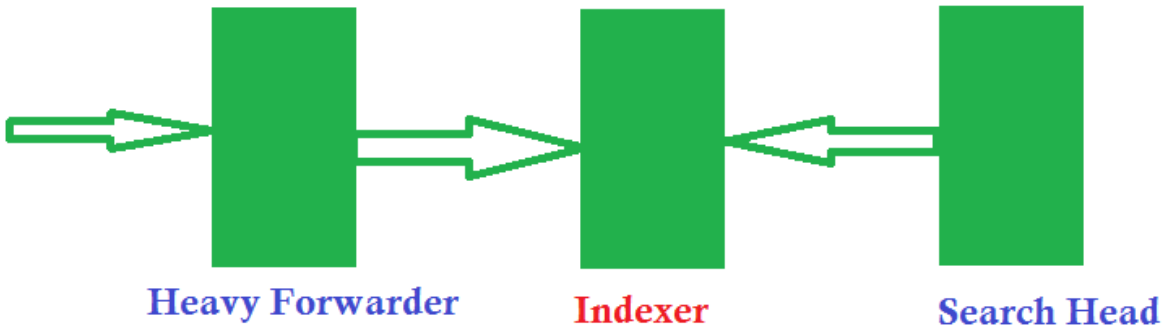
Configurations of Receiving and Forwarding Channel in Splunk Enterprise 9.4.7 on Windows



Receiving Channel Configuration (Indexer Side)

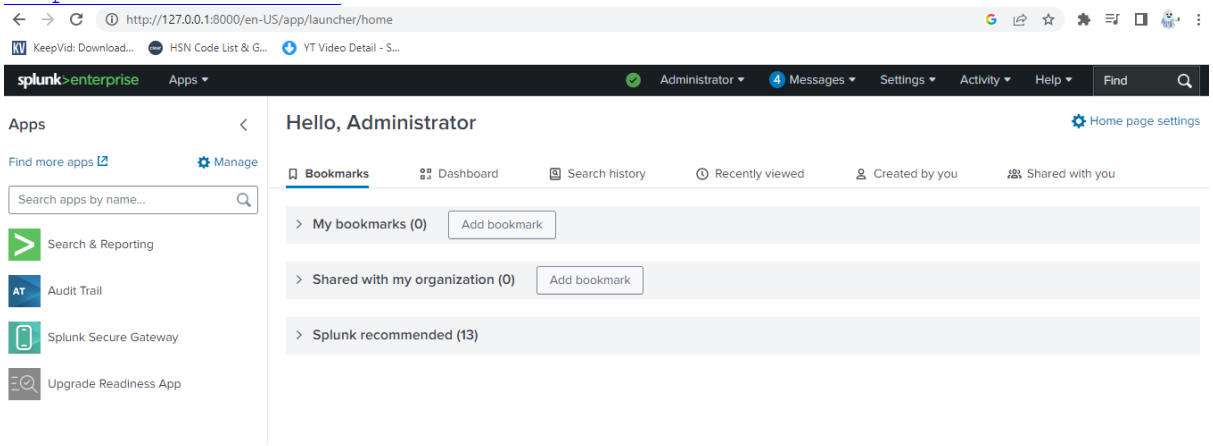
The **receiving channel** allows Splunk to **listen for incoming data** from forwarders.

Method 1: Using Splunk Web (Recommended)

Steps:

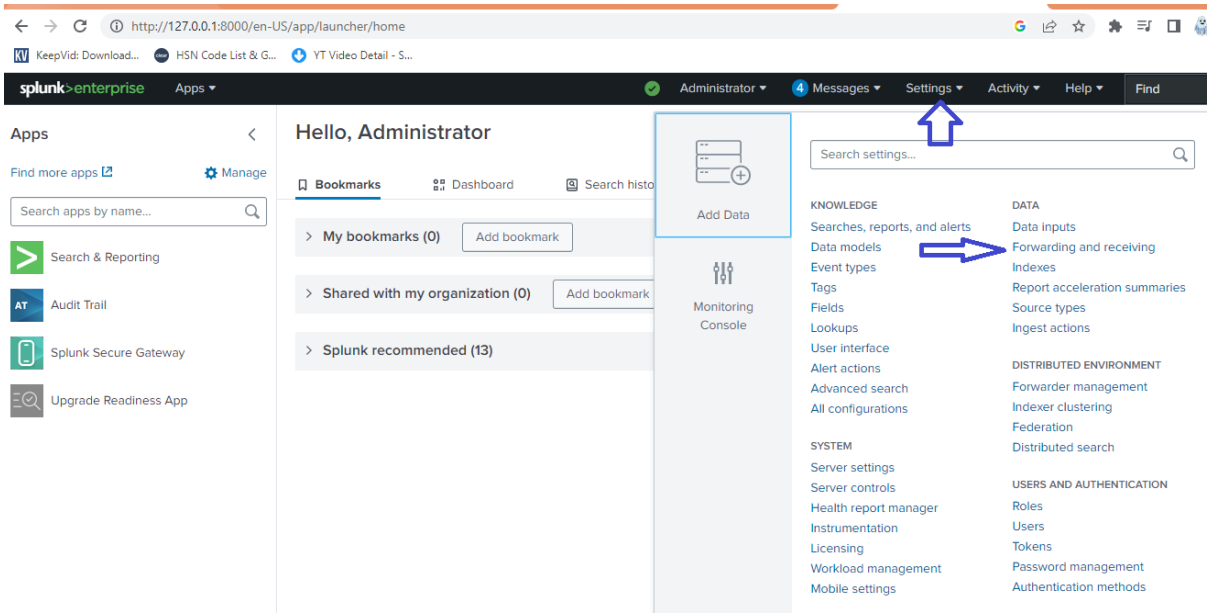
1. Log in to **Splunk Web**

http://127.0.0.1:8000

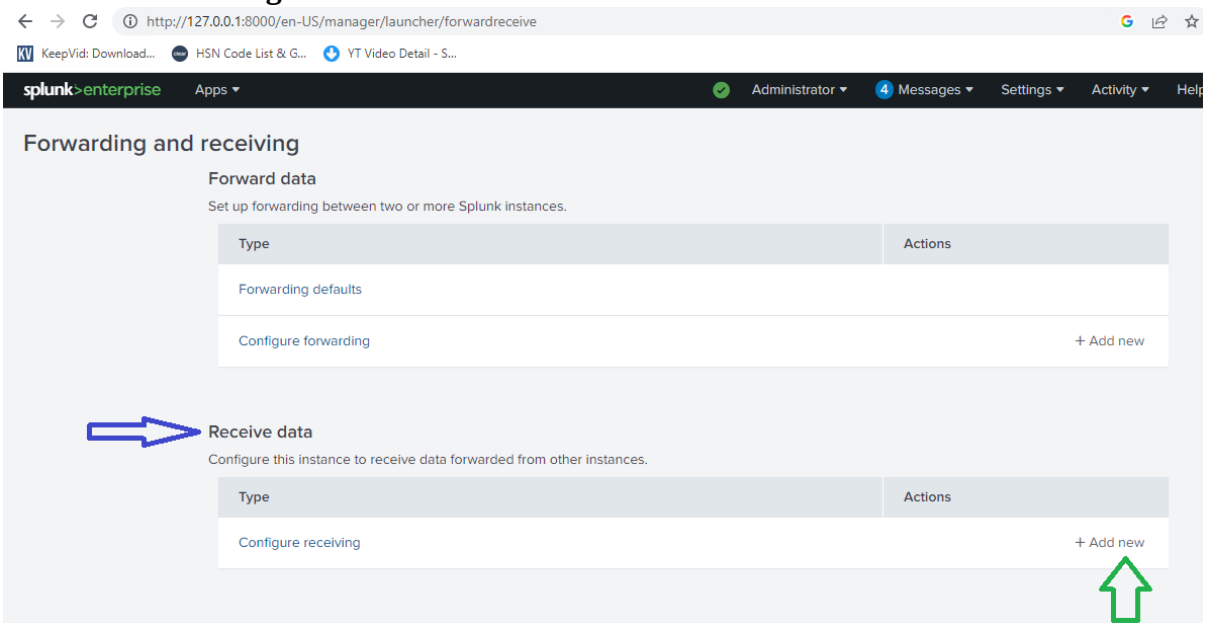


2. Go to:

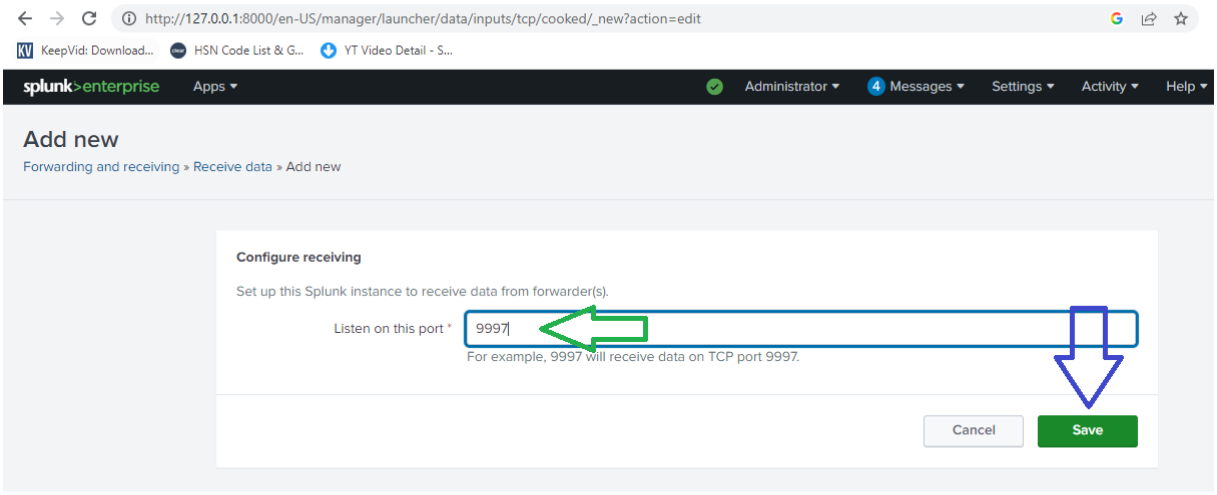
`Settings → Forwarding and Receiving → Configure Receiving`



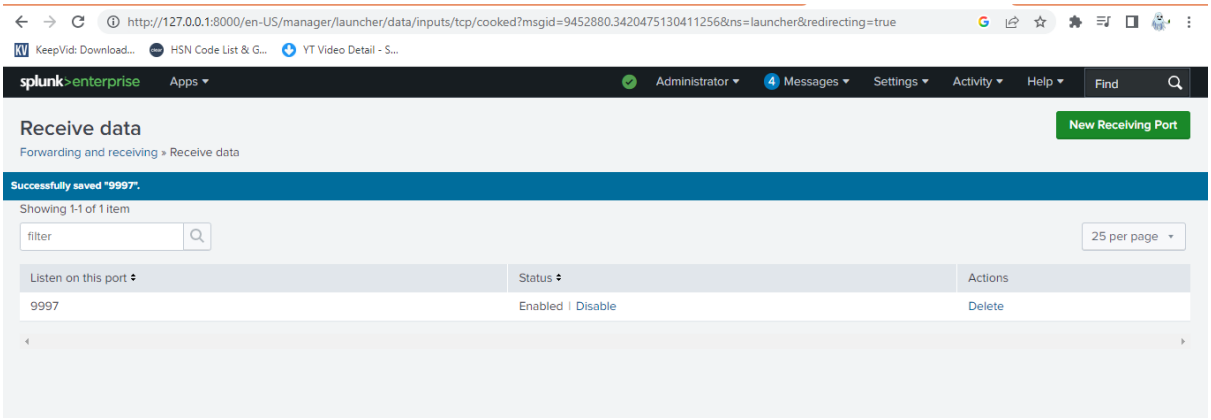
3. Click **New Receiving Port**



4. Enter the port number: 9997



5. Click **Save**

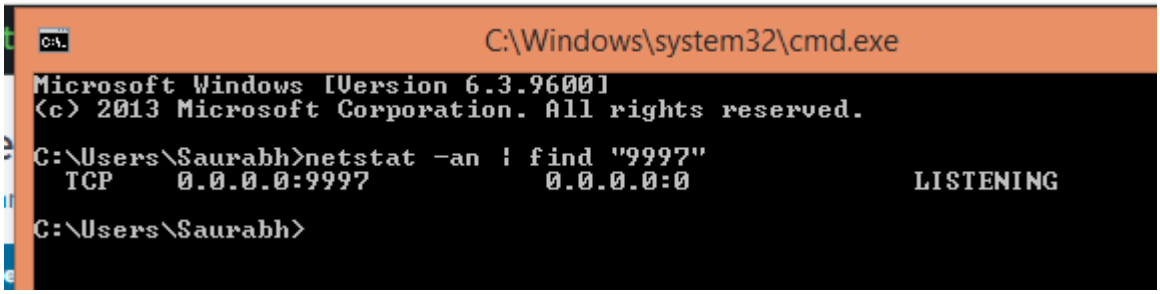


✓ Splunk Heavy Forwarded is now listening for incoming data.

Verify Receiving Port

From command prompt:

```
netstat -an | find "9997"
```



---

2. Forwarding Channel Configuration (Forwarder(Indexer) Side)

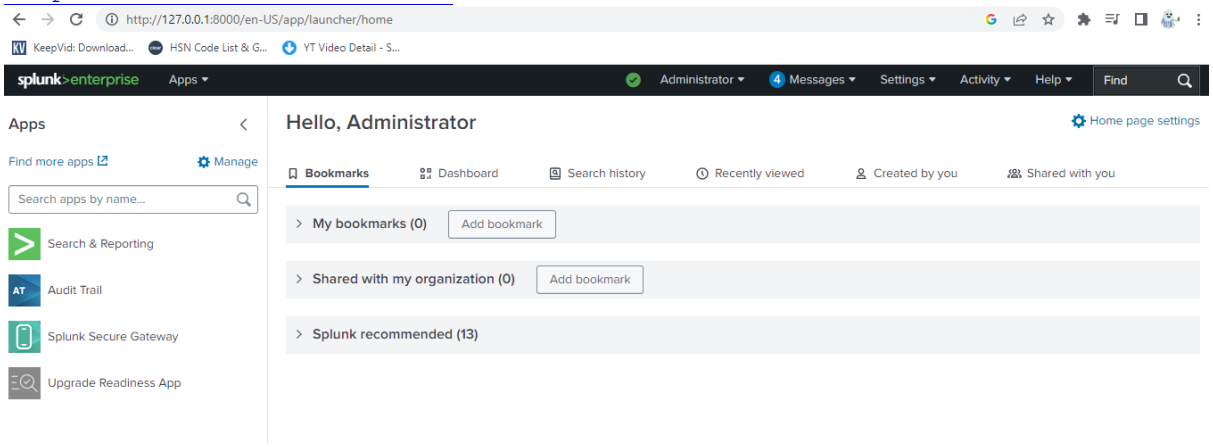
The **forwarding channel** sends data from a Heavy forwarder to the indexer.

Method 1: Using Splunk Web (Heavy Forwarder)

Steps:

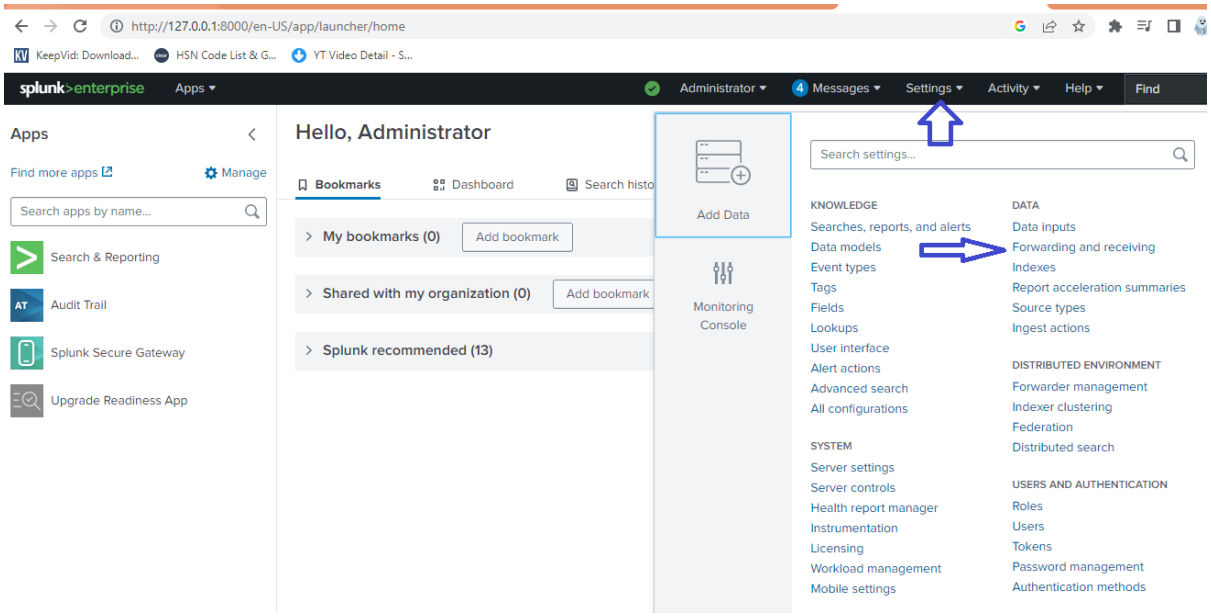
1. Log in to the **forwarder**

http://<forwarder-host>:8000

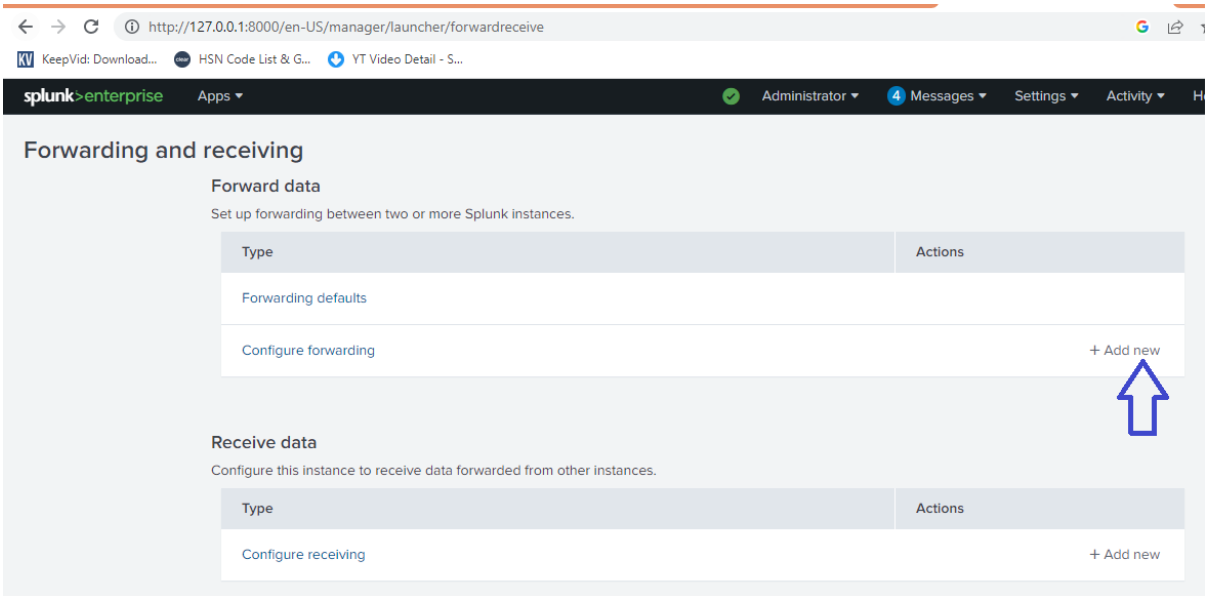


2. Go to:

`Settings → Forwarding and Receiving → Configure Forwarding`

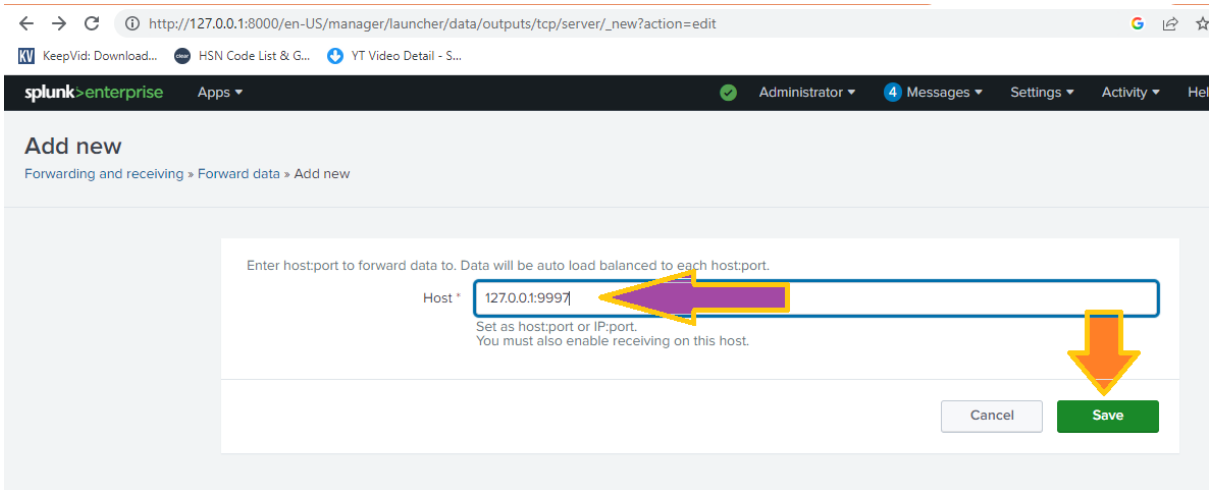


3. Click **Add New**



4. Enter Indexer details:

```
Indexer Host: <indexer-IP or hostname>
Port: 9997
```



5. Click **Save**

Indexer → Search Head communication does NOT use "forwarding & receiving (9997)".
That channel is **only for Forwarder → Indexer** data ingestion.

For **Indexer ↔ Search Head**, Splunk uses the **management/search channel (TCP 8089)** and is configured as **Search Peers**.

Configure Search Head → Indexer (Search Peer)

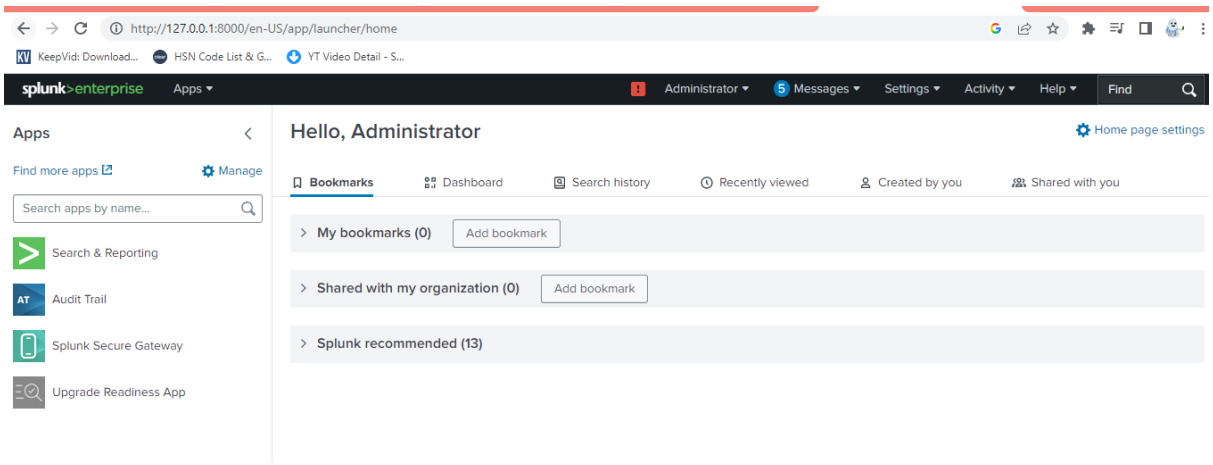
This is the **key step**.

Method 1: Using Splunk Web (Recommended)

On the Search Head

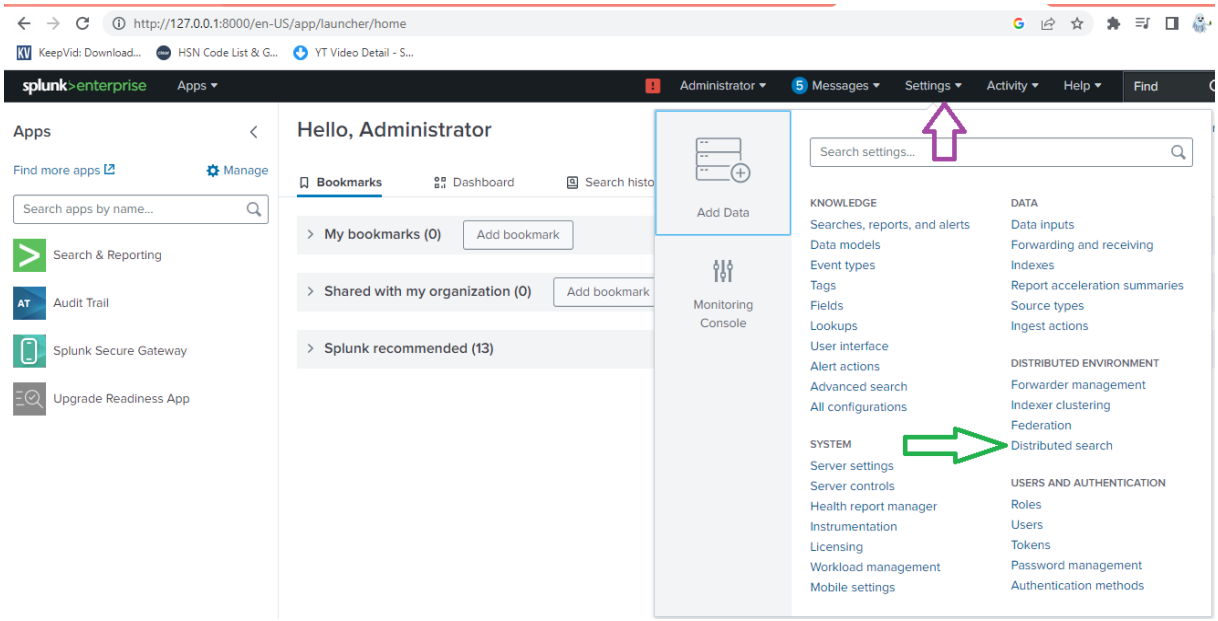
1. Log in:

http://<127.0.0.1>:8000

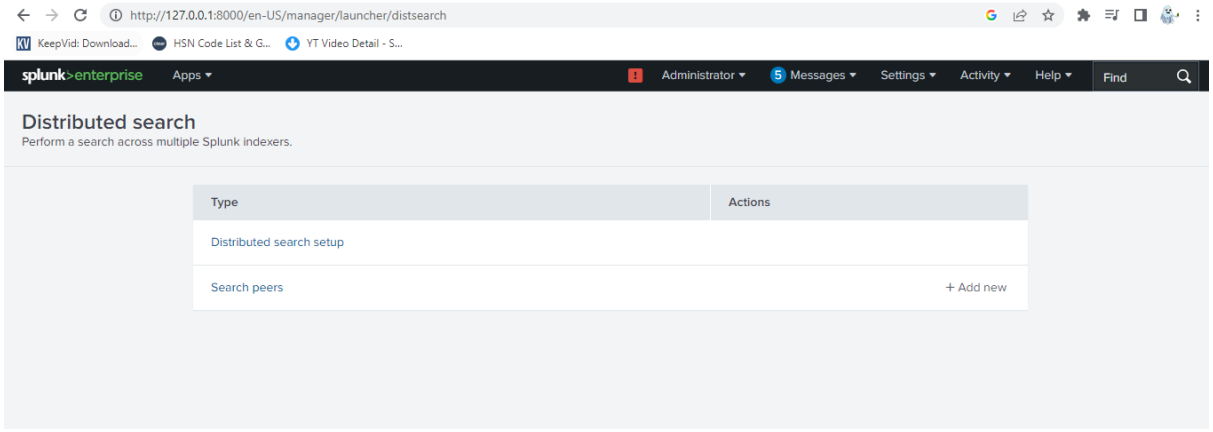


2. Navigate to:

`Settings → Distributed Search → Search Peers`



3. Click **Add New**



4. Enter:

```
Peer URI: https://<indexer-ip>:8089
Remote Username: admin
Remote Password: <indexer-admin-password>
```

5. Click **Save**

✓ Indexer is now a **search peer**