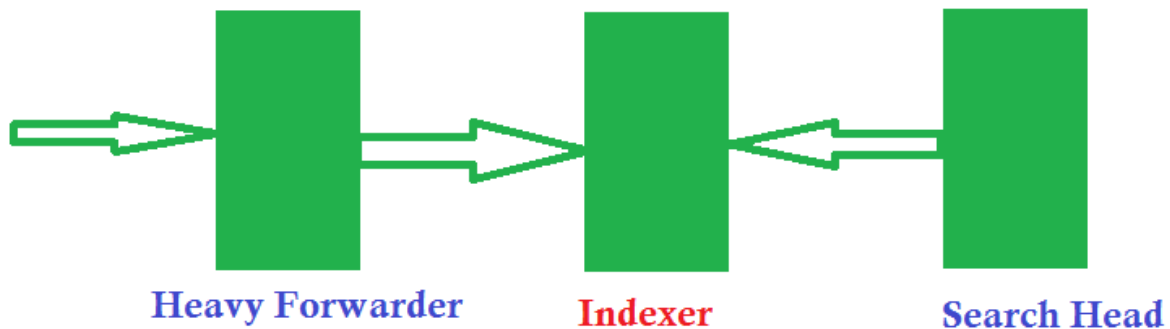


# Configurations of Receiving and Forwarding Channel in Splunk Enterprise 9.4.7 on Windows



## Receiving Channel Configuration (Indexer Side)

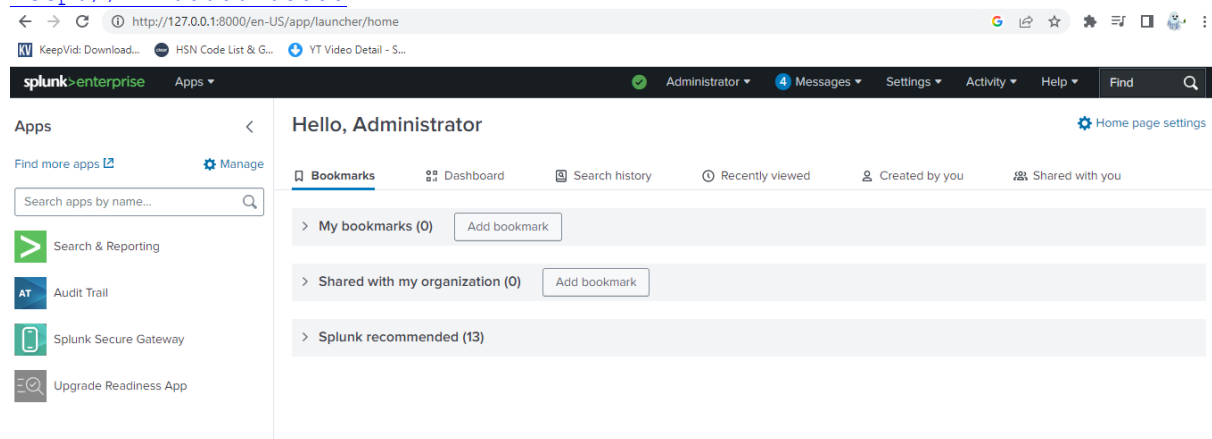
The **receiving channel** allows Splunk to **listen for incoming data** from forwarders.

## Method 1: Using Splunk Web (Recommended)

Steps:

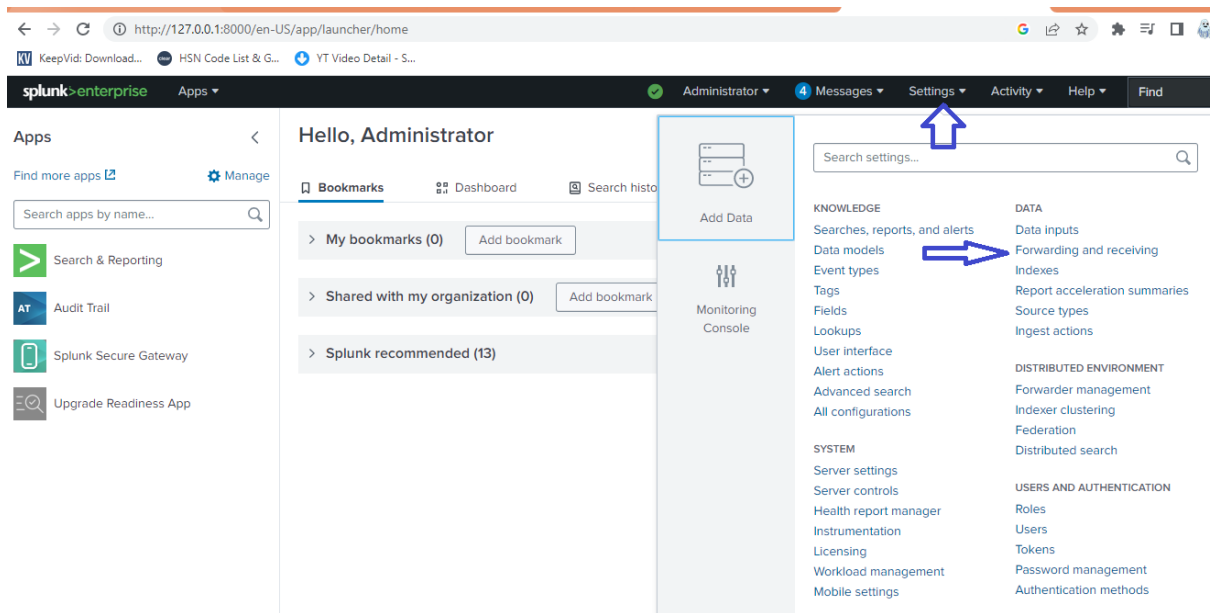
1. Log in to **Splunk Web**

<http://127.0.0.1:8000>

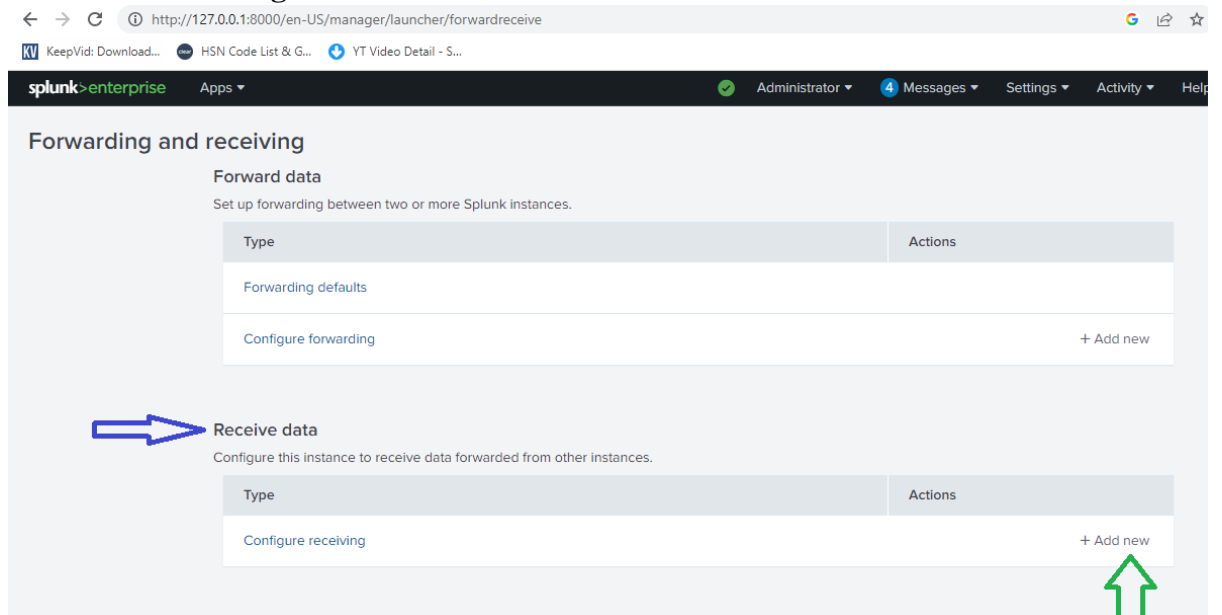


2. Go to:

Settings → Forwarding and Receiving → Configure Receiving



### 3. Click New Receiving Port



#### 4. Enter the port number: 9997

← → ↻ http://127.0.0.1:8000/en-US/manager/launcher/data/inputs/tcp/cooked/\_new?action=edit

splunk>enterprise Apps Administrator 4 Messages Settings Activity Help

Add new  
Forwarding and receiving » Receive data » Add new

**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

#### 5. Click Save

← → ↻ http://127.0.0.1:8000/en-US/manager/launcher/data/inputs/tcp/cooked?msgid=9452880.3420475130411256&ns=launcher&redirecting=true

splunk>enterprise Apps Administrator 4 Messages Settings Activity Help Find

Receive data  
Forwarding and receiving » Receive data

New Receiving Port

Successfully saved "9997".  
Showing 1-1 of 1 item

filter 25 per page

Listen on this port	Status	Actions
9997	Enabled   Disable	Delete

✓ Splunk Heavy Forwarded is now listening for incoming data.

## Verify Receiving Port

From command prompt:

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

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Saurabh>netstat -an | find "9997"
TCP      0.0.0.0:9997      0.0.0.0:0        LISTENING

C:\Users\Saurabh>
```

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

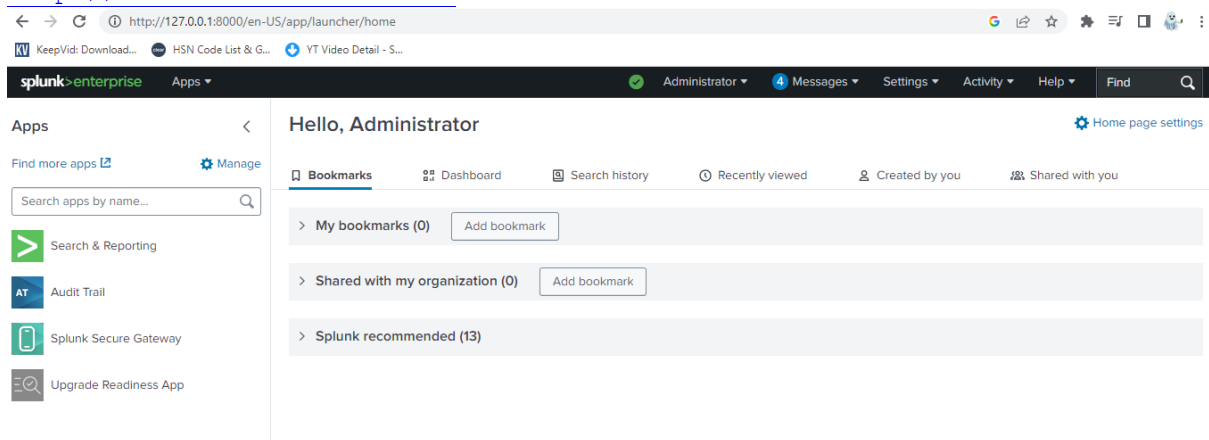
The **forwarding channel** sends data from a Heavy forwarder to the indexer.

## Method 1: Using Splunk Web (Heavy Forwarder)

Steps:

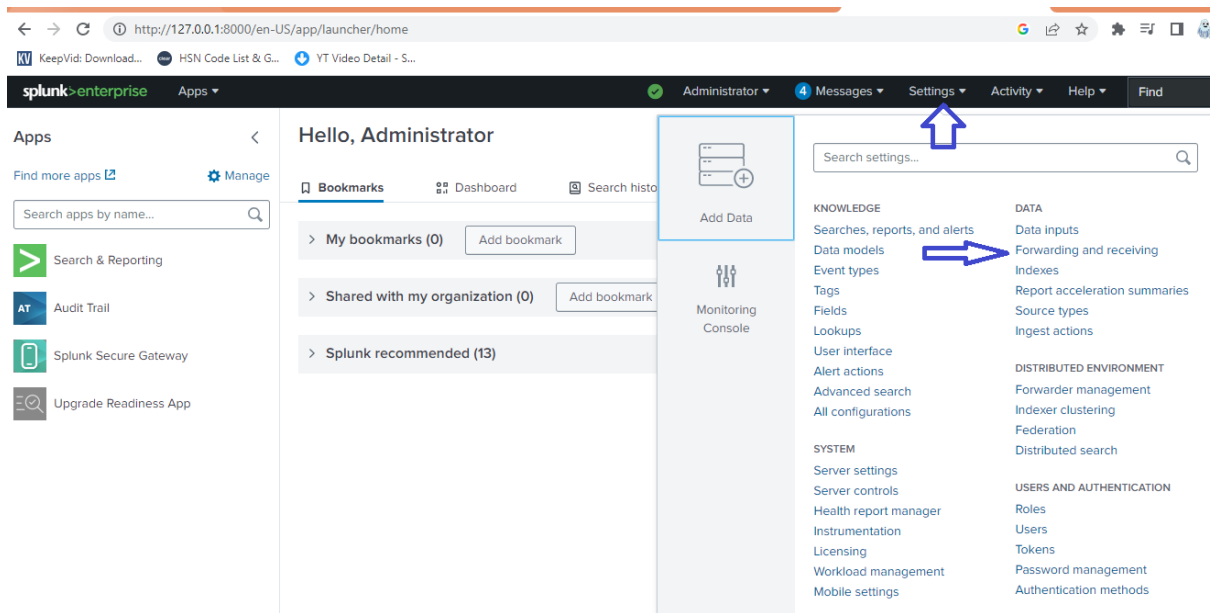
1. Log in to the **forwarder**

<http://<forwarder-host>:8000>

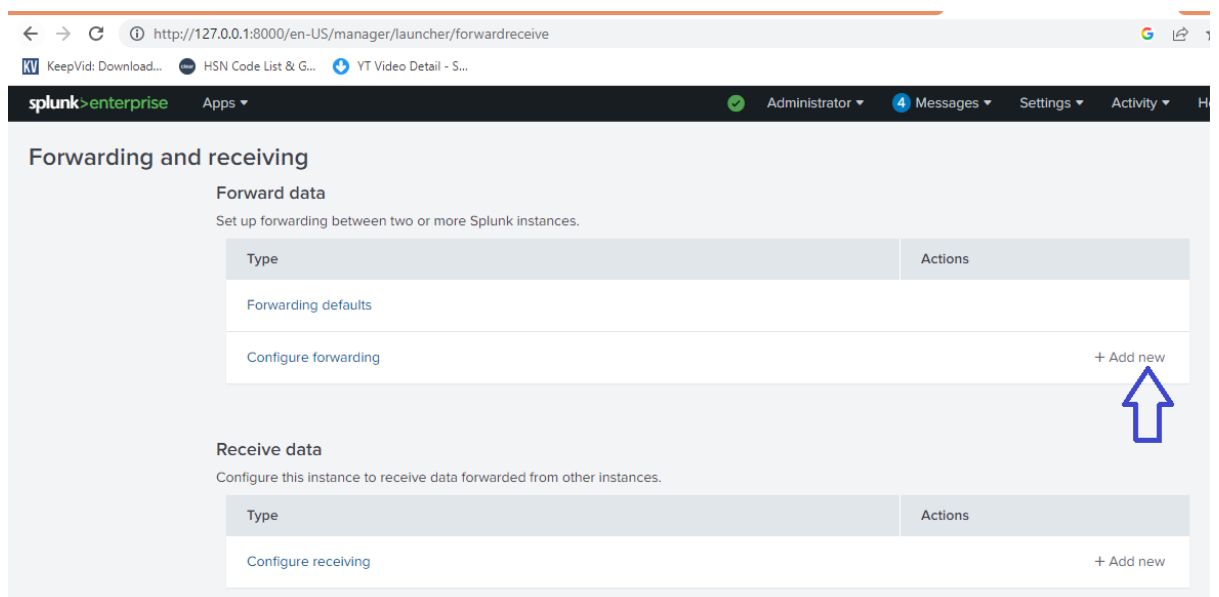


2. Go to:

Settings → Forwarding and Receiving → Configure Forwarding



### 3. Click Add New



### 4. Enter Indexer details:

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

http://127.0.0.1:8000/en-US/manager/launcher/data/outputs/tcp/server/\_new?action=edit

splunk>enterprise Apps Administrator 4 Messages Settings Activity Hel

Add new  
Forwarding and receiving > Forward data > Add new

Enter host:port to forward data to. Data will be auto load balanced to each host:port.

Host \* 127.0.0.1:9997  
Set as host:port or IP:port.  
You must also enable receiving on this host.

Cancel Save

## 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**.

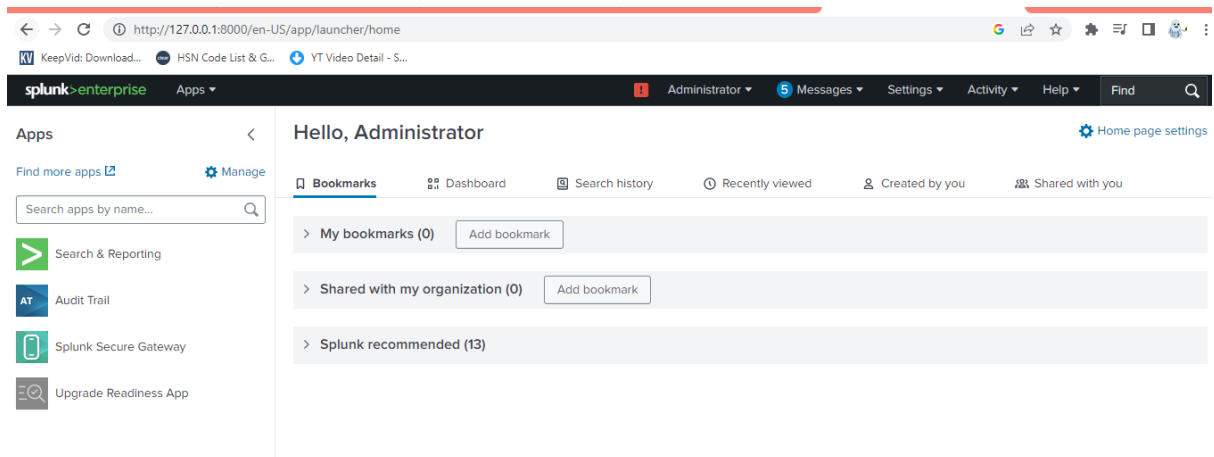
---

## Method 1: Using Splunk Web (Recommended)

On the Search Head

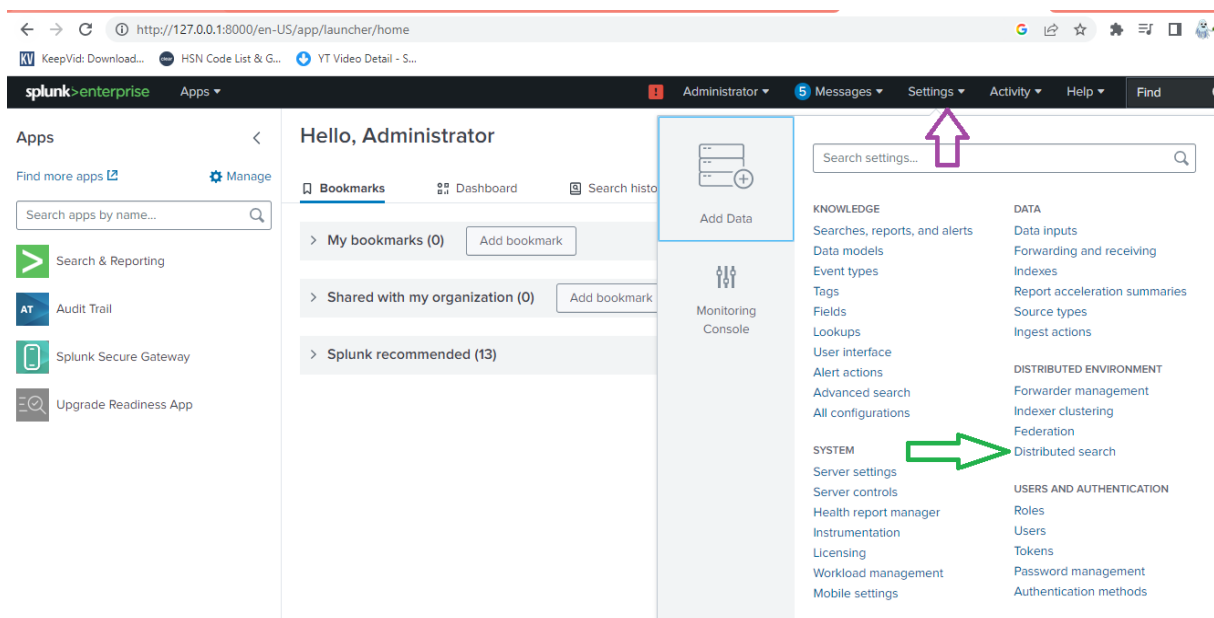
### 1. Log in:

<http://<127.0.0.1>:8000>

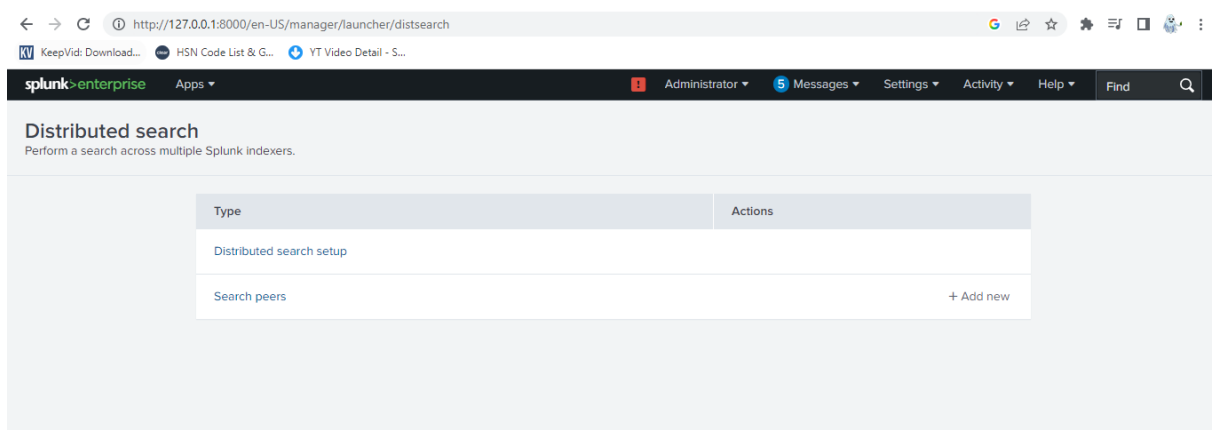


## 2. Navigate to:

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**

The screenshot shows the 'Add new' page in the Splunk Enterprise web interface. The breadcrumb trail is 'Distributed search > Search peers > Add new'. The page title is 'Add search peers'. Below the title, there is a text box for 'Peer URI \*' which is currently empty. A tooltip below the text box reads: 'Specify the search peer as servername:mgmt\_port or URI:mgmt\_port. You must prefix the URI with its scheme. For example: 'https://sp1.example.com:8089'.' Below this, there is a section for 'Distributed search authentication' with three text boxes: 'Remote username \*' containing 'saurabh', 'Remote password \*' containing '\*\*\*\*\*', and 'Confirm password' which is empty. At the bottom right of the form are 'Cancel' and 'Save' buttons.

This screenshot is similar to the one above but includes annotations. A yellow arrow points to the 'Peer URI \*' text box, which now contains the value '127.0.0.1:8089'. Another yellow arrow points to the 'Save' button at the bottom right of the form. The rest of the form, including the 'Distributed search authentication' section, remains the same as in the previous screenshot.