



Splunk Setup for Real-time Active Directory Monitoring

Lab Created by: **Hasan Sadiq**

Follow Me: <https://www.linkedin.com/in/hasan-sadiq-485b30314/>

Introduction:

Splunk is a software that is used to search, and analyze machine data generated by various. CPU running on web or local servers, IoT devices, mobile apps, sensors, or data created by the user. It completes the needs of IT infrastructure by analyzing the logs generated by systems in various processes in a structured or semi-structured format with proper data modelling and then it allows users to create Reports, Alerts, Tags, and Dashboards on these data.

Splunk Architecture

There are three main components of Splunk: –

- Splunk Forwarder
- Splunk Indexer
- Splunk Head

You can download Splunk by following the below link.

https://www.splunk.com/en_us/download/splunk-enterprise.html

Create a Splunk Account and download Splunk for Linux version by the given above link.

We choose .tgz Package for the installation in **Linux**

Download and install Splunk

```
(root@kali)-[/home/hasan]
# cd Downloads

(root@kali)-[/home/hasan/Downloads]
# ls
splunk-9.3.0-51ccf43db5bd-Linux-x86_64.tgz

(root@kali)-[/home/hasan/Downloads]
#
```

This command uses the wget utility to download the specified Splunk package from the provided URL.

wget https://download.splunk.com/products/releases/9.3.0/linux/splunk-9.3.0-51ccf43db5bd-Linux-x86_64.tgz

```
(root@kali)-[/home/hasan/Downloads]
# ls
splunk-9.3.0-51ccf43db5bd-Linux-x86_64.tgz

(root@kali)-[/home/hasan/Downloads]
# wget -O splunk-9.3.0-51ccf43db5bd-Linux-x86_64.tgz "https://download.splunk.com/products/splunk/releases/9.3.0/linux/splunk-9.3.0-51ccf43db5bd-Linux-x86_64.tgz"
--2024-07-26 08:58:43-- https://download.splunk.com/products/splunk/releases/9.3.0/linux/splunk-9.3.0-51ccf43db5bd-Linux-x86_64.tgz
Resolving download.splunk.com (download.splunk.com)... 18.64.141.103, 18.64.141.42, 18.64.141.92, ...
Connecting to download.splunk.com (download.splunk.com)|18.64.141.103|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 996384325 (950M) [binary/octet-stream]
Saving to: 'splunk-9.3.0-51ccf43db5bd-Linux-x86_64.tgz'

splunk-9.3.0-51ccf43db5bd-Linux-x86_64.tg 100%[=====] 950.23M 803KB/s in 30m 48s

2024-07-26 09:29:32 (527 KB/s) - 'splunk-9.3.0-51ccf43db5bd-Linux-x86_64.tgz' saved [996384325/996384325]
```

After Downloading the Splunk File on Linux extract the File with given Command
tar xvf splunk-9.3.0-51ccf43db5bd-Linux-x86_64.tgz

```
(root@kali)-[/home/hasan/Downloads]
# tar -xvf splunk-9.3.0-51ccf43db5bd-Linux-x86_64.tgz
splunk/
splunk/swidtag/
splunk/swidtag/splunk-Splunk-Enterprise-primary.swidtag
splunk/opt/
splunk/opt/packages/
splunk/opt/packages/identity-0.0.1-808de82.tar.gz
```

It shows the initial step of starting the Splunk software, where the user is presented with the terms and conditions that govern its use.

```
(root@kali)-[/home/hasan/Downloads/splunk]
# ./bin/splunk start
SPLUNK GENERAL TERMS

Last Updated: August 12, 2021

These Splunk General Terms ("General Terms") between Splunk Inc., a Delaware corporation, with its principal place of business at 270 Brannan Street, San Francisco, California 94107, U.S.A ("Splunk" or "we" or "us" or "our") and you ("Customer" or "you" or "your") apply to the purchase of licenses and subscriptions for Splunk's Offerings. By clicking on the appropriate button, or by downloading, installing, accessing or using the Offerings, you agree to these General Terms. If you are entering into these General Terms on behalf of Customer, you represent that you have the authority to bind Customer. If you do not agree to these General Terms, or if you are not authorized to accept the General Terms on behalf of the Customer, do not download, install, access, or use any of the Offerings.
```

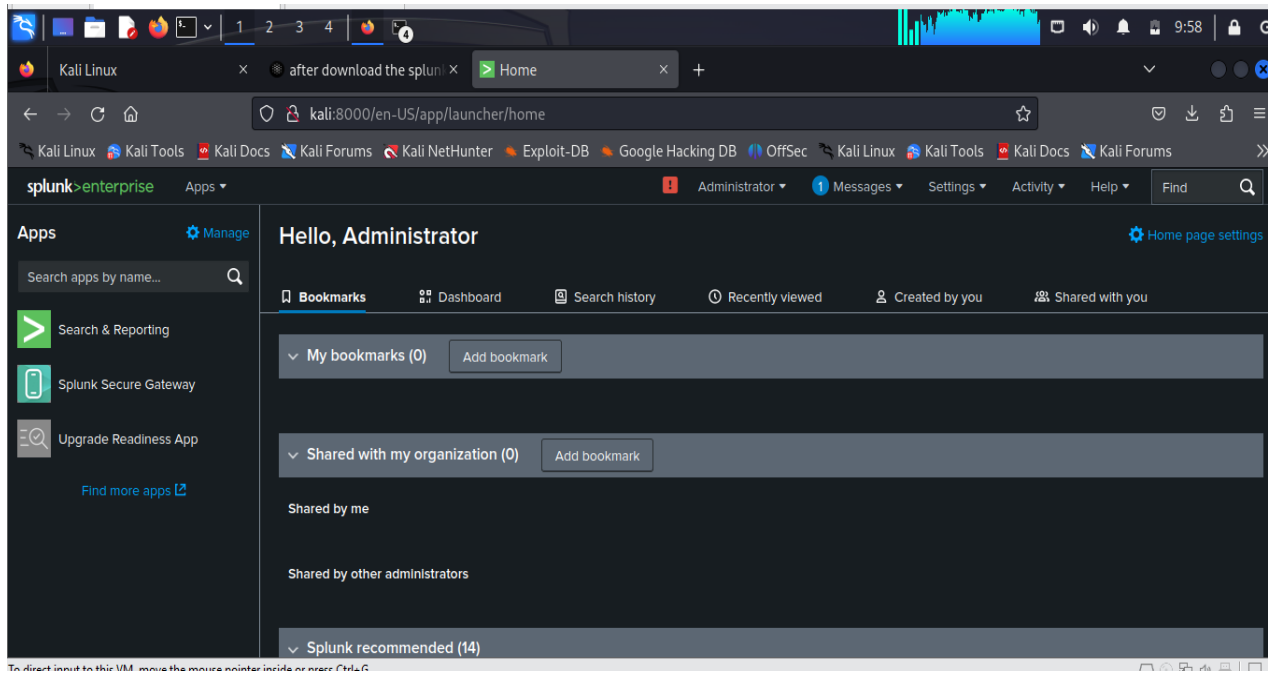
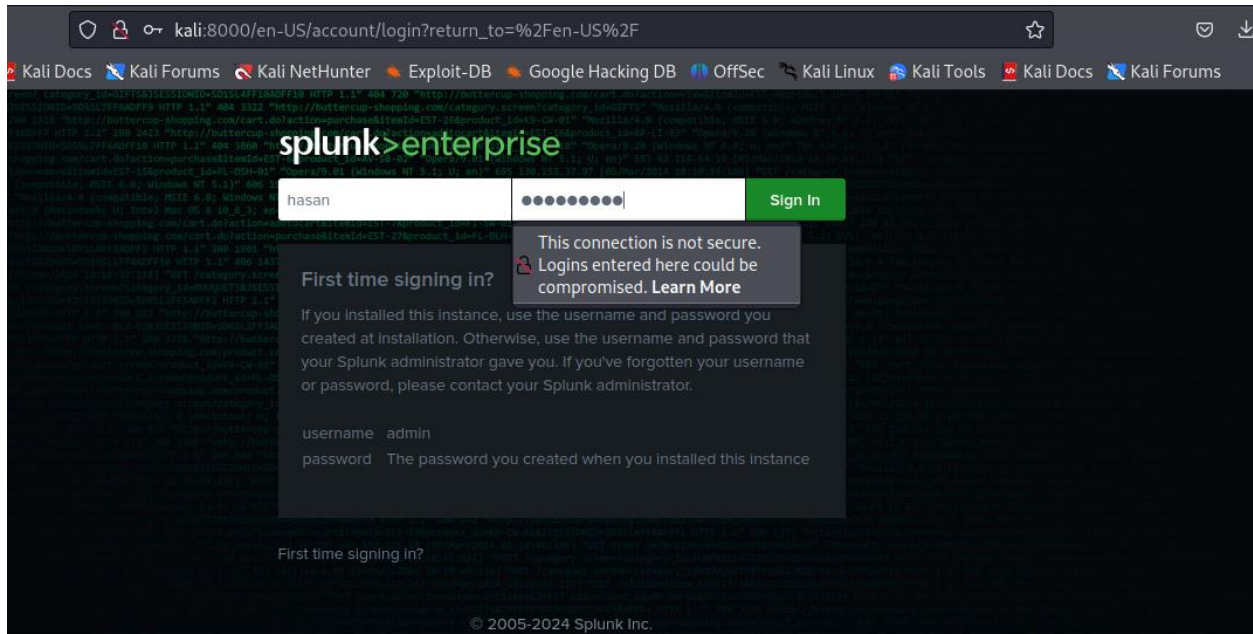
Splunk installation has been completed successfully

```
If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

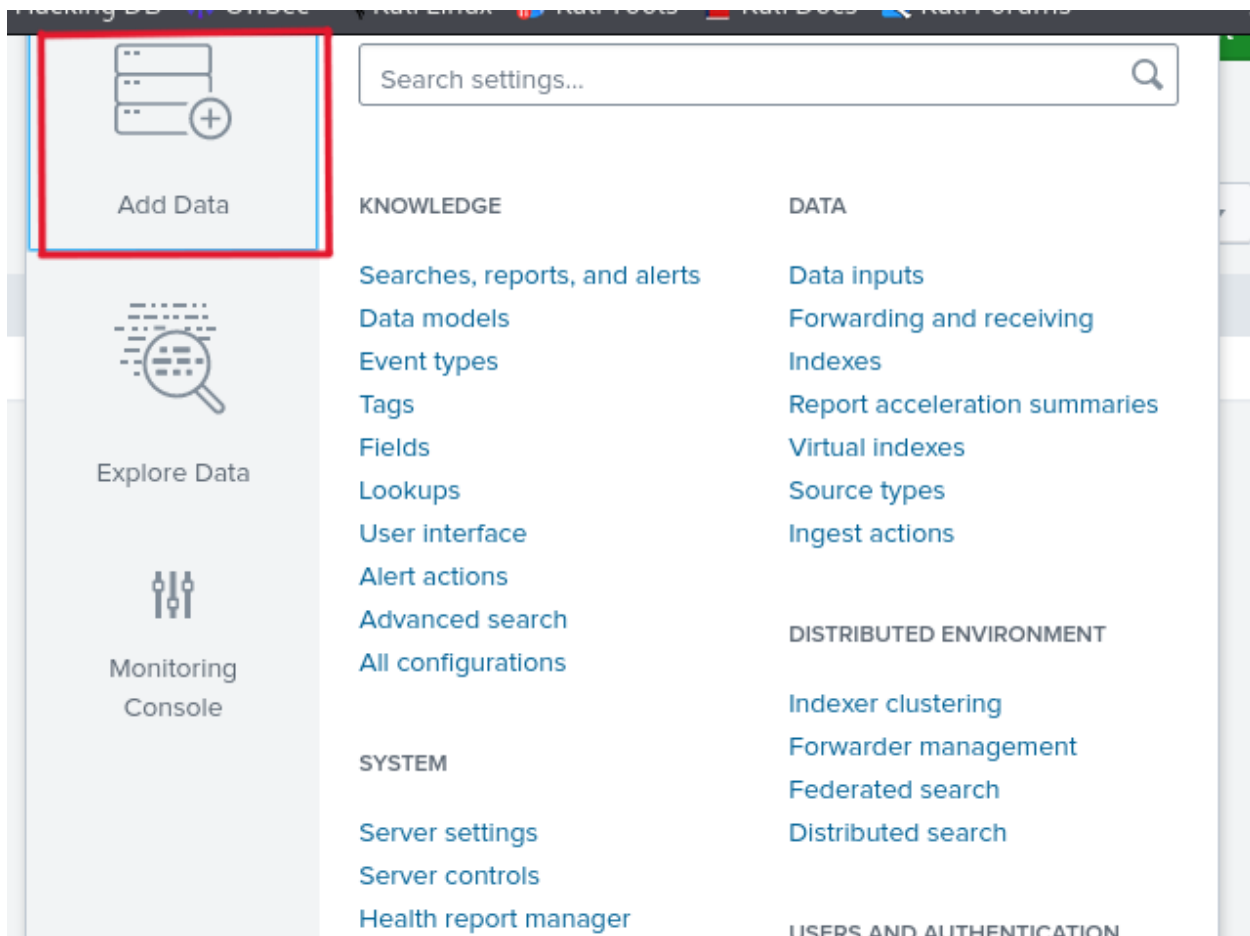
The Splunk web interface is at http://kali:8000

(root@kali)-[/home/hasan/Downloads/splunk]
#

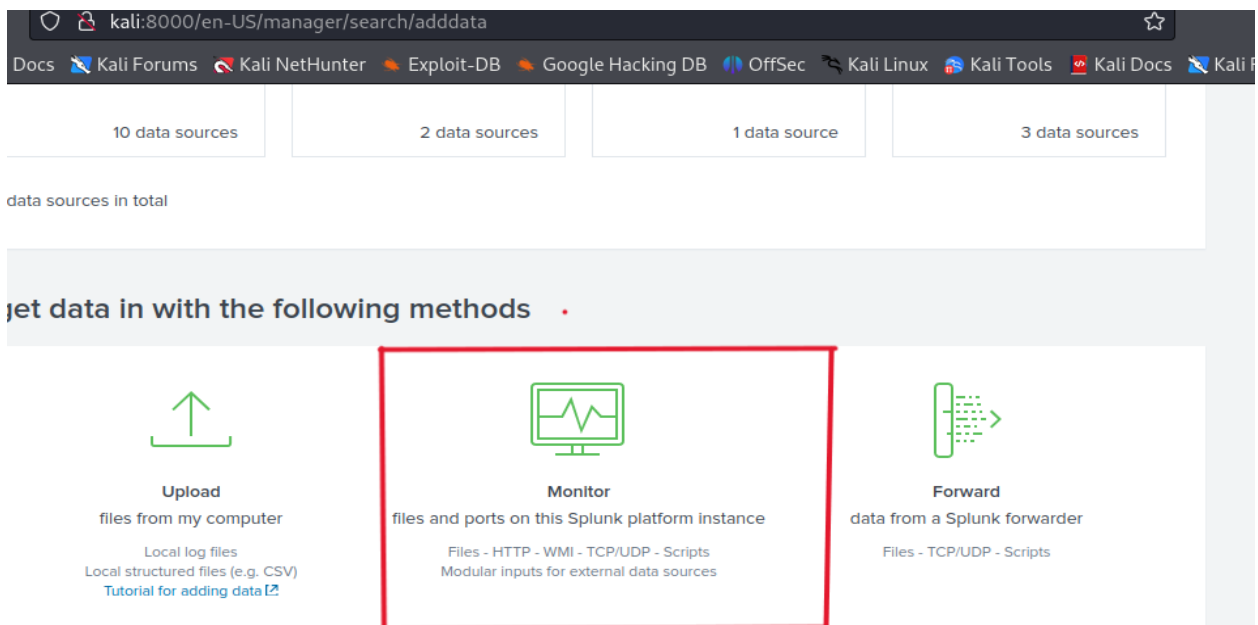
(root@kali)-[/home/hasan/Downloads/splunk]
#
```



Go to settings and Click on **Add Data**



Select the **Monitor** Option



Select Source

Add Data

< Back

Next >

Files & Directories

Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector

Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP

Configure the Splunk platform to listen on a network port.

Scripts

Get data from any API, service, or database with a script.

Splunk Assist Instance Identifier

Assigns a random identifier to every node

← Select an option

Select the file or Directory for Monitoring

Add Data

< Back

Next >

Files & Directories

Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector

Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP

Configure the Splunk platform to listen on a network port.

Scripts

Get data from any API, service, or database with a script.

Splunk Assist Instance Identifier

Assigns a random identifier to every node

Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. The Splunk platform monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. [Learn More](#)

File or Directory ?


Browse

On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

Continuously Monitor

Index Once

Include list ?

Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. The Splunk platform monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. [Learn More](#) 

File or Directory ?

/var/log

Browse

On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

Continuously Monitor

Index Once

Includelist ?

Review All the **Settings**

Review

Input Type	Directory Monitor
Source Path	/var/log
Includelist	N/A
Excludelist	N/A
Source Type	Automatic
App Context	search
Host	kali
Index	default

Successfully set up a data source and are ready to start exploring and **analyzing your data.**

Add Data

Select Source

Input Settings

Review

Done

✓

File input has been created successfully.

Configure your inputs by going to Settings > [Data Inputs](#)

Start Searching

Search your data now or see [examples and tutorials](#). [🔗](#)

Add More Data

Add more data inputs now or see [examples and tutorials](#). [🔗](#)

Download Apps

Apps help you do more with your data. [Learn more](#). [🔗](#)

Build Dashboards

Visualize your searches. [Learn more](#). [🔗](#)

With the help of this given command you are successfully using Splunk to search for and analyze events on your system.

source="/var/log/*" host=kali

/home/kali - the splunk in x

Search | Splunk 9.3.0

kali:8000/en-US/app/search/search?q=search source%3D"%2Fvar%2Flog%2F*" host%3D"kali"&earliest=0&late=

source="/var/log/*" host=kali

Configuration initialization for /home/nasan/Downloads/splunk/etc took longer than expected (6535ms) when dispatching a search with search ID 1723022436.83. This might indicate an issue w storage performance or the knowledge bundle size. If you want this message displayed more or less often, change the value of the 'search_startup_config_timeout_ms' setting in 'limits.conf' to higher number.

✓ 46,859 events (before 8/7/24 5:20:46.000 AM) No Event Sampling

Job

II

Events (46,859)

Patterns

Statistics

Visualization

Format Timeline

Zoom Out

+ Zoom to Selection

x Deselect

List

Format

20 Per Page

< Hide Fields

All Fields

Time

Event

> 8/7/24 5:19:27.000 AM [9362.084] (EE) event2 - VirtualPS/2 VMware VMMouse: client bug: event processing lagging behind by 21ms, y

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

- Navigation Bar:** Includes links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, and Kali Linux.
- Search Bar:** Contains the query `source%3D"%2Fvar%2Flog%2F*" host%3D"kali"&earliest`.
- Field List:** On the left, under "INTERESTING FIELDS", there are various date and time fields like `# date_hour 17`, `# date_mday 11`, etc.
- Table:** The main table displays search results with columns for Time and Event. The data shows multiple instances of the macchanger tool being disabled in `/etc/default/macchanger` on `8/7/24` at `5:17:09.000 AM` from host `kali`.

Time	Event
5:17:09.000 AM	host = kali source = /var/log/macchanger.log sourcetype = macchanger
8/7/24 5:17:09.000 AM	disabled in /etc/default/macchanger
5:17:09.000 AM	host = kali source = /var/log/macchanger.log sourcetype = macchanger
8/7/24 5:17:09.000 AM	disabled in /etc/default/macchanger
5:17:09.000 AM	host = kali source = /var/log/macchanger.log sourcetype = macchanger
8/7/24 5:17:09.000 AM	disabled in /etc/default/macchanger
5:17:09.000 AM	host = kali source = /var/log/macchanger.log sourcetype = macchanger
8/7/24 5:17:09.000 AM	disabled in /etc/default/macchanger
5:17:09.000 AM	host = kali source = /var/log/macchanger.log sourcetype = macchanger
8/7/24 5:17:09.000 AM	disabled in /etc/default/macchanger
5:17:09.000 AM	host = kali source = /var/log/macchanger.log sourcetype = macchanger
8/7/24 5:17:09.000 AM	disabled in /etc/default/macchanger
5:17:09.000 AM	host = kali source = /var/log/macchanger.log sourcetype = macchanger

It shows that you are in the process of creating a new dashboard in **Splunk** and adding a visualization panel to it.

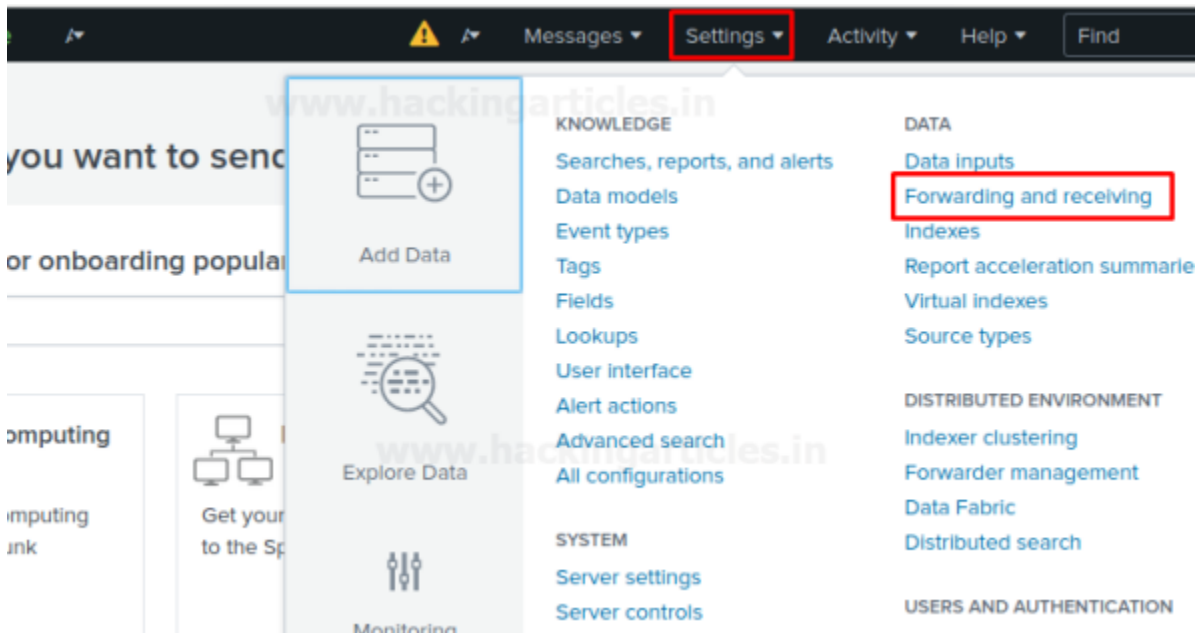
The screenshot shows the "Save Panel to New Dashboard" dialog box in Splunk. The dialog has the following fields and options:

- Dashboard Title:** `sys-logs` (with an "Edit ID" link).
- Description:** `For Monitor the system logs` (highlighted with a blue border).
- Permissions:** `Private` (with a dropdown arrow).
- How do you want to build your dashboard?:** A link to [What's this?](#)
- Buttons:** "Cancel" and "Save to Dashboard" (in green).

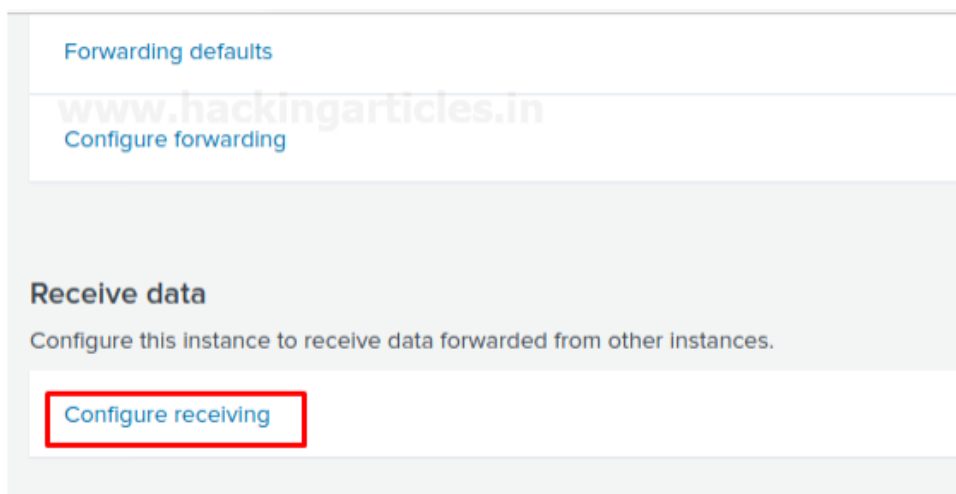
In the background, a "Save As" button is highlighted with a red rectangle.

SIEM: Windows Client Monitoring with Splunk

Go to settings Add Data and then Click on **Forwarding and receiving**



Select the **Configure receiving** Option



The most suitable receiver port on indexer is **port 9997**

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

Port 9997 is **Enabled**

splunk>enterprise Apps Administrator Messages Settings Activity

Receive data

Forwarding and receiving » Receive data

Successfully saved "9997".

Showing 1-1 of 1 item

filter

Listen on this port	Status
9997	Enabled Disable

Splunk Universal Forwarder on a Windows Machine or server.

You can download Splunk forwarder by following the below link

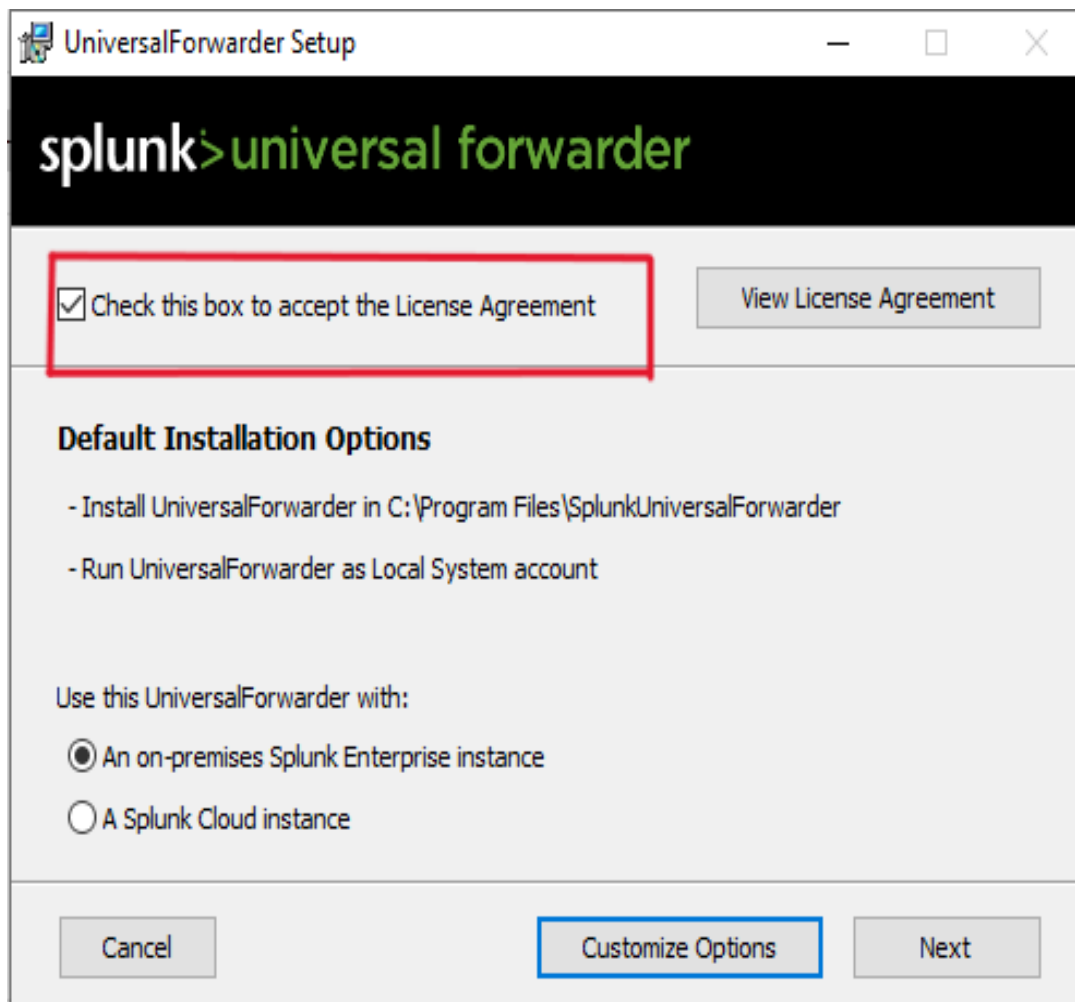
https://www.splunk.com/en_us/download/universal-forwarder.html

Today (1)

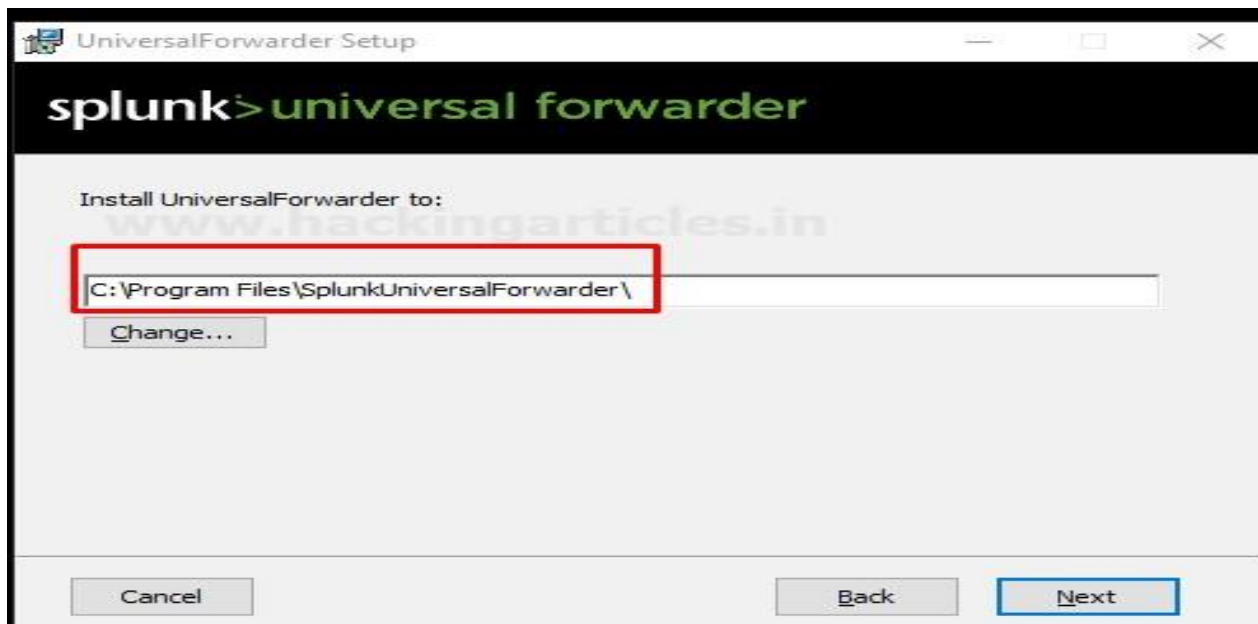
splunkforwarder-9.3.0-51ccf43db5bd-x64-relea...

Last week (2)

Accept the License Agreement and then click on Next



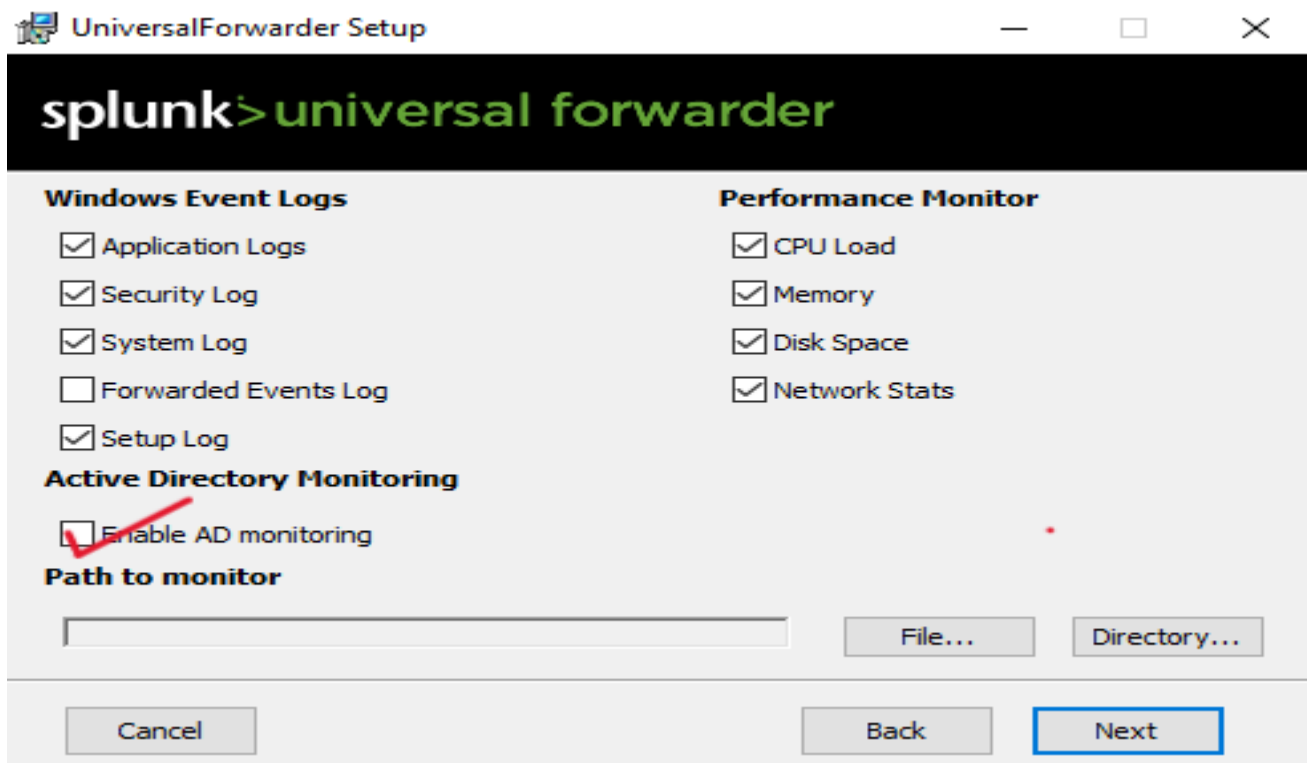
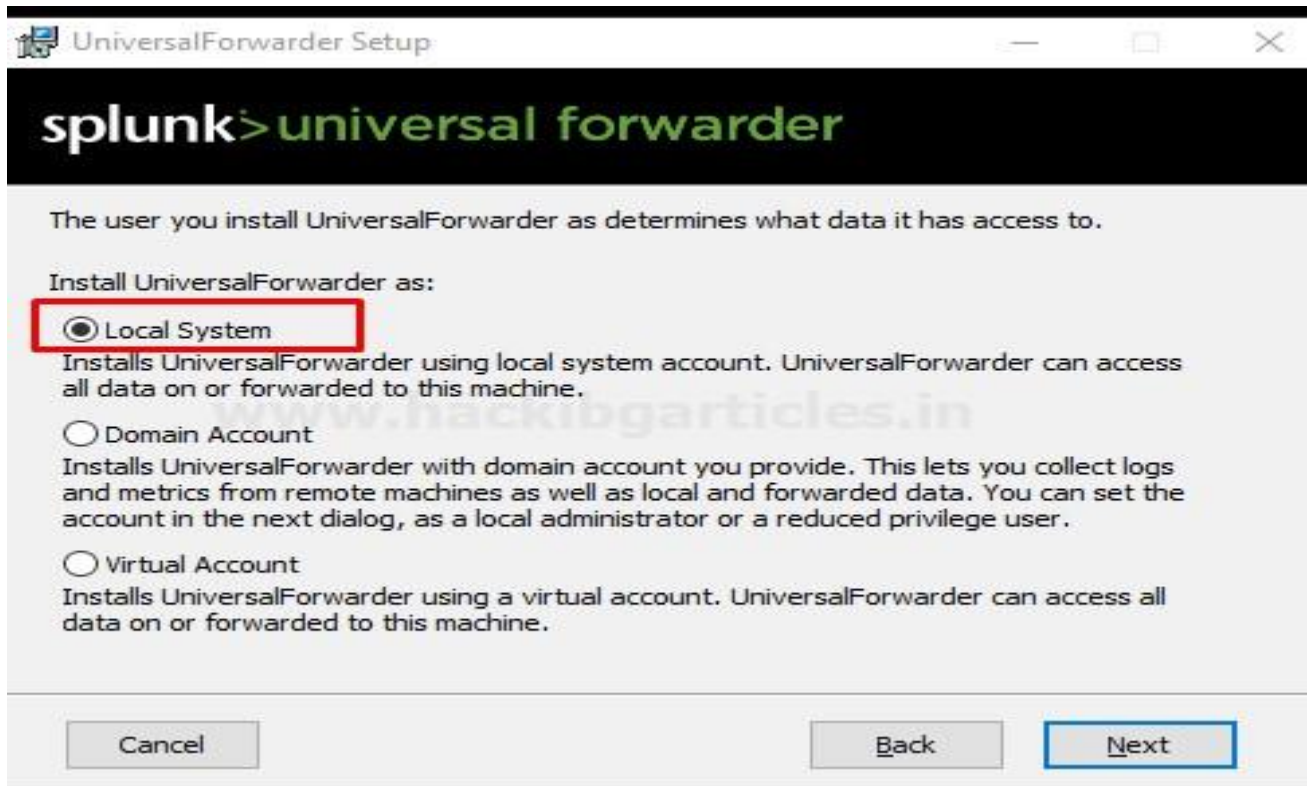
Select the installation directory wherever you want to install it



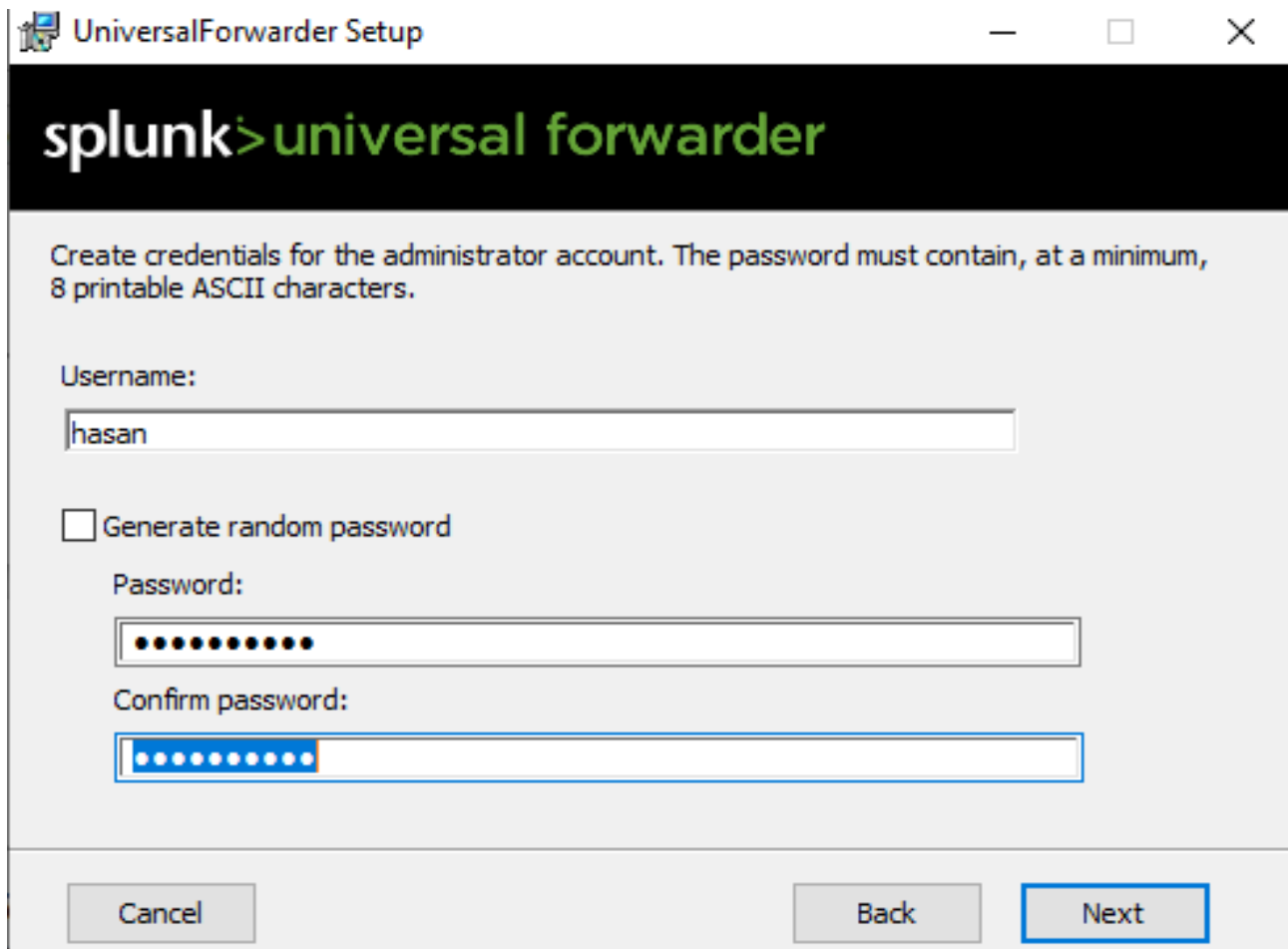
If you do not have the SSL certificate, then don't worry forwarded Splunk data will still be encrypted with the default Splunk certificate all you need to do is go with **Next option**.



Select the Local System Option



Give the username and Password



UniversalForwarder Setup

splunk>universal forwarder

Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.

Username:
hasan

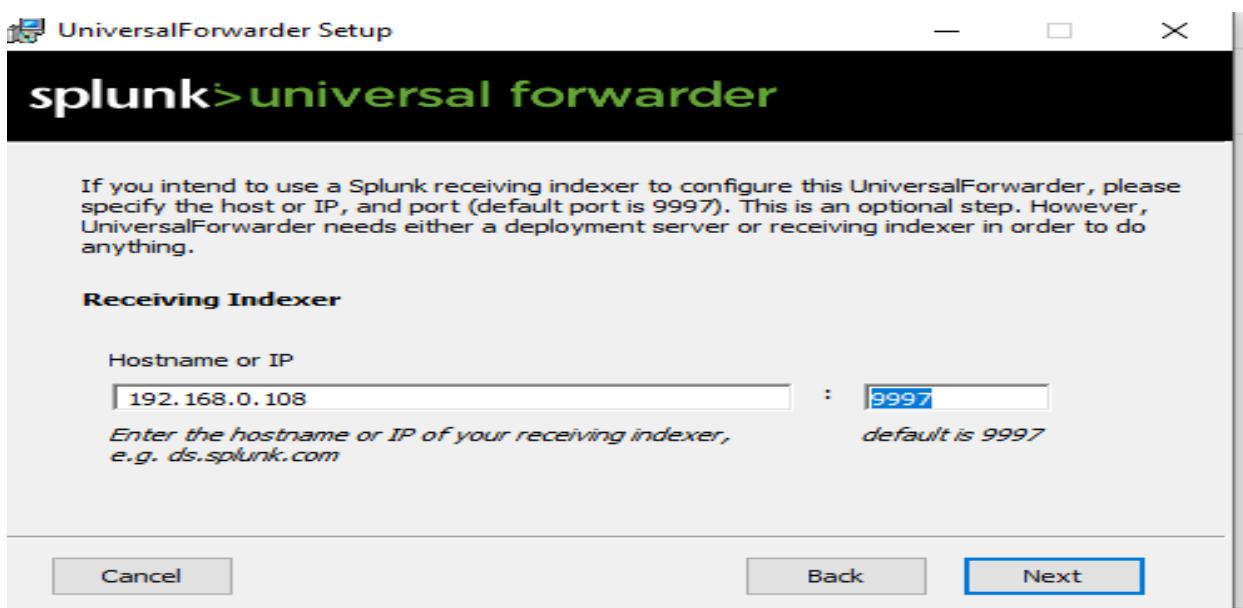
☐ Generate random password

Password:
●●●●●●●●

Confirm password:
●●●●●●●●

Cancel Back Next

Receiving indexer by entering the **Hostname or IP** and port



UniversalForwarder Setup

splunk>universal forwarder

If you intend to use a Splunk receiving indexer to configure this UniversalForwarder, please specify the host or IP, and port (default port is 9997). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

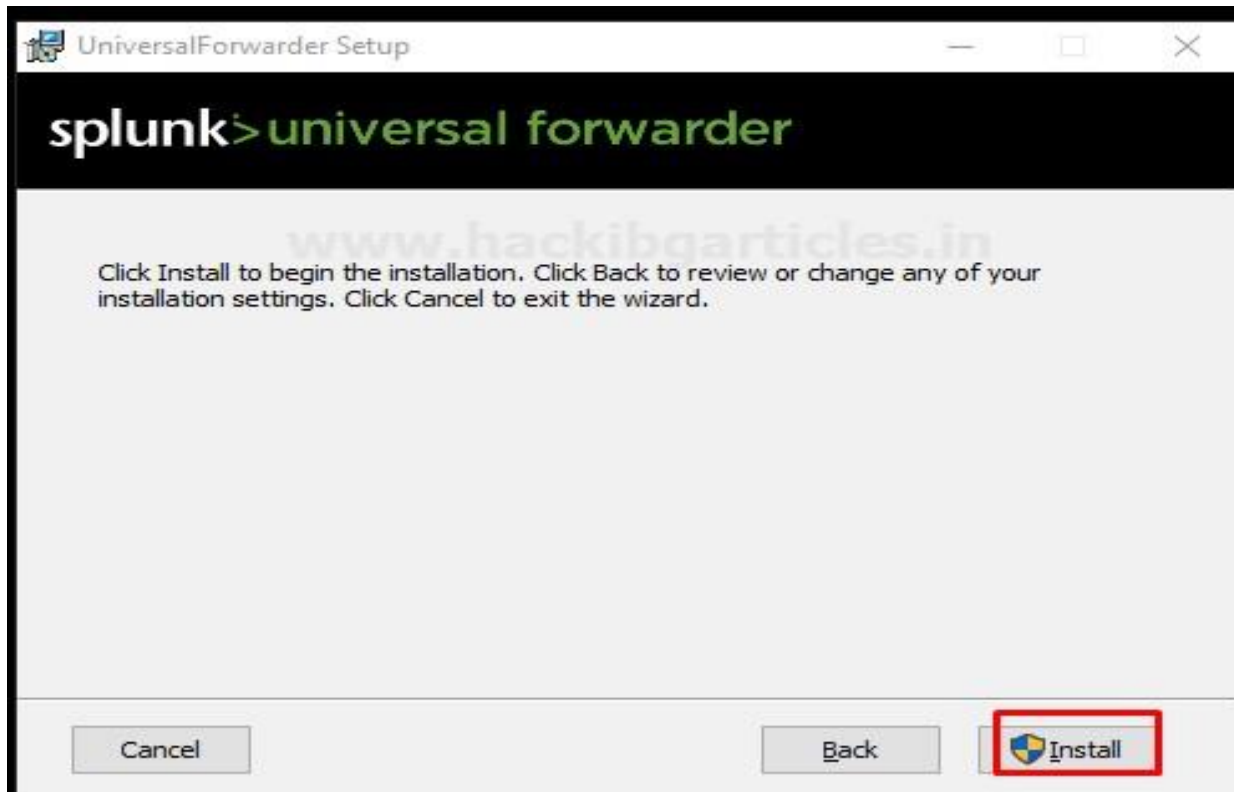
Receiving Indexer

Hostname or IP
192.168.0.108 : 9997

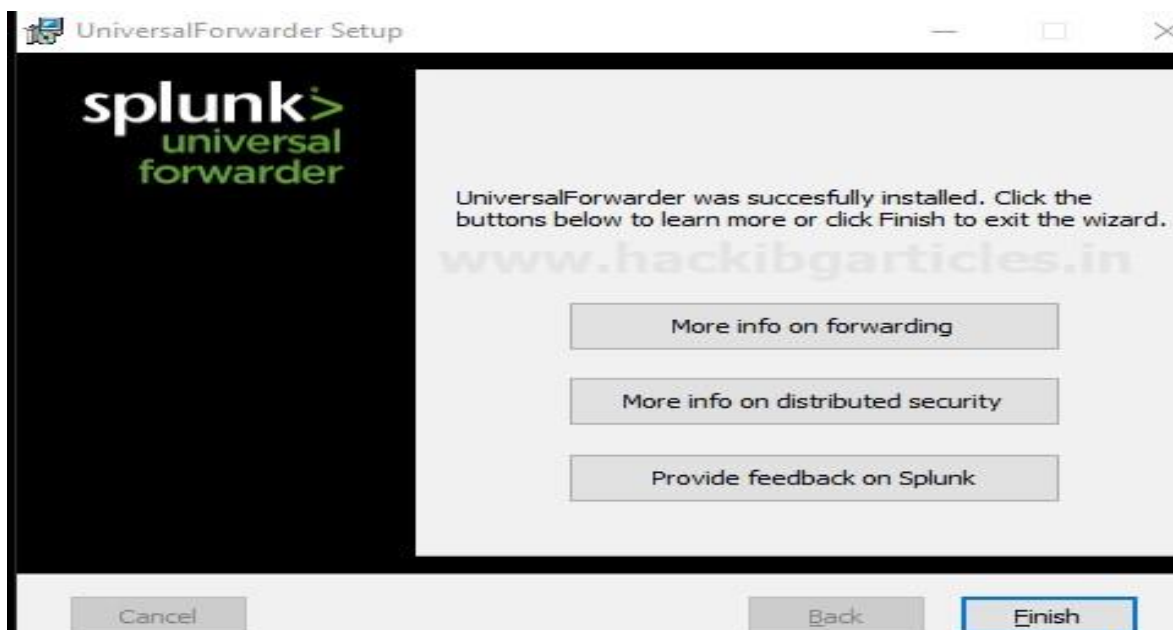
Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com *default is 9997*

Cancel Back Next

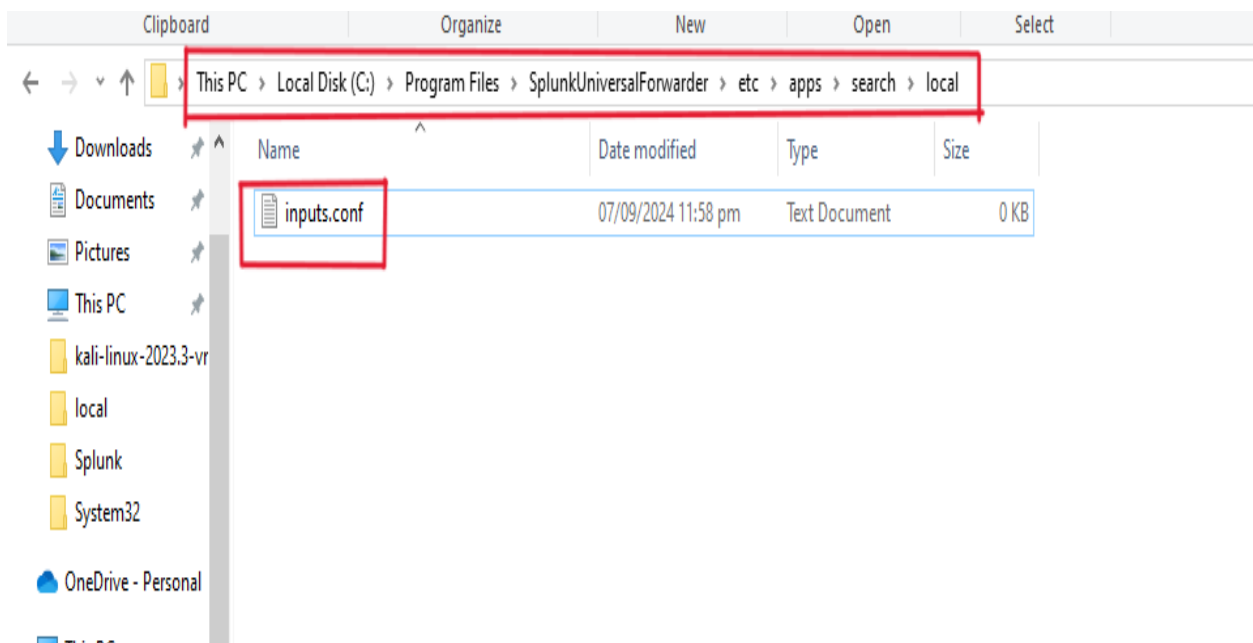
Finally select option Install it will install **Splunk forwarder** in your windows



After that finish, the **installation process**.



Go to Local Disk(c) >Program Files>Splunk Universal Forwarder>etc>apps>search and then make a new Folder **local** and create a config file **inputs.conf**

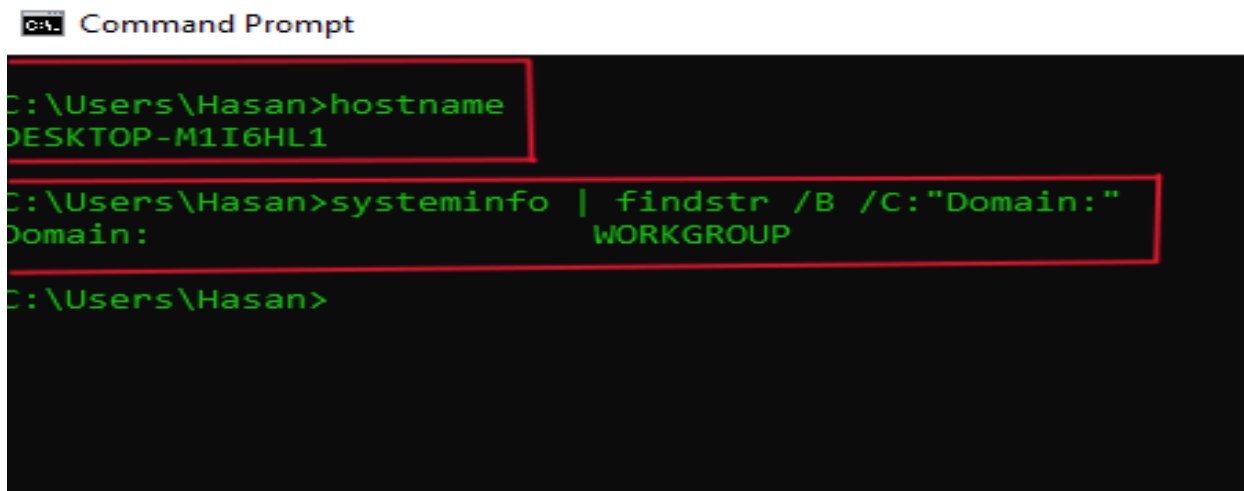


Open a Command Prompt with Administrative Privileges and then Find the **Hostname and Domain name** of System,

Commands for Find the Host name and Domain name of Your System

hostname

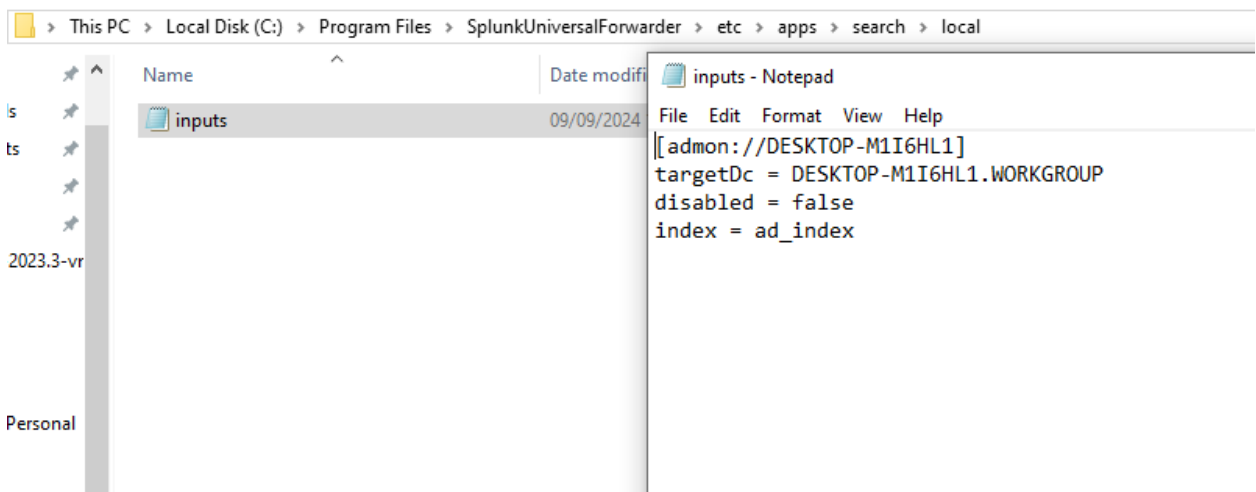
systeminfo | findstr /B /C: "Domain:"



Save the Hostname and domain name in **inputs.conf** file with the help Command Prompt. these commands are configuring the Splunk Universal Forwarder to monitor a specific host or device and send the collected data to a specified index.

```
Administrator: Command Prompt
C:\Windows\system32>cd C:\Program Files\SplunkUniversalForwarder\etc\apps\search\local
C:\Program Files\SplunkUniversalForwarder\etc\apps\search\local>echo
ECHO is on.
C:\Program Files\SplunkUniversalForwarder\etc\apps\search\local>echo [admon://DESKTOP-M1I6HL1] >> inputs.conf
C:\Program Files\SplunkUniversalForwarder\etc\apps\search\local>echo targetDc = DESKTOP-M1I6HL1.WORKGROUP >> inputs.conf
C:\Program Files\SplunkUniversalForwarder\etc\apps\search\local>echo disabled = false >> inputs.conf
C:\Program Files\SplunkUniversalForwarder\etc\apps\search\local>echo index = ad_index >> inputs.conf
C:\Program Files\SplunkUniversalForwarder\etc\apps\search\local>
```

Check the data was Successfully saved on **inputs.conf** File.



Splunk Forwarder was started

```
C:\>cd C:\Program Files\SplunkUniversalForwarder\bin

C:\Program Files\SplunkUniversalForwarder\bin>splunk start
The splunk daemon (splunkd) is already running.

C:\Program Files\SplunkUniversalForwarder\bin>splunk restart
SplunkForwarder: Stopped

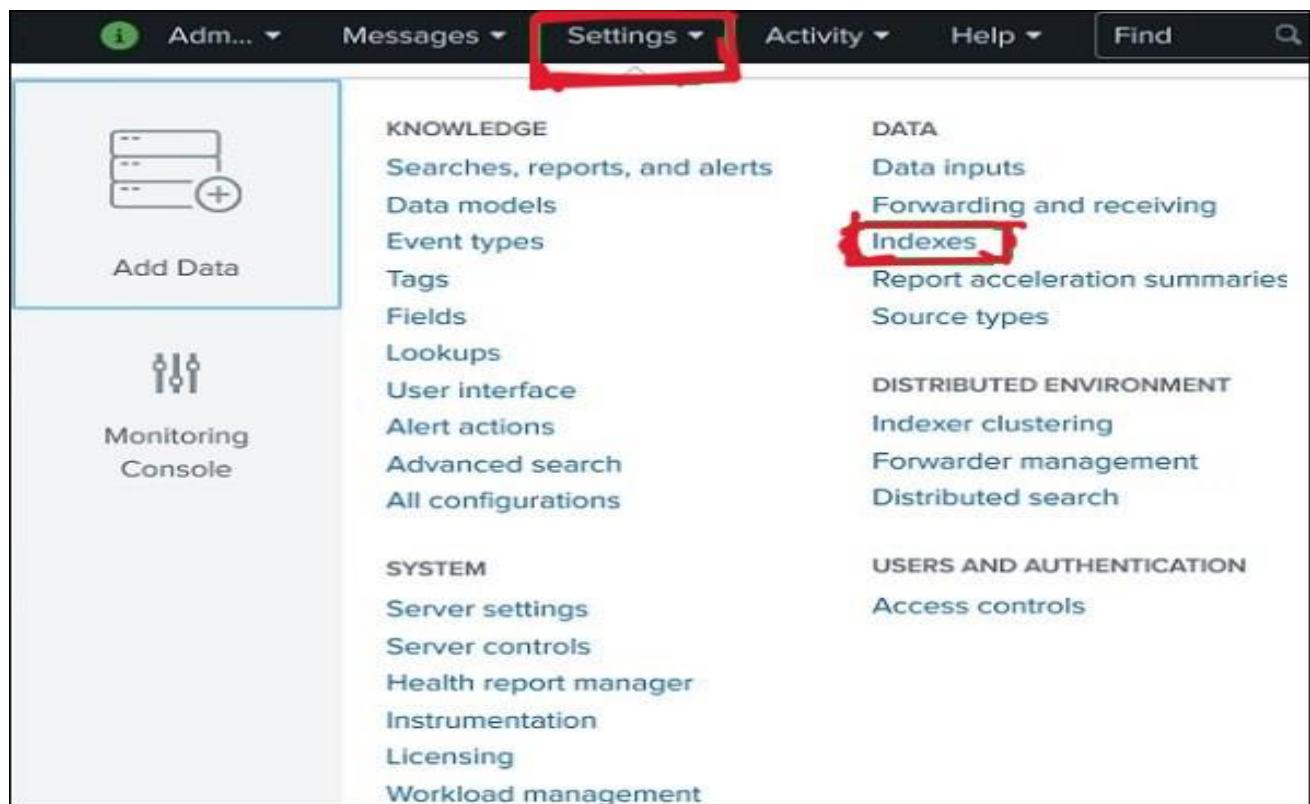
Splunk> Winning the War on Error

Checking prerequisites...
  Checking mgmt port [8090]: open
  Checking conf files for problems...
  Done
  Checking default conf files for edits...
  Validating installed files against hashes from 'C:\Program Files\SplunkUniversalForwarder\splunkforwarder'
  All installed files intact.
  Done
All preliminary checks passed.

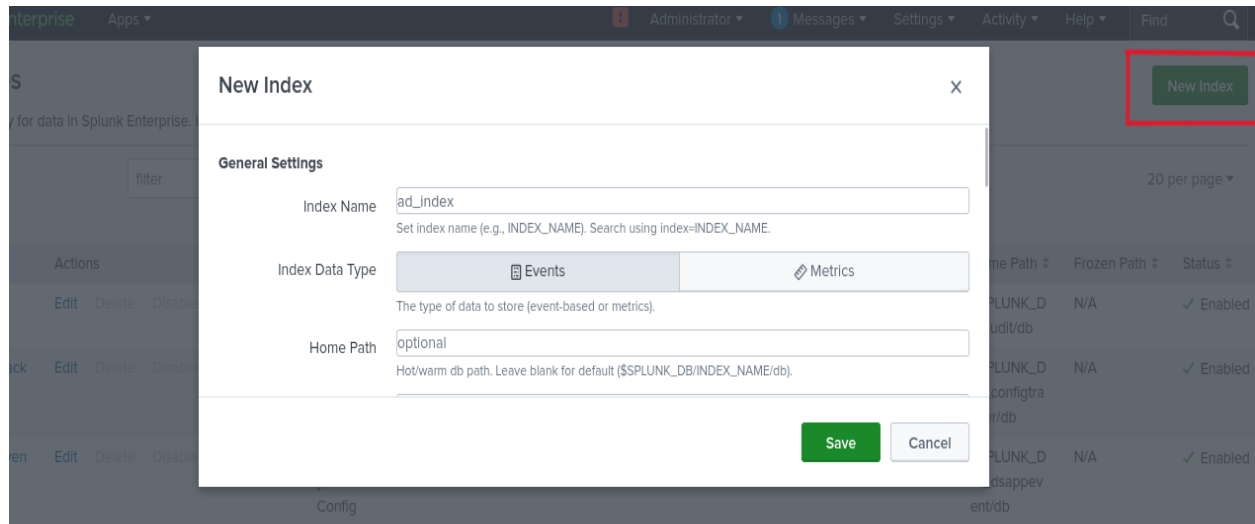
Starting splunk server daemon (splunkd)...
SplunkForwarder: Starting (pid 22804)
Done

C:\Program Files\SplunkUniversalForwarder\bin>
```

Go to Setting and Then Click on **Indexes**



Click on new Index and index name is **ad_index**

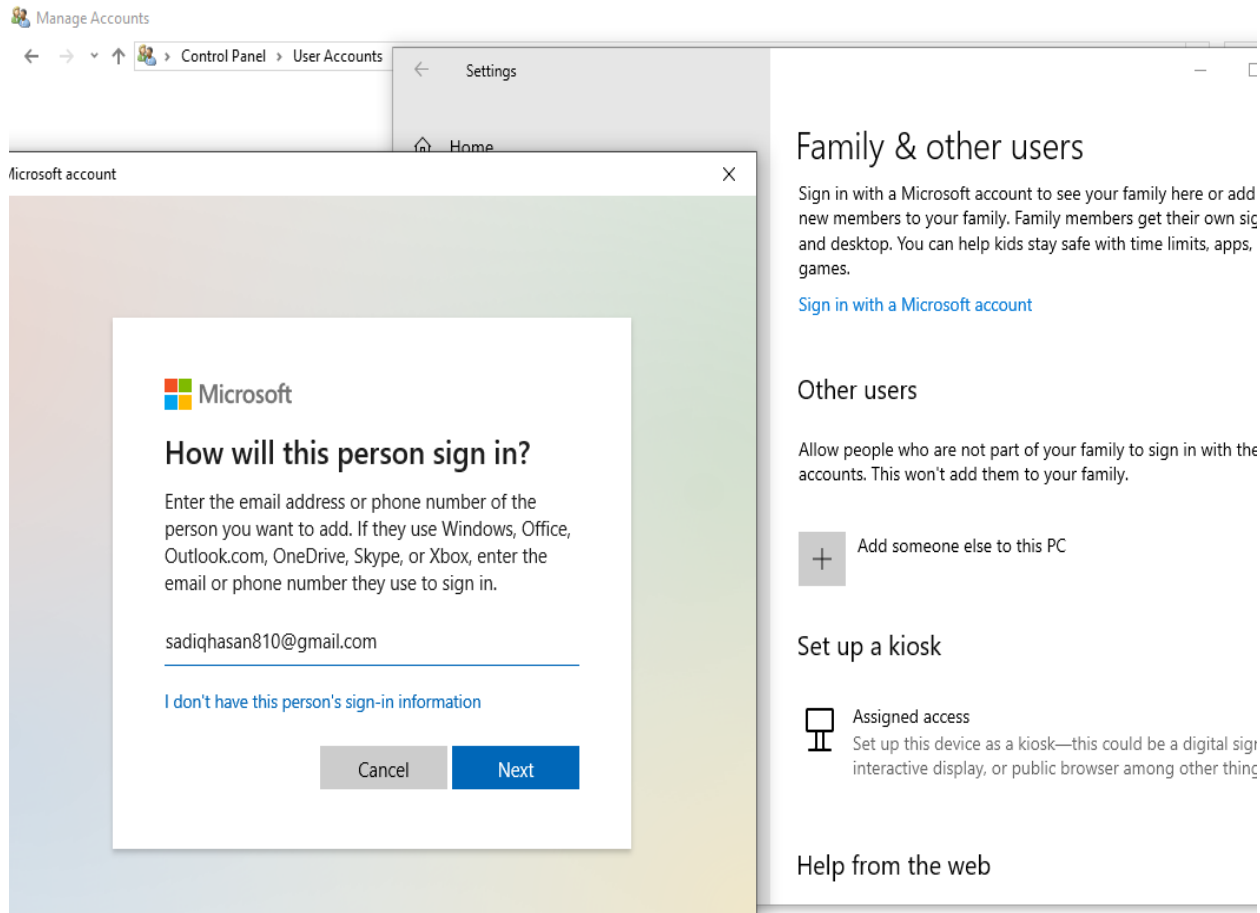


ad_index was Successfully adding in the indexes list and 0 Event has shown

_metrics_rol	Edit	Delete	Disable	Metrics	system	1 MB	488.28 GB	0
_telemetry	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0
_thefishbuck	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0
ad_index	Edit	Delete	Disable	Events	search	1 MB	500 GB	0
history	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0

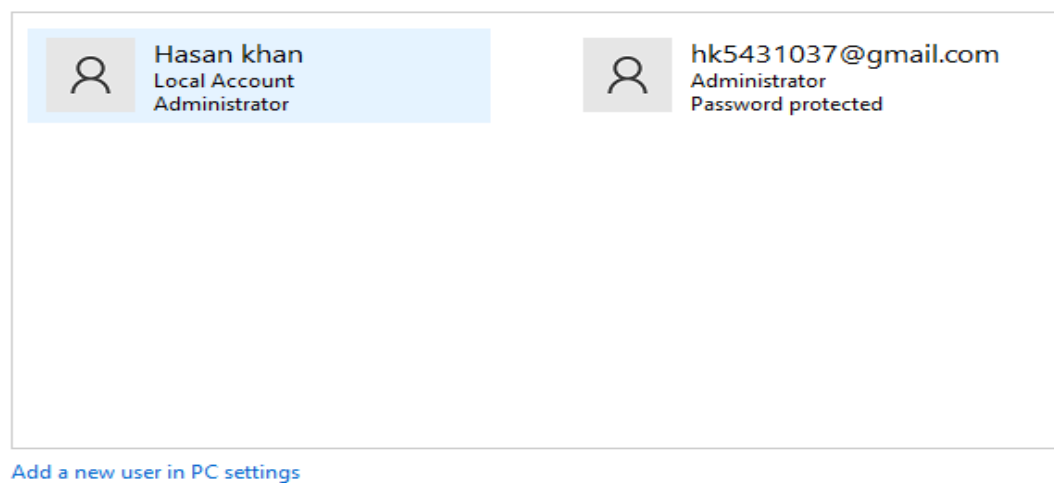
Now we create an **Event** for **ad_index**

Go to control panel and **Add Other User**



Successfully Add another user and I add a Password for another user and for Create an Events for **ad_index**

Choose the user you would like to change



ad_index was show the events.

Name ^	Actions	Type ↕	App ↕	Current Size ↕	Max Size ↕	Event Count ↕	Ear
_audit	Edit Delete Disable	Events	system	2 MB	488.28 GB	5,45K	10 c
_internal	Edit Delete Disable	Events	system	26 MB	488.28 GB	214K	10 c
_introspecti on	Edit Delete Disable	Events	system	49 MB	488.28 GB	48K	10 c
_telemetry	Edit Delete Disable	Events	system	1 MB	488.28 GB	9	9 d
_thefishbuck et	Edit Delete Disable	Events	system	1 MB	488.28 GB	0	
ad_index	Edit Delete Disable	Events	search	1 MB	500 GB	0	

