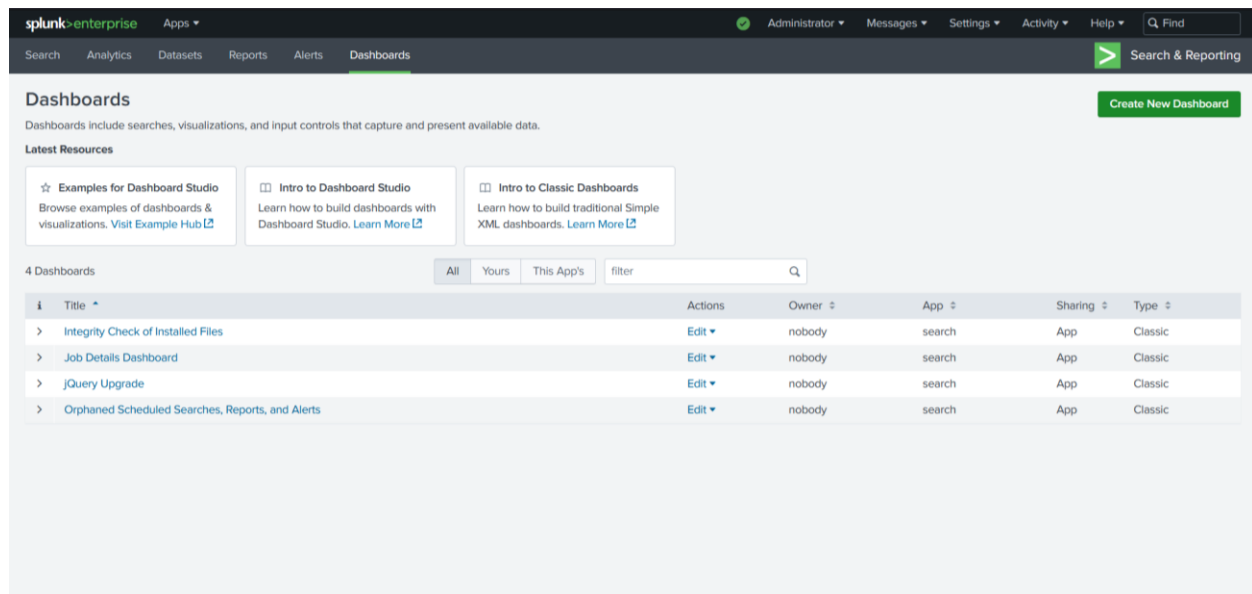
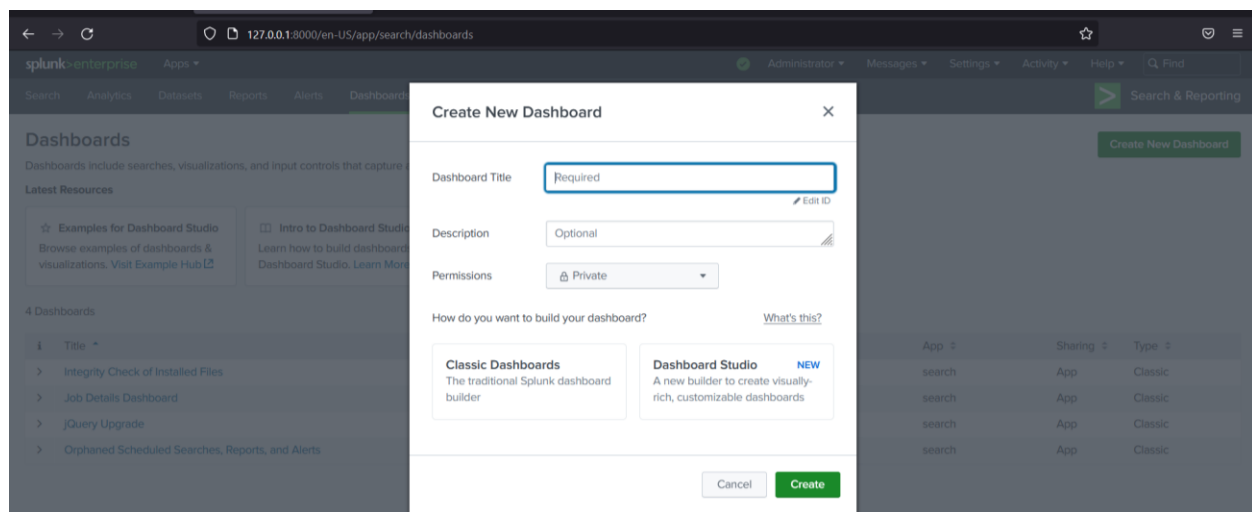


Alert generation on USB plugging

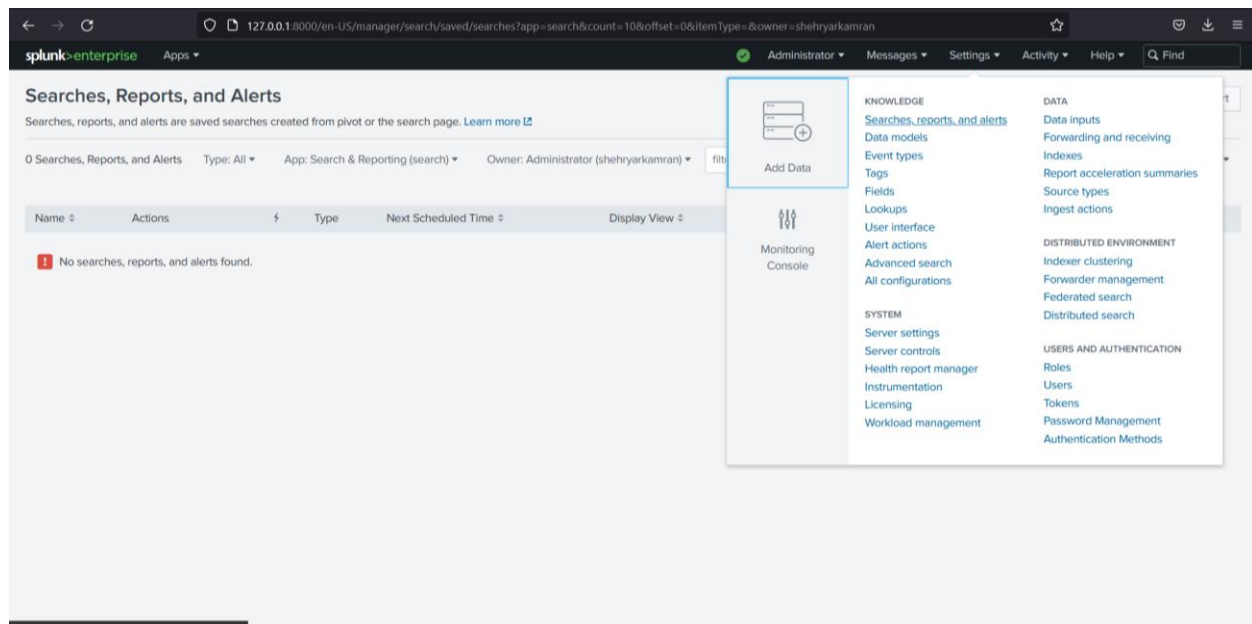
STEP 1: Create Dashboard



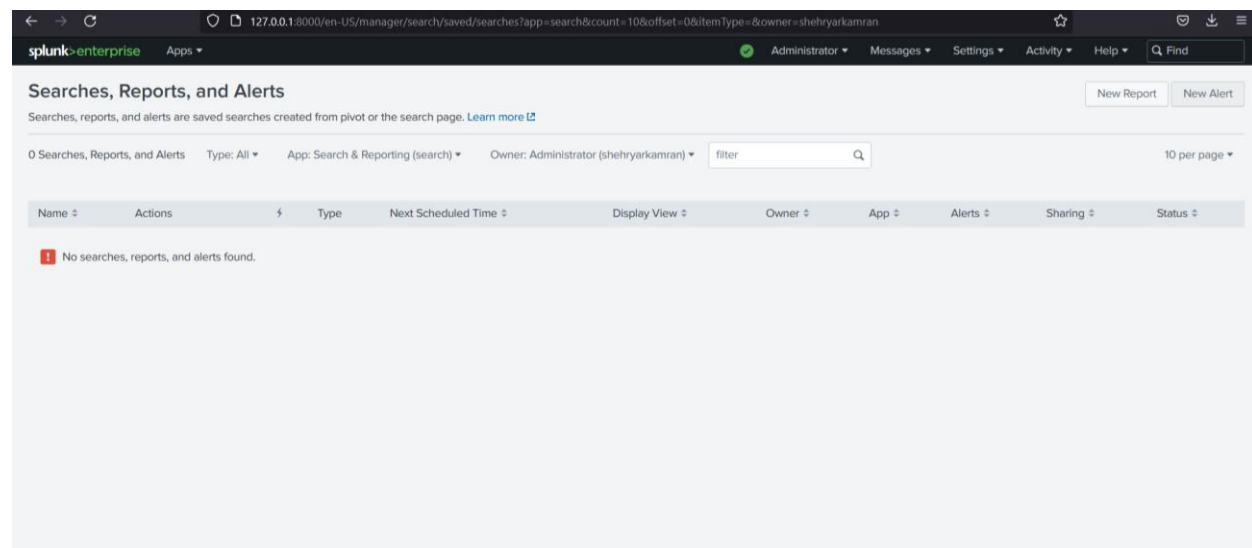
STEP 2: Enter data in required fields; Name of Dashboard, Type of Dashboard, Build of Dashboard



STEP 3: Click on settings and then click on Searches, reports and alerts



STEP 4: Click on new alert button on top right side



STEP 5: Fill Create Alert dialog box where you have to enter Title, search, App, Permission, Alert Type, Expires, Trigger Action

Create Alert

Settings

Title: USB DETECTION ALERT

Description: Optional

Search

```
| tstats 'security_content_summariesonly' count earliest(_time) AS earliest
latest(_time) AS latest from datamodel=Change_Analysis where (nodename =
All_Changes) All_Changes.result="Removable Storage device" (All_Changes
.result_id=4663 OR All_Changes.result_id=4656) (All_Changes.src_priority=high
) by All_Changes.dest
| "drop_dm_object_name("All_Changes")"
| "security_content_ctime(earliest)"
| "security_content_ctime(latest)"
| "detect_usb_device_insertion.filter"
```

App: Log Event Alert Action (alert_logevent)

Permissions: Private

Alert type: Real-time

Cancel Save

After that alert will come to entry section

Searches, Reports, and Alerts

Searches, reports, and alerts are saved searches created from pivot or the search page. [Learn more](#)

1 Searches, Reports, and Alerts Type: All App: Search & Reporting (search) Owner: Administrator (shehyarkamran) filter 10 per page

Name	Actions	Type	Next Scheduled Time	Display View	Owner	App	Alerts	Sharing	Status
USB	Edit Run View Recent	Alert	2022-08-29 06:00:00 Pakistan Standard Time	none	shehyarkamran	search	0	Private	Enabled

Logs

Jobs

Manage your jobs. [Learn More](#)

1 Jobs App: Search & Reporting (search) Owner: All Status: All label="USB" 10 Per Page

Edit Selected 1 Job selected

i	Owner	Application	Events	Size	Created at	Expires	Runtime	Status	Actions
>	shehyarkamran	search	0	100 KB	Aug 25, 2022 4:10:15 PM	Aug 25, 2022 4:13:45 PM	00:01:30	Running (real-time)	Job Job Job Job

USB [real-time]