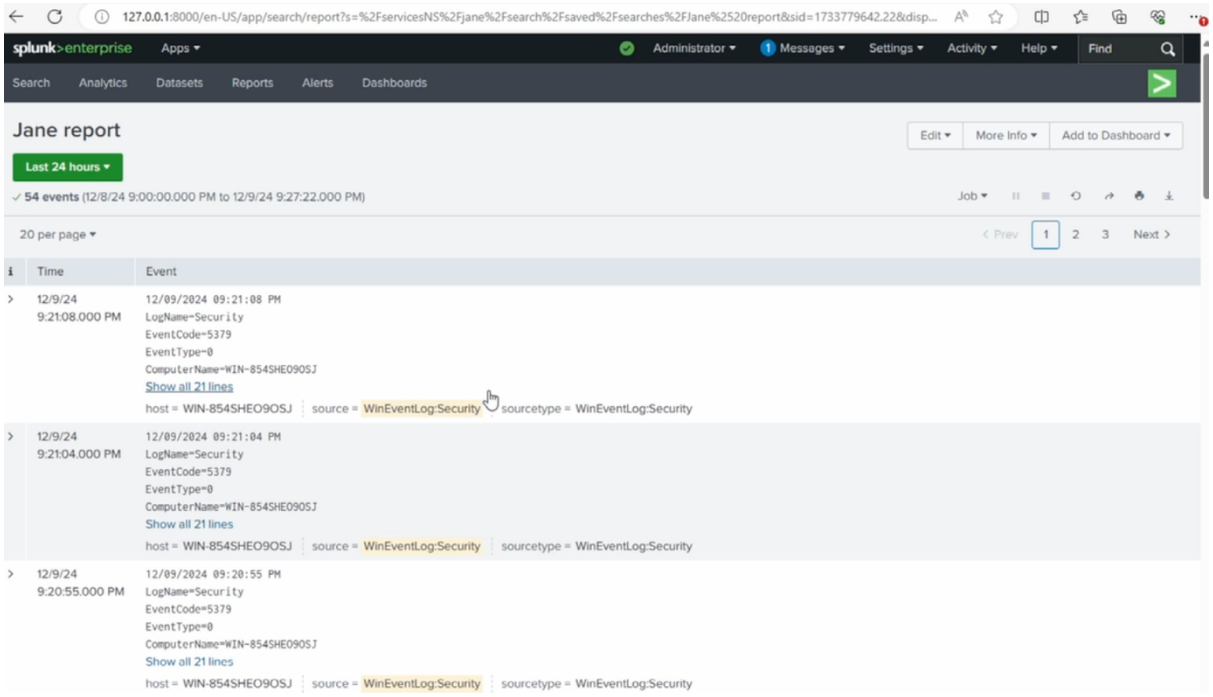
Splunk Reports

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



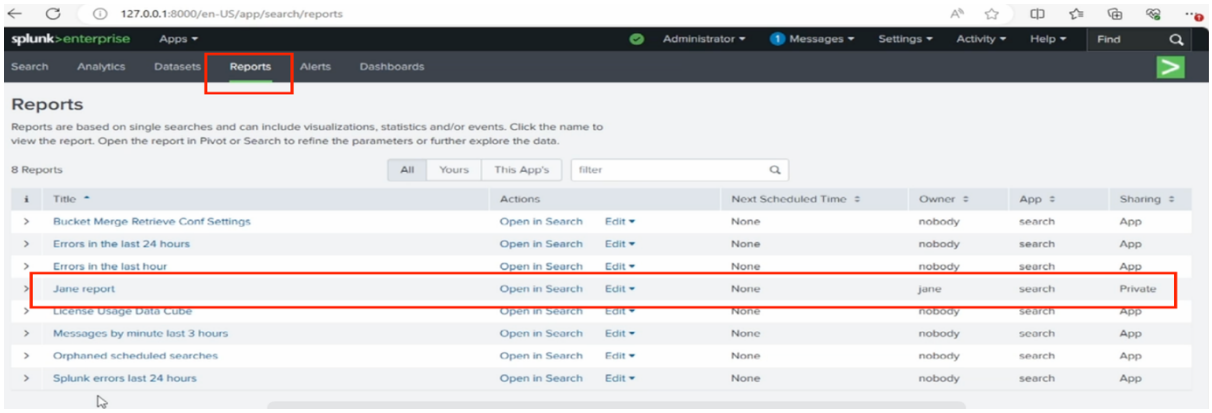

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
Save As
Create Table View
Close
source="WinEventLog:*" index="jane1" Account_Name=Jane
Report
Alert
Existing Dashboard
New Dashboard
Event Type
Last 24 hours
54 events (12/8/24 9:00:00.000 PM to 12/9/24 9:27:22.000 PM)
No Event Sampling
Smart Mode
Events (54)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
127.0.0.1:8000/en-US/app/search/search?q=search%20source%3D"WinEventLog%3A*"%20index%3D"jane1"%20Account_Name%3DJan
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 Editing
Add to Dashboard
View

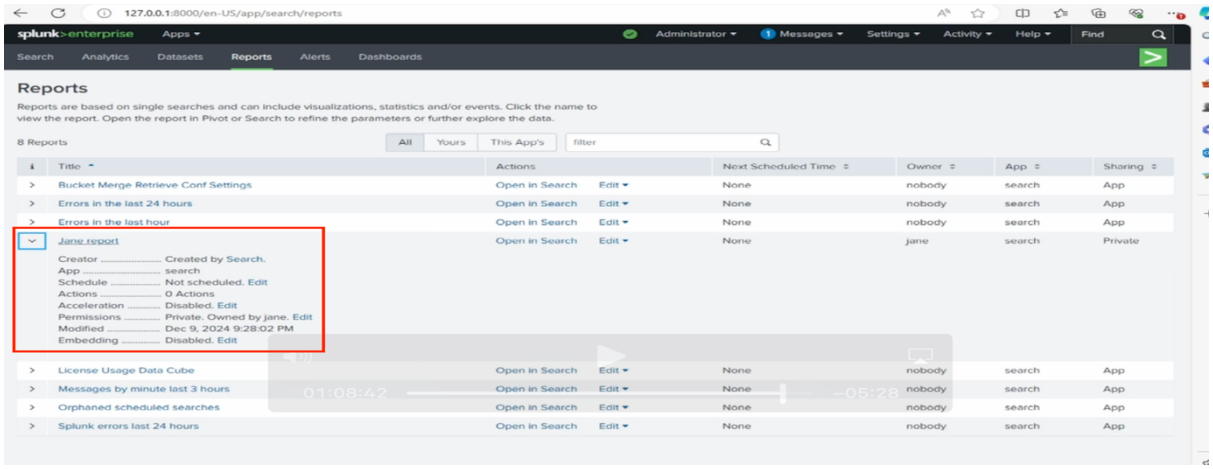

127.0.0.1:8000/en-US/app/search/report?s=%2FservicesNS%2Fjane%2Fsearch%2Fsaved%2Fsearches%2FJane%2520report&sid=1733779642.22&disp...
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Jane report
Edit
More Info
Add to Dashboard
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
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-854SHEO9OSJ
Show all 21 lines
host = WIN-854SHEO9OSJ 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-854SHEO9OSJ
Show all 21 lines
host = WIN-854SHEO9OSJ 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-854SHEO9OSJ
Show all 21 lines
host = WIN-854SHEO9OSJ source = WinEventLog:Security sourcetype = WinEventLog:Security

To Edit an Existing Report

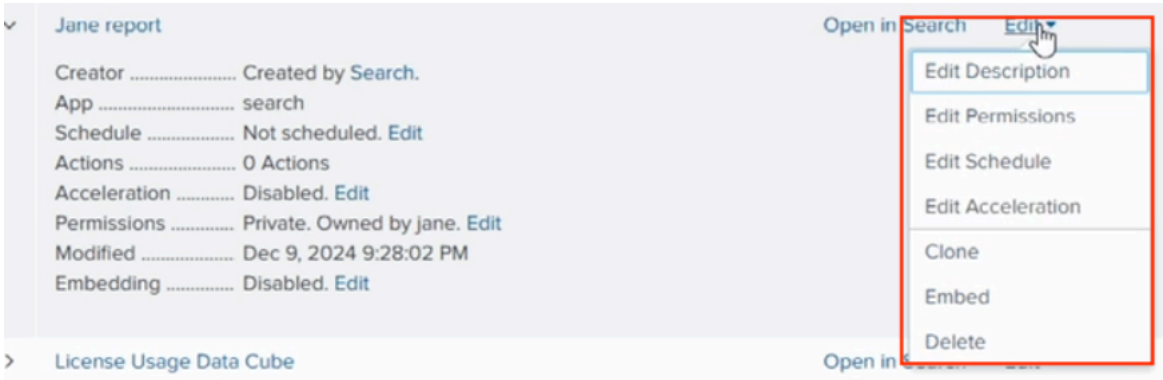
At the Search tap click on Report > Select the Report you created



Detailed information of the “Jane report”

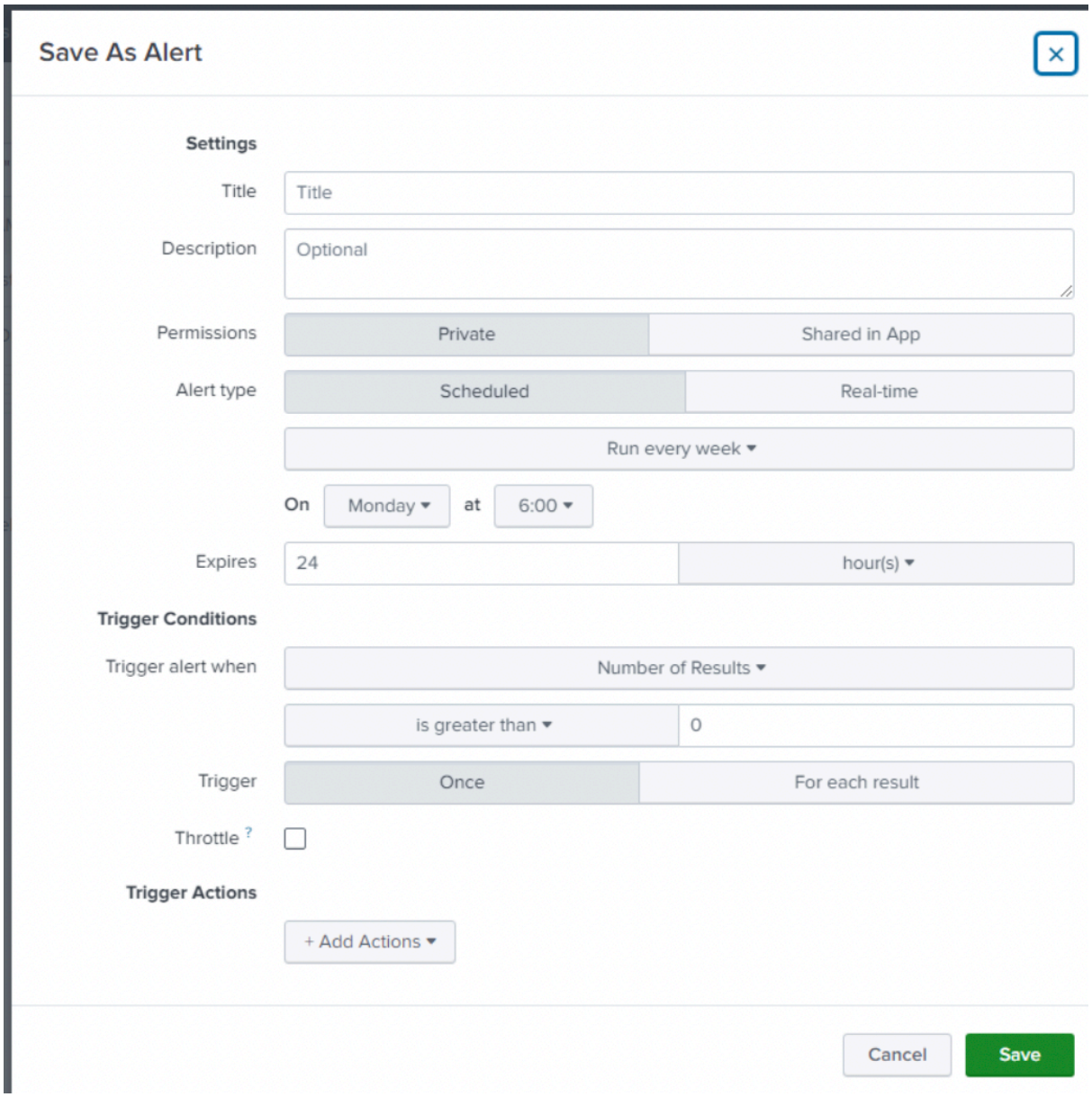


Select Edit button to edit “Jane Report”



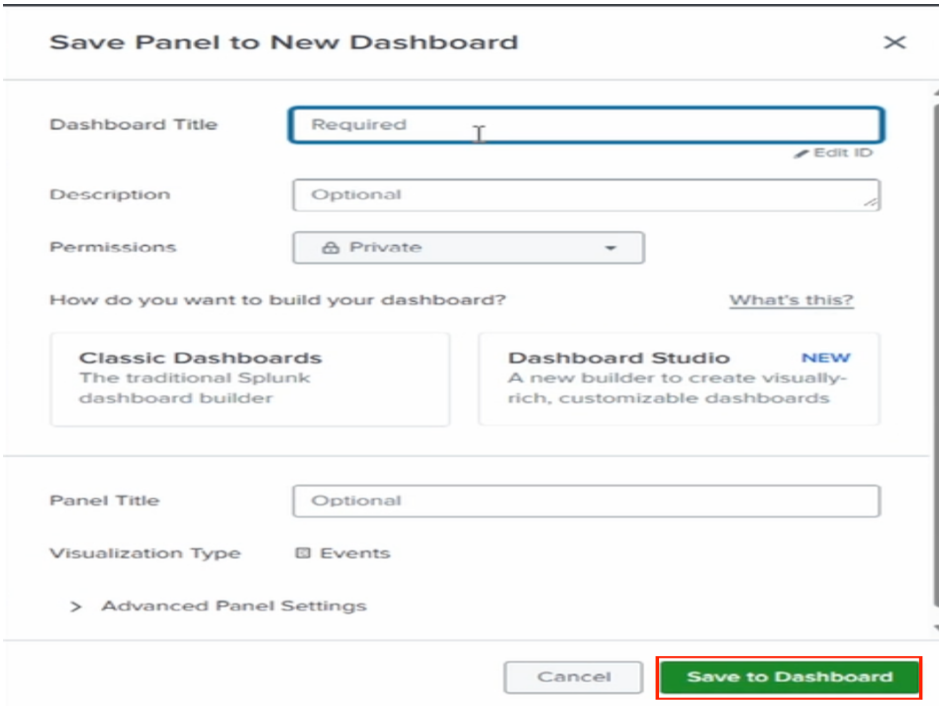
Set Alert

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

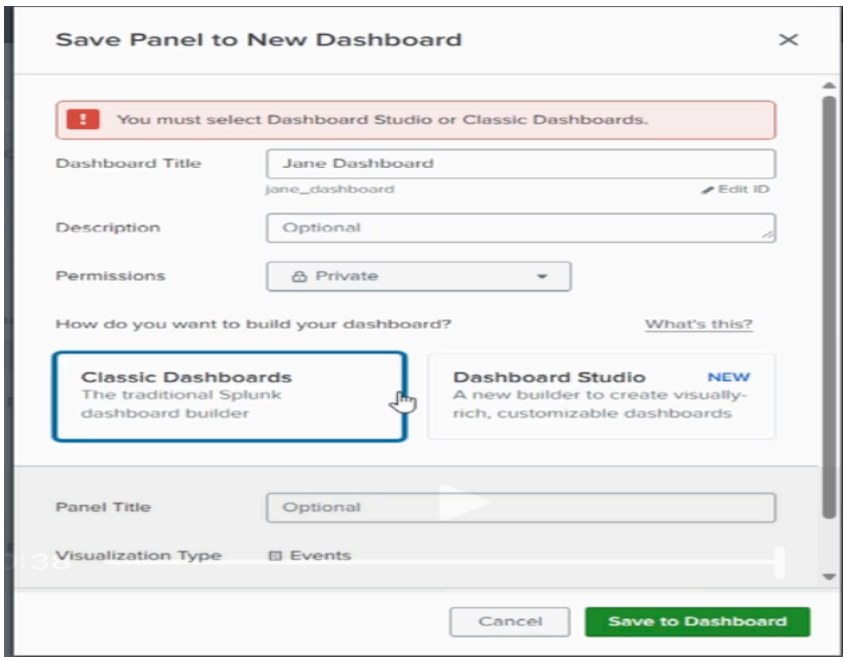


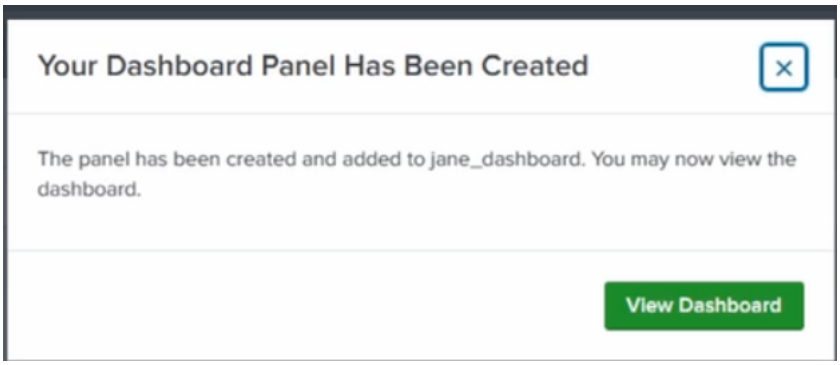
Save to Dashboard

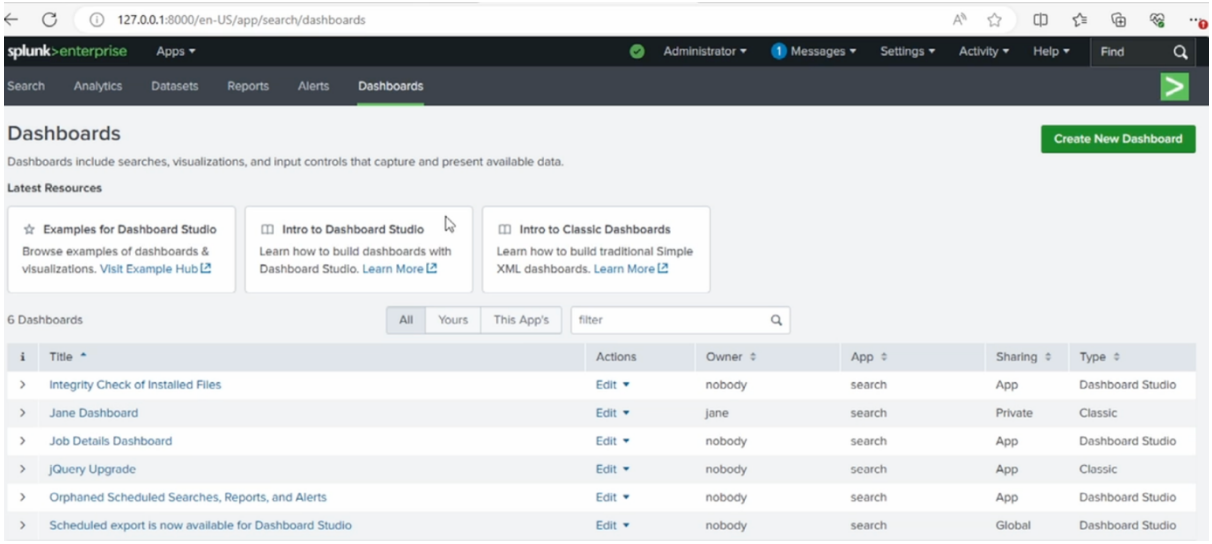
Click on Save As > New Dashboard > “fill in the dashboard title, description e.t.c” > Save to Dashboard



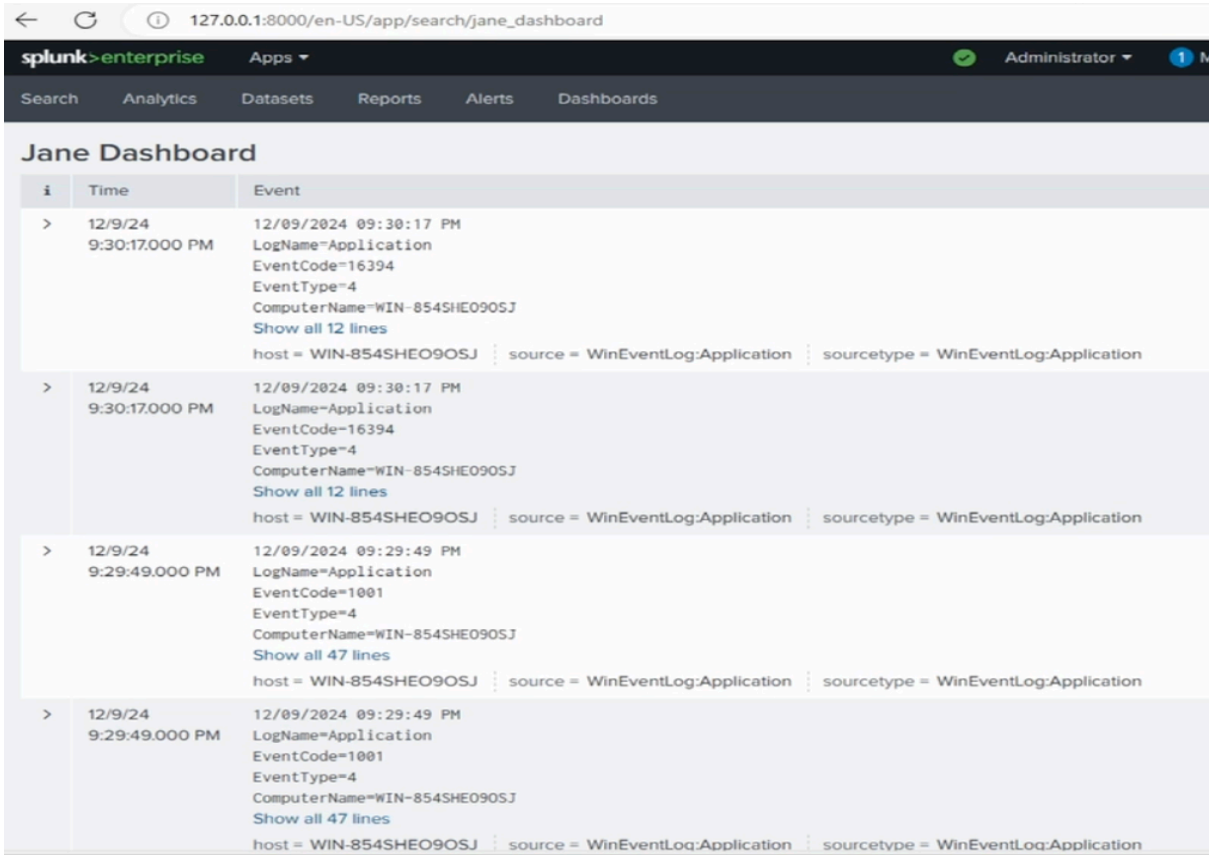
NOTE: You most select “Classic or Studio Dashboard



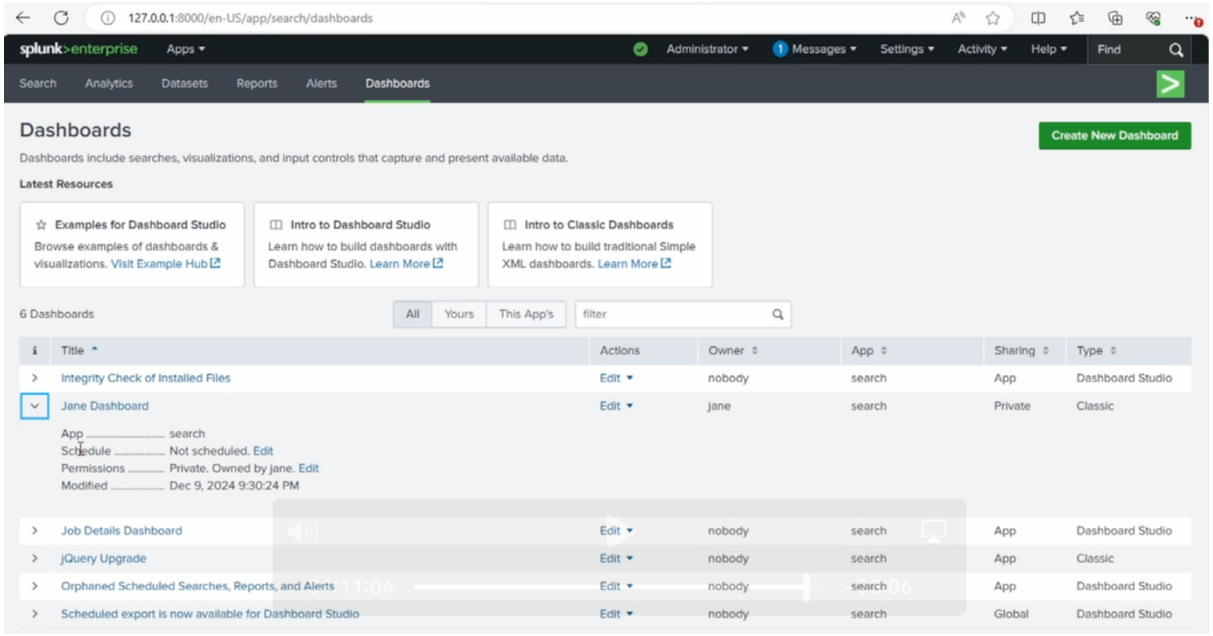

Your Dashboard Panel Has Been Created
The panel has been created and added to jane_dashboard. You may now view the dashboard.
View Dashboard


127.0.0.1:8000/en-US/app/search/dashboards
splunk>enterprise
Apps
Administrator
1 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
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

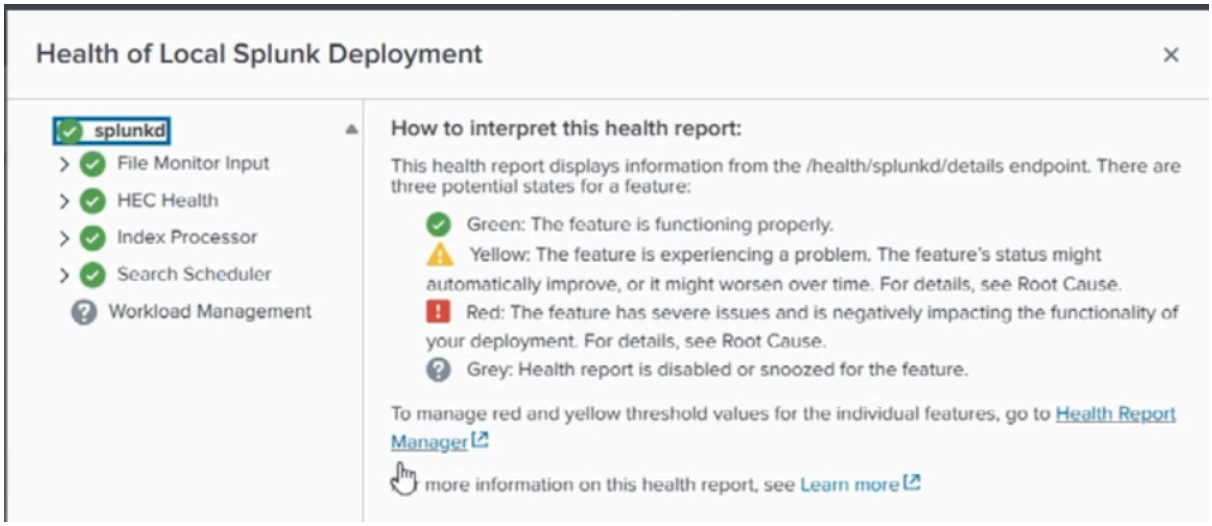
Detailed information of the “Jane Dashboard”



Select Edit button to edit “Jane Dashboard”

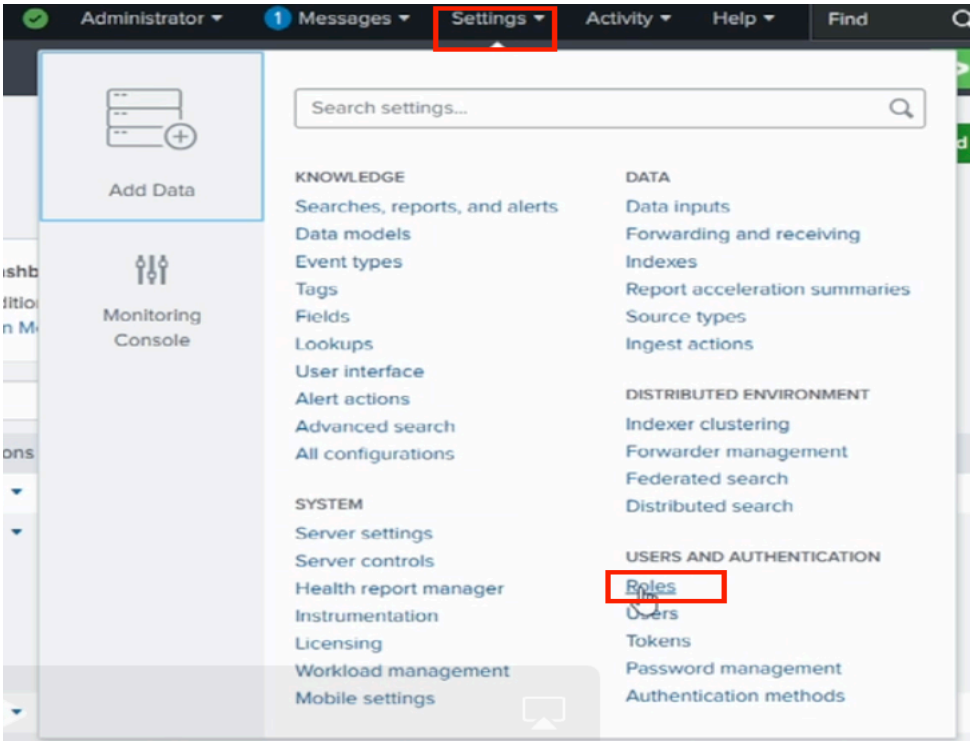


Splunk Health Status Check

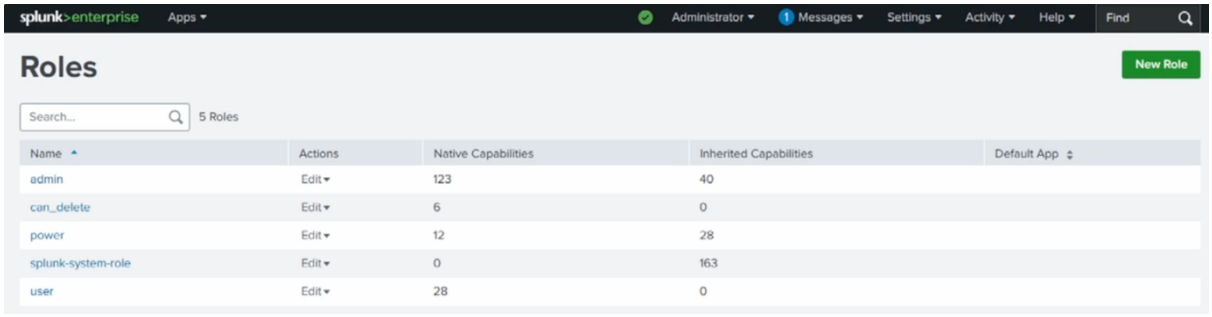


User management on Splunk

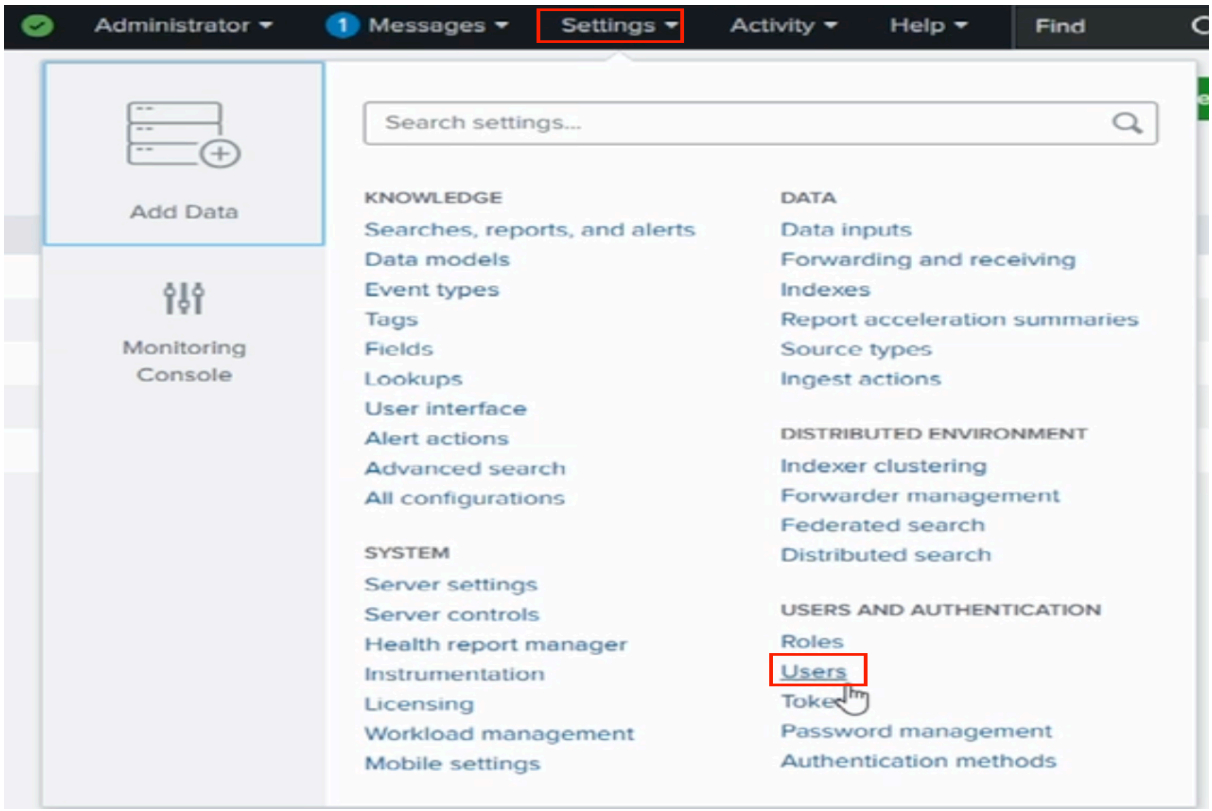
To find and Create a new Role click on Settings > Roles



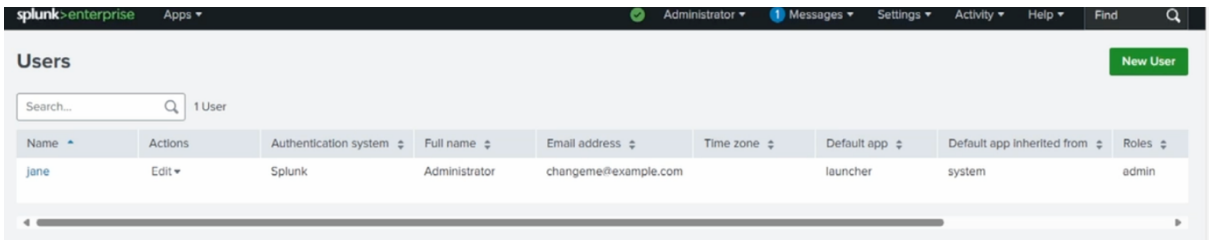
Here you can “Edit or Add New Role”



To Create a New User click on Settings > Users



Here you can “Edit or Add New User”



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).