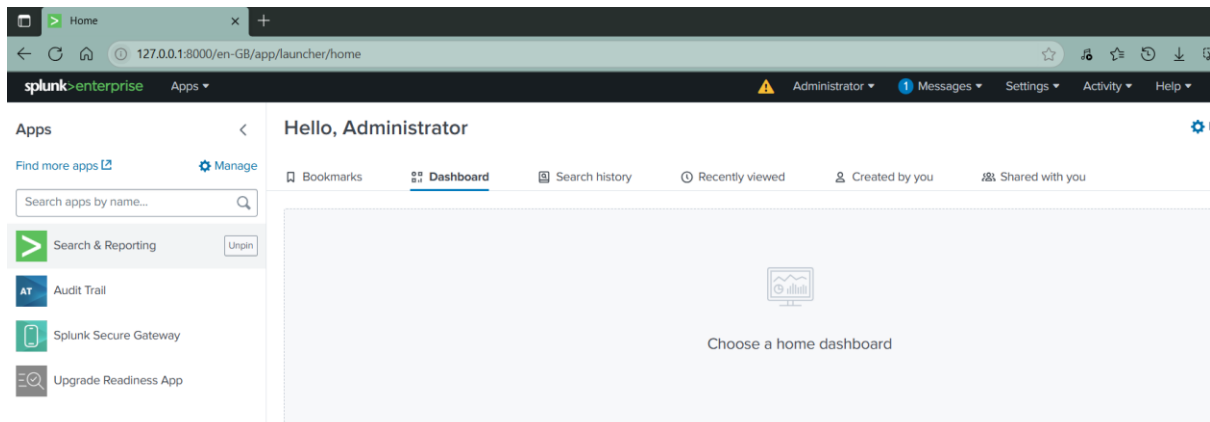


**Day 21 of Learning Cyber Security****Platform: Kali Linux****Name:** Ayesha Nadeem**Topic:** Splunk**splunk****Contact Me:** [ayeshanm8@gmail.com](mailto:ayeshanm8@gmail.com)**Date:** 21<sup>th</sup> July, 2025

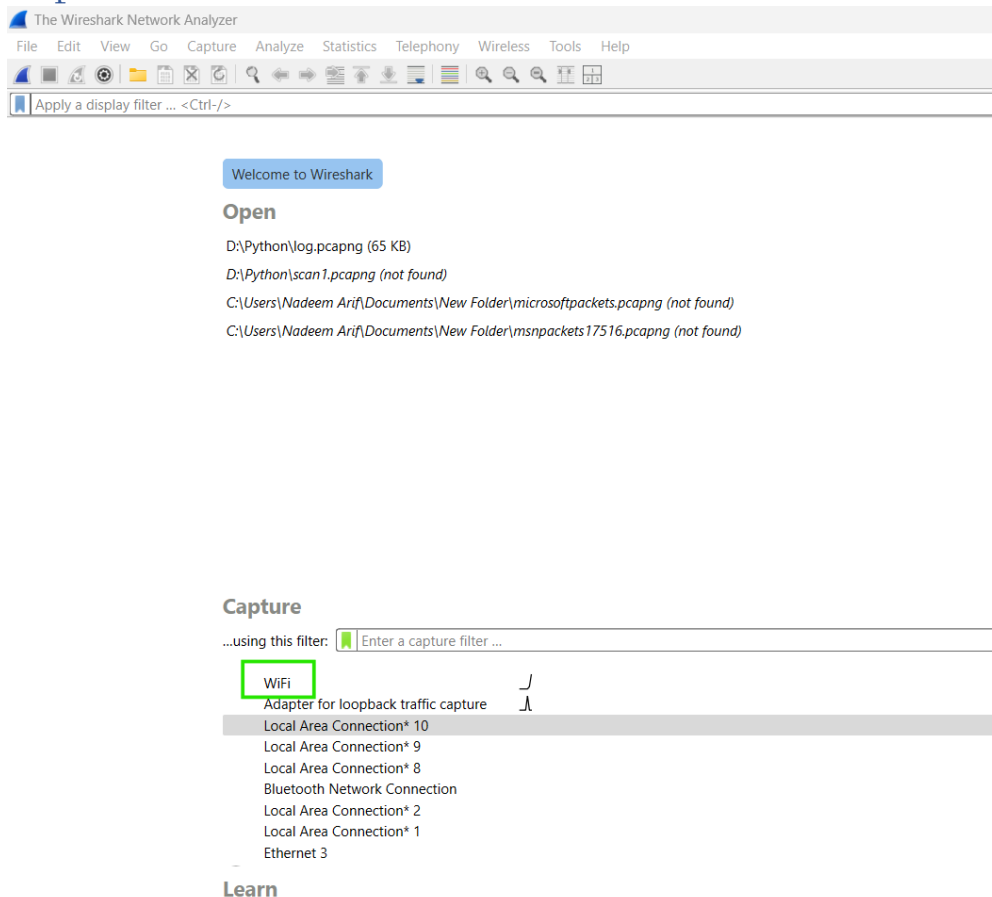
# Splunk Enterprise

## Welcome to Splunk dashboard



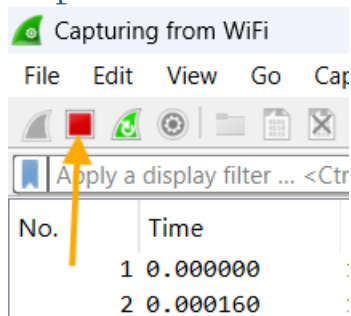
## Save log file form wireshark:

### Step 1:



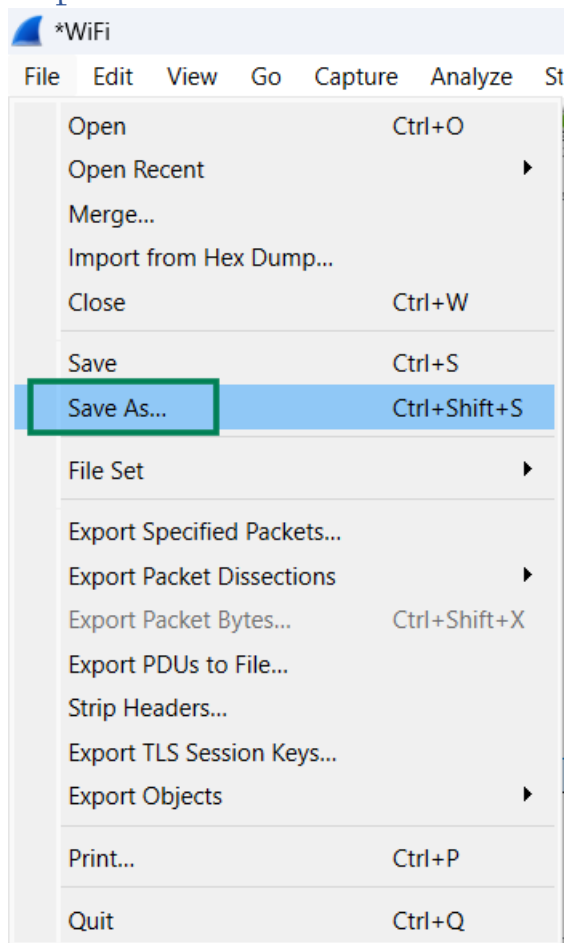
Double click on WiFi/eth0 to start capturing packet.

## Step 2:

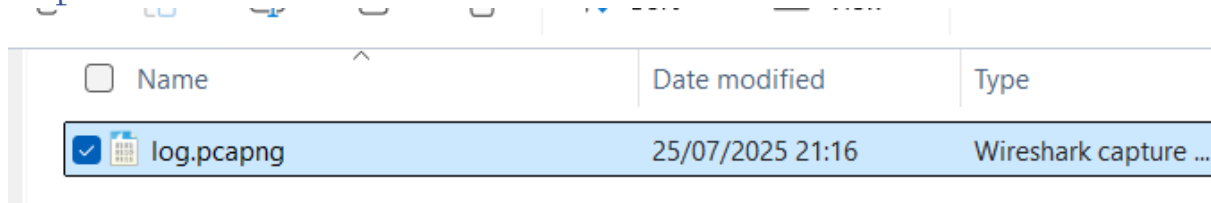


Click on red button to stop capturing packet.

## Step 3:

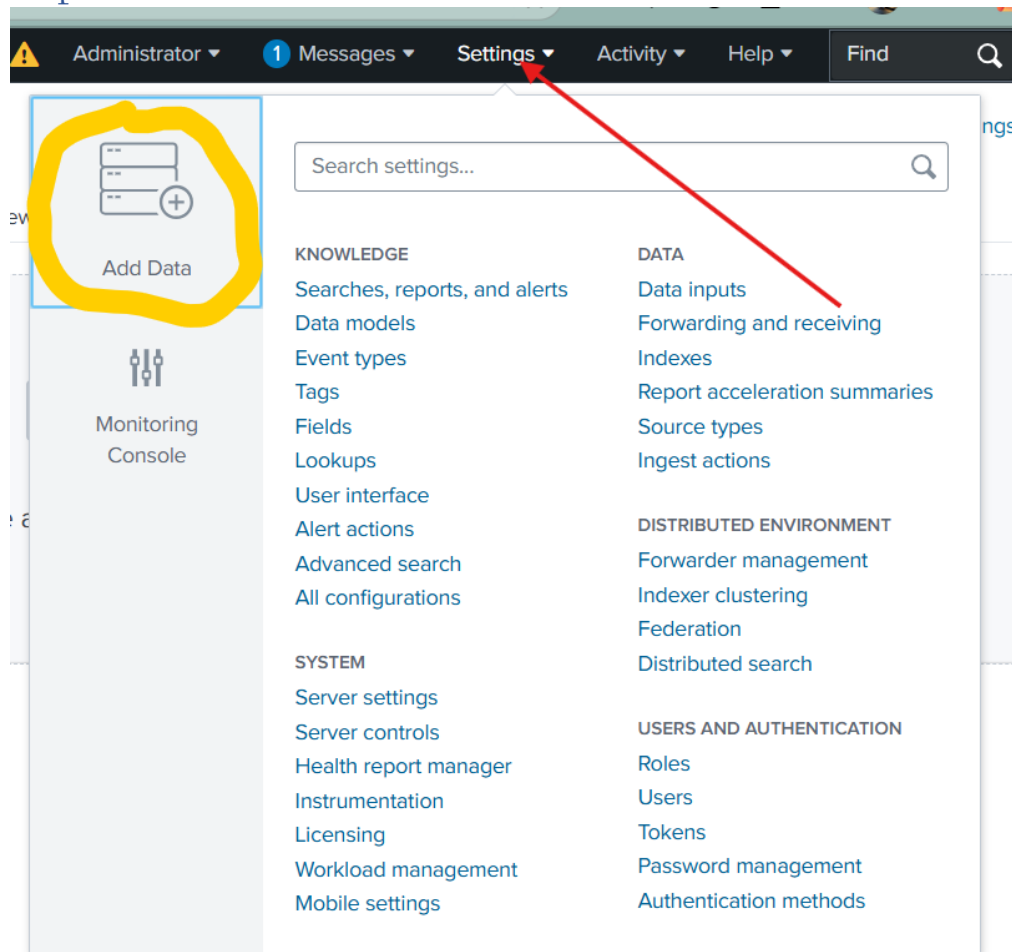


## Step 4:



## Upload doc in splunk:


Step 1:



Step 2:


4 data sources in total

### Or get data in with the following methods



**Upload**  
files from my computer

Local log files  
Local structured files (e.g. CSV)  
[Tutorial for adding data](#)



**Monitor**  
files and ports on this Splunk platform instance

Files - HTTP - WMI - TCP/UDP - Scripts  
Modular inputs for external data sources

## Step 3:

## Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping

Selected File: **log.pcapng**

Select File

Drop your data file here

The maximum file upload size is 500 Mb



File Successfully Uploaded

Click on next

## Step 4:

### Save Source Type

Name

My Report

Description

Analysing malicious activity in WiFi network

Category

Custom ▼

App

Search & Reporting ▼

Cancel

Save

Click on save.

### Step 5:

**Add Data**

Select Source Set Source Type **Input Settings** Review Done

< Back **Review >**

#### Input Settings

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

**Host**

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

☒ Constant value  
☐ Regular expression on path  
☐ Segment in path

Host field value

### Step 6:

**Add Data**

Select Source Set Source Type **Input Settings** **Review** Done

< Back **Submit >**

#### Review

Input Type ..... Uploaded File  
File Name ..... log.pcapng  
Source Type ..... My Report  
Host ..... LAPTOP-A41FU8FM  
Index ..... Default

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

Applied Cyber Security © 2025 by Ayesha Nadeem is licensed under CC BY-NC 4.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by-nc/4.0/>

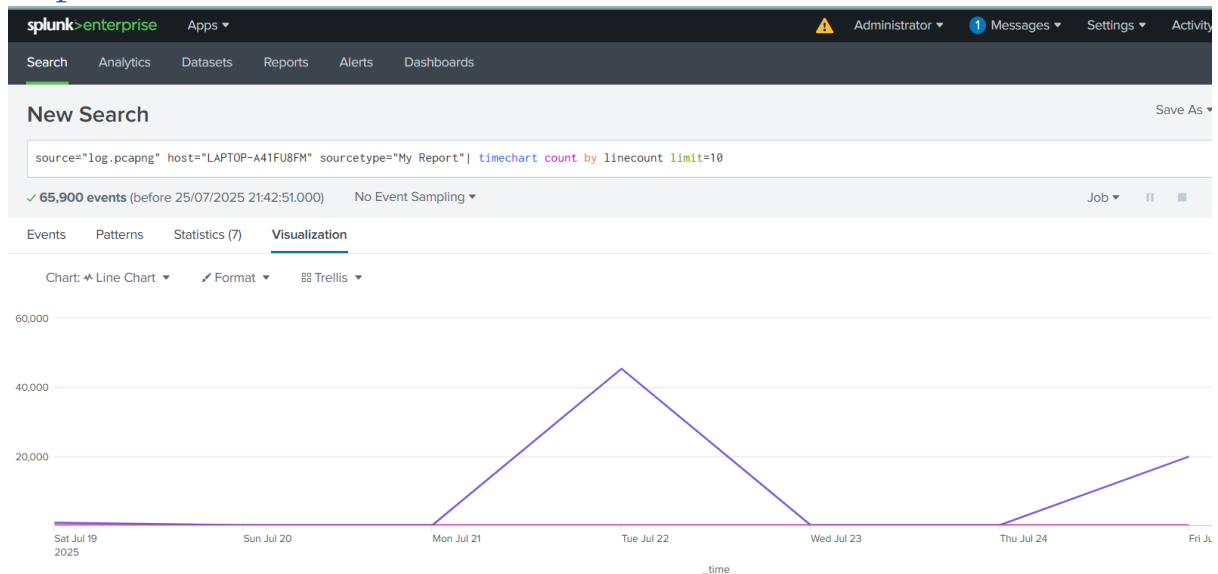
## Generate Report:

### Step 1:

The screenshot shows the Splunk field selection interface for the field 'linecount'. The left sidebar lists 'SELECTED FIELDS' (host 1, source 1, sourcetype 1) and 'INTERESTING FIELDS' (index 1, linecount 2, punct 100+, splunk\_server 1, timestamp 1). The main panel shows 'linecount' with '2 Values, 100% of events'. A green box highlights the 'Reports' section, which includes 'Average over time', 'Maximum value over time', 'Minimum value over time', 'Top values', 'Top values by time' (highlighted with a red arrow), and 'Rare values'. Below the reports, statistics are shown: Avg: 2.2427184466019416, Min: 1, Max: 257, Std Dev: 17.836365165865413. A table shows the distribution of values:

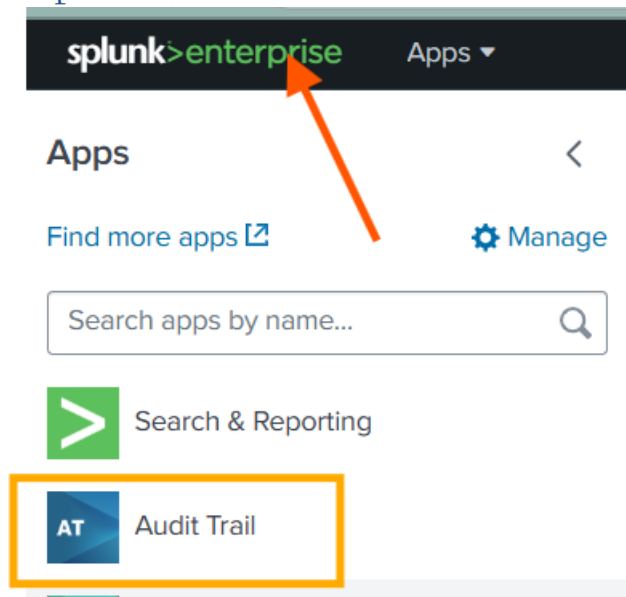
Values	Count	%
1	205	99.514%
257	1	0.485%

### Step 2:



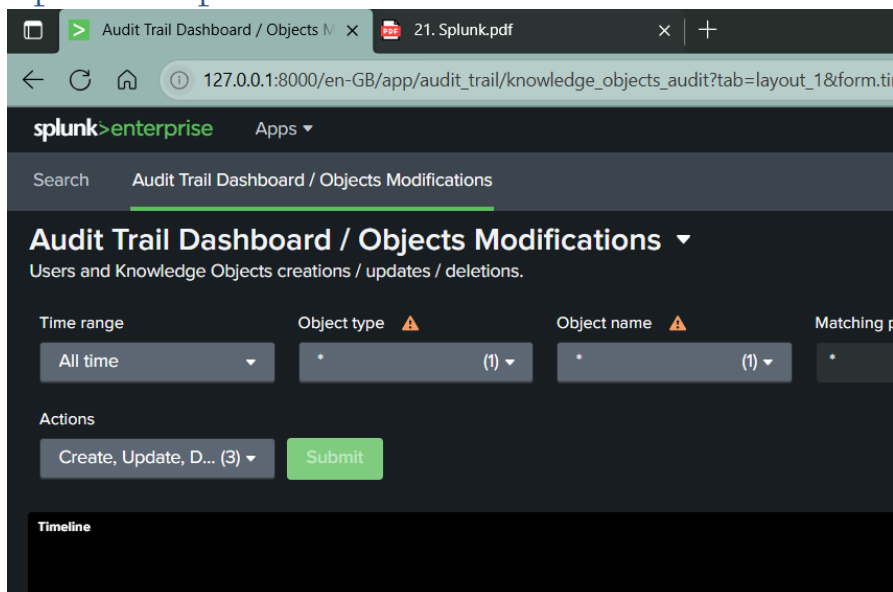


Step 3:



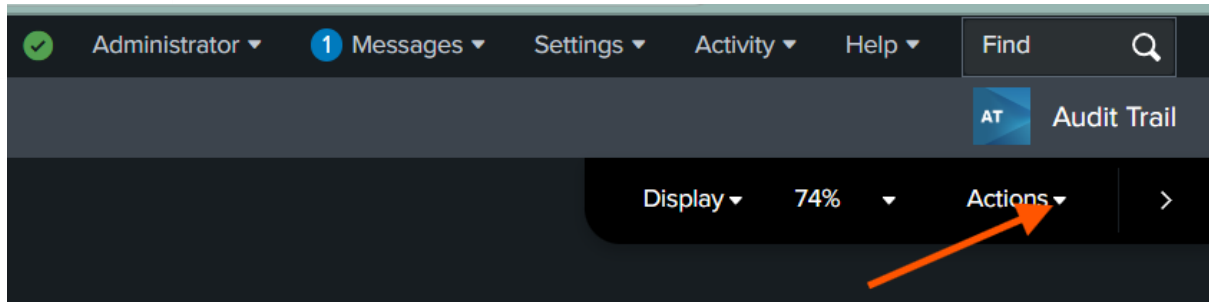
- Click on logo of splunk to land on homepage.
- Next click on Audit Trail

Optional Steps:

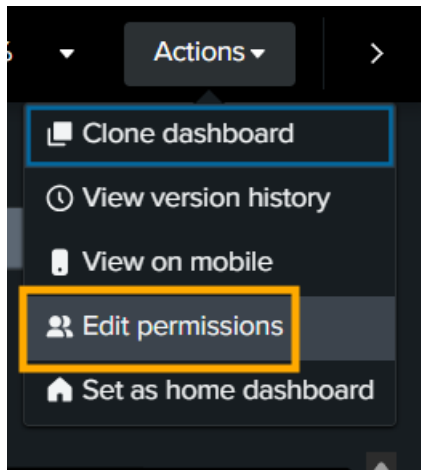


If you see warning sign then follow these steps:

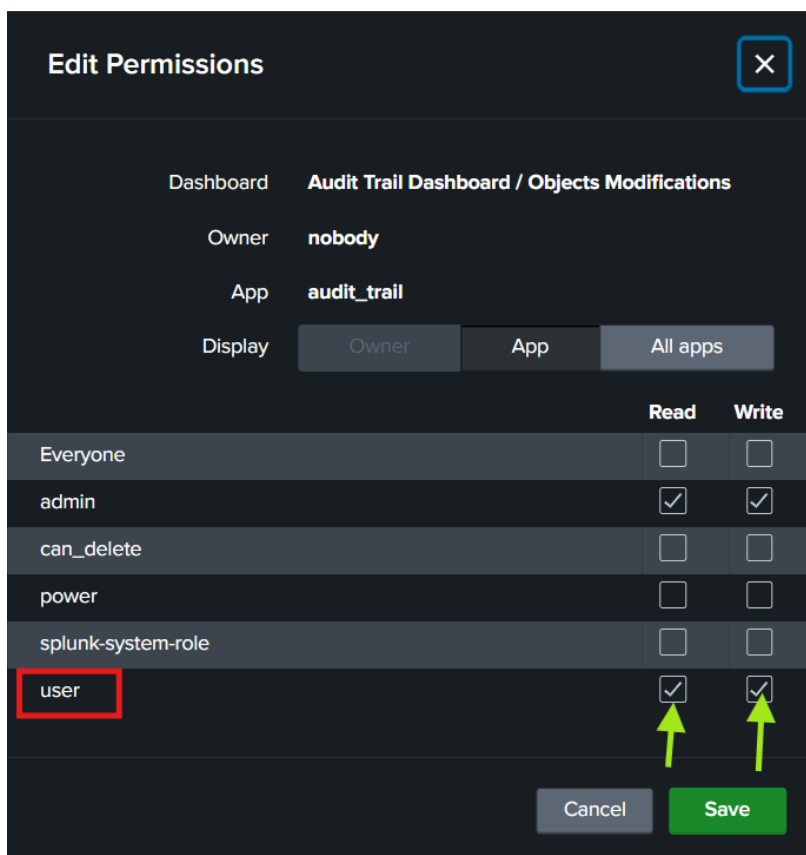
1. First go to Actions located at right top corner

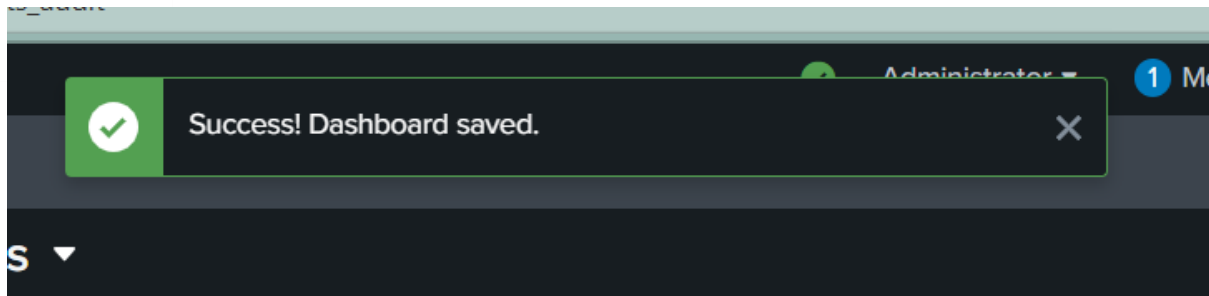


2. Then go to edit permission

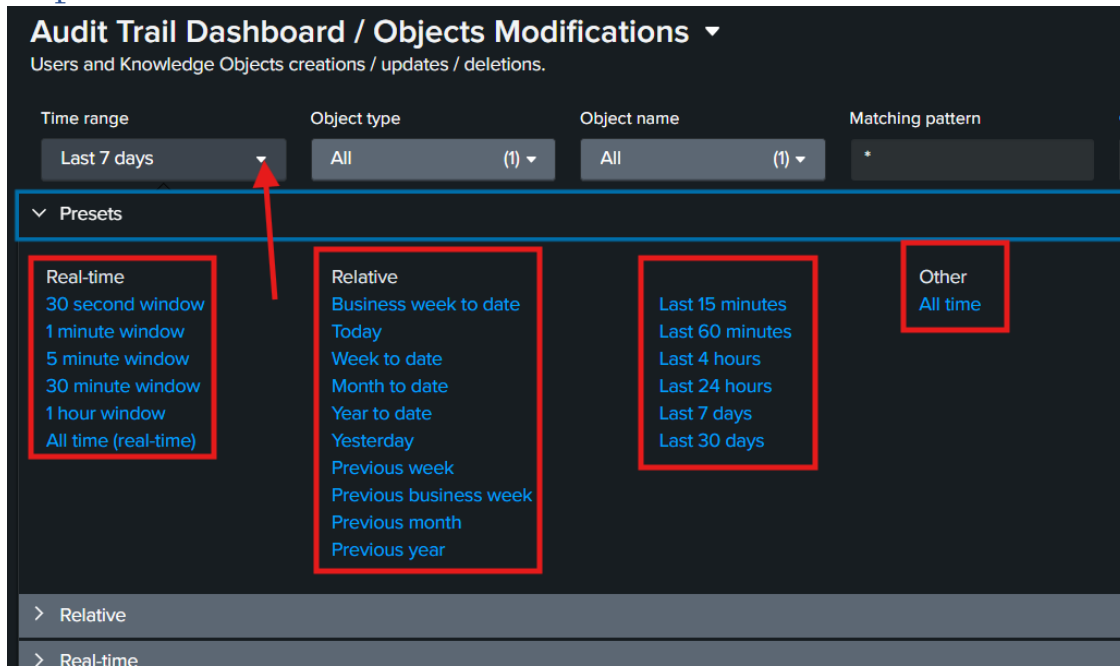


3. Extend the user permissions



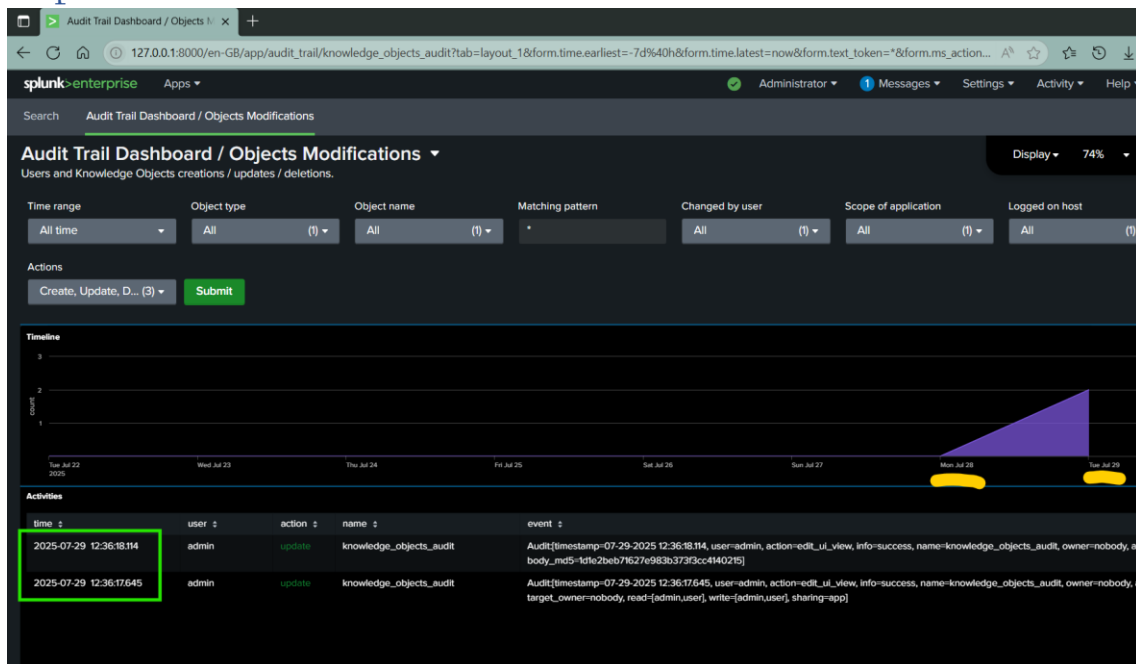


#### Step 4:

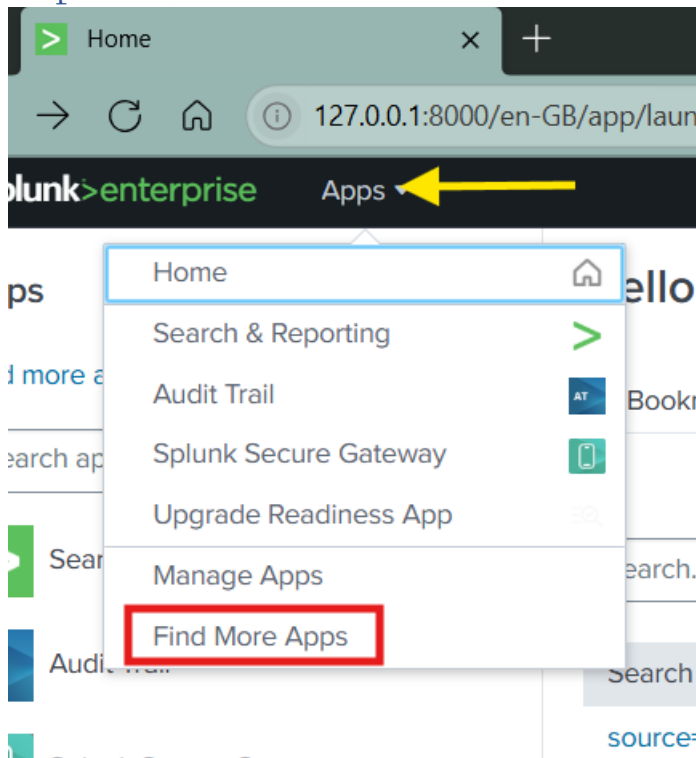


Select any time range and submit.

#### Step 5:



## Step 6:



## Step 7:

Look out for app and run them for more security information auditing

You can install app like:

- Threat Hunting Essentials
- Splunk App for Stream