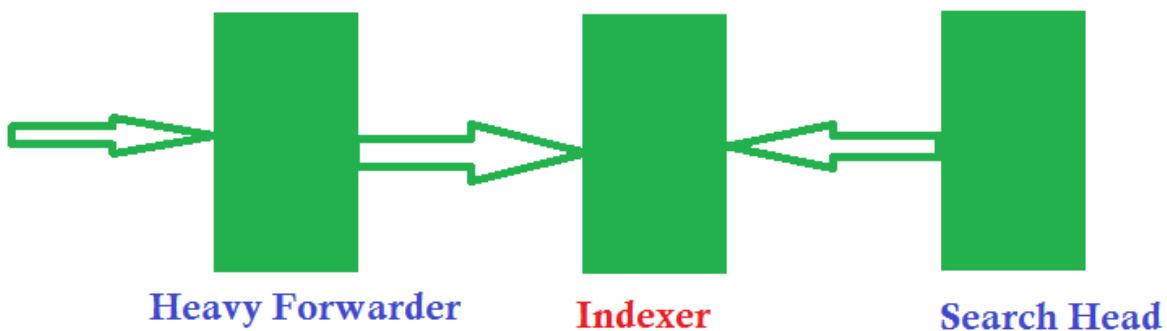


# Configurations of Receiving and Forwarding Channel in Splunk Enterprise

## 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**

The screenshot shows the Splunk Web interface with the URL <http://127.0.0.1:8000>. The top navigation bar includes links for KeepVid: Download..., HSN Code List & G..., YT Video Detail - S..., and a search bar. The main menu bar has items for Administrator, Messages, Settings, Activity, Help, Find, and a magnifying glass icon. On the left, there's a sidebar with 'Apps' and a search bar. The main content area displays 'Hello, Administrator' and a 'Bookmarks' section with three categories: 'My bookmarks (0)', 'Shared with my organization (0)', and 'Splunk recommended (13)'. Each category has an 'Add bookmark' button.

2. Go to:

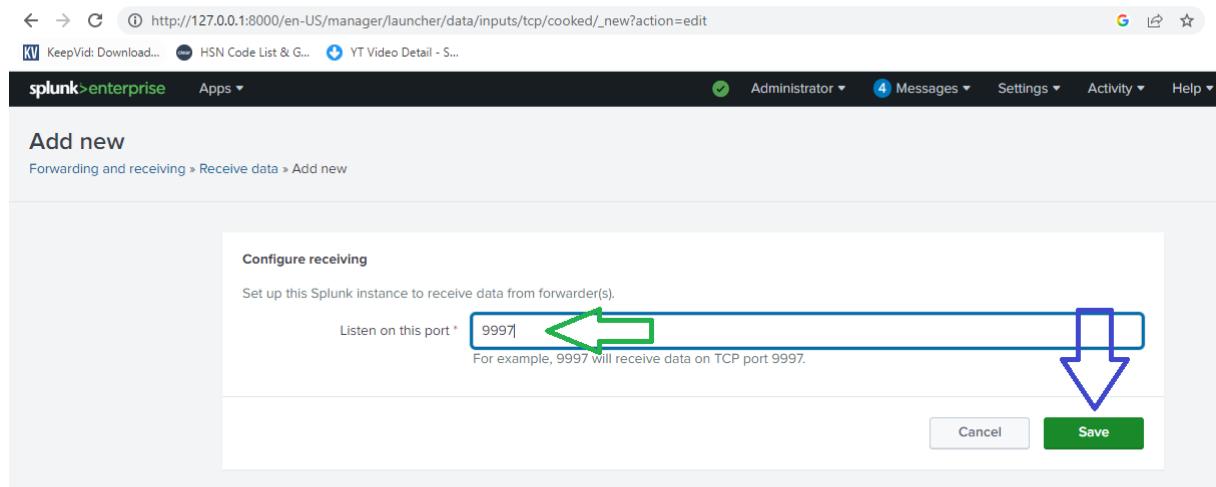
Settings → Forwarding and Receiving → Configure Receiving

The screenshot shows the Splunk Enterprise home page. At the top, there's a navigation bar with links for 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below the navigation bar is a search bar labeled 'Search settings...'. To the left, there's a sidebar titled 'Hello, Administrator' with sections for 'Bookmarks', 'Dashboard', and 'Search history'. Under 'Bookmarks', there are three categories: 'My bookmarks (0)', 'Shared with my organization (0)', and 'Splunk recommended (13)'. On the right side, there's a large panel divided into two columns. The left column is titled 'KNOWLEDGE' and includes links for 'Searches, reports, and alerts', 'Data models', 'Monitoring Console', 'Event types', 'Tags', 'Fields', 'Lookups', 'User interface', 'Alert actions', 'Advanced search', and 'All configurations'. The right column is titled 'DATA' and includes links for 'Data inputs', 'Forwarding and receiving', 'Indexes', 'Report acceleration summaries', 'Source types', 'Ingest actions', 'DISTRIBUTED ENVIRONMENT', 'Forwarder management', 'Indexer clustering', 'Federation', 'Distributed search', 'SYSTEM', 'Server settings', 'Server controls', 'Health report manager', 'Instrumentation', 'Licensing', 'Workload management', 'Mobile settings', 'USERS AND AUTHENTICATION', 'Roles', 'Users', 'Tokens', 'Password management', and 'Authentication methods'. Two blue arrows point from the text below to specific sections: one to 'Forwarding and receiving' in the KNOWLEDGE column and another to 'Receive data' in the DATA column.

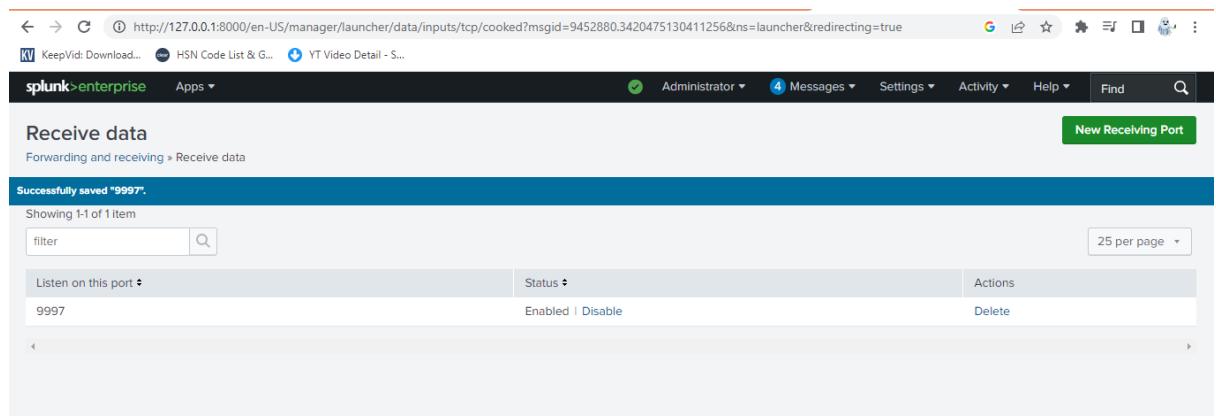
### 3. Click New Receiving Port

The screenshot shows the 'Forwarding and receiving' configuration page. At the top, there's a header with 'Administrator', 'Messages', 'Settings', 'Activity', and 'Help'. Below the header, there are two main sections: 'Forward data' and 'Receive data'. The 'Forward data' section is titled 'Forward data' and has a sub-section 'Forwarding defaults'. The 'Receive data' section is titled 'Receive data' and has a sub-section 'Configure receiving'. Both sections have a 'Type' column and an 'Actions' column. A blue arrow points to the 'Receive data' section, and a green arrow points to the 'Actions' column in the 'Receive data' section.

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"
```

```
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**

The screenshot shows the Splunk Web interface for a user named 'Administrator'. The top navigation bar includes links for 'Messages' (4 notifications), 'Settings', 'Activity', 'Help', and a search bar. On the left, there's a sidebar titled 'Apps' with options like 'Search & Reporting', 'Audit Trail', 'Splunk Secure Gateway', and 'Upgrade Readiness App'. The main content area displays a 'Hello, Administrator' message and sections for 'Bookmarks', 'Dashboard', 'Search history', 'Recently viewed', 'Created by you', and 'Shared with you'. There are also buttons for 'Add bookmark' and 'Add to dashboard'.

2. Go to:

Settings → Forwarding and Receiving → Configure Forwarding

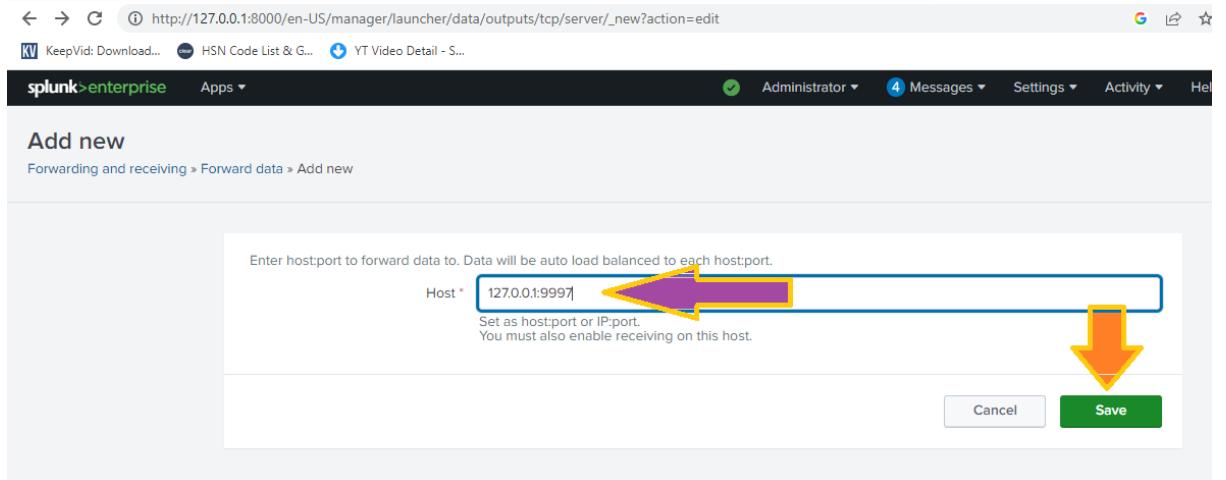
The screenshot shows the Splunk Enterprise home page. On the left, there's a sidebar with 'Apps' and a search bar. The main area has a title 'Hello, Administrator' and a 'Bookmarks' section with three categories: 'My bookmarks (0)', 'Shared with my organization (0)', and 'Splunk recommended (13)'. To the right is a large navigation menu with several sections: 'KNOWLEDGE' (Searches, reports, and alerts; Data models), 'DATA' (Data inputs; Forwarding and receiving), 'MONITORING CONSOLE' (Monitoring Console), 'SYSTEM' (Server settings; Health report manager; Instrumentation; Licensing; Workload management; Mobile settings), 'DISTRIBUTED ENVIRONMENT' (Forwarder management; Indexer clustering; Federation; Distributed search), and 'USERS AND AUTHENTICATION' (Roles; Users; Tokens; Password management; Authentication methods). Two blue arrows point to the 'Forwarding and receiving' link under the DATA section and the '+ Add new' button at the bottom of the 'Forward data' table.

### 3. Click Add New

The screenshot shows the 'Forwarding and receiving' configuration page. It has two main sections: 'Forward data' and 'Receive data'. The 'Forward data' section is titled 'Forward data' and says 'Set up forwarding between two or more Splunk instances.' It contains a table with one row for 'Forwarding defaults'. The 'Receive data' section is titled 'Receive data' and says 'Configure this instance to receive data forwarded from other instances.' It contains a table with one row for 'Configure receiving'. Both tables have a '+ Add new' button at the bottom right. A blue arrow points to the '+ Add new' button in the 'Forward data' section.

### 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>

The screenshot shows the Splunk Enterprise home page with the URL <http://127.0.0.1:8000/en-US/app/launcher/home>. The top navigation bar includes links for KeepVid: Download..., HSN Code List & G..., YT Video Detail - S..., Administrator, Messages, Settings, Activity, Help, and Find. The main content area displays a "Hello, Administrator" message and a "Bookmarks" section. The "Bookmarks" tab is selected, showing three categories: "My bookmarks (0)", "Shared with my organization (0)", and "Splunk recommended (13)". Each category has an "Add bookmark" button. Below the categories, there is a search bar labeled "Search apps by name..." and a sidebar with links to various Splunk apps like Search & Reporting, Audit Trail, Splunk Secure Gateway, and Upgrade Readiness App.

## 2. Navigate to:

Settings → Distributed Search → Search Peers

The screenshot shows the Splunk Enterprise home page with the URL <http://127.0.0.1:8000/en-US/app/launcher/home>. The top navigation bar includes links for KeepVid: Download..., HSN Code List & G..., YT Video Detail - S..., Administrator, Messages, Settings, Activity, Help, and Find. The main content area displays a "Hello, Administrator" message and a "Bookmarks" section. A large blue callout box highlights the "Search settings..." search bar at the top right. To the right of the search bar is a sidebar with several sections: KNOWLEDGE (Searches, reports, and alerts, Data models, Event types, Tags, Fields, Lookups, User interface, Alert actions, Advanced search, All configurations), DATA (Data inputs, Forwarding and receiving, Indexes, Report acceleration summaries, Source types, Ingest actions), DISTRIBUTED ENVIRONMENT (Forwarder management, Indexer clustering, Federation, Distributed search), SYSTEM (Server settings, Server controls, Health report manager, Instrumentation, Licensing, Workload management, Mobile settings), and USERS AND AUTHENTICATION (Roles, Users, Tokens, Password management, Authentication methods). A green arrow points from the "Distributed search" link in the SYSTEM section to the "Distributed search" link in the sidebar.

## 3. Click Add New

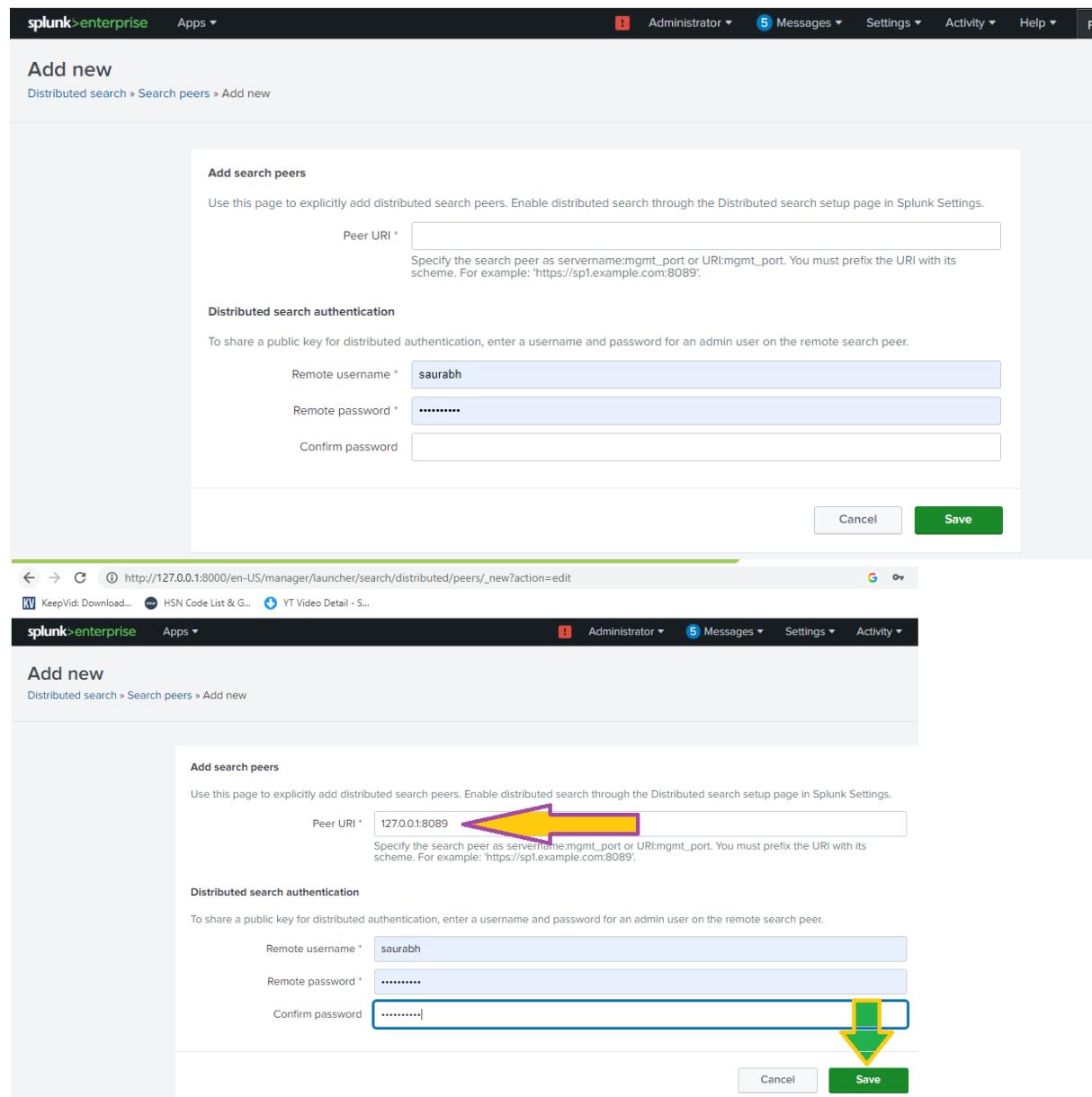
The screenshot shows the "Distributed search" setup page with the URL <http://127.0.0.1:8000/en-US/manager/launcher/distsearch>. The top navigation bar includes links for KeepVid: Download..., HSN Code List & G..., YT Video Detail - S..., Administrator, Messages, Settings, Activity, Help, and Find. The main content area displays a "Distributed search" title and a subtitle "Perform a search across multiple Splunk indexers.". Below this is a table with two rows. The first row has columns for "Type" (Distributed search setup) and "Actions". The second row has columns for "Type" (Search peers) and "Actions" (+ Add new). The table is enclosed in a light gray border.

#### 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 Splunk Enterprise interface for adding a new search peer. The top navigation bar includes 'splunk>enterprise', 'Apps', and user status ('Administrator'). Below the header, the URL is http://127.0.0.1:8000/en-US/manager/launcher/search/distributed/peers/\_new?action=edit. The page title is 'Add new' under 'Distributed search > Search peers > Add new'. The main form is titled 'Add search peers' and contains instructions: 'Use this page to explicitly add distributed search peers. Enable distributed search through the Distributed search setup page in Splunk Settings.' It has two sections: 'Peer URI' (containing 'https://127.0.0.1:8089') and 'Distributed search authentication' (with fields for 'Remote username' (saurabh), 'Remote password' (redacted), and 'Confirm password' (redacted)). At the bottom are 'Cancel' and 'Save' buttons, with the 'Save' button highlighted by a yellow arrow.