Table of Content

Installing Splunk Enterprise on Windows

Step 1 Download the Installer

- Download the latest Splunk Enterprise MSI installer from the Splunk Download Page.

Step 2 Start the Installer

- Double-click the `splunk.msi` file to launch the installer.
- Accept the License Agreement to proceed.

Step 3 Installation Options

The installer provides two options:

1. Default Installation:

- Installs to `C:\Program Files\Splunk`
- Uses default network ports
- Runs as the Local System user
- Prompts for an admin password
- Creates a Start Menu shortcut

2. Custom Installation:

- Allows specifying an installation path
- Configures a different user account for running Splunk
- Adjusts additional settings

Step 4 Choose Installation Location

- By default, Splunk installs to `C:\Program Files\Splunk`.
- Click **Change...** to specify a different path if needed.

Step 5 Choose the User for Splunk

- The installer prompts for a user.
- Select either **Local System** or a specific user in `DOMAIN\Username` format.
- Ensure the user has administrative privileges.

Step 6 Set Up Splunk Admin Credentials

- Create a Splunk administrator account by entering a username and password.
- These credentials are used for logging into Splunk Enterprise.

Step 7 Begin Installation

- Review the installation summary.
- Click **Install** to start the installation process.

Step 8 Complete the Installation

- After installation, check the options to:
    - **Launch Splunk in Browser**
    - **Create Start Menu Shortcut**
- Click **Finish** to complete the setup.

Installing Splunk in a Docker Environment

- **Prerequisites**
- **Running Splunk in Docker**

Prerequisites

The current Splunk Docker image supports the **Docker runtime engine** and requires the following system prerequisites:

Operating System & Chipset Requirements

- **Linux-based OS** (Debian, CentOS, etc.)
- **Supported Chipsets**:
    - `splunk/splunk` image: **x86-64**
    - `splunk/universalforwarder` image: **x86-64** and **s390x**

System & Software Requirements

- **Kernel Version**: > 4.0
- **Docker Engine**:
    - **Docker Enterprise Engine**: 17.06.2 or later
    - **Docker Community Engine**: 17.06.2 or later

- **Docker Storage Driver**: `overlay2`

For more details, refer to Splunk's official documentation on **supported architectures and platforms** for containerized environments and **hardware capacity recommendations**.

Running Splunk in Docker

Step 1: Download the Universal Forwarder Image

Pull the latest Splunk Universal Forwarder image from Docker Hub:

```
docker pull splunk/splunk:latest
```

Step 2: Create a Docker Network

To enable communication between the Splunk Enterprise instance and the Universal Forwarder, create a custom bridge network:

```
docker network create splunk-net
```

Step 2: Start a Splunk Container

Run the following command to start a single instance of the Splunk Universal Forwarder:

```
docker run -d --network splunk-net -p 8000:8000 -p 8088:8088 -e
"SPLUNK_START_ARGS=--accept-license" -e "SPLUNK_PASSWORD=<password>" --name splunk
splunk/splunk:latest
```

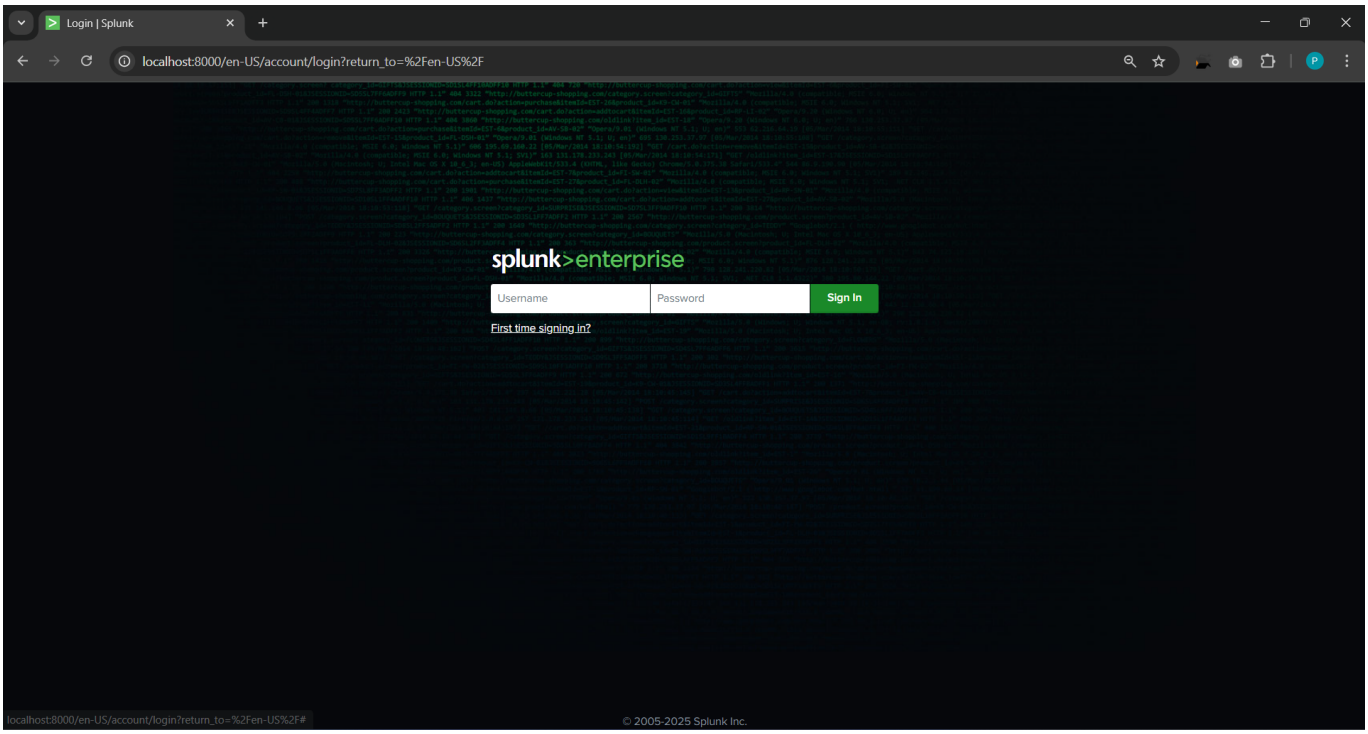
Command Breakdown

- `docker run -d`: Runs the container in **detached mode**.
- `-p 8000:8000`: Maps port **8000 on the host** to **8000 in the container**.
- `-e "SPLUNK_START_ARGS=--accept-license"`: Accepts the Splunk license agreement (required for the container to start).
- `-e "SPLUNK_PASSWORD=<password>"`: Specifies the Splunk admin password (replace `<password>` with a strong password that meets Splunk's requirements).
- `splunk/splunk:latest`: Specifies the **Splunk image** to use.

Step 3: Access Splunk Web Interface

Once the container is running and reaches the **"healthy" state**, you can access Splunk Web at:

- `http://localhost:8000`



- **Login with:**
  - **Username:** `admin`
  - **Password:** `<password>` (the value set in the `SPLUNK_PASSWORD` environment variable)

Configure Forwarders

Universal forwarders

- Universal forwarders stream data from your machine to a data receiver. Your receiver is usually a Splunk platform index where you store your data. You can use the universal forwarder to monitor your data in real time.

- Use the universal forwarder to ensure that your data is correctly formatted before sending it to Splunk. You can also manipulate your data before it reaches the indexes or manually add the data.

Benefits of the universal forwarder

Universal forwarders provide the following benefits:

- They are highly scalable
- They use significantly less hardware resources than other Splunk products
- You can install thousands of them without impacting network performance and cost
- The universal forwarder does not have a user interface, which helps minimize resource use

Step 1: Run a Docker Linux Container

Before installing Splunk Universal Forwarder, you need a running **Ubuntu-based Docker container**.

1. Start a Docker Container with Ubuntu

```
docker run -itd -p 9997:9997 --name splunk-uf --hostname splunk-uf --network
splunk-net ubuntu:latest
```

```
C:\Windows\System32> docker run -itd -p 9997:9997 --name splunk-uf --hostname splunk-uf --network splunk-net ubuntu:latest
f4523dbb9a535627b0744594d1258e686ee7eca46ce619346dda4677794b8b08
```

Explanation:

- `docker run -itd` → Runs the container in interactive, detached mode.
- `-p 9997:9997` → Maps port **9997** from the host to the container (Splunk listens on this port for forwarding logs).
- `--name splunk-uf` → Assigns the container the name **splunk-uf**.
- `--hostname splunk-uf` → Sets the container's hostname to **splunk-uf**.
- `--network splunk-net` → Connects the container to a Docker network named **splunk-net** (ensure the network exists).
- `ubuntu:latest` → Uses the **latest Ubuntu** image as the base system.

2. Access the Container's Shell

```
docker exec -it splunk-uf bash
```

```
C:\Windows\System32>docker exec -it splunk-uf bash
root@splunk-uf:/#
```

Explanation:

- `docker exec -it` → Runs a command inside an active container interactively.
- `splunk-uf` → The container name.
- `bash` → Opens a **bash shell** inside the container.

Step 2: Installing Splunk Universal Forwarder in Linux

Now that we have a **running Ubuntu environment**, follow these steps to install **Splunk Universal Forwarder (UF)**.

3. Switch to Root User

```
apt update
apt install sudo wget dpkg curl # install required packages
sudo su
```

- Logs in as the **root user** to perform administrative tasks.

4. Create a Dedicated Splunk User & Group

```
useradd -m splunkfwd
groupadd splunkfwd
```

```
root@splunk-uf:/# useradd -m splunkfwd
root@splunk-uf:/# groupadd splunkfwd
groupadd: group 'splunkfwd' already exists
root@splunk-uf:/#
```

Explanation:

- `useradd -m splunkfwd` → Creates a user named **splunkfwd** with a home directory.
- `groupadd splunkfwd` → Creates a group named **splunkfwd**.

5. Navigate to the `/opt` Directory

```
cd /opt
```

- The `/opt` directory is commonly used for installing third-party software.

6. Download the Splunk Universal Forwarder Package

```
wget -O splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64.deb
"https://download.splunk.com/products/universalforwarder/releases/9.4.1/linux/splu
nkforwarder-9.4.1-e3bdab203ac8-linux-amd64.deb"
```

```
root@splunk-uf:/opt# wget -O splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64.deb "https://download.splunk.com/products/universalforwarder/releases/9.
4.1/linux/splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64.deb"
--2025-03-19 06:08:29--  https://download.splunk.com/products/universalforwarder/releases/9.4.1/linux/splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64
.deb
Resolving download.splunk.com (download.splunk.com)... 18.161.216.73, 18.161.216.43, 18.161.216.62, ...
Connecting to download.splunk.com (download.splunk.com)|18.161.216.73|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 99029222 (94M) [binary/octet-stream]
Saving to: ‘splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64.deb’

splunkforwarder-9.4.1-e3bdab203ac8-l 100%[===================================================================>]  94.44M  10.9MB/s    in 21s

2025-03-19 06:08:51 (4.41 MB/s) - ‘splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64.deb’ saved [99029222/99029222]
```

Explanation:

- `wget` → Downloads the installation package from Splunk’s official website.
- `-O splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64.deb` → Saves the file with a specific name.

7. Install the Splunk Universal Forwarder

```
dpkg -i splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64.deb
```

```
root@splunk-uf:/opt# dpkg -i splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64.deb
(Reading database ... 18716 files and directories currently installed.)
Preparing to unpack splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64.deb ...
This looks like an upgrade of an existing Splunk Server. Checking to see what component we are installing
no need to run the pre-install check
This looks like an upgrade of an existing Splunk Server. Attempting to stop the installed Splunk Server...
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
splunkd is not running.
Unpacking splunkforwarder (9.4.1) over (9.4.1) ...
Setting up splunkforwarder (9.4.1) ...
find: ‘/opt/splunkforwarder/lib/python3.7/site-packages’: No such file or directory
find: ‘/opt/splunkforwarder/lib/python3.9/site-packages’: No such file or directory
complete
```

- `dpkg -i` installs the **Debian package** for Splunk Universal Forwarder.

8. Set the Splunk Installation Directory

```
export SPLUNK_HOME="/opt/splunkforwarder"
```

```
root@splunk-uf:/opt# export SPLUNK_HOME="/opt/splunkforwarder"
root@splunk-uf:/opt#
```

Explanation:

- `export SPLUNK_HOME="/opt/splunkforwarder"` → Defines the **Splunk home directory**.

9. Change Ownership of the Splunk Directory

```
chown -R splunkfwd:splunkfwd $SPLUNK_HOME
```

```
root@splunk-uf:/opt# chown -R splunkfwd:splunkfwd $SPLUNK_HOME
root@splunk-uf:/opt#
```

Explanation:

- `chown -R` → Changes the ownership recursively (applies to all files and folders).
- `splunkfwd:splunkfwd` → Assigns ownership to the **splunkfwd user and group**.

10. Start Splunk Universal Forwarder

```
sudo $SPLUNK_HOME/bin/splunk start --accept-license
```

```
root@splunk-uf:~# sudo $SPLUNK_HOME/bin/splunk start --accept-license
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: admin
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Creating unit file...
Error calling execve(): No such file or directory
Error launching  command: No such file or directory
Failed to create the unit file. Please do it manually later.


Splunk> The Notorious B.I.G. D.A.T.A.

Checking prerequisites...
        Checking mgmt port [8089]: open
                Creating: /opt/splunkforwarder/var/lib/splunk
                Creating: /opt/splunkforwarder/var/run/splunk
                Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n
                Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/static/css
                Creating: /opt/splunkforwarder/var/run/splunk/upload
                Creating: /opt/splunkforwarder/var/run/splunk/search_telemetry
                Creating: /opt/splunkforwarder/var/run/splunk/search_log
                Creating: /opt/splunkforwarder/var/spool/splunk
                Creating: /opt/splunkforwarder/var/spool/dirmoncache
                Creating: /opt/splunkforwarder/var/lib/splunk/authDb
                Creating: /opt/splunkforwarder/var/lib/splunk/hashDb
                Creating: /opt/splunkforwarder/var/run/splunk/collect
                Creating: /opt/splunkforwarder/var/run/splunk/sessions
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done
```

Explanation:

- `sudo` → Runs the command as **root** or **admin**.
- `$SPLUNK_HOME/bin/splunk start` → Starts the **Splunk Universal Forwarder service**.
- `--accept-license` → Automatically accepts the **Splunk license agreement** (required for first-time setup).
- you will be promted to create **username** and **password** provide same as **Splunk Administration**.

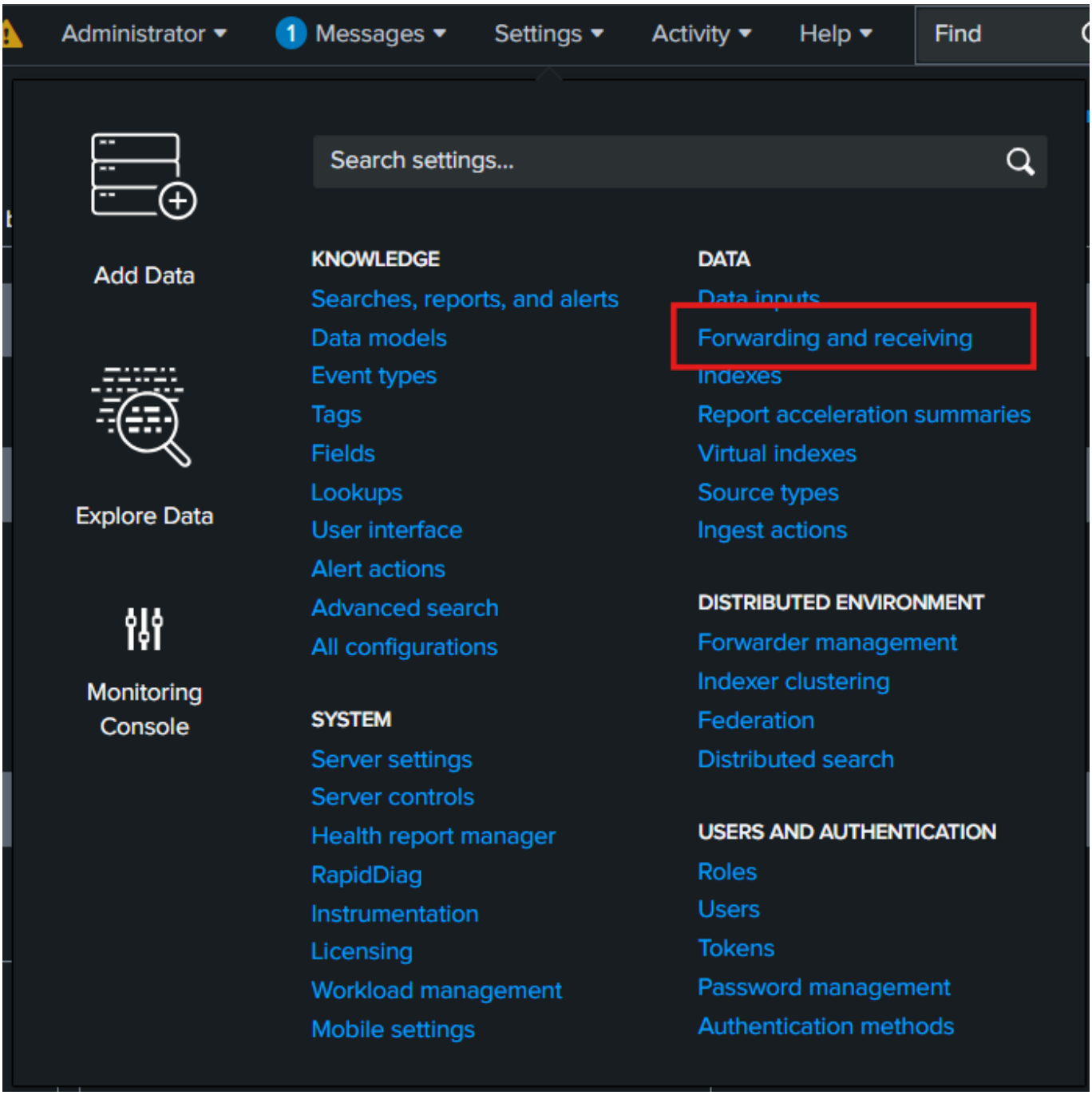
Step 3: Configure Splunk Universal Forwarder

11. Enable a Receiver on Splunk Enterprise

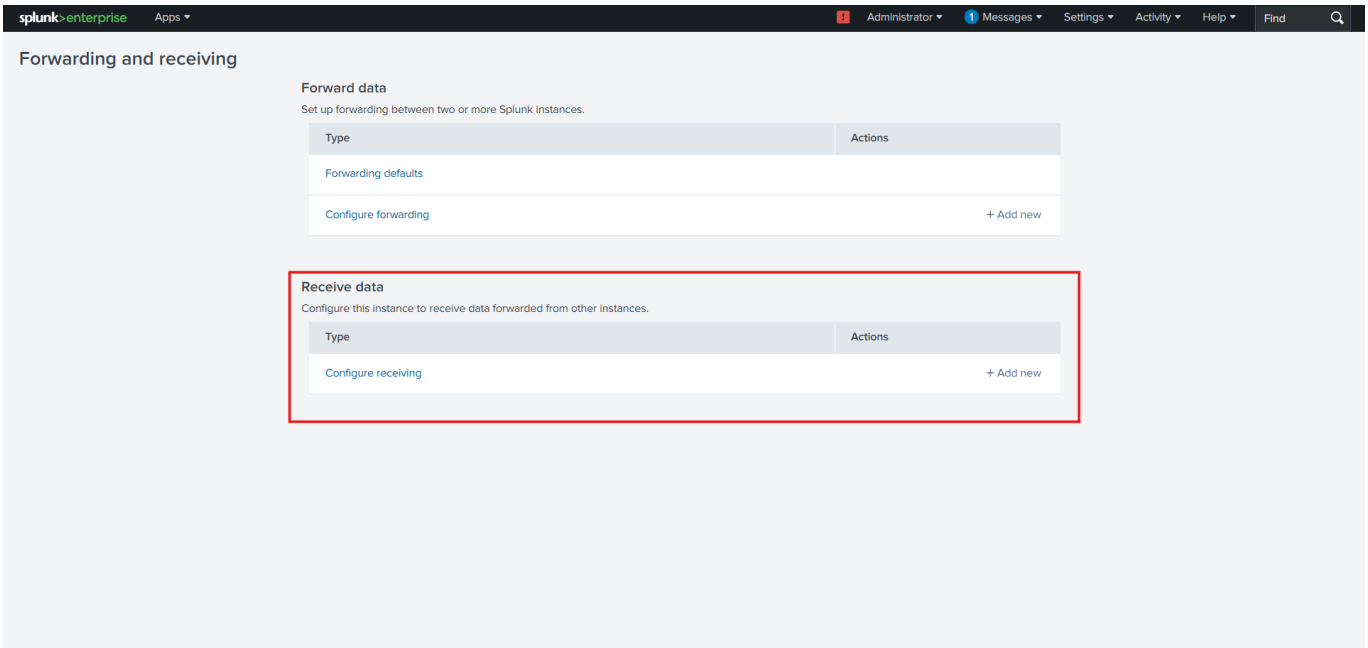
Before the Universal Forwarder can send logs, the **Splunk Enterprise instance** must be configured to receive them.

Configure a Receiver Using Splunk Web

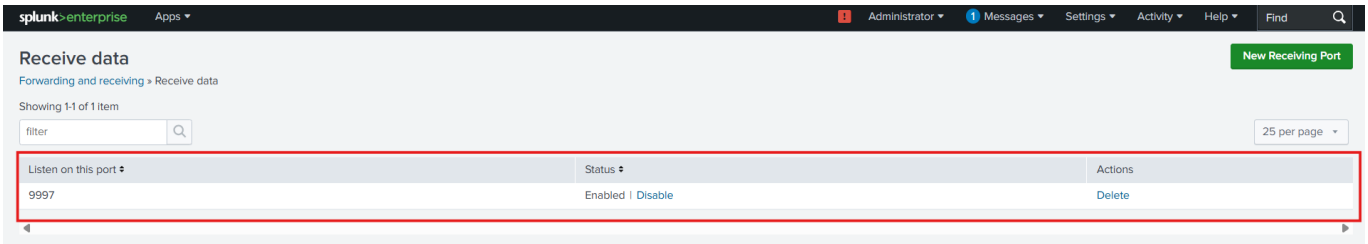
- **Log into Splunk Web** as a user with **admin** privileges.
- Navigate to **Settings > Forwarding and receiving**.



- Select "**Configure Receiving**".



- Check if any receiver ports are **already open** (to avoid conflicts).
  - The **default receiver port** for Splunk indexers is **9997**.
- (Optional) If no port is set, click **"New Receiving Port"**.
- Add **port 9997**, then **Save** the changes.
- Make the **port 9997** is **Enabled**.



12. Configure Universal Forwarder to Send Logs

Now, configure the **forward-server** to send logs from the Universal Forwarder to Splunk Enterprise.

Add a Forward-Server

Run the following command inside the Universal Forwarder container:

```
/opt/splunkforwarder/bin/splunk add forward-server splunk:9997
```

```
root@splunk-uf:~# /opt/splunkforwarder/bin/splunk add forward-server splunk:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Splunk username: admin
Password:
Added forwarding to: splunk:9997.
```

Explanation:

- `splunk` → The hostname of the **Splunk Enterprise container** (inside the **Docker network splunk-net**).
- `9997` → The **default receiving port** for Universal Forwarders.

Verify the forward-server list:

```
/opt/splunkforwarder/bin/splunk list forward-server
```

```
root@splunk-uf:~# /opt/splunkforwarder/bin/splunk list forward-server
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Active forwards:
        splunk:9997
Configured but inactive forwards:
        None
```

If configured correctly, you should see:

```
Active forwards:
   splunk:9997
```

13. Configure Data Inputs

To specify which logs the **Universal Forwarder** should monitor, add a **data input**:

```
/opt/splunkforwarder/bin/splunk add monitor /var/log
```

```
root@splunk-uf:~# /opt/splunkforwarder/bin/splunk add monitor /var/log
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added monitor of '/var/log'.
root@splunk-uf:~#
```

Explanation:

- `/var/log` → Common system logs directory (adjust this based on your needs).

Verify the monitored inputs:

```
/opt/splunkforwarder/bin/splunk list monitor
```

```
root@splunk-uf:~# /opt/splunkforwarder/bin/splunk list monitor
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Monitored Directories:
        $SPLUNK_HOME/var/log/splunk
                /opt/splunkforwarder/var/log/splunk/audit.log
                /opt/splunkforwarder/var/log/splunk/audit_v2.log
                /opt/splunkforwarder/var/log/splunk/btool.log
                /opt/splunkforwarder/var/log/splunk/conf.log
                /opt/splunkforwarder/var/log/splunk/first_install.log
                /opt/splunkforwarder/var/log/splunk/health.log
                /opt/splunkforwarder/var/log/splunk/license_usage.log
                /opt/splunkforwarder/var/log/splunk/mergebuckets.log
                /opt/splunkforwarder/var/log/splunk/mongod.log
                /opt/splunkforwarder/var/log/splunk/mongod_upgrade.log
                /opt/splunkforwarder/var/log/splunk/remote_searches.log
                /opt/splunkforwarder/var/log/splunk/scheduler.log
                /opt/splunkforwarder/var/log/splunk/search_messages.log
                /opt/splunkforwarder/var/log/splunk/searchhistory.log
                /opt/splunkforwarder/var/log/splunk/splunkd-utility.log
                /opt/splunkforwarder/var/log/splunk/splunkd_access.log
                /opt/splunkforwarder/var/log/splunk/splunkd_stderr.log
                /opt/splunkforwarder/var/log/splunk/splunkd_stdout.log
                /opt/splunkforwarder/var/log/splunk/splunkd_ui_access.log
                /opt/splunkforwarder/var/log/splunk/wlm_monitor.log
        $SPLUNK_HOME/var/log/splunk/configuration_change.log
                /opt/splunkforwarder/var/log/splunk/configuration_change.log
        $SPLUNK_HOME/var/log/splunk/license_usage_summary.log
                /opt/splunkforwarder/var/log/splunk/license_usage_summary.log
        $SPLUNK_HOME/var/log/splunk/metrics.log
                /opt/splunkforwarder/var/log/splunk/metrics.log
        $SPLUNK_HOME/var/log/splunk/splunk_instrumentation_cloud.log*
                /opt/splunkforwarder/var/log/splunk/splunk_instrumentation_cloud.log
        $SPLUNK_HOME/var/log/splunk/splunkd.log
                /opt/splunkforwarder/var/log/splunk/splunkd.log
        $SPLUNK_HOME/var/log/watchdog/watchdog.log*
                /opt/splunkforwarder/var/log/watchdog/watchdog.log
        $SPLUNK_HOME/var/run/splunk/search_telemetry/*search_telemetry.json
        $SPLUNK_HOME/var/spool/splunk/tracker.log*
        /var/log
                /var/log/alternatives.log
                /var/log/apt
                /var/log/apt/eipp.log.xz
                /var/log/apt/history.log
                /var/log/apt/term.log
                /var/log/bootstrap.log
                /var/log/btmp
                /var/log/dpkg.log
                /var/log/faillog
```

14. Restart Splunk Universal Forwarder

After making changes, restart the forwarder for the new configurations to take effect:

```
/opt/splunkforwarder/bin/splunk restart
```

```
root@splunk-uf:~# /opt/splunkforwarder/bin/splunk restart
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
.
Stopping splunk helpers...

Done.

Splunk> The Notorious B.I.G. D.A.T.A.

Checking prerequisites...
        Checking mgmt port [8089]: open
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded
Python interpreter; must be set to "1" for increased security
Done
```

15. Verify Data in Splunk Enterprise

Once the Universal Forwarder is running, check if the data is being received by Splunk Enterprise:

1. Log in to Splunk Web UI

- Open a browser and go to **http://localhost:8000**
- Log in with your **admin** credentials

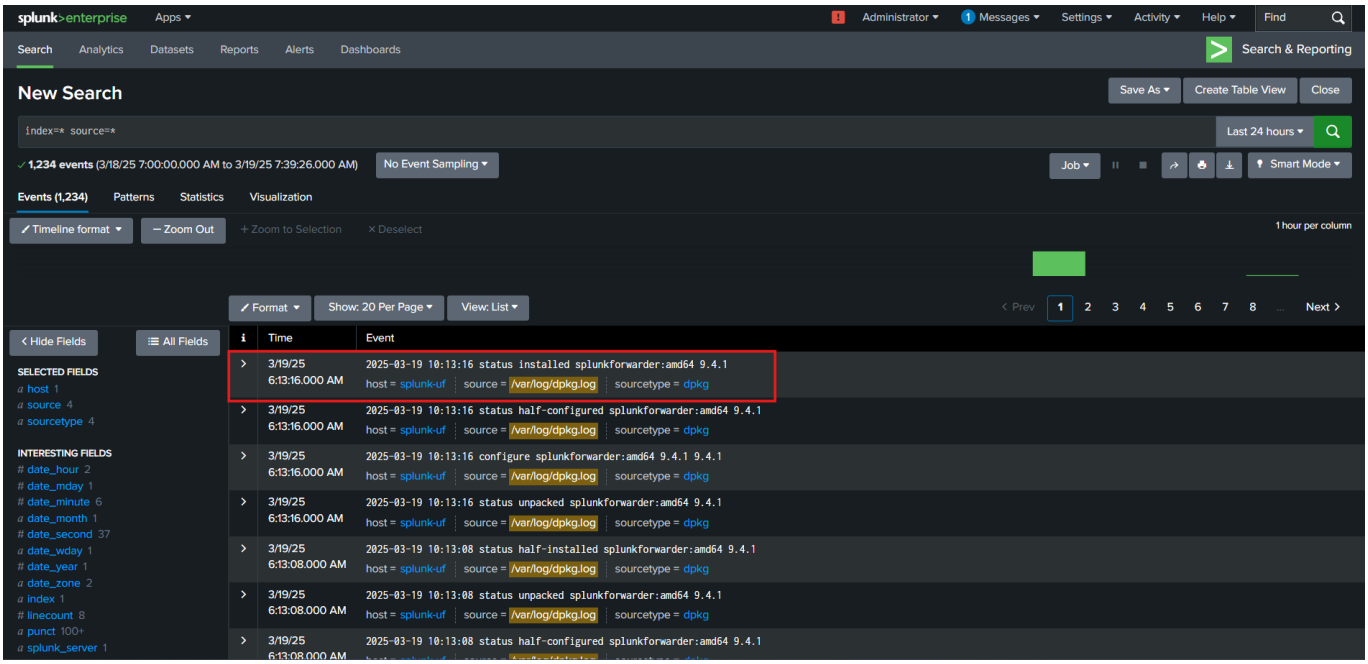
2. Go to Search & Reporting

- Navigate to **Search & Reporting**

3. Run a Search Query

Use the following query to check if logs are coming from the Universal Forwarder:

```
index=* source=*
```



If everything is set up correctly, you should see logs appearing in **Splunk Search**.

Step 4: Configure using Docker image

Step 1: Run Splunk Universal Forwarder in Docker

To start a **Splunk Universal Forwarder container**, use the following command:

```
docker run -itd -p 9997:9997 --name splunk-uf --hostname splunk-uf --network
splunk-net vijaynvb/splunk-uf:latest
```

Explanation:

- `-itd` → **Interactive, TTY, Detached mode** (runs in the background).
- `-p 9997:9997` → **Maps port 9997** from the host to the container (Splunk's default forwarder port).
- `--name splunk-uf` → **Container name** (`splunk-uf`).
- `--hostname splunk-uf` → **Sets hostname** inside the container.
- `--network splunk-net` → **Assigns the container to the Docker network** `splunk-net`.
- `vijaynvb/splunk-uf:latest` → **Uses a custom Splunk UF image**.

The custom Docker image (`vijaynvb/splunk-uf:latest`) is a pre-configured Splunk Universal Forwarder setup that automates installation, license acceptance, user permissions, and log forwarding configurations. It streamlines deployment by eliminating manual setup, ensuring consistency, and optimizing for Docker networking, making it ready to connect with Splunk Enterprise instantly. This approach saves time, reduces errors, and provides a reliable, repeatable environment for log monitoring and forwarding.

After running the command, Docker will return a **container ID**, confirming that the container has started.

Step 2: Access the Running Splunk UF Container

To enter the container's shell, use:

```
docker exec -it splunk-uf bash
```

Now you're inside the **Splunk Universal Forwarder container**.

Step 3: Start Splunk UF Manually

If Splunk UF is not running automatically, start it manually:

```
/opt/splunkforwarder/bin/splunk start
```

Uploading Tutorial Data

This Step guides you through uploading **tutorial data** in Splunk, ensuring that your search results are consistent with the tutorial steps.

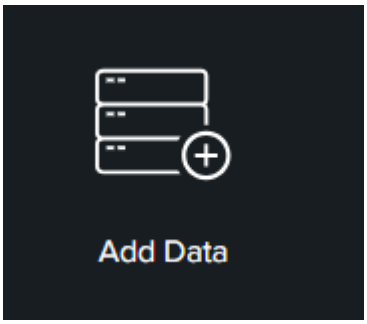
Prerequisites

Before uploading the data, ensure that:

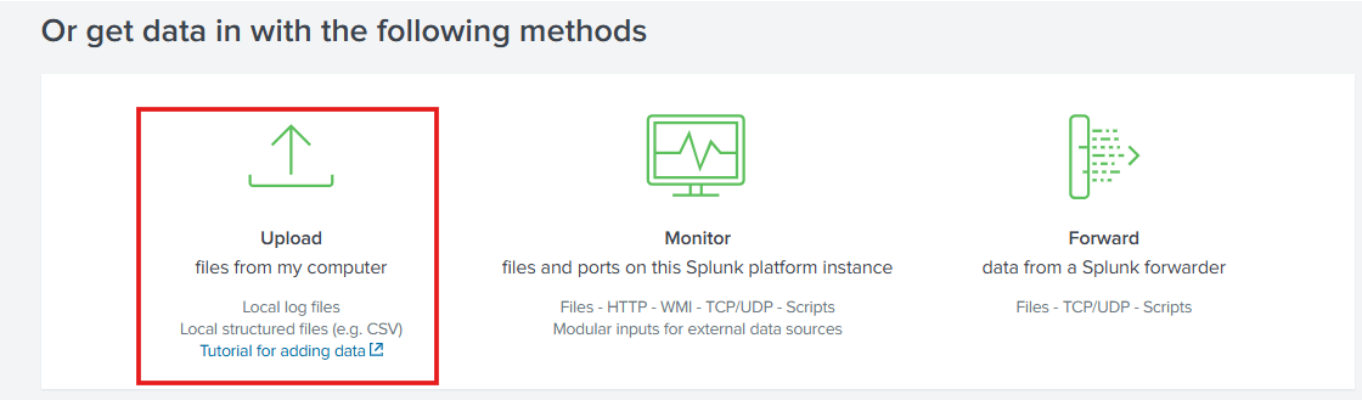
- You have downloaded the **tutorialdata.zip** file on your computer.
- The file **remains compressed** (ZIP format). Some browsers automatically extract ZIP files; check your download settings.
- You understand the **type of data** being uploaded. *(Refer to: "What is in the tutorial data?")*

Step 1: Open the Add Data Wizard

1. If a **Welcome window** appears, close it.
2. Click **Settings > Add Data**.

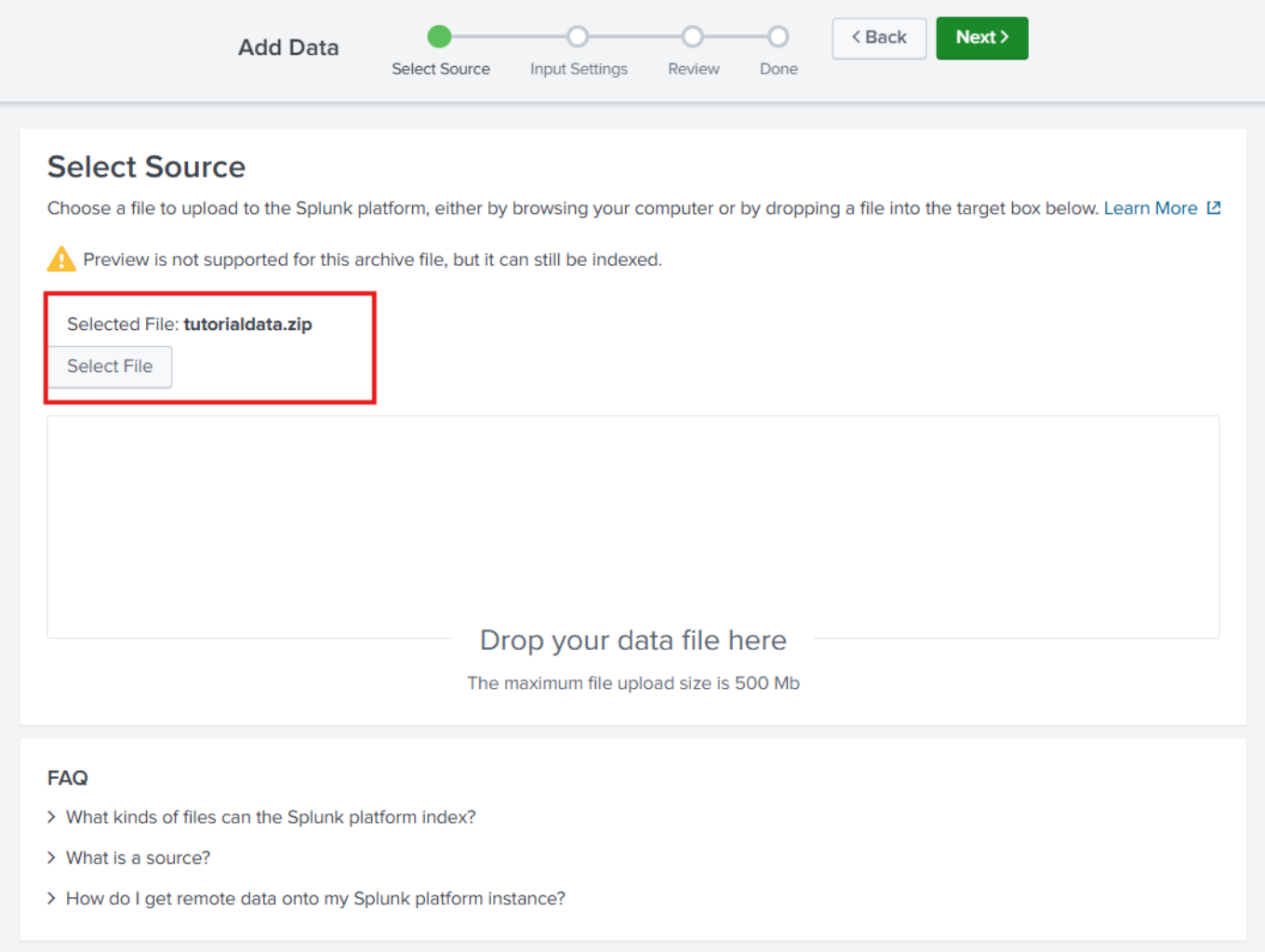


3. In the **Add Data** window, scroll down to the section **"Or get data in with the following methods"** and click **Upload**.



Step 2: Select and Upload the Data File

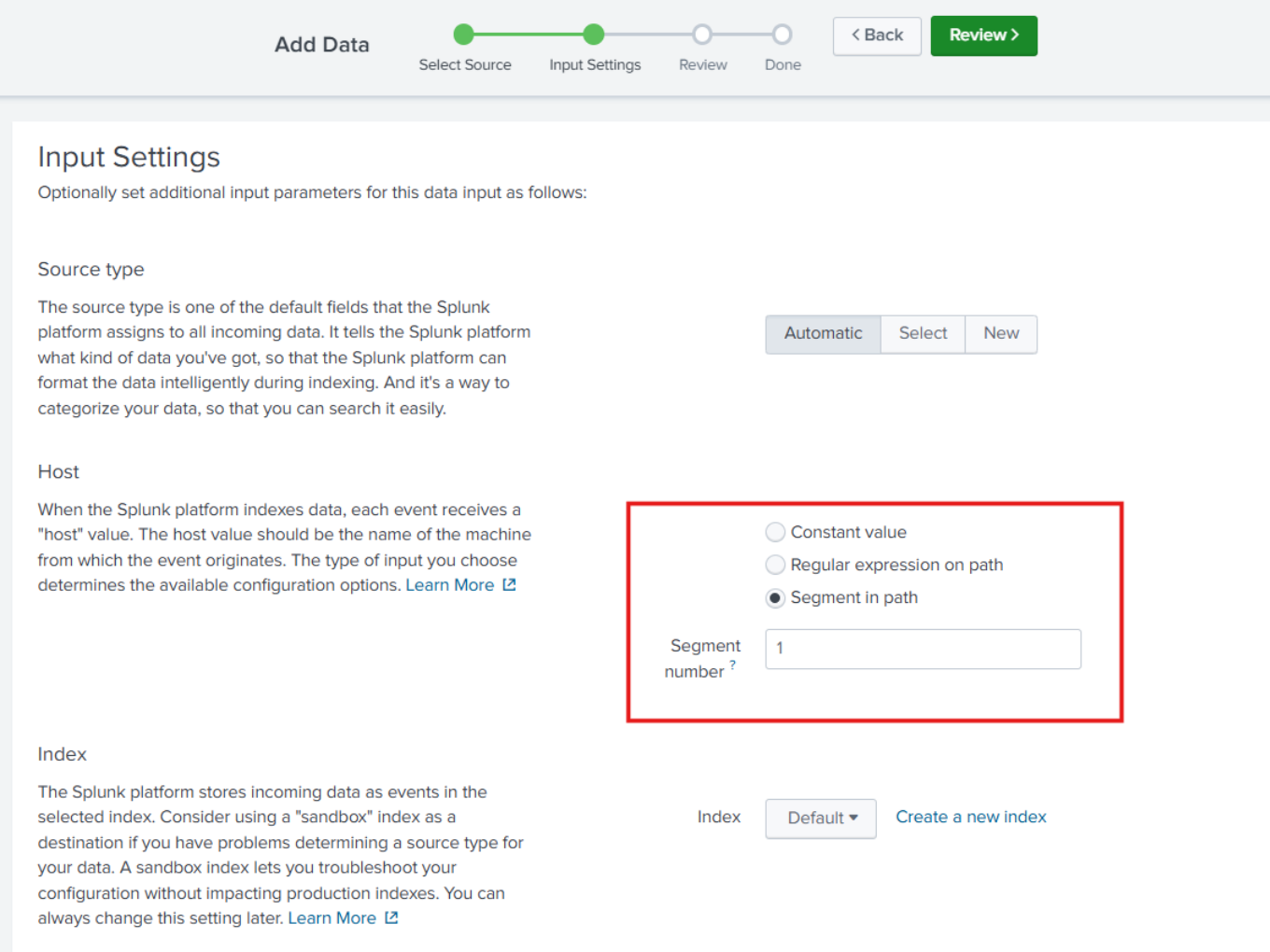
1. Under **Select Source**, click **Select File**.
2. Browse to your **downloaded tutorialdata.zip** file and select it.
3. Click **Open**.
4. Since Splunk **recognizes ZIP files**, it will skip the **Set Source Type** step. *(For non-ZIP files, you may need to specify a data source type.)*
5. Click **Next** to proceed to **Input Settings**.



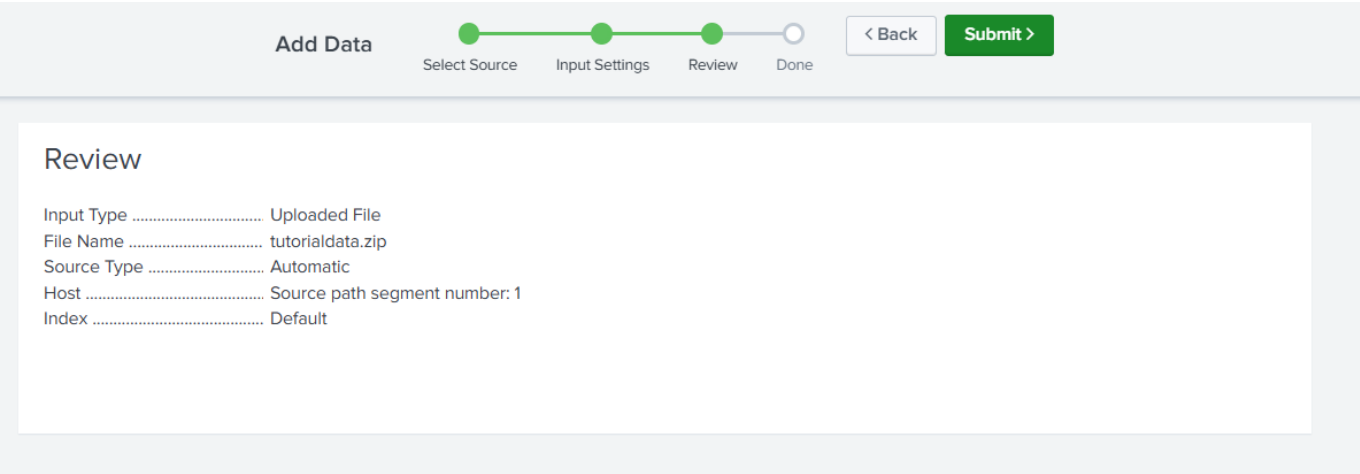
Step 3: Configure Input Settings

In the **Input Settings** screen:

1. **Modify the Host setting** to assign host values from the ZIP file path:
    - Select **Segment in path**.
    - Enter **1** for the segment number.



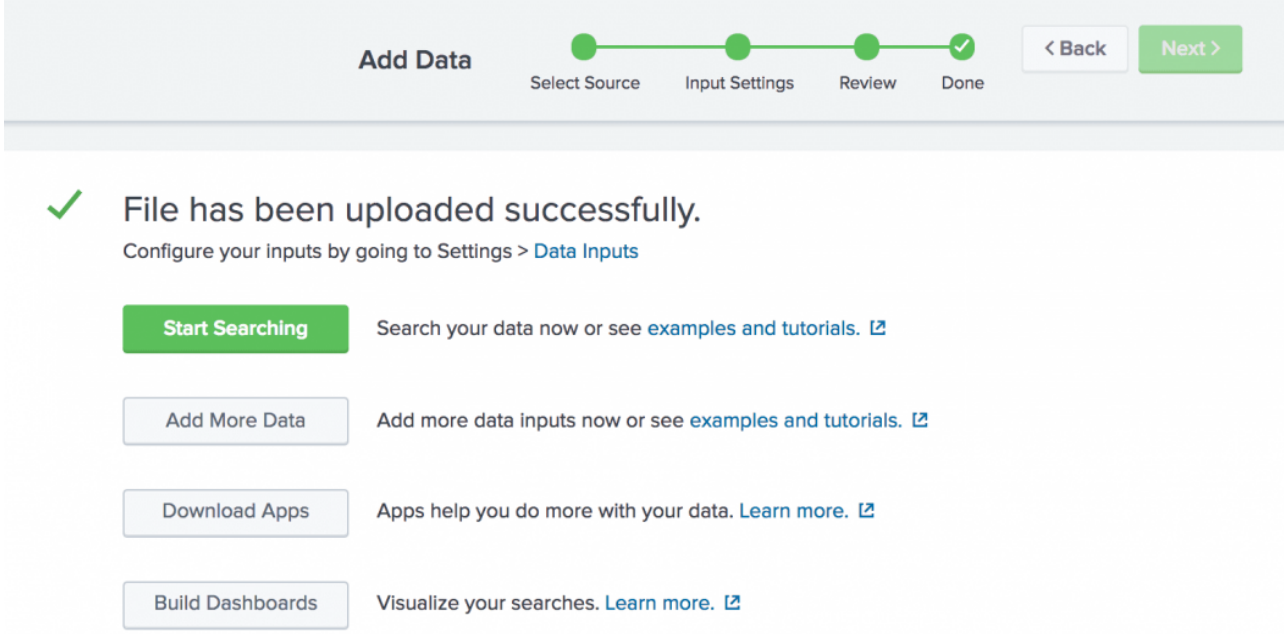
2. Click **Review** to see a summary of your input settings.



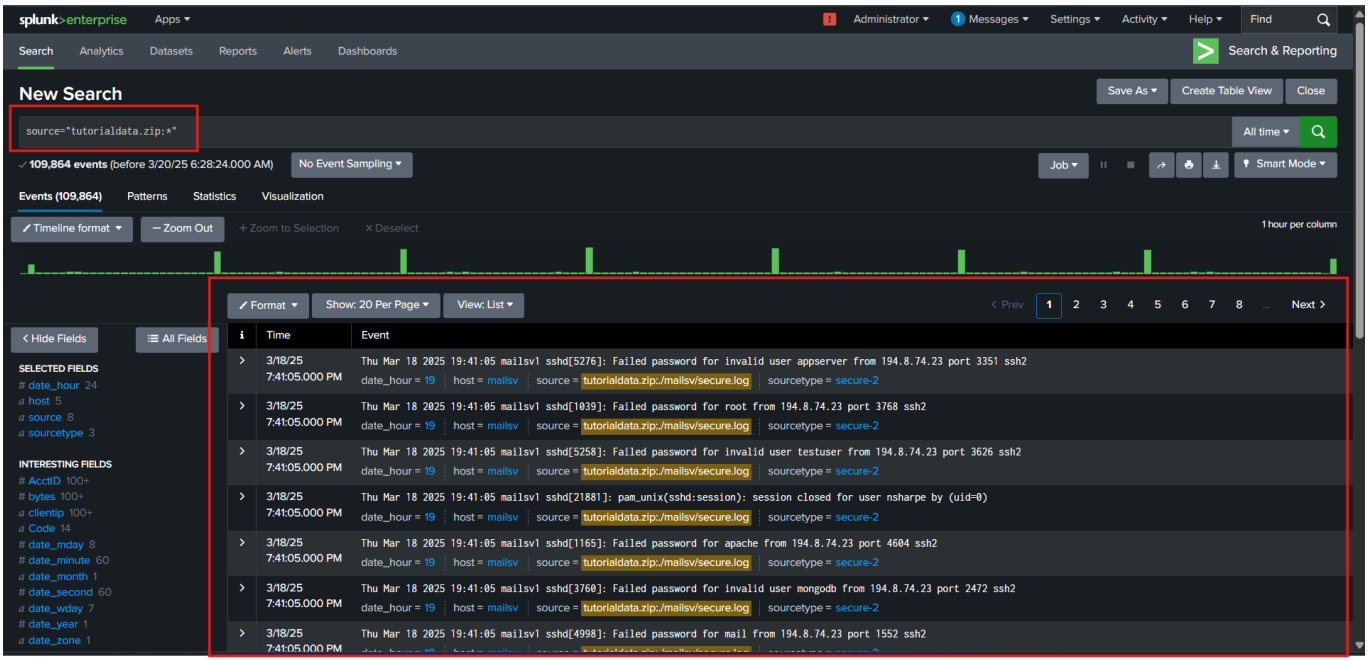
3. Verify the settings and then click **Submit** to upload the data.

Step 4: Verify the Data Upload

1. A confirmation message will appear, indicating the successful upload.
2. To view the data:
    - Click **Start Searching** to open the **Search app**.



- A simple search will automatically run, displaying **indexed events** from the uploaded tutorial data.



Step 5: Return to Splunk Home

1. Click the **Splunk logo** to return to the home screen.
2. You're all set! Your tutorial data is now **indexed and ready for use**.