

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

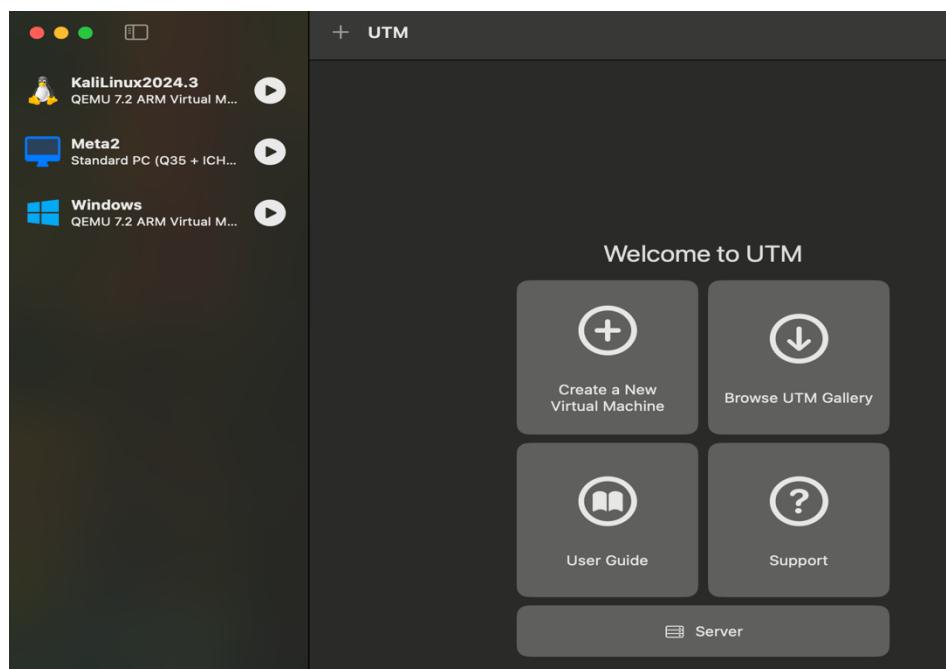
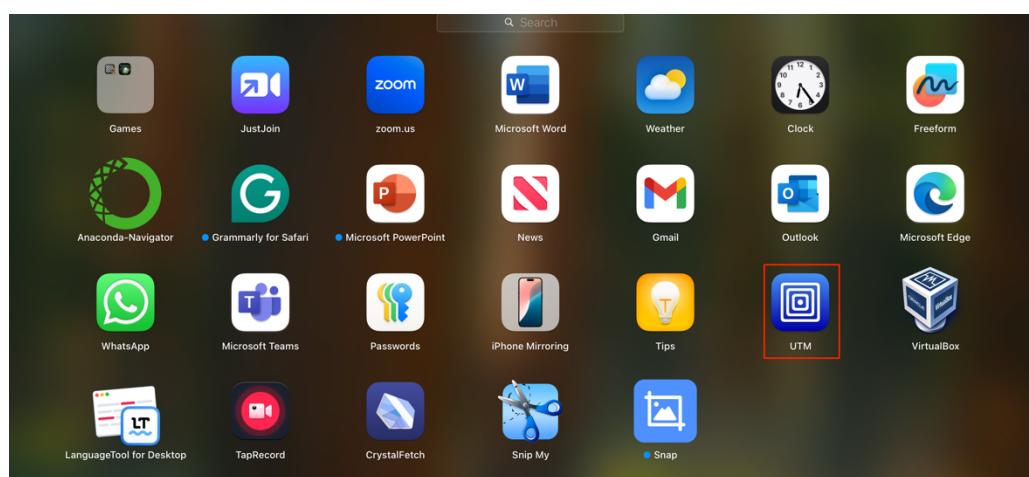
1. Installation and Setting up of Window 11Pro

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.

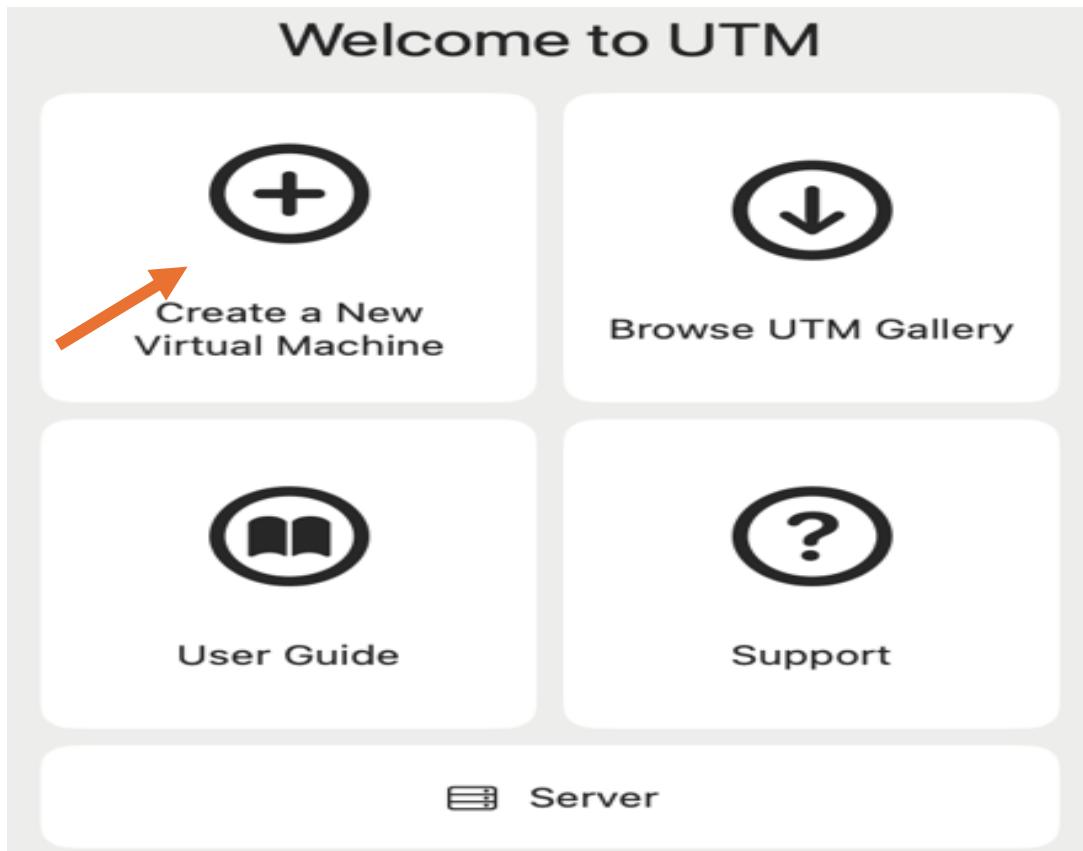
NOTE: If you don't have UTM already installed, visit the UTM Website <https://mac.getutm.app/> to download the latest version of UTM. Click the download button to get the application, once downloaded open the download file and move UTM to Application folder.

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.



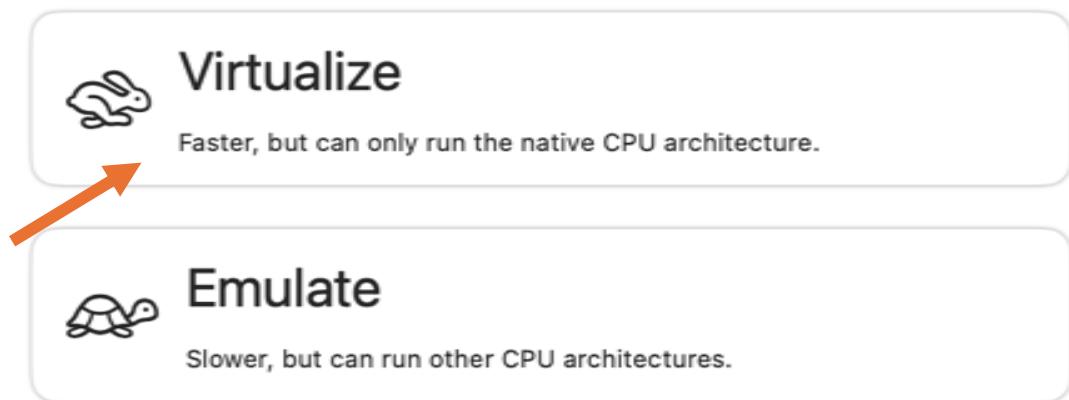
Click on “+ New”: Create a new virtual machine



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, which is a tool for legally obtaining the newest Windows builds from Microsoft.



Alternatively, you can also download an older ISO directly from Microsoft's website or use a browser like Safari or Chrome to download as Microsoft's website sometimes does not work correctly.

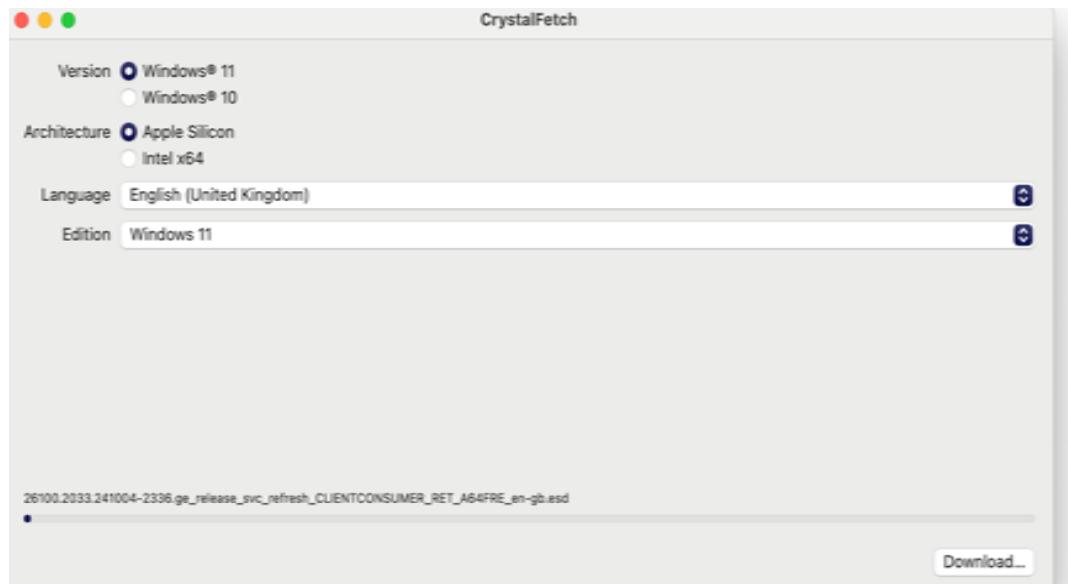
- [Download Windows 11 for Intel Macs](#)
- [Download Windows 11 for Apple Silicon Macs](#)



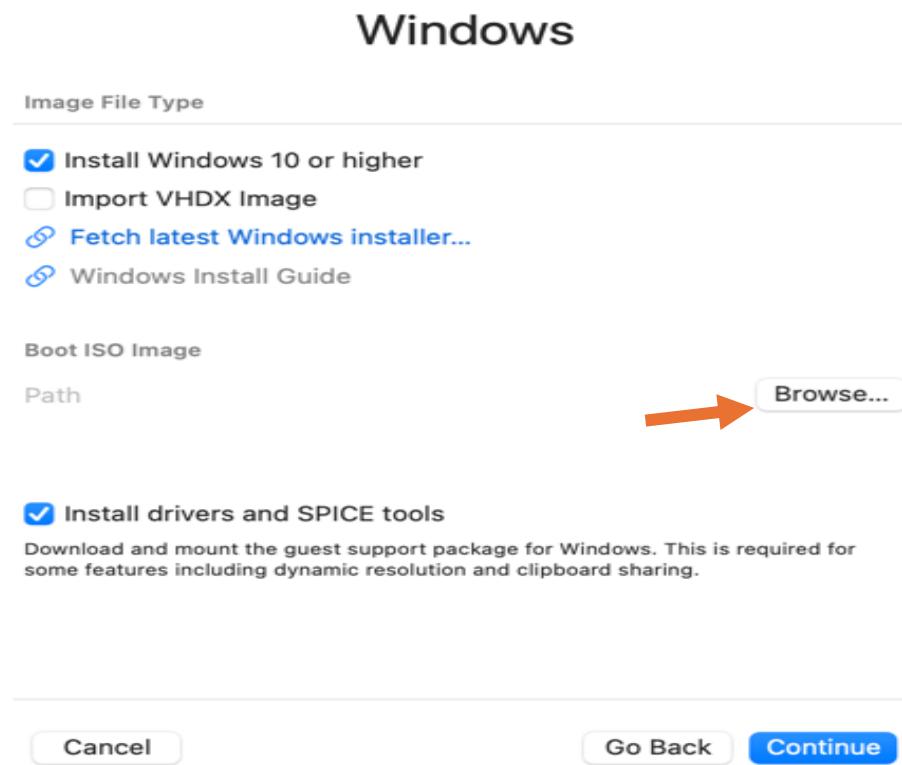
CrystalFetch ISO Downloader

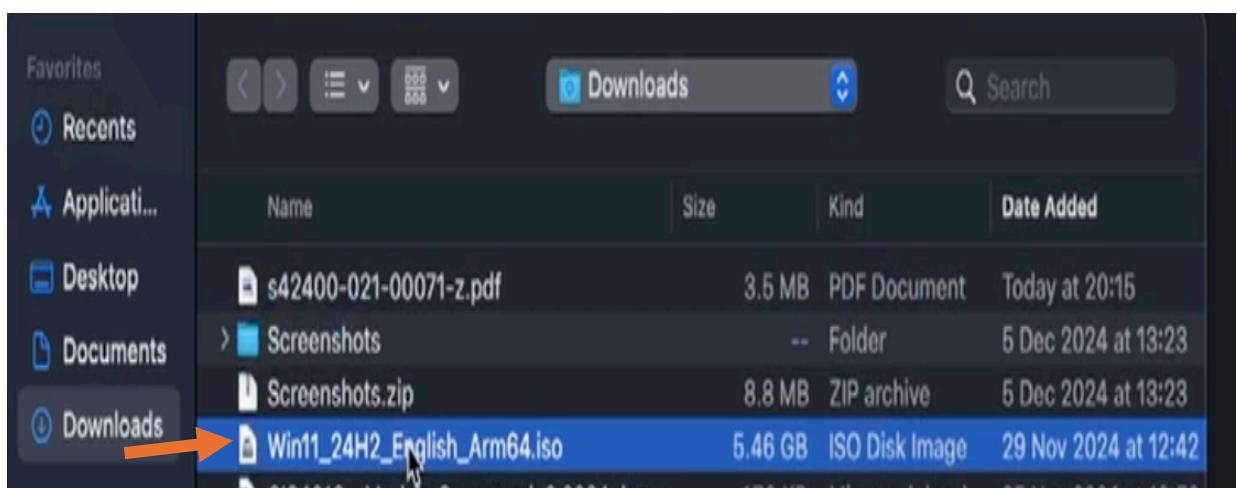
Installer for Windows® 11

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.



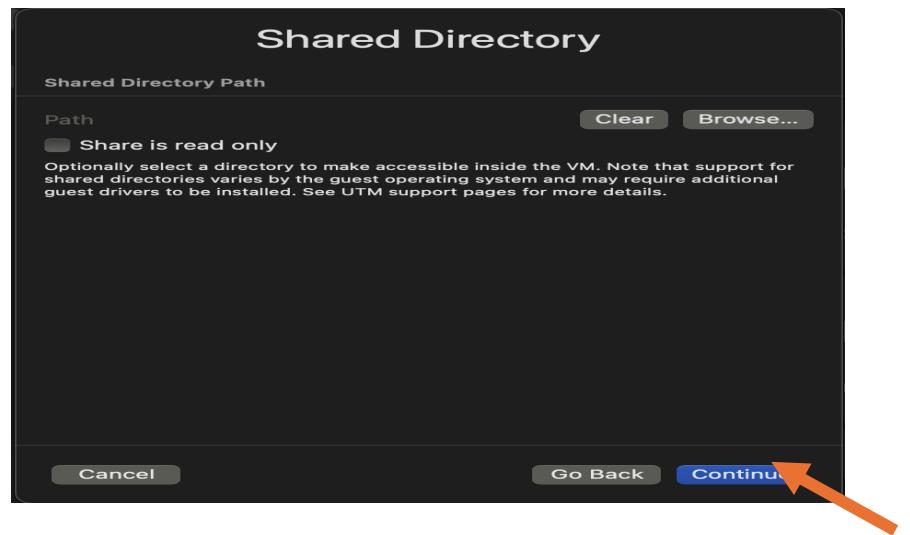


Step 2: Configure the Virtual Machine

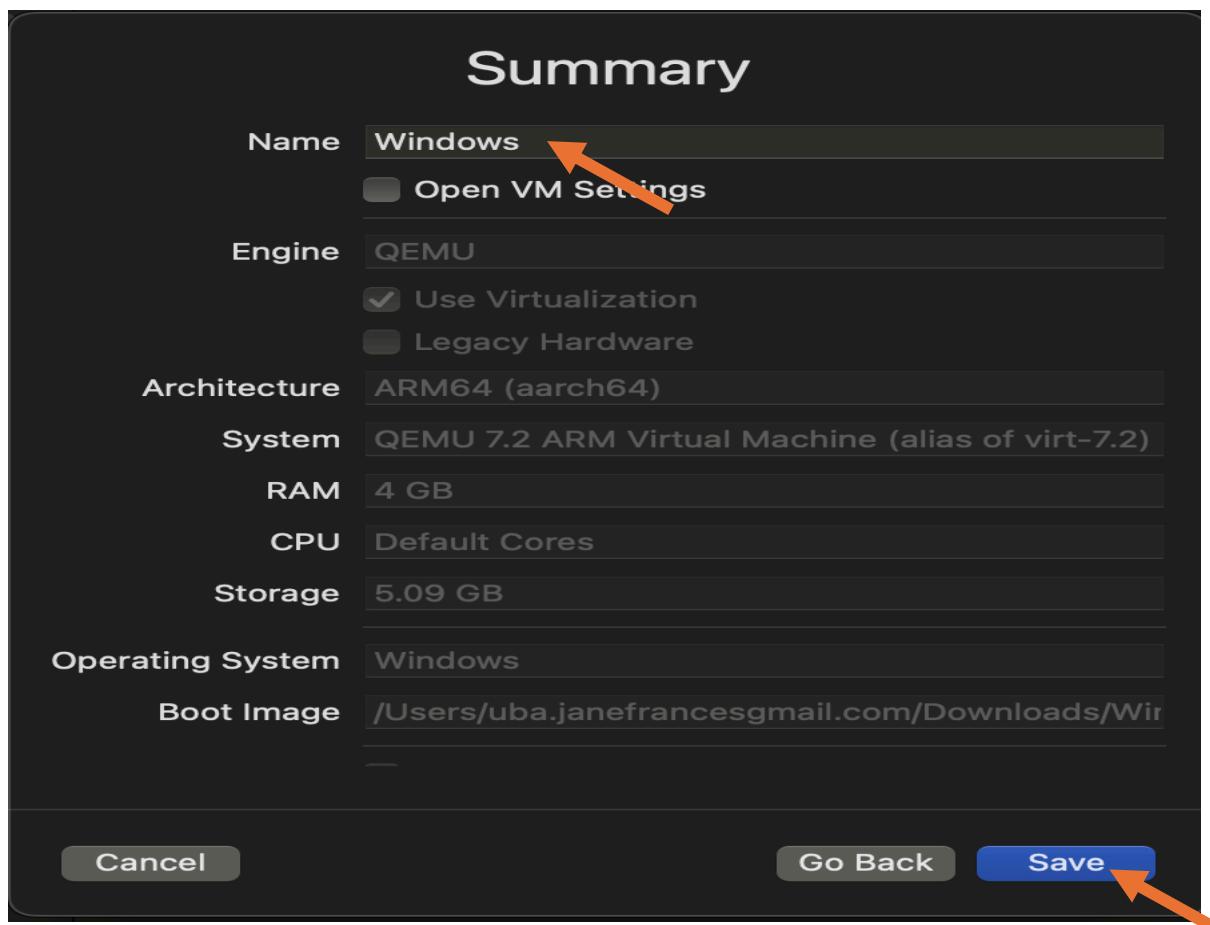
Set the Hardware Preferences: Configure the amount of memory (RAM) and CPU cores.
Recommend: 4 GB RAM and 4 CPU cores for optimal performance, click continue to set the storage.



Do not check the Shared Directory, click continue

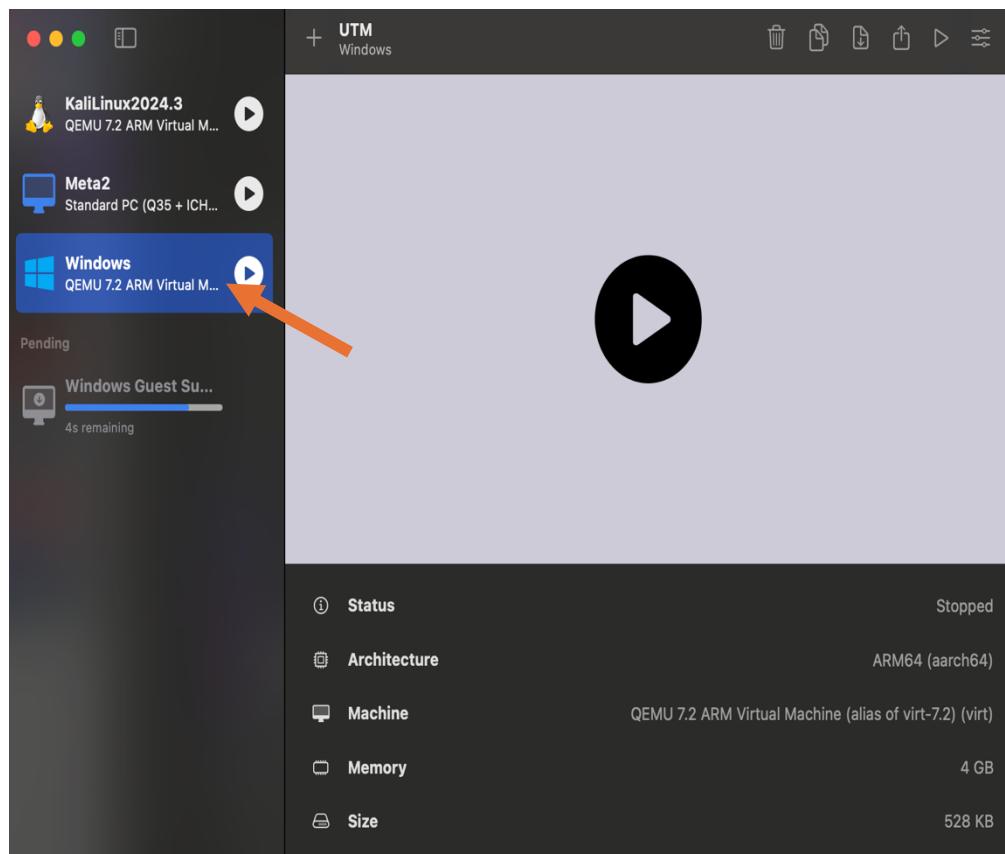


Enter a name for the VM, "Windows" and click Save

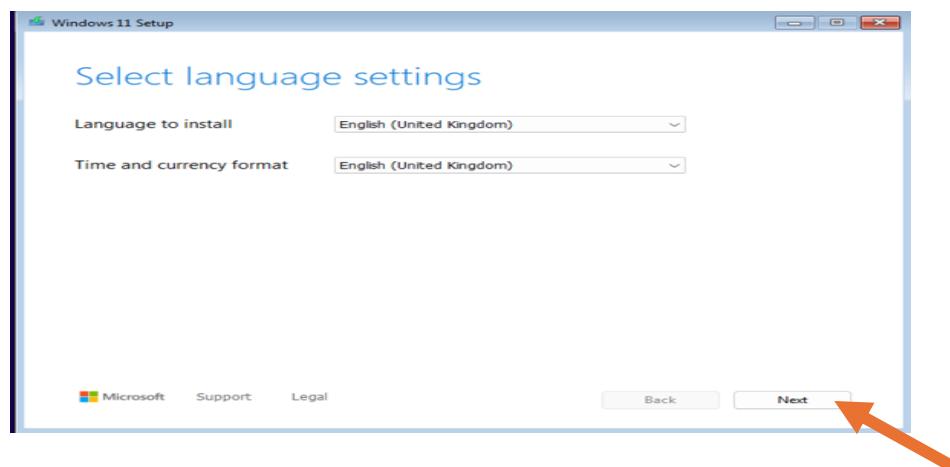


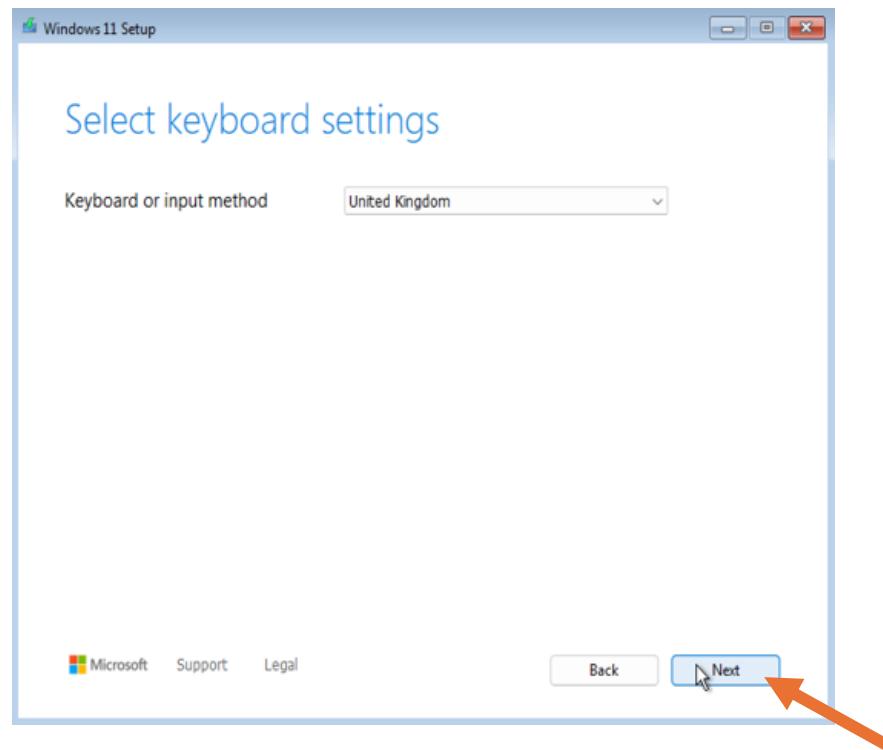
Step 3: Start the Installation

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

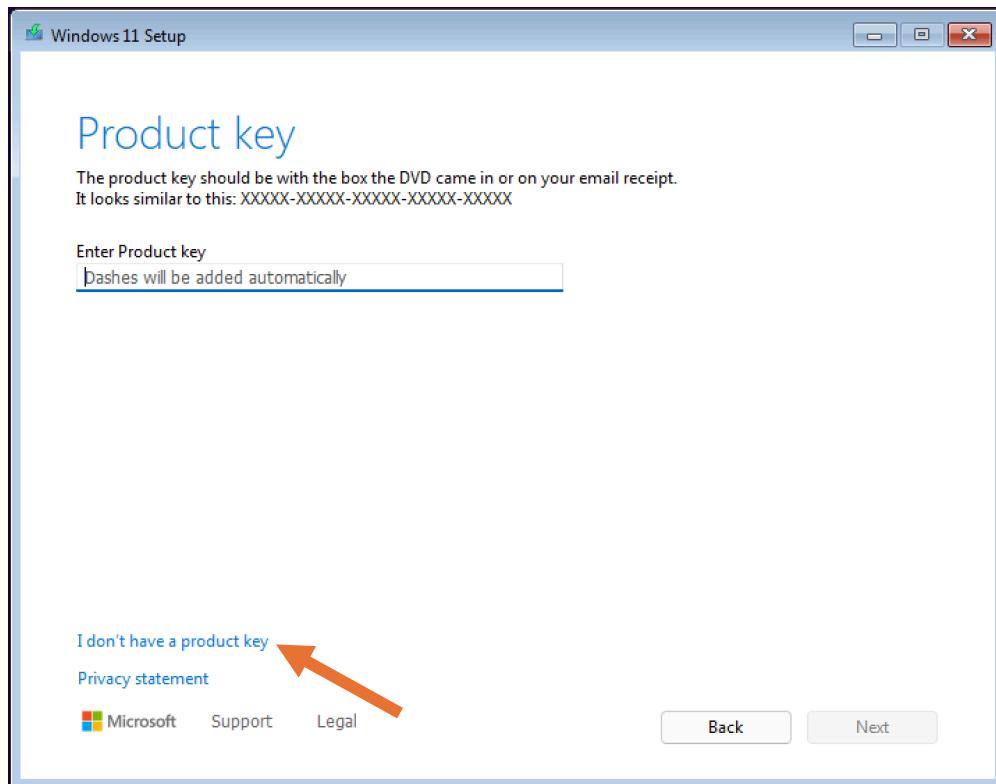


Follow Windows setup steps, the Windows 11 pro installer will launch kindly follow the on-screen instructions steps to complete the installation.

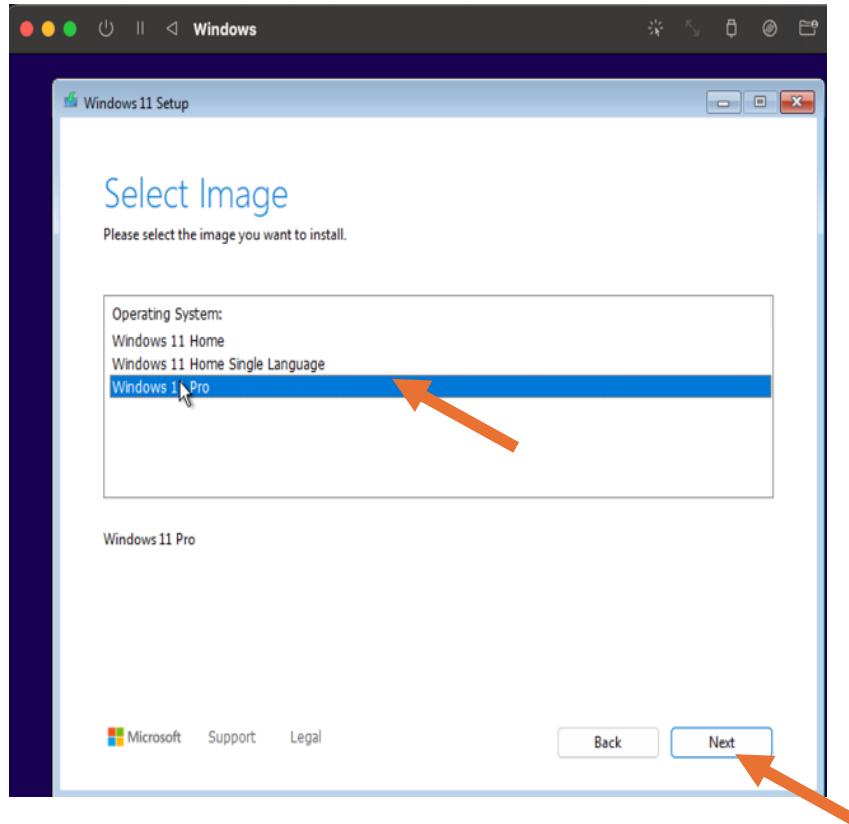




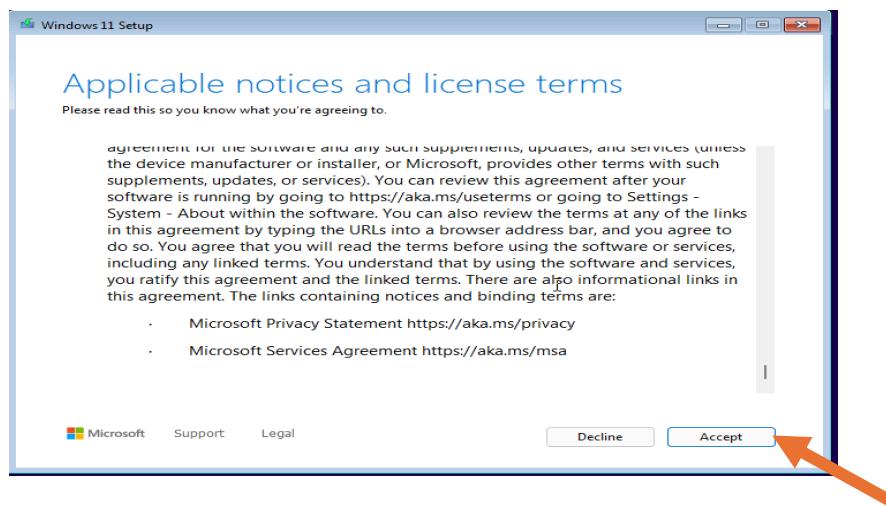
Product key: Add product key if you have, otherwise select I don't have product key.



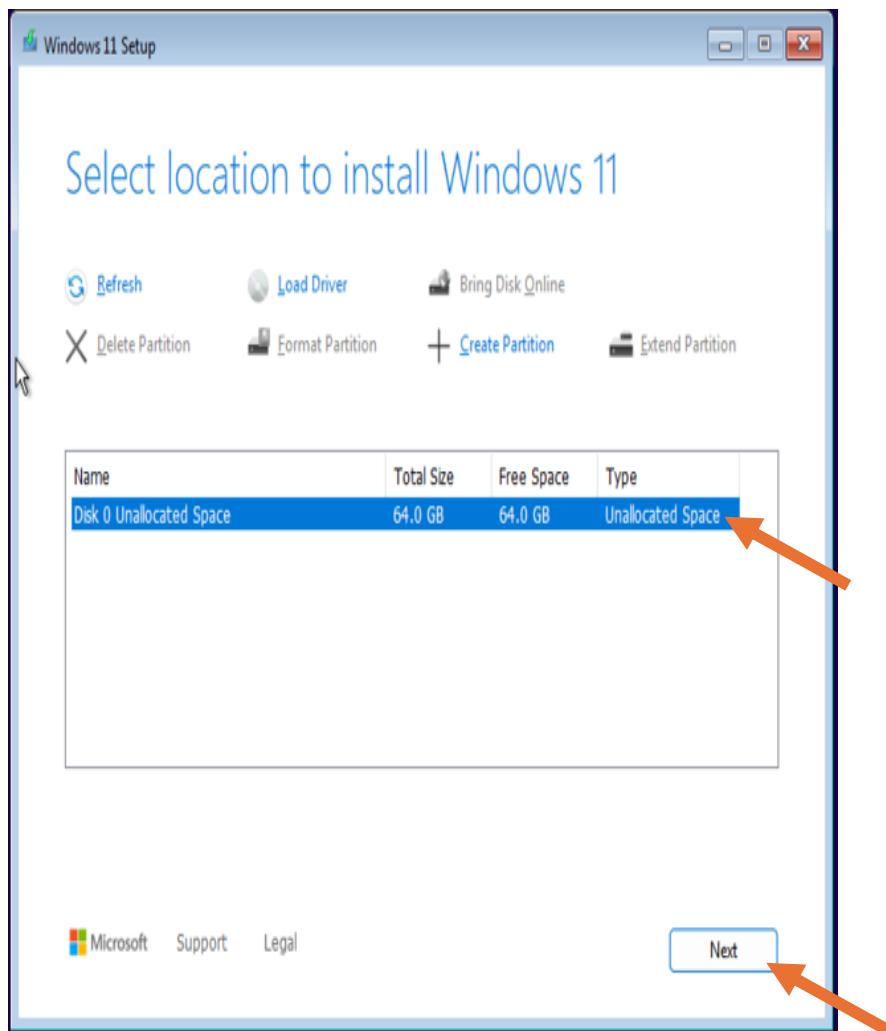
Select the version on the Windows and Click Next



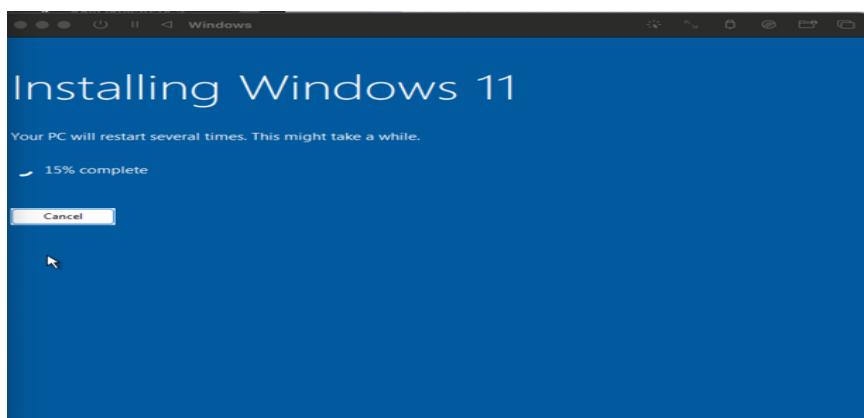
Accept the Licence



Select the Drive Space and click Next

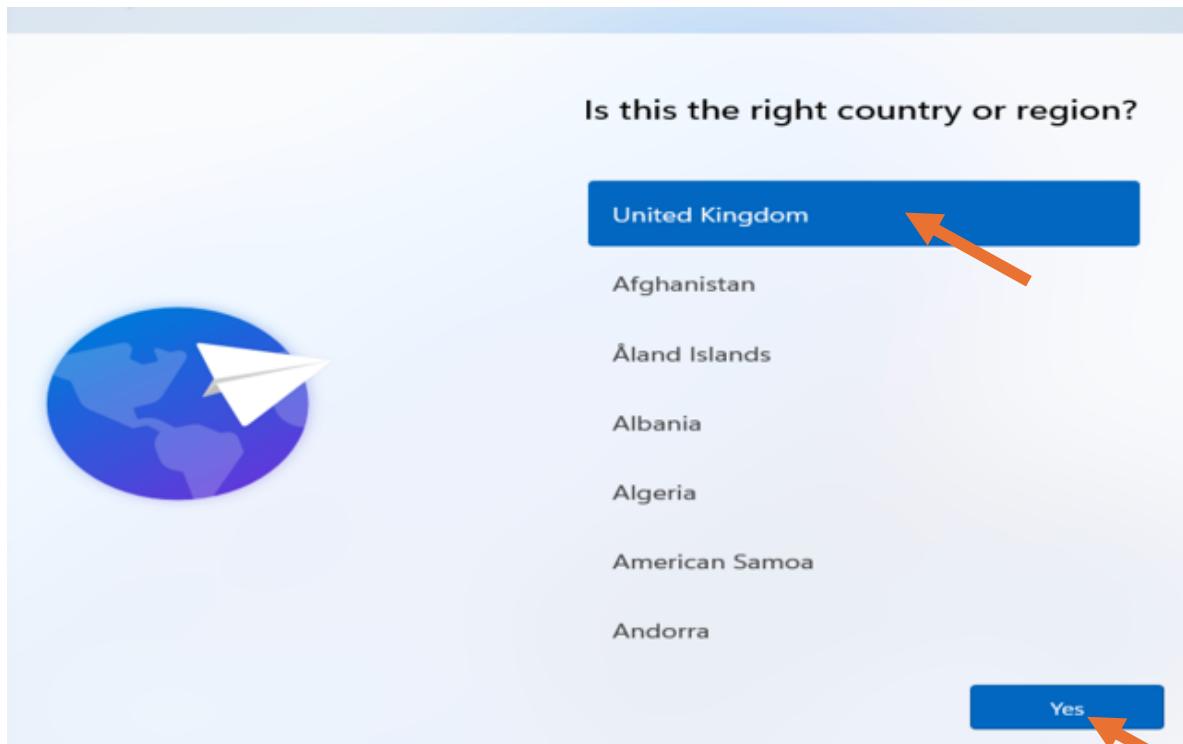


Wait for the Installation to complete



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

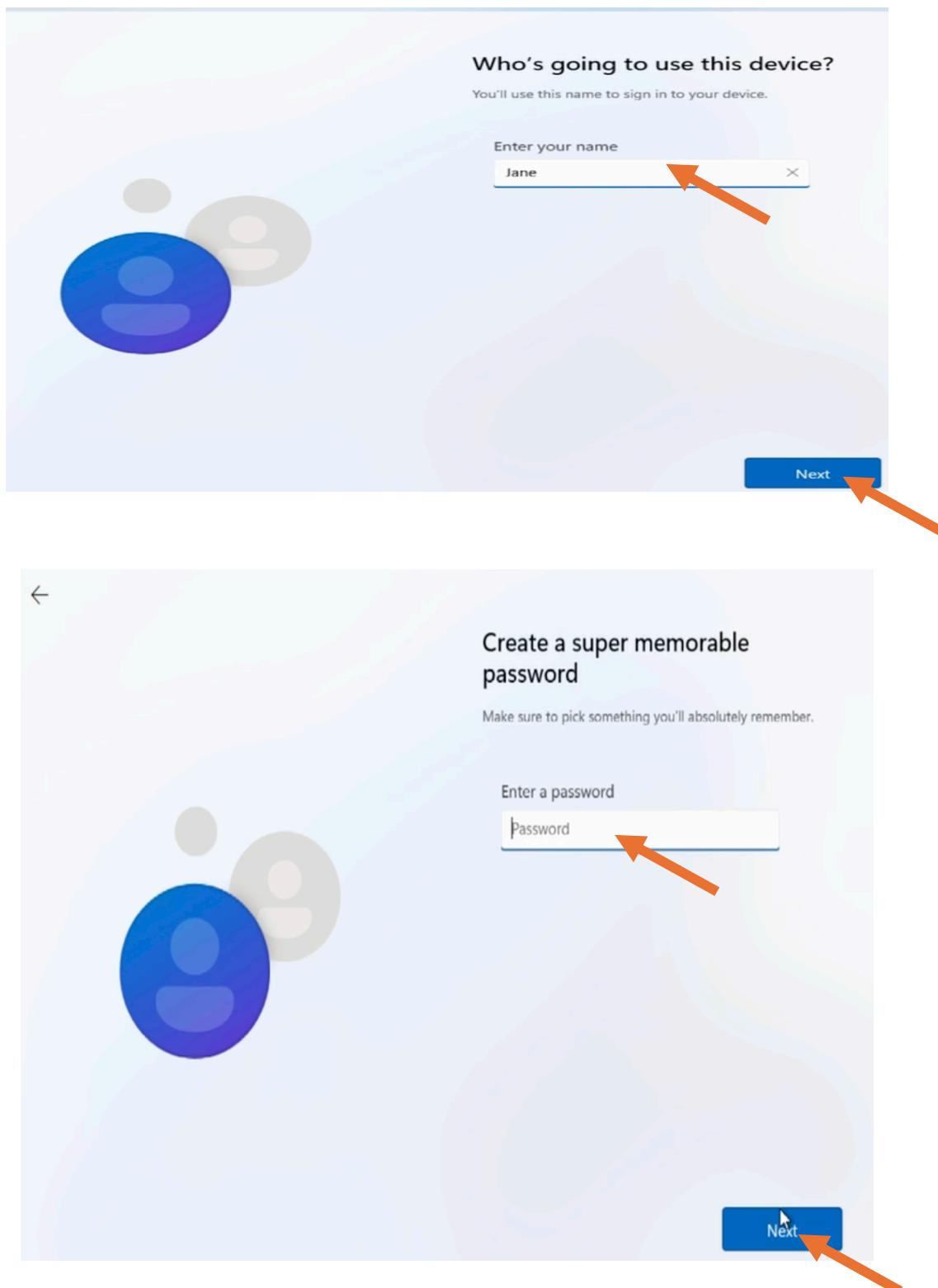
Select the Country

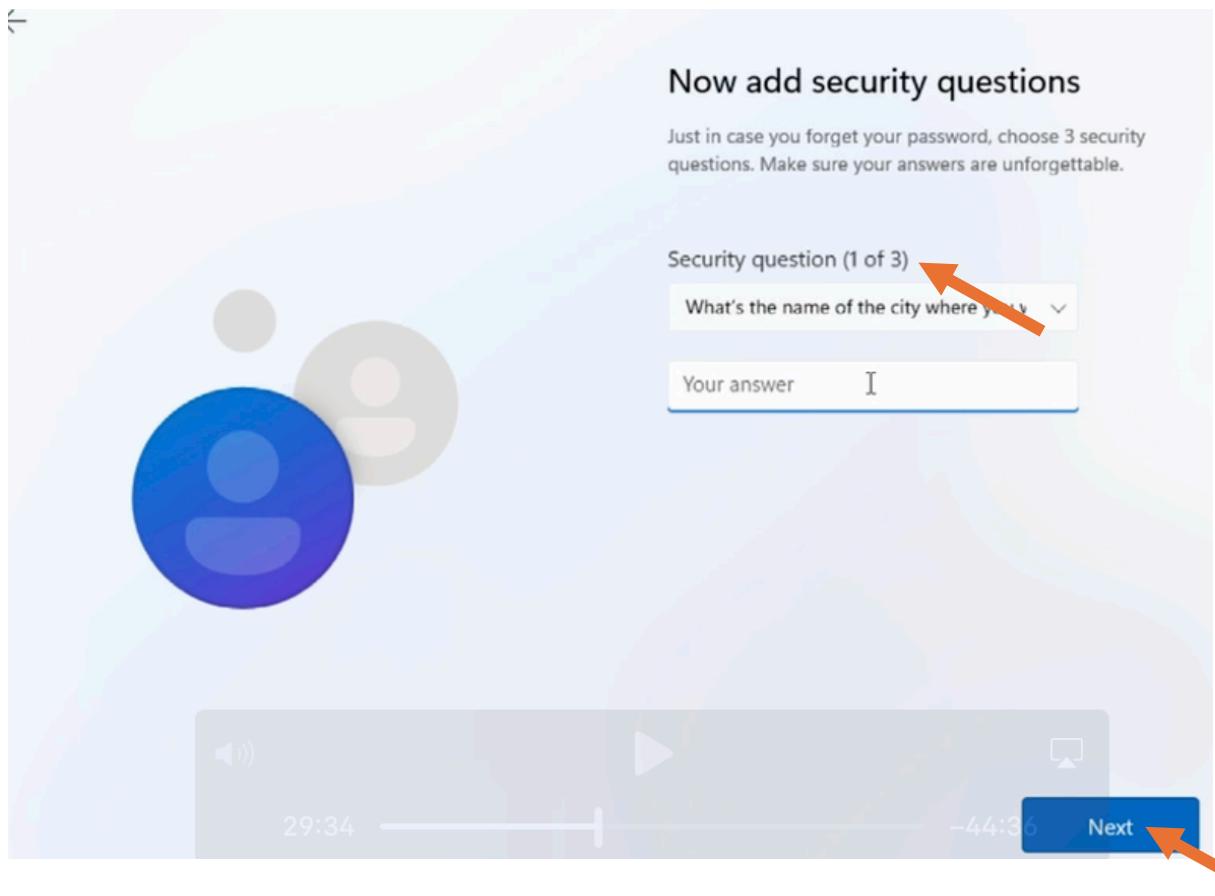


Select the Keyboard Layout

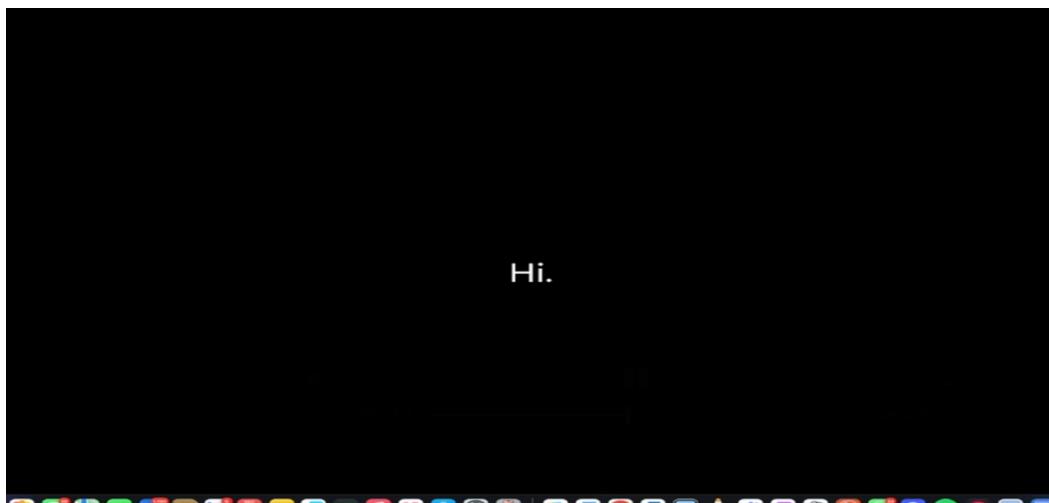


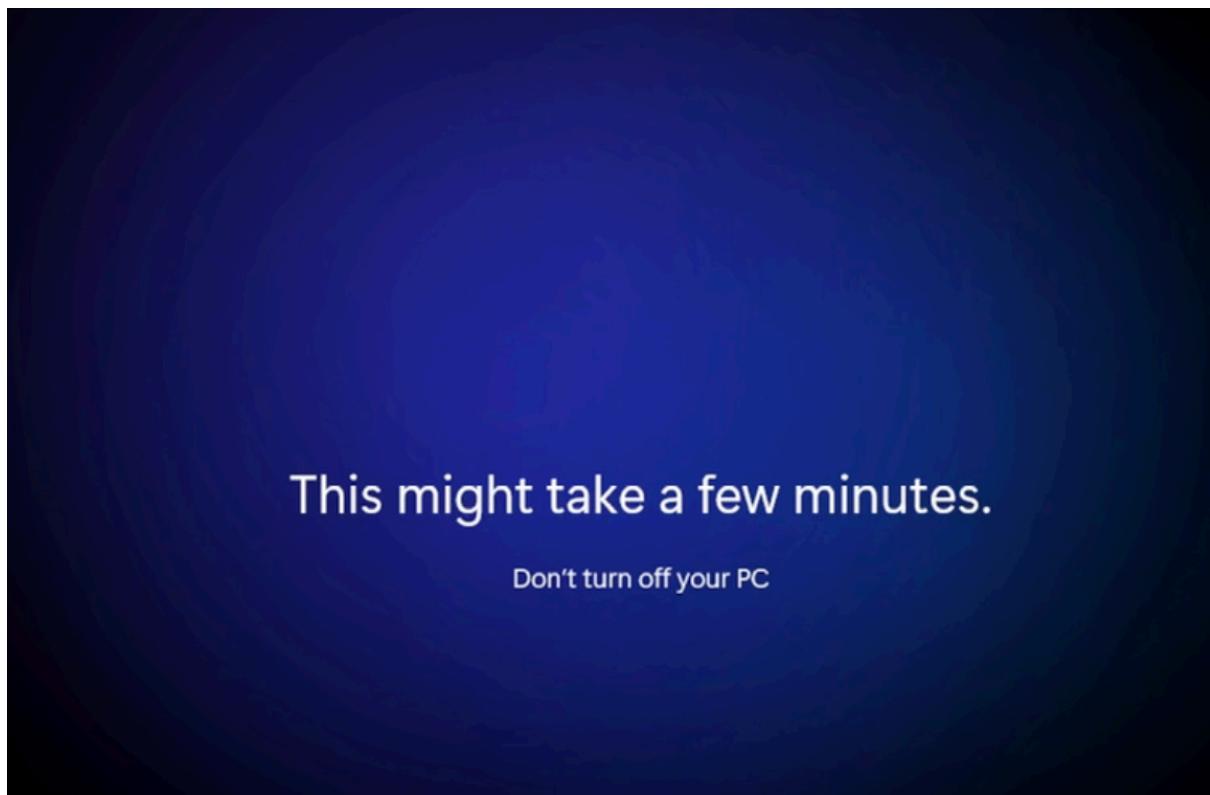
Create your login details “Name, Password and 3 security Questions and Answers”



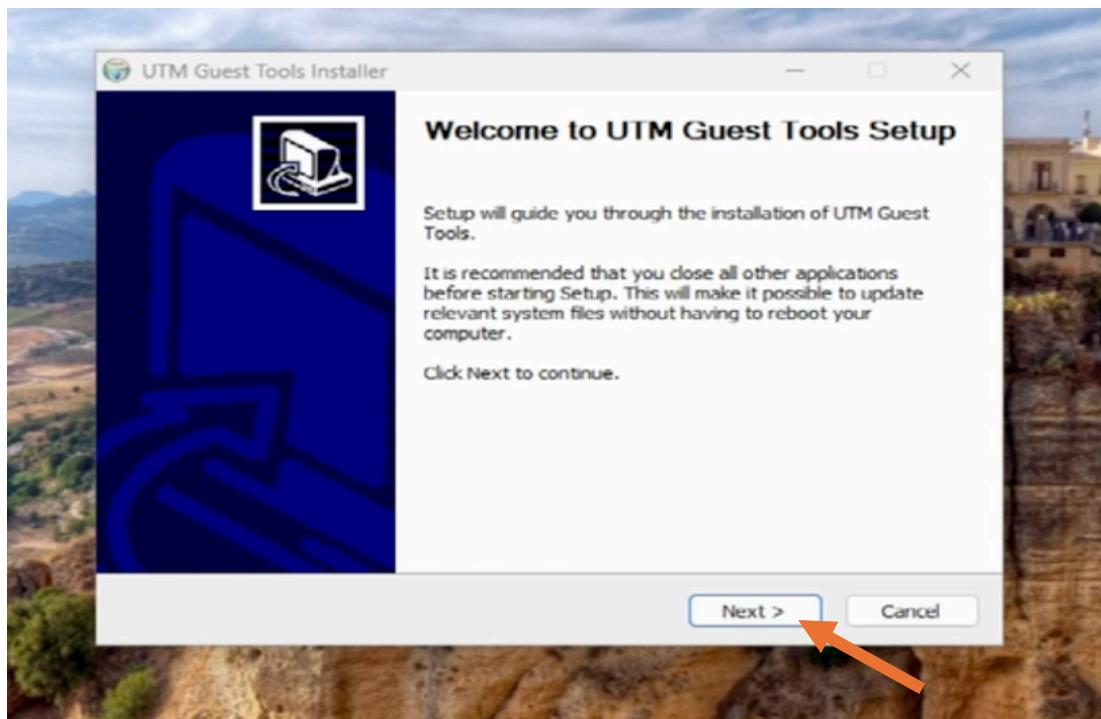


Congratulation you are now booting the windows it will take few minutes so be patient

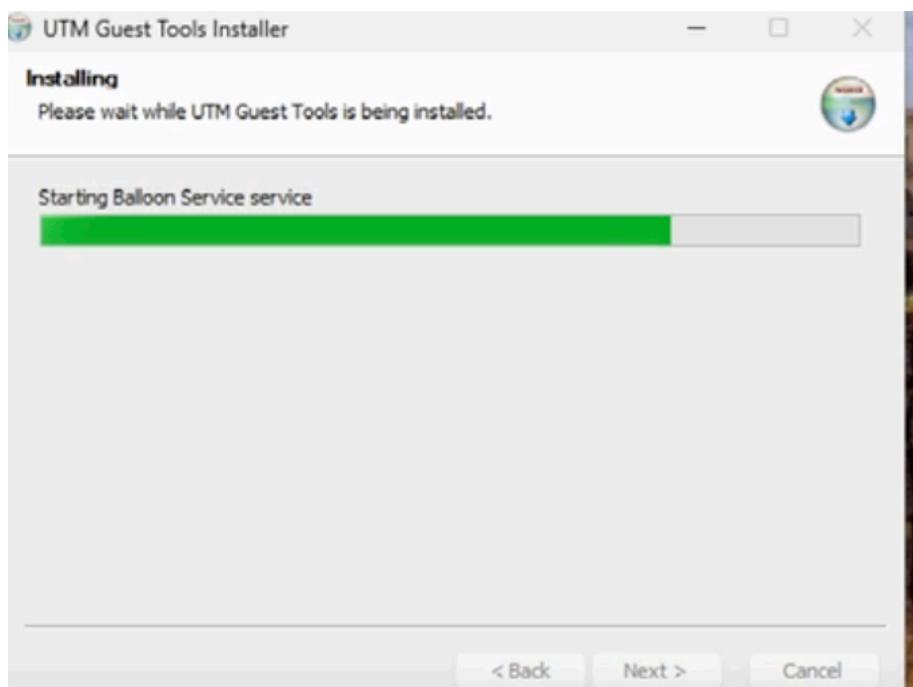
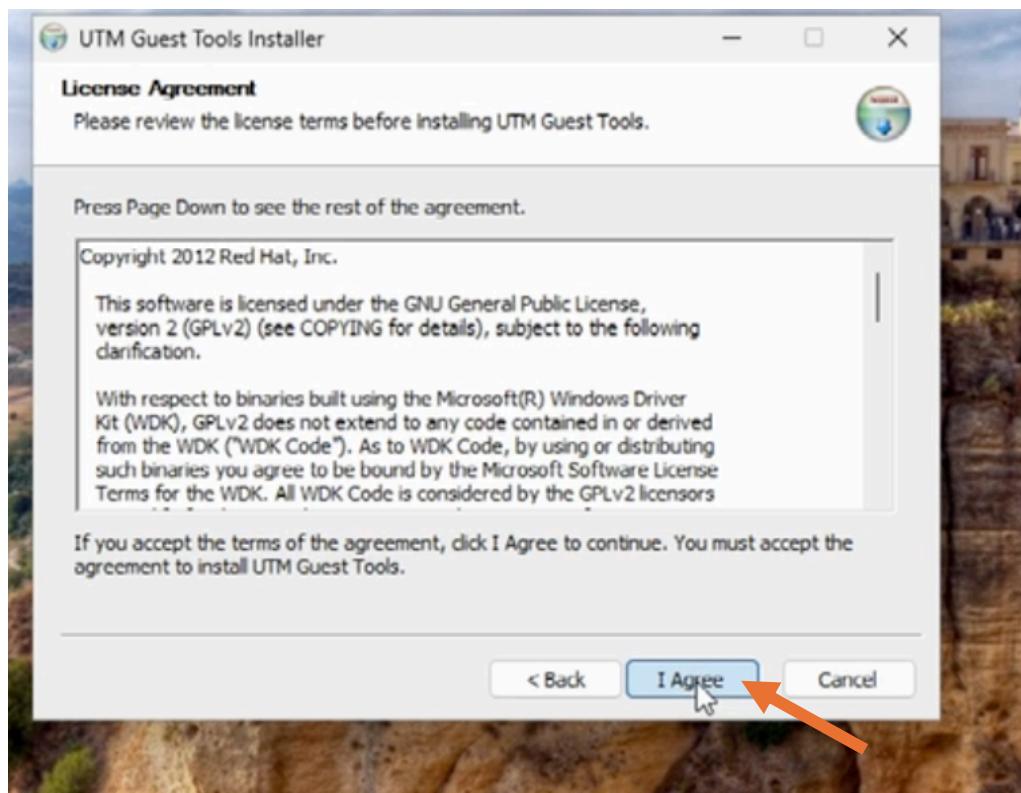


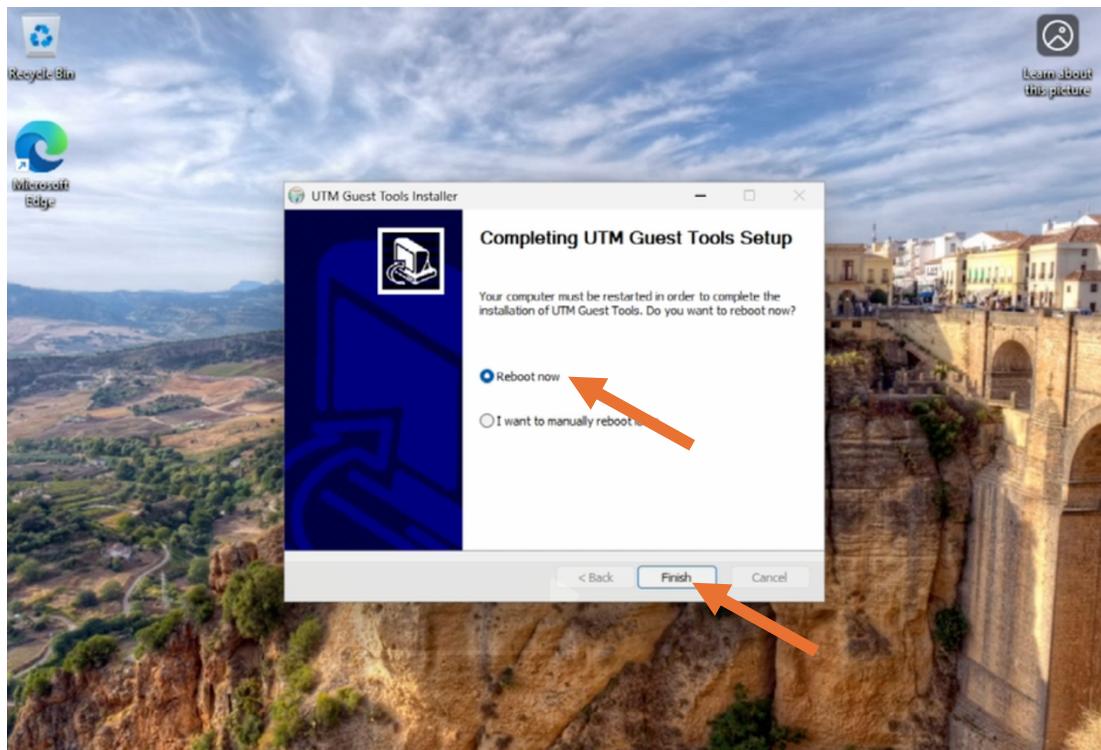


It will automatically launch the Guest Tools Installer. Click on “Next” to install the Guest Tools.



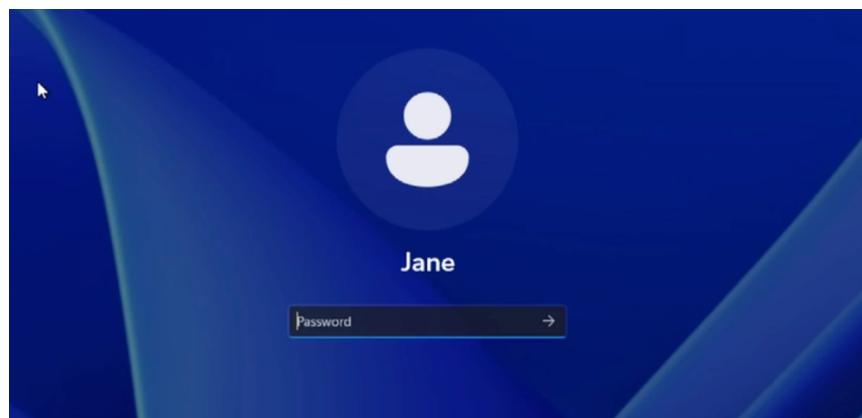
Licence Agreement: Click on “I Agree”, it will automatically be installed. Once done check “Reboot Now” and click on “Finish”.





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

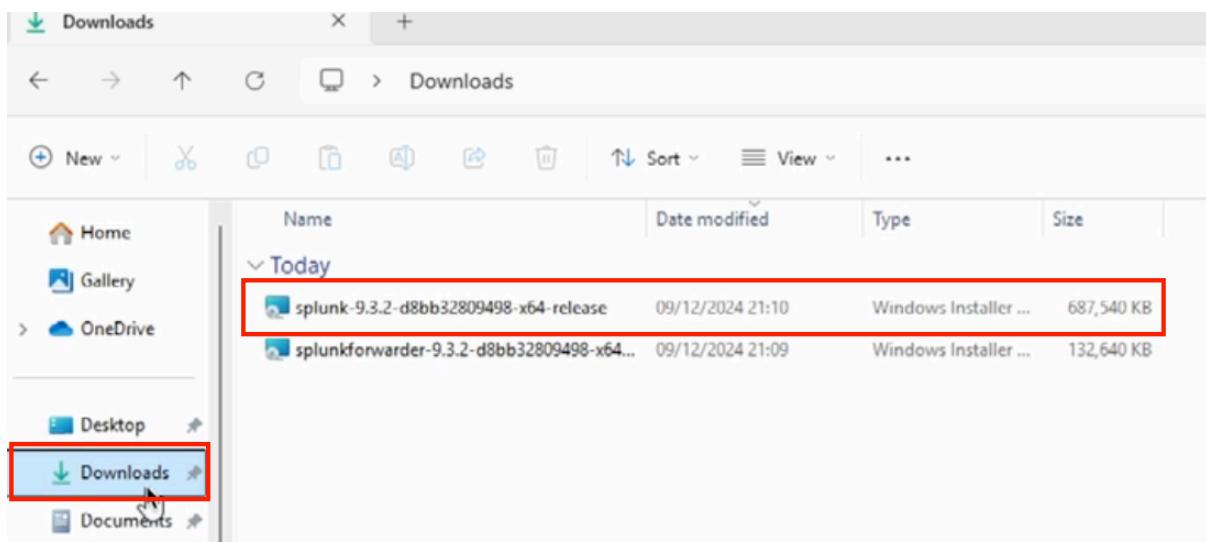
Visit the Splunk website https://www.splunk.com/en_us/download/splunk-cloud.html click on Free Splunk button for 14 days trial if you don't want to be a paid customer.

Create an account and login

The screenshot shows the Splunk website for the 9.3.2 free trial. At the top, there's a navigation bar with links for Products, Solutions, Why Splunk?, Resources, Company, Support, and a search icon. Below the navigation, a "FREE TRIAL" banner features the text "Splunk Enterprise 9.3.2" and the subtext "Try Splunk Enterprise free for 60 days. No credit card required." There are three icons with descriptions: a line graph for managing data in an on-premises environment, a clock for searching and visualizing data on dashboards, and a cloud for installing on Windows or Linux. A section titled "Once you sign up for the Splunk Enterprise trial, you'll see how it helps you to:" lists five bullet points: tackling hardest security and observability use cases, streaming and indexing data at any scale, setting up real-time alerts, and customizing for unique business needs. On the right, a large form titled "Start Your Free Download" asks for a business email, password, first name, last name, job title, phone number, and company. A "Log In" link is also present.

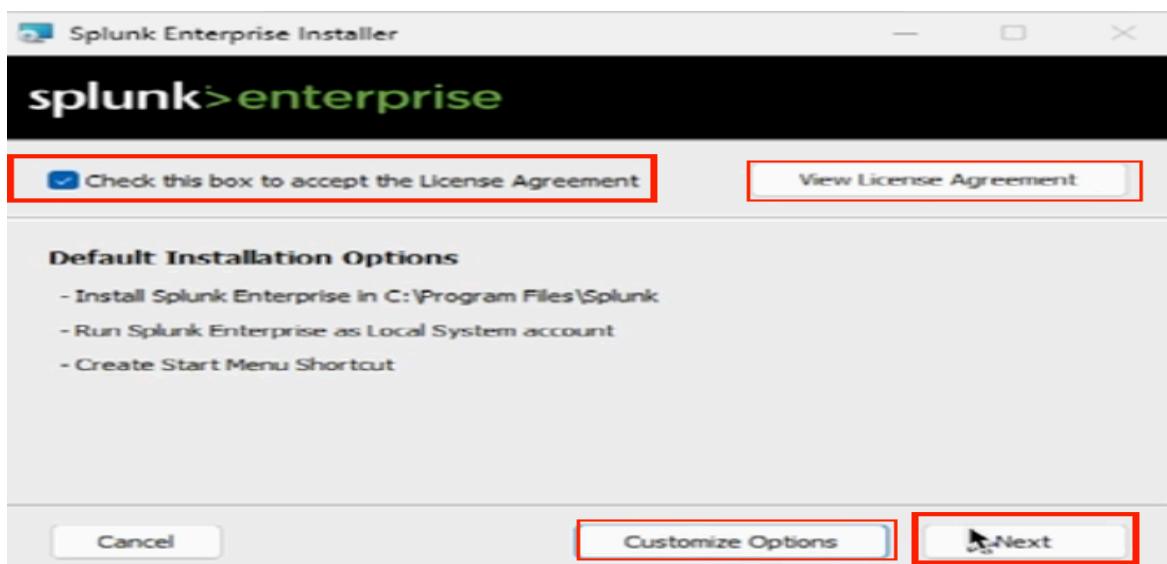
Download .msi installer

The screenshot shows the "Choose Your Download" page for Splunk Enterprise 9.3.2. It features a "GET STARTED" button and the "Choose Your Download" heading. Below this, a section for "Splunk Enterprise 9.3.2" is shown with the text: "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." A "Choose Your Installation Package" section offers options for Windows, Linux, and Mac OS. The Windows section is highlighted with a red border and shows a 64-bit icon, the text "Windows 10 Windows Server .msi", "671.43 MB", a "Download Now" button, a "Copy wget link" button, and a "More" dropdown menu.

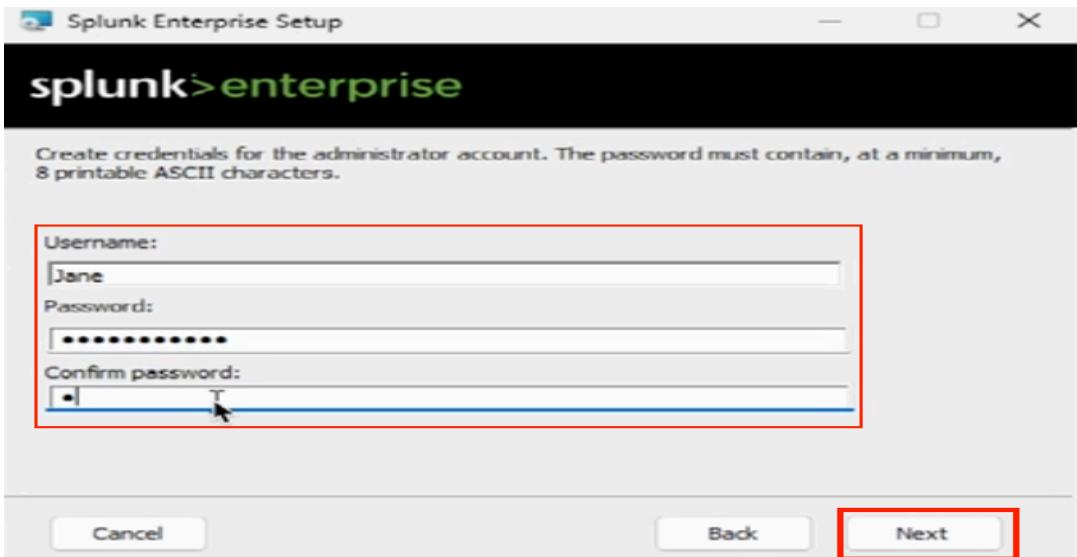


View and read the Licence Agreement for better understanding of how your data will be used.

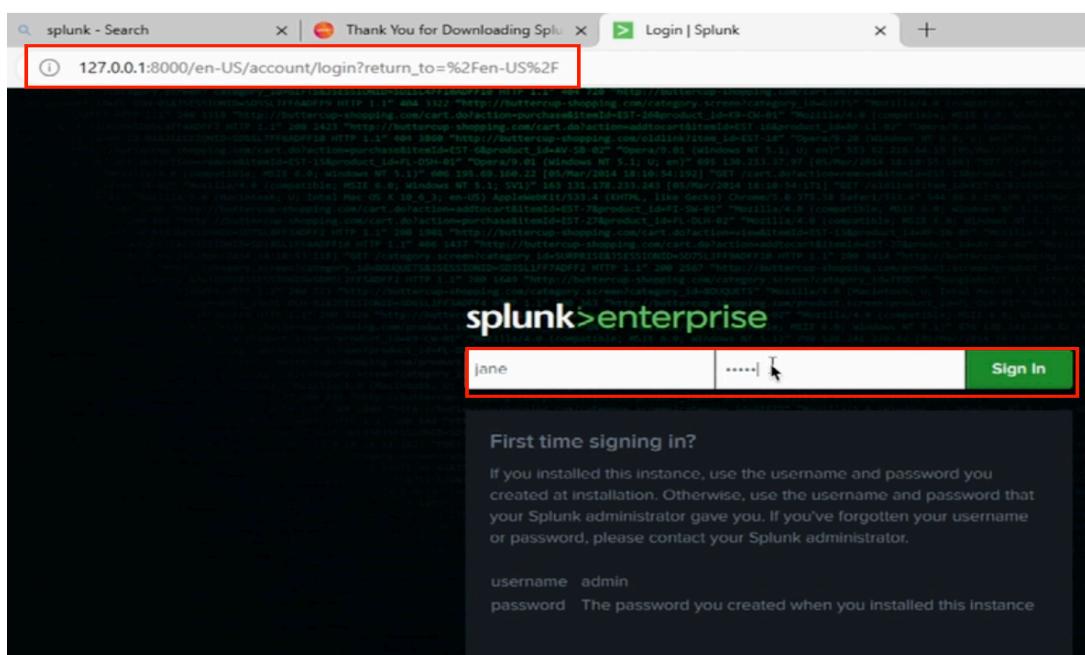
Check the box and accept the Licence Agreement, customize Options will be automatically selected but if not press the button, and click Next



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



The screenshot shows the Splunk Enterprise home page. The URL in the address bar is 127.0.0.1:8000/en-US/app/launcher/home. The main content area is titled "Hello, Administrator". It features several sections: "My bookmarks (0)", "Shared with my organization (0)", "Shared by me", "Shared by other administrators", and "Splunk recommended (14)". Under "Common tasks", there are four boxes: "Add data" (Add data from a variety of common sources), "Search your data" (Turn data into doing with Splunk search), "Visualize your data" (Create dashboards that work for your data), and "Manage alerts" (Manage the alerts that monitor your data).

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.

The screenshot shows the Windows Services application window. The title bar says "Services". The main pane is titled "Services (Local)". A table lists various services with columns: Name, Description, Status, Startup Type, and Log On As. The "Splunkd Service" is highlighted with a red box. Its details are shown in a tooltip: "Description: Splunkd is the indexing and searching engine for Splunk, a data platform for operational intelligence. It is required for Splunk instances acting as an indexer. If it is stopped, Splunk will not process data and will be unavailable for search. Splunkweb depends on Splunkd. Please see www.splunk.com for more information. Questions can be submitted to www.splunk.com/answers or for supported customers www.splunk.com/page/submit_issue". The "Status" column shows "Running", "Startup Type" shows "Automatic", and "Log On As" shows "Local System". Other services listed include Remote Procedure Call (RPC), Remote Registry, Retail Demo Service, Routing and Remote Access, RPC Endpoint Mapper, Secondary Logon, Secure Socket Tunneling Pr..., Security Accounts Manager, Security Center, Sensor Data Service, Sensor Monitoring Service, Sensor Service, Server, Shared PC Account Manager, Shell Hardware Detection, Smart Card, Smart Card Device Enumerator, Smart Card Removal Policy, SNMP Trap, Software Protection, SPICE VDAgent, Spice webdav proxy, and Spot Verifier.

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

The screenshot shows the Splunk Universal Forwarder 9.3.2 download page. At the top, there's a brief description of what universal forwarders do. Below it, a section titled "Choose Your Installation Package" lists various operating systems with their respective icons. A red box highlights the "Windows 10, 11" entry, which includes the ".msi" file extension, a size of 129.53 MB, and a "Download Now" button.

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

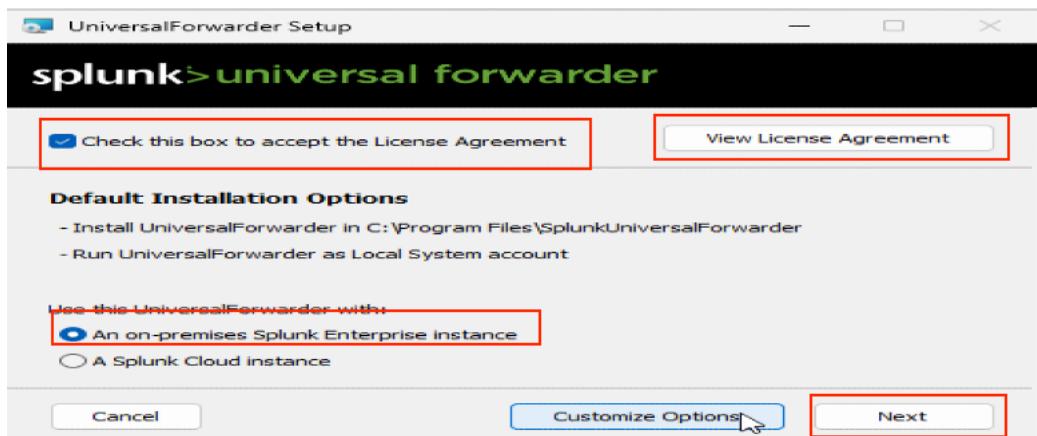
Windows Linux Mac OS Free BSD Solaris AIX

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

Launch the Splunk Universal Forwarder

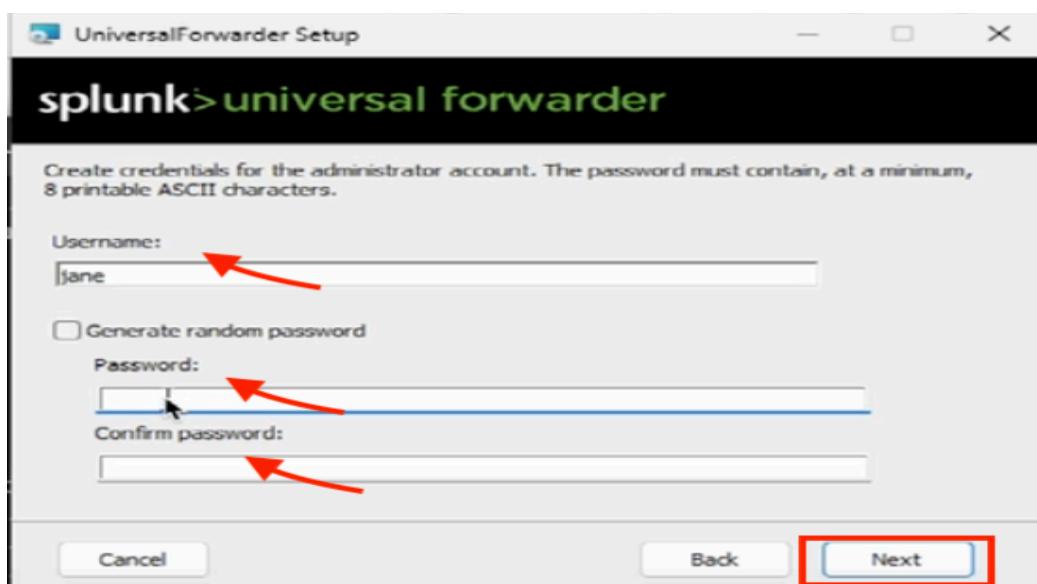
View and read the Licence Agreement for better understanding of how your data will be used.

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



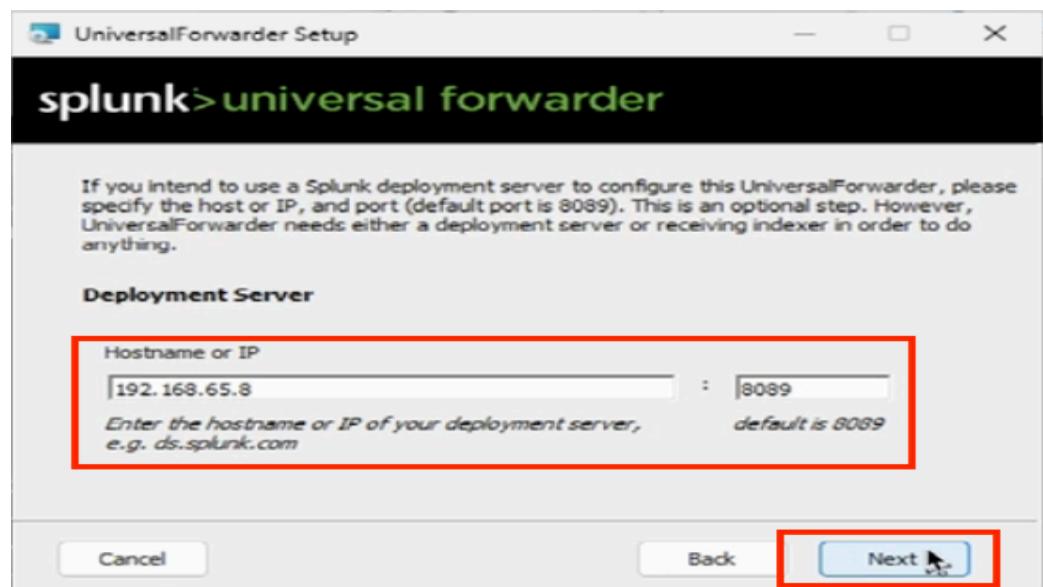
Set Username and Password to the Universal Forwarder and click Next

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.

The screenshot shows an 'Administrator: Command Pro' window. It displays the output of the 'ipconfig' command. The output includes:

```
Microsoft Windows [Version 10.0.26100.1742]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Jane>ipconfig

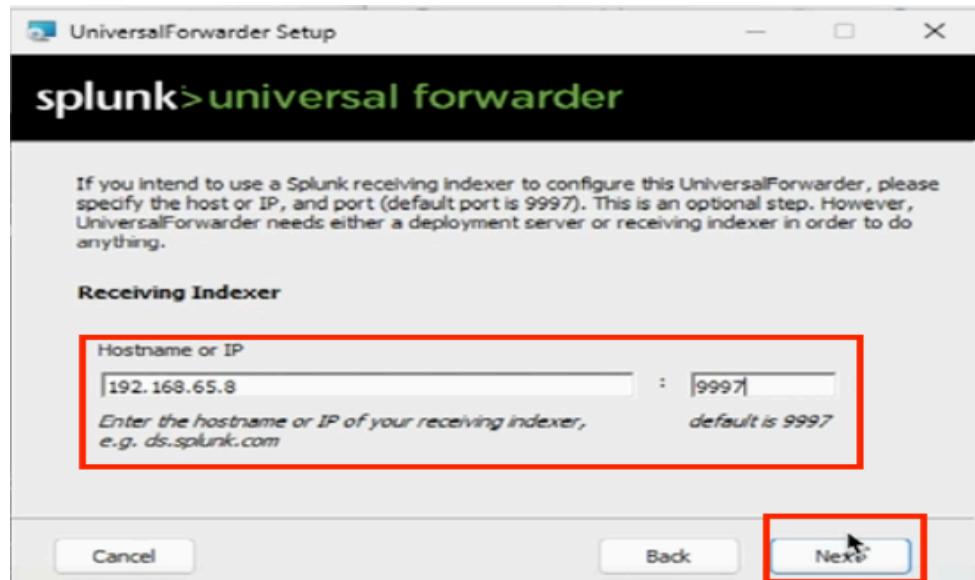
Windows IP Configuration

Ethernet adapter Ethernet:

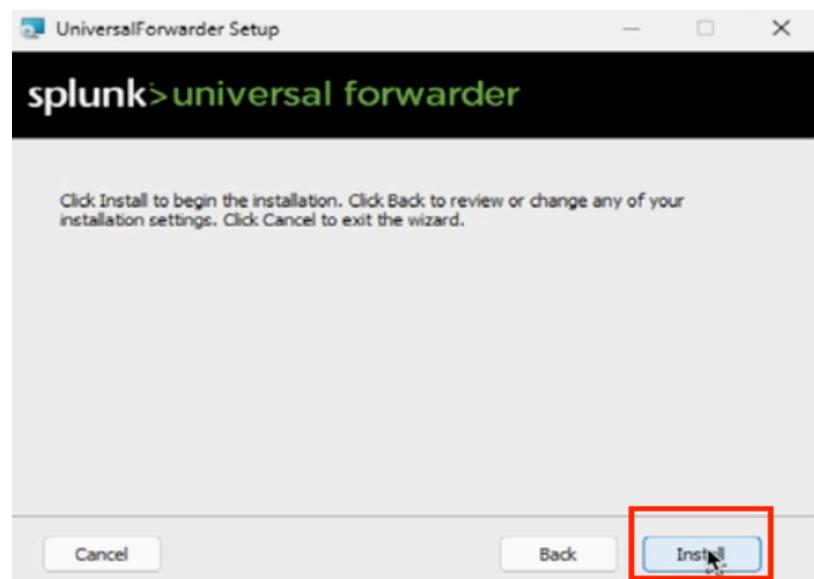
Connection-specific DNS Suffix . : users.local
IPv6 Address . . . . . : fda6:e290:1235:cf99:acff:1314:389d:65bd
Temporary IPv6 Address . . . . . : fda6:e290:1235:cf99:4475:1c54:6e3a:2eee
Link-local IPv6 Address . . . . . : fe80::5d97:ec2c:392e:1f12%6
IPv4 Address . . . . . : 192.168.65.8
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.65.1
```

The 'IPv4 Address' line is highlighted with a red box.

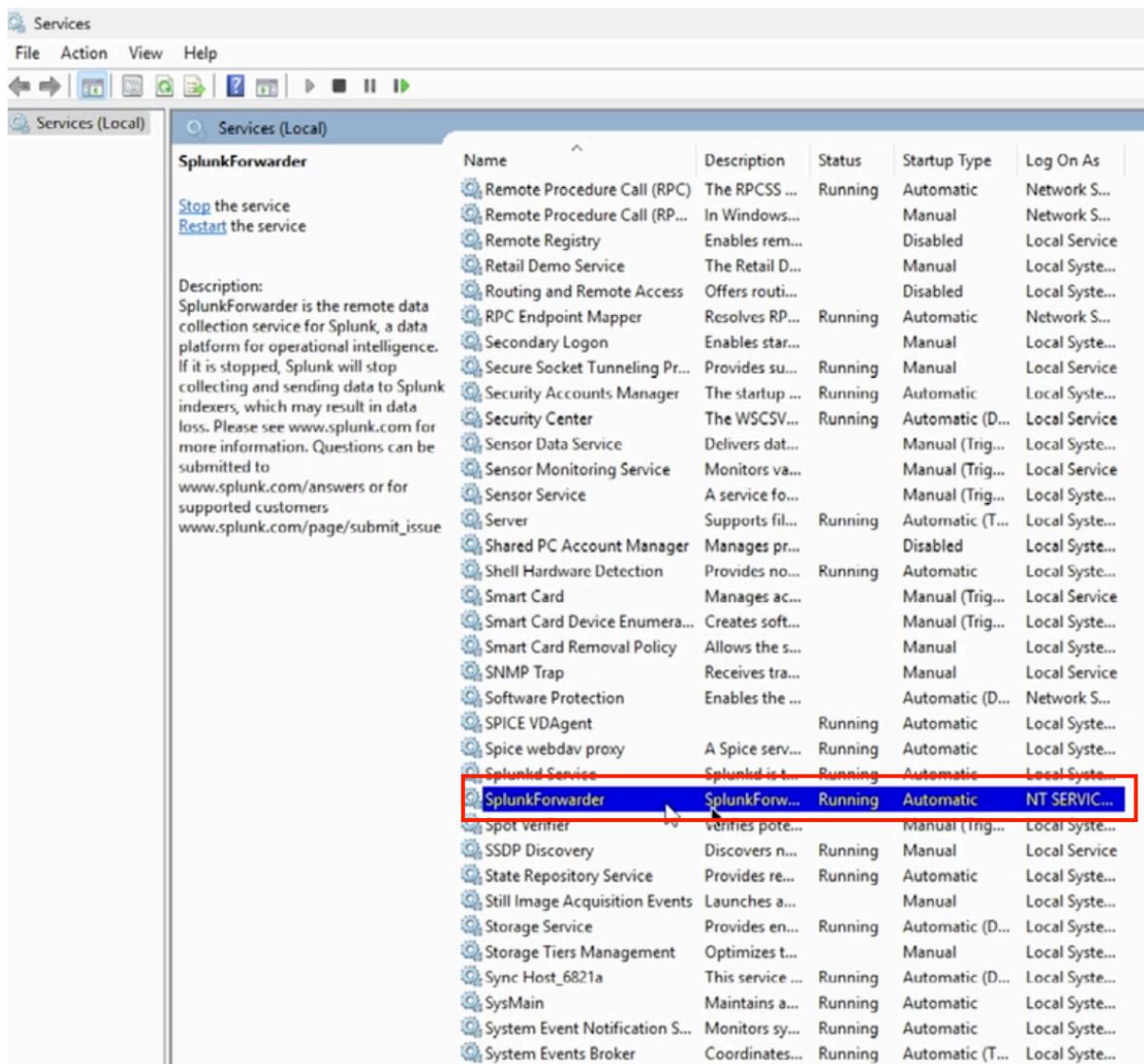
Write the server IP address which is the same as the Deployment server and port which is 9997 “Note: 9997nis a default port” to the Receiving Indexer and click Next



Launch the install



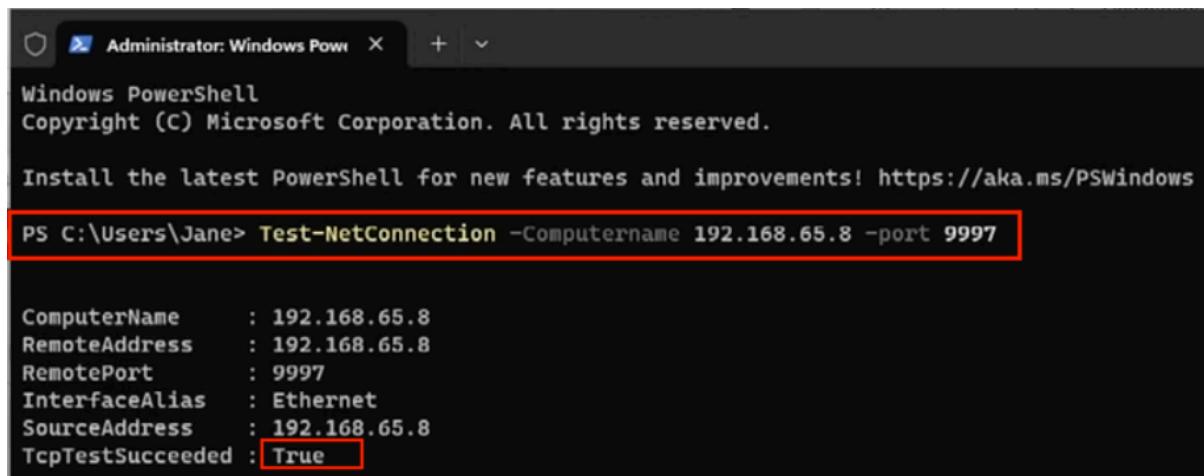
Check the Splunk Universal Forwarder Service Status. Type services on the Windows search to find Splunkforwarder Service. Monitor the service, status and startup type, check the state of the Splunk Universal Forwarder to see if it is up. The status must be running.



The screenshot shows the Windows Services snap-in. On the left, there's a tree view under 'Services (Local)' with 'SplunkForwarder' selected. A context menu is open with options 'Stop the service' and 'Restart the service'. Below the tree, a detailed description of the service is provided. On the right, a list of all local services is shown in a table format. The 'SplunkForwarder' service is highlighted with a red border in the table. The table columns are: Name, Description, Status, Startup Type, and Log On As. The 'SplunkForwarder' row shows: Name 'SplunkForwarder', Description 'SplunkForwarder is the remote data collection service for Splunk, a data platform for operational intelligence.', Status 'Running', Startup Type 'Automatic', and Log On As 'NT SERVICE\SYSTEM'.

Name	Description	Status	Startup Type	Log On As
Remote Procedure Call (RPC)	The RPCSS ...	Running	Automatic	Network S...
Remote Procedure Call (RP...	In Windows...	Manual	Network S...	
Remote Registry	Enables rem...	Disabled	Local Service	
Retail Demo Service	The Retail D...	Manual	Local Syste...	
Routing and Remote Access	Offers routi...	Disabled	Local Syste...	
RPC Endpoint Mapper	Resolves RP...	Running	Automatic	Network S...
Secondary Logon	Enables star...	Manual	Local Syste...	
Secure Socket Tunneling Pr...	Provides su...	Running	Manual	Local Service
Security Accounts Manager	The startup ...	Running	Automatic	Local Syste...
Security Center	The WSCSV...	Running	Automatic (D...	Local Service
Sensor Data Service	Delivers dat...	Manual (Trig...	Local Syste...	
Sensor Monitoring Service	Monitors va...	Manual (Trig...	Local Service	
Sensor Service	A service fo...	Manual (Trig...	Local Syste...	
Server	Supports fil...	Running	Automatic (T...	Local Syste...
Shared PC Account Manager	Manages pr...	Disabled	Local Syste...	
Shell Hardware Detection	Provides no...	Running	Automatic	Local Syste...
Smart Card	Manages ac...	Manual (Trig...	Local Service	
Smart Card Device Enumera...	Creates soft...	Manual (Trig...	Local Syste...	
Smart Card Removal Policy	Allows the s...	Manual	Local Syste...	
SNMP Trap	Receives tra...	Manual	Local Service	
Software Protection	Enables the ...	Automatic (D...	Network S...	
SPICE VDAgent		Running	Automatic	Local Syste...
Spice webdav proxy	A Spice serv...	Running	Automatic	Local Syste...
Splunkd Service	Splunkd is t...	Running	Automatic	Local Syste...
SplunkForwarder	SplunkForw...	Running	Automatic	NT SERVIC...
Spot Verifier	verifies pote...	Manual (Trig...	Local Syste...	
SSDP Discovery	Discovers n...	Running	Manual	Local Service
State Repository Service	Provides re...	Running	Automatic	Local Syste...
Still Image Acquisition Events	Launches a...	Manual	Local Syste...	
Storage Service	Provides en...	Running	Automatic (D...	Local Syste...
Storage Tiers Management	Optimizes t...	Manual	Local Syste...	
Sync Host_6821a	This service ...	Running	Automatic (D...	Local Syste...
SysMain	Maintains a...	Running	Automatic	Local Syste...
System Event Notification S...	Monitors sy...	Running	Automatic	Local Syste...
System Events Broker	Coordinates...	Running	Automatic (T...	Local Syste...

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



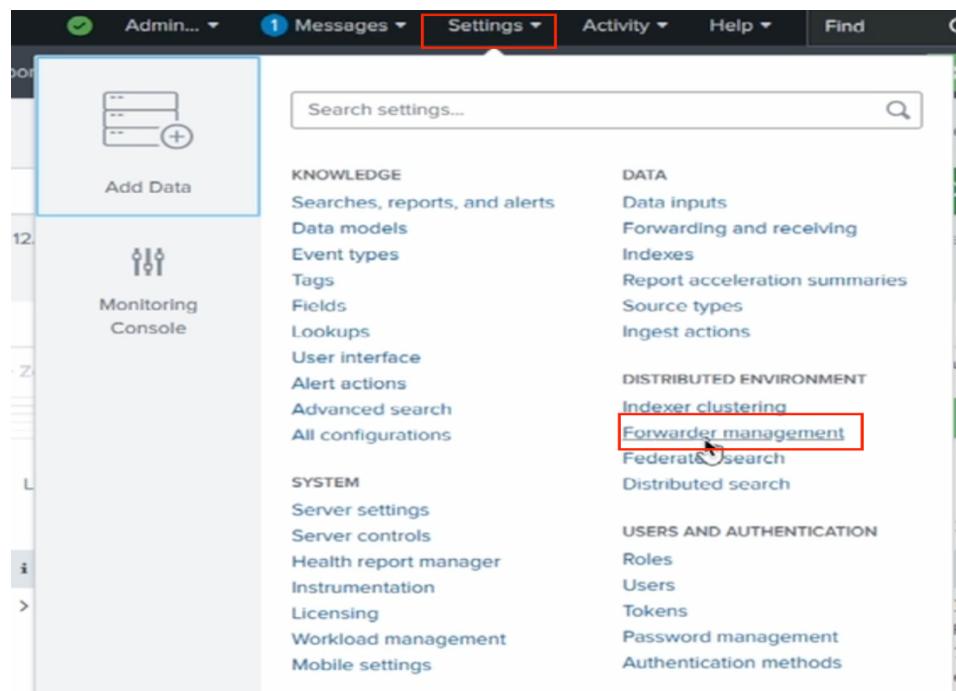
```
Administrator: Windows Pow X + ▾
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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.

The screenshot shows the 'Forwarder Management' page in the Splunk web interface. At the top, it displays statistics: 1 Client (PHONED HOME IN THE LAST 24 HOURS), 0 Clients (DEPLOYMENT ERRORS), and 0 Total downloads (IN THE LAST 1 HOUR). Below this, there are tabs for 'Apps (0)', 'Server Classes (0)', and 'Clients (1)'. The 'Clients' tab is selected. A search bar shows 'filter'. The main table lists one client: WIN-854SHE09OSJ, with details: Host Name, Client Name, Instance Name, IP Address, Actions, Machine Type, Deployed Apps, and Phone Home. The row for this client is highlighted with a red border.

Host Name	Client Name	Instance Name	IP Address	Actions	Machine Type	Deployed Apps	Phone Home
WIN-854SHE09OSJ	1AFA00DE-C9C6-4050-8A51-092EB32D461C	WIN-854SHE09OSJ	192.168.65.8	Delete Record	windows-x64	0 deployed	a few seconds ago

4. Detailed function of Splunk SIEM Service

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

The screenshot shows the 'Settings' menu in the Splunk web interface. The 'Forwarding and receiving' option under the 'DATA' section is highlighted with a red box. Other options in the 'DATA' section include Data Inputs, Forwarding and receiving, Indexes, Report acceleration summaries, Source types, and Ingest actions. The left sidebar contains links for Add Data, Monitoring Console, and other settings like Knowledge, System, and Distributed Environment.

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

The screenshot shows the 'Forwarding and receiving' page in the Splunk interface. Under the 'Receive data' section, there is a table with a single row labeled 'Configure receiving'. A hand cursor icon is positioned over this row, indicating it should be clicked to proceed.

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”.

The screenshot shows the 'Receive data' configuration page. At the top right, a green button labeled 'New Receiving Port' is highlighted with a hand cursor icon, indicating it should be clicked to add a new receiving port.

The screenshot shows the Splunk Enterprise web interface at the URL `127.0.0.1:8000/en-GB/manager/launcher/data/inputs/tcp/cooked/_new`. The top navigation bar includes links for **splunk>enterprise**, **Apps**, **Administrator**, **Messages**, **Settings**, **Activity**, **Help**, **Find**, and a search icon. The main title is **Add new**, with a subtitle **Forwarding and receiving > Receive data > Add new**. A sub-section titled **Configure receiving** contains the instruction **Set up this Splunk instance to receive data from forwarder(s).** Below this is a form field labeled **Listen on this port *** with an empty input field. A placeholder text below the field says **For example, 9997 will receive data on TCP port 9997.** At the bottom right of the configuration panel are **Cancel** and **Save** buttons. A watermark for **Activate Windows** is visible in the bottom right corner of the page.

This screenshot shows the same configuration page as the first one, but with the value **9997** entered into the **Listen on this port *** field. The rest of the interface and the watermark are identical to the first screenshot.

splunk>enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find New Receiving Port

Receive data

Forwarding and receiving > Receive data

Successfully saved "9997".

Show 1-1 of 1 item

Listen on this port	Status	Actions
9997	Enabled Disable	Delete

filter 25 per page ▾

Activate Windows
Go to Settings to activate Windows.

This screenshot shows the Splunk interface for managing receiving ports. It displays a success message 'Successfully saved "9997".' and a table with one item. The table has columns for 'Listen on this port', 'Status', and 'Actions'. The single row shows port 9997 with an 'Enabled' status and a 'Delete' action button. There are also 'filter' and '25 per page' dropdowns at the top of the table. A watermark for activating Windows is visible in the bottom right corner.

Add Data from Forwarder

Go to Settings click Add Data
Select Forward below

Admin... ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Repo

Add Data

Monitoring Console

Search settings...

KNOWLEDGE

- Searches, reports, and alerts
- Data models
- Event types
- Tags
- Fields
- Lookups
- User interface
- Alert actions
- Advanced search
- All configurations

DATA

- Data inputs
- Forwarding and receiving
- Indexes
- Report acceleration summaries
- Source types
- Ingest actions

DISTRIBUTED ENVIRONMENT

- Indexer clustering
- Forwarder management
- Federated search
- Distributed search

SYSTEM

- Server settings
- Server controls
- Health report manager
- Instrumentation
- Licensing
- Workload management
- Mobile settings

USERS AND AUTHENTICATION

- Roles
- Users
- Tokens
- Password management
- Authentication methods

This screenshot shows the Splunk Settings menu. The 'Add Data' option under the 'Forwarding and receiving' section is highlighted with a red box. The 'Settings' button in the top navigation bar is also highlighted with a red box. The rest of the menu items are listed in a tree structure on the left, and a search bar is at the top right.

The screenshot shows the Splunk Enterprise interface at the URL 127.0.0.1:8000/en-US/manager/system/adddatamethods/selectforwarders. The top navigation bar includes links for enterprise, Apps, Administrator, Messages, Settings, Activity, and Help. The main content area has a heading "What data do you want to send to the Splunk platform?". Below it, a section titled "Follow guides for onboarding popular data sources" contains four cards:

- Cloud computing**: Get your cloud computing data in to the Splunk platform. 10 data sources.
- Networking**: Get your networking data in to the Splunk platform. 2 data sources.
- Operating System**: Get your operating system data in to the Splunk platform. 1 data source.
- Security**: Get your security data in to the Splunk platform. 3 data sources.

A total of 4 data sources are listed in total. Below this, another section titled "Or get data in with the following methods" shows three options:

- Upload**: 01:04:37, files from my computer.
- Monitor**: files and ports on this Splunk platform instance.
- Forward**: 09:33, data from a Splunk forwarder.

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

Available host(s) Selected host(s)

WIN-854SHEO9OSJ WINDOWS	WIN-854SHEO9OSJ WINDOWS
----------------------------	----------------------------

New Server Class Name

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

Server Class

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

Server Class

List of Forwarders

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

The screenshot shows the 'Add Data' wizard at the 'Select Source' step. On the left, a sidebar lists monitoring options: 'Local Event Logs' (selected and highlighted with a red box), 'Files & Directories', 'TCP / UDP', 'Local Performance Monitoring', and 'Scripts'. The main area shows a list of available items under 'Select Event Logs': 'Application', 'ForwardedEvents', 'Security', 'Setup', and 'System'. An 'add all >' button is next to the list. To the right, a 'Selected Item' panel lists 'Application', 'ForwardedEvents', 'Security', 'Setup', and 'System'. A red box highlights the 'Next >' button at the top right of the screen.

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.

The screenshot shows the 'Add Data' wizard at the 'Input Settings' step. The 'Index' section has a dropdown menu. 'Default' is selected and highlighted with a red box. Other options in the dropdown are 'history', 'jane1', 'main', and 'summary'. A 'Create a new index' link is also visible. The 'FAQ' section contains links to 'How do indexes work?' and 'How do I know when to create or use multiple indexes?'.

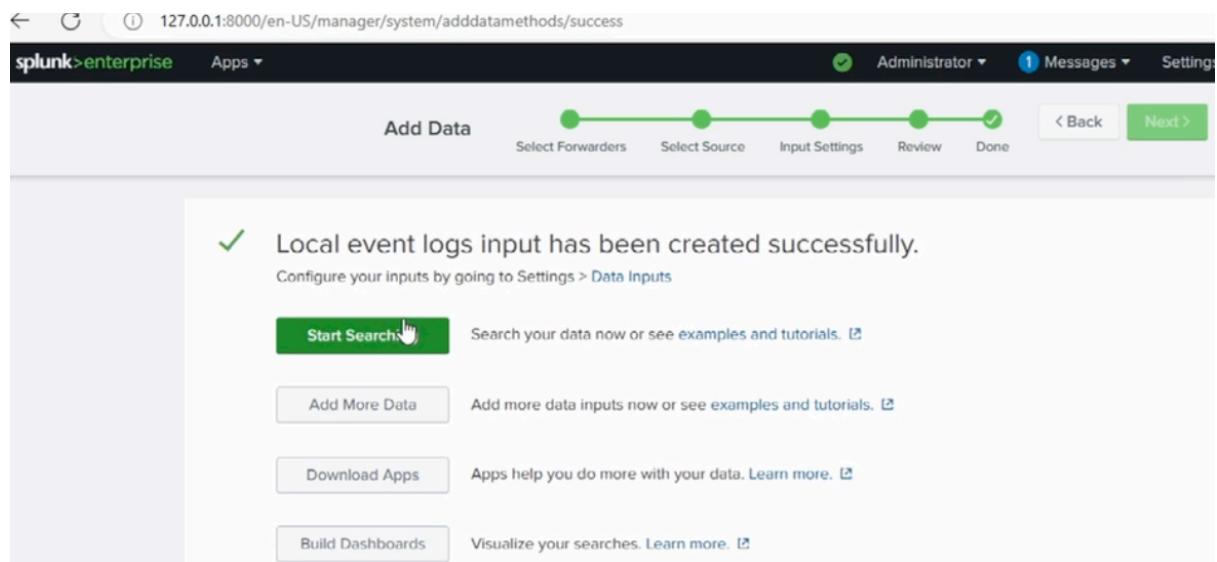
Click on Review button to check the logs you have created once viewed click on submit.
You can now click on “start searching” to find last connection on client’s computer

The screenshot shows the 'Input Settings' step of the 'Add Data' wizard. The top navigation bar includes 'splunk>enterprise', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', and 'Help'. Below the navigation is a progress bar with five steps: 'Select Forwarders' (green), 'Select Source' (green), 'Input Settings' (green), 'Review' (light gray), and 'Done' (light gray). A 'Back' button and a 'Next >' button (with a hand cursor icon) are at the bottom right. The main content area is titled 'Input Settings' with the sub-instruction 'Optional set additional input parameters for this data input as follows:'. It has two sections: 'Index' and 'FAQ'. In the 'Index' section, it says 'The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later.' with a 'Learn More' link. It also shows an 'Index' dropdown set to 'jane1' and a 'Create a new index' link. The 'FAQ' section lists two items: 'How do indexes work?' and 'How do I know when to create or use multiple indexes?'. A 'Help' link is located at the bottom right of the content area.

The screenshot shows the 'Review' step of the 'Add Data' wizard. The top navigation bar is identical to the previous screenshot. The progress bar shows 'Select Forwarders' (green), 'Select Source' (green), 'Input Settings' (green), 'Review' (green), and 'Done' (light gray). A 'Back' button and a 'Submit >' button (with a hand cursor icon) are at the bottom right. The main content area is titled 'Review' and displays the configuration settings:

- Server Class Name WIN-854SHEO9OSJ
- List of Forwarders WINDOWS | WIN-854SHEO9OS▲
- Collection Name localhost
- Input Type Windows Event Logs
- Event Logs Application
ForwardedEvents
Security
Setup
System
- Index jane1

A dropdown menu for 'Event Logs' is open, showing the options: Application, ForwardedEvents, Security, Setup, and System.



	Time	Event
>	12/9/24 9:28:51.000 PM	12/09/2024 09:28:51 PM LogName=Security EventCode=4672 EventType=0 ComputerName=WIN-854SHE09OSJ Show all 31 lines host = WIN-854SHE09OSJ source = WinEventLog:Security sourcetype = WinEventLog:Security
>	12/9/24 9:28:51.000 PM	12/09/2024 09:28:51 PM LogName=Security EventCode=4624 EventType=0 ComputerName=WIN-854SHE09OSJ Show all 71 lines host = WIN-854SHE09OSJ source = WinEventLog:Security sourcetype = WinEventLog:Security

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

Presets			
REAL-TIME	RELATIVE	OTHER	
30 second window	Today	Last 15 minutes	All time
1 minute window	Week to date	Last 60 minutes	
5 minute window	Business week to date	Last 4 hours	
30 minute window	Month to date	Last 24 hours	
1 hour window	Year to date	Last 7 days	
All time (real-time)	Yesterday	Last 30 days	
	Previous week		
	Previous business week		
	Previous month		
	Previous year		

> Relative

> Real-time

> Date Range

> Date & Time Range

> Advanced

Check Indexes Settings

Click on Settings > Indexes

The screenshot shows the Splunk Settings interface. The top navigation bar includes 'Administrator', 'Messages', 'Settings' (which is highlighted with a red box), 'Activity', 'Help', and 'Find'. Below the navigation is a search bar labeled 'Search settings...'. The main content area is divided into several sections: 'KNOWLEDGE' (Searches, reports, and alerts; Data models; Event types; Tags; Fields; Lookups; User interface; Alert actions; Advanced search; All configurations), 'DATA' (Data inputs; Forwarding and receiving; Indexes - this link is also highlighted with a red box; Report acceleration summaries; Source types; Ingest actions), 'DISTRIBUTED ENVIRONMENT' (Forwarder management; Indexer clustering; Federation; Distributed search), 'SYSTEM' (Server settings; Server controls; Health report manager; Instrumentation; Licensing; Workload management; Mobile settings), and 'USERS AND AUTHENTICATION' (Roles; Users; Tokens; Activate Windows - a tooltip says 'Go to Settings to activate Windows.'; Password management; Authentication methods). A sidebar on the left features 'Add Data' and 'Monitoring Console'.

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

The screenshot shows the Splunk Indexes page. The top navigation bar is identical to the previous screenshot. The main content area is titled 'Indexes' and contains a message: 'A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. Learn more' with a link icon. Below this is a table with 15 indexes listed. The table has columns for Name, Actions (Edit, Delete, Disable), Type (Events), App (system), Current Size, Max Size, Event Count, Earliest Event, Latest Event, Home Path, and Frozen. The first few rows show indexes like '_audit', '_configtracker', '_dsappevent', '_dsclient', '_dsphome', and '_internal'. A green 'New Index' button is located in the top right corner of the table header. A tooltip for the 'Activate Windows' link in the bottom right corner of the table says 'Go to Settings to activate Windows.'

Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Home Path	Frozen
_audit	Edit Delete Disable	Events	system	2 MB	488.28 GB	9.98K	9 hours ago	a few seconds ago	\$SPLUNK_D\audit\ldb	N/A
_configtracker	Edit Delete Disable	Events	system	4 MB	488.28 GB	249	9 hours ago	6 minutes ago	\$SPLUNK_D\configtracker\ldb	N/A
_dsappevent	Edit Delete Disable	Events	SplunkDeploymentServer Config	1 MB	488.28 GB	0			\$SPLUNK_D\dsappevent\ldb	N/A
_dsclient	Edit Delete Disable	Events	SplunkDeploymentServer Config	1 MB	488.28 GB	1	24 minutes ago	24 minutes ago	\$SPLUNK_D\dsclient\ldb	N/A
_dsphome	Edit Delete Disable	Events	SplunkDeploymentServer Config	1 MB	488.28 GB	22	22 minutes ago	a minute ago	\$SPLUNK_D\dsphone\home\ldb	N/A
_internal	Edit Delete Disable	Events	system	7 MB	488.28 GB	82K	9 hours ago	a few seconds ago	Activate Windows Go to Settings to activate Windows.	\$SPLUNK_D\internal\ldb N/A

_metrics_rollup	Edit	Delete	Disable	Metrics	system	1 MB	488.28 GB	0	seconds ago	B\metrics\ldb
_telemetry	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0		\$SPLUNK_DB\telemetry\ldb
_thefishbucket	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0		\$SPLUNK_DB\fishbucket\ldb
history	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0		\$SPLUNK_DB\historydb\ldb
jane33	Edit	Delete	Disable	Events	search	1 MB	500 GB	0		\$SPLUNK_DB\jane33\ldb
main	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0		\$SPLUNK_DB\defaultdb\ldb
splunklogger	Edit	Delete	Enable	Events	system	0 B	488.28 GB	0		\$SPLUNK_DB\splunklogger\ldb
summary	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0		\$SPLUNK_DB\summarydb\ldb

Activate Windows
Go to Settings to activate Windows.

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

The screenshot shows the Splunk web interface with the URL `127.0.0.1:8000/en-US/manager/search/data/indexes`. A modal dialog box is open, titled "New Index". The "General Settings" section contains the following fields:

- Index Name:** Jane1
- Index Data Type:** Events (selected)
- Home Path:** optional
- Cold Path:** optional
- Thawed Path:** optional
- Data Integrity Check:** Enable (selected)

At the bottom of the dialog are two buttons: "Save" (highlighted with a cursor) and "Cancel".

Go to settings > Data input > local events logs collection

The screenshot shows the Splunk Settings interface. The top navigation bar includes 'Administrator', 'Messages' (with a count of 1), 'Settings' (highlighted with a red box), 'Activity', 'Help', and 'Find'. On the left, there's a sidebar with 'Add Data' (highlighted with a blue box) and 'Monitoring Console'. The main content area has a search bar 'Search settings...'. Under 'DATA', the 'Data inputs' option is highlighted with a red box. Other options include 'Forwarding and receiving', 'Indexes', 'Report acceleration summaries', 'Source types', and 'Ingest actions'. Under 'DISTRIBUTED ENVIRONMENT', there are links for 'Forwarder management', 'Indexer clustering', 'Federation', and 'Distributed search'. Under 'USERS AND AUTHENTICATION', there are links for 'Roles', 'Users', 'Tokens', 'Password management', and 'Authentication methods'. A link to 'Activate Windows' is also present.

The screenshot shows the 'Data inputs' page. The top navigation bar includes 'splunk > enterprise', 'Apps', 'Admin...', 'Messages' (with a count of 1), 'Settings' (highlighted with a red box), 'Activity', 'Help', and 'Find'. The main content area is titled 'Data inputs' with a sub-instruction: 'Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to Forwarding and receiving.' Below this, the 'Local inputs' section is shown with a table:

Type	Inputs	Actions
Local event log collection Collect event logs from this machine.	-	Edit
Remote event log collections Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.	1	+ Add new
Files & Directories Index a local file or monitor an entire directory.	19	+ Add new
Local performance monitoring Collect performance data from local machine.	0	+ Add new
Remote performance monitoring Collect performance and event information from remote hosts. Requires domain credentials.	0	+ Add new
HTTP Event Collector	0	+ Add new

The event logs are then added to newly created index "Jane1"

This screenshot shows the 'Event Log Collections' configuration page for the 'localhost' source. The 'Logs' section lists several Windows Event Logs: AMSI/Debug, Application, Els_Hyphenation/Analytic, EndpointMapper, and FirstUXPerf-Analytic. The 'Available log(s)' list has checkboxes next to each item, and the 'Selected log(s)' list contains the same five items with their checkboxes checked. Below this, there is a note: 'Select the Windows Event Logs you want to index from the list.' The 'Index' section shows the 'Set the destination index for this source' dropdown set to 'default'. At the bottom right are 'Cancel' and 'Save' buttons.

This screenshot shows the same configuration page for 'localhost', but with the 'Index' dropdown set to 'jane1'. The 'Save' button at the bottom right is highlighted with a cursor icon, indicating it is the active button.

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

The screenshot shows the Splunk Manager Indexes interface. The main table lists various indexes with their details. The 'jane1' index is highlighted with a red box. The table columns include: Name, Edit, Delete, Disable, Type, Source, Size, Total Events, Last Event, Last Update, Status, and Enabled. The 'jane1' row shows: Name 'jane1', Type 'Events', Source 'search', Size '1MB', Total Events '500 GB', Last Event '4.77K', Last Update 'an hour ago', Status '\$SPLUNK_DB:jane1db', and Enabled 'Enabled'. A cursor is hovering over the '4768 events' link in the 'main' index row.

Name	Edit	Delete	Disable	Type	Source	Size	Total Events	Last Event	Last Update	Status	Enabled	
_introspection	Edit	Delete	Disable	Events	system	3 MB	488.28 GB	1.04K	16 minutes ago	a few seconds ago	\$SPLUNK_DB:Internaldb	Enabled
_metrics	Edit	Delete	Disable	Metrics	system	5 MB	488.28 GB	6.45K	16 minutes ago	a few seconds ago	\$SPLUNK_DB:metricsdb	Enabled
_metrics_rollup	Edit	Delete	Disable	Metrics	system	1 MB	488.28 GB	0			\$SPLUNK_DB:metrics_rrollupdb	Enabled
_telemetry	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	1	6 minutes ago	6 minutes ago	\$SPLUNK_DB:telemetrydb	Enabled
_thefishbucket	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB:fishbucketdb	Enabled
history	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB:historydb	Enabled
jane1	Edit	Delete	Disable	Events	search	1MB	500 GB	4.77K	an hour ago	in 7 hours	\$SPLUNK_DB:jane1db	Enabled
main	Edit	Delete	Disable	Events	system	1MB	488.28 GB	0	4768 events		\$SPLUNK_DB:defaultdb	Enabled
splunklogger	Edit	Delete	Enable	Events	system	0 B	488.28 GB	0			\$SPLUNK_DB:splunkloggerdb	Disabled
summary	Edit	Delete	Disable	Events	system	1MB	488.28 GB	0			\$SPLUNK_DB:summarydb	Enabled

Splunk Reports

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

The screenshot shows the Splunk Enterprise search interface at the URL `127.0.0.1:8000/en-US/app/search/search?q=search%20source%3DWinEventLog%3A%20index%3Djane1%20Account_Name%3DJane&earliest=-2...`. The search bar contains the query `source="WinEventLog:*" index="jane1" Account_Name=Jane`. The results table shows 54 events from December 9, 2024, between 9:00:00.000 PM and 9:27:22.000 PM. The table has columns for host, source, and sourcetype. The first event is from host `WIN-854SHE09OSJ` at 12/09/2024 9:21:08 PM, with LogName=Security, EventCode=5379, EventType=0, and ComputerName=WIN-854SHE09OSJ. The second event is from the same host at 12/09/2024 9:21:04.000 PM. The third event is from the same host at 12/09/2024 9:20:55 PM.

host	source	sourcetype
WIN-854SHE09OSJ	WinEventLog:Security	WinEventLog:Security
WIN-854SHE09OSJ	WinEventLog:Security	WinEventLog:Security
WIN-854SHE09OSJ	WinEventLog:Security	WinEventLog:Security

The screenshot shows the Splunk Enterprise search interface. In the top right corner, a context menu is open over a search result table. The menu items include 'Save As', 'Report' (which is highlighted with a red box), 'Create Table View', 'Close', 'Alert', 'Existing Dashboard', 'New Dashboard', and 'Event Type'. Below the menu, the search bar contains the query: 'source="WinEventLog:*" index="jane1" Account_Name=Jane'. The results table shows 54 events from 12/8/24 9:00:00.000 PM to 12/9/24 9:27:22.000 PM. A 'Save As' dialog box is overlaid on the interface, titled 'Save As Report'. It has fields for 'Title' (containing 'Jane report'), 'Description' (containing 'optional'), 'Content' (set to 'Events'), and a 'Time Range Picker' with 'Yes' selected. At the bottom right of the dialog is a green 'Save' button, which is also highlighted with a red box.

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](#)

The screenshot shows the Splunk interface after a report has been created. At the top, a modal window says "Your Report Has Been Created". Below it, a message says "You may now view your report, add it to a dashboard, change additional settings, or continue editing it." Under "Additional Settings", there are four options: Permissions, Schedule, Acceleration, and Embed. At the bottom of the modal are three buttons: "Continue Editing", "Add to Dashboard", and a green "View" button which is highlighted with a red box. Below the modal is the main Splunk search results page. The title is "Jane report". It shows a summary of "Last 24 hours" with "54 events" from "12/8/24 9:00:00.000 PM to 12/9/24 9:27:22.000 PM". There are 20 events per page, with page 1 selected. The events list shows three entries, each with a timestamp, log name, event code, event type, computer name, and source information. The first two entries are expanded to show 21 lines of log data, while the third is collapsed.

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-854SHE09OSJ Show all 21 lines host = WIN-854SHE09OSJ 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-854SHE09OSJ Show all 21 lines host = WIN-854SHE09OSJ 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-854SHE09OSJ Show all 21 lines host = WIN-854SHE09OSJ source = WinEventLog:Security sourcetype = WinEventLog:Security

To Edit an Existing Report

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

The screenshot shows the Splunk interface with the 'Reports' tab selected. The page displays a list of 8 reports. One report, 'Jane report', is highlighted with a red box and has its 'Edit' button also highlighted with a red box.

Detailed information of the “Jane report”

The screenshot shows the Splunk interface with the 'Reports' tab selected. A red box highlights the detailed information card for the 'Jane report'. The card lists various properties: Creator (Created by Search), App (search), Schedule (Not scheduled), Actions (0 Actions), Acceleration (Disabled), Permissions (Private, Owned by jane), Modified (Dec 9, 2024 9:28:02 PM), and Embedding (Disabled). Below the card, the list of reports is visible again.

Select Edit button to edit “Jane Report”

The screenshot shows the Splunk interface with the 'Reports' tab selected. The 'Jane report' card is open, and a red box highlights the 'Edit' button in the top right corner of the card. A dropdown menu is open, listing options: Open in Search, Edit (highlighted with a red box), Edit Description, Edit Permissions, Edit Schedule, Edit Acceleration, Clone, Embed, and Delete.

Set Alert

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

Save As Alert

Settings

Title:

Description: Optional

Permissions: Private Shared in App

Alert type: Scheduled Real-time

Run every week ▾

On: at:

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 ▾

Save to Dashboard

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

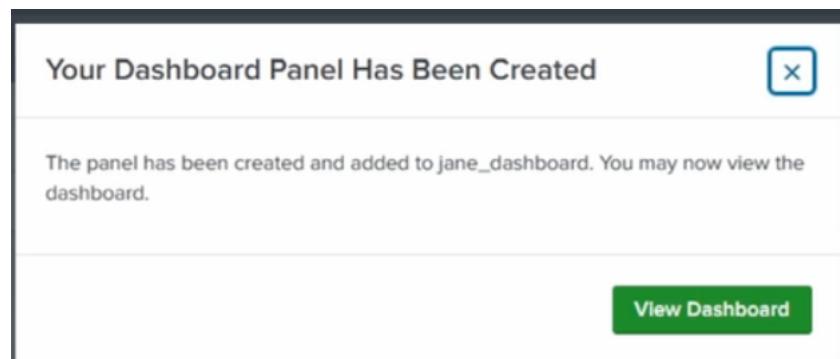
Save Panel to New Dashboard

Dashboard Title	Required
Description	Optional
Permissions	Private
How do you want to build your dashboard?	
Classic Dashboards The traditional Splunk dashboard builder	
Dashboard Studio NEW A new builder to create visually-rich, customizable dashboards	
Panel Title	Optional
Visualization Type	<input type="checkbox"/> Events
> Advanced Panel Settings	
Cancel Save to Dashboard	

NOTE: You must select “Classic or Studio Dashboard

Save Panel to New Dashboard

! You must select Dashboard Studio or Classic Dashboards.	
Dashboard Title	Jane Dashboard jane_dashboard
Description	Optional
Permissions	Private
How do you want to build your dashboard?	
Classic Dashboards The traditional Splunk dashboard builder	
Dashboard Studio NEW A new builder to create visually-rich, customizable dashboards	
Panel Title	Optional
Visualization Type	<input type="checkbox"/> Events
Cancel Save to 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

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

Create New Dashboard

Latest Resources

- Examples for Dashboard Studio
- Intro to Dashboard Studio
- Intro to Classic Dashboards

6 Dashboards

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”

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-854SHE09OSJ Show all 12 lines host = WIN-854SHE09OSJ 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-854SHE09OSJ Show all 12 lines host = WIN-854SHE09OSJ 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-854SHE09OSJ Show all 47 lines host = WIN-854SHE09OSJ 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-854SHE09OSJ Show all 47 lines host = WIN-854SHE09OSJ source = WinEventLog:Application sourcetype = WinEventLog:Application

Select Edit button to edit “Jane Dashboard”

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

Splunk Health Status Check

Health of Local Splunk Deployment

splunkd

- > ✓ File Monitor Input
- > ✓ HEC Health
- > ✓ Index Processor
- > ✓ Search Scheduler
- ?
- Workload Management

How to interpret this health report:

This health report displays information from the /health/splunkd/details endpoint. There are three potential states for a feature:

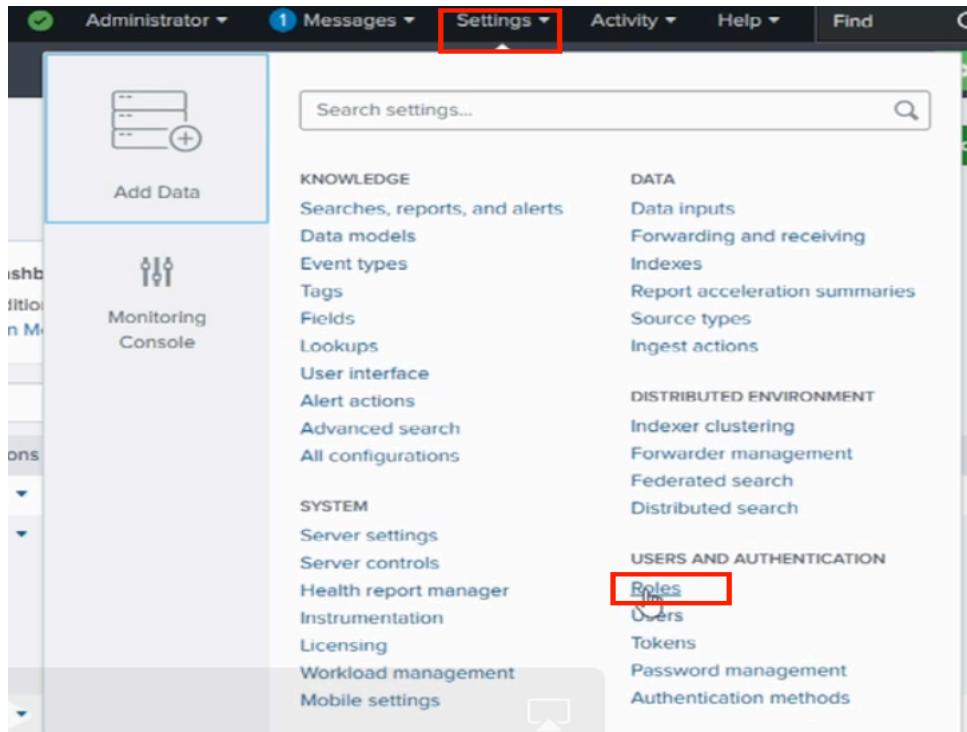
- ✓ Green: The feature is functioning properly.
- ⚠ Yellow: The feature is experiencing a problem. The feature's status might automatically improve, or it might worsen over time. For details, see Root Cause.
- ❗ Red: The feature has severe issues and is negatively impacting the functionality of your deployment. For details, see Root Cause.
- ?
- Grey: Health report is disabled or snoozed for the feature.

To manage red and yellow threshold values for the individual features, go to [Health Report Manager](#)

 more information on this health report, see [Learn more](#)

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 Splunk. At the top, there is a search bar and a 'New Role' button. Below the header, a table lists five roles: admin, can_delete, power, splunk-system-role, and user. Each row includes an 'Actions' column with an 'Edit' dropdown, and columns for 'Native Capabilities' and 'Inherited Capabilities'. A 'Default App' column is also present.

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

The screenshot shows the 'Settings' page in Splunk. On the left, there is a sidebar with icons for 'Add Data' (selected), 'Monitoring Console', and other settings. The main area contains a search bar and a list of configuration categories: KNOWLEDGE, SYSTEM, DATA, DISTRIBUTED ENVIRONMENT, USERS AND AUTHENTICATION, and a 'Tokens' section. The 'Users' link under 'USERS AND AUTHENTICATION' is highlighted with a red box.

Here you can “Edit or Add New User”

The screenshot shows the 'Users' page in Splunk. At the top, there is a search bar and a 'New User' button. Below the header, a table lists one user: Jane. The table has columns for Name, Actions, Authentication system, Full name, Email address, Time zone, Default app, Default app inherited from, and Roles.

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).