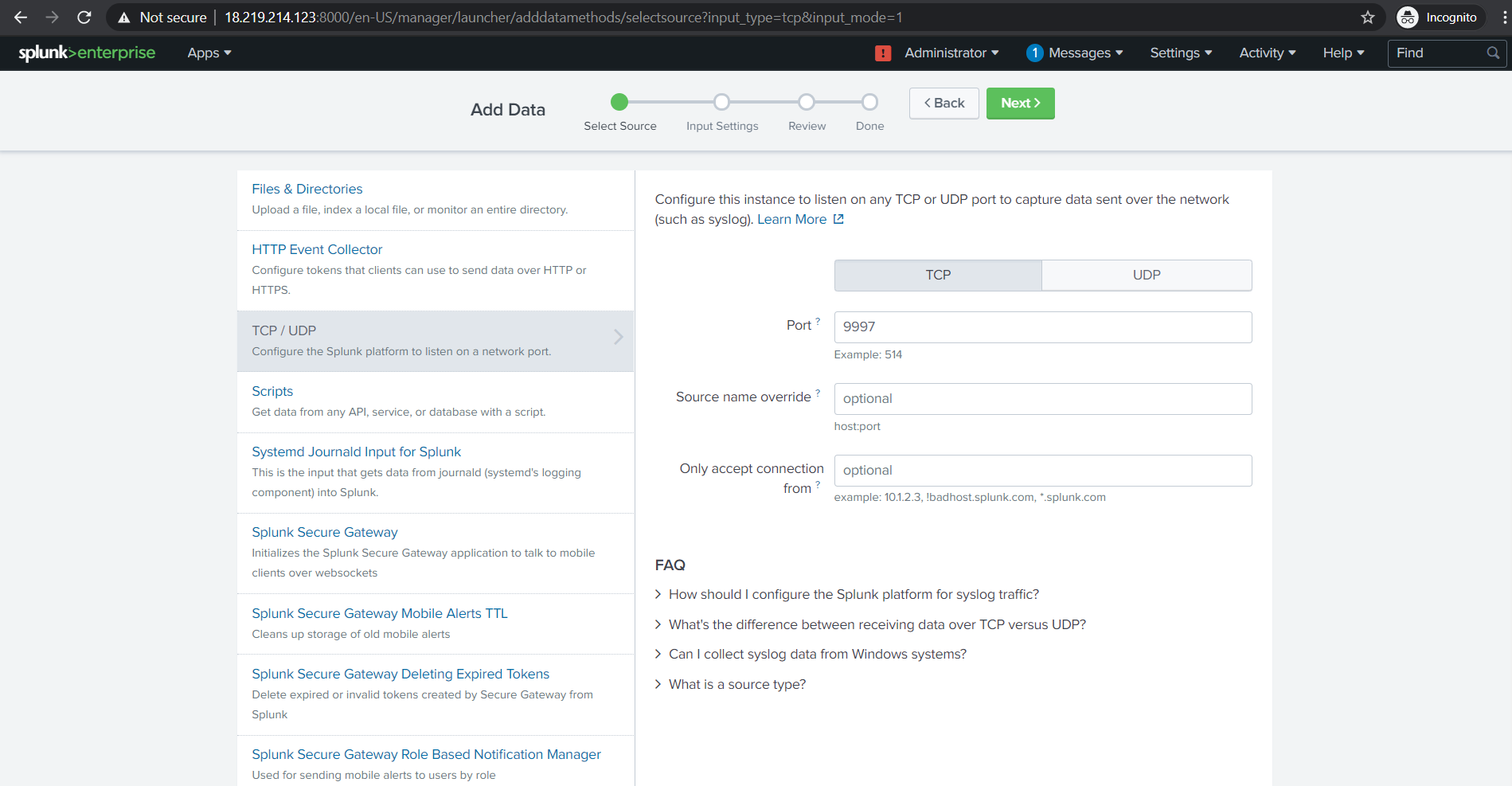
**Splunk TCP input**

1. Login Splunk
2. Settings -> Data (data inputs)
3. Select TCP (Add new)
4. Enter TCP parameters
5. Click submit



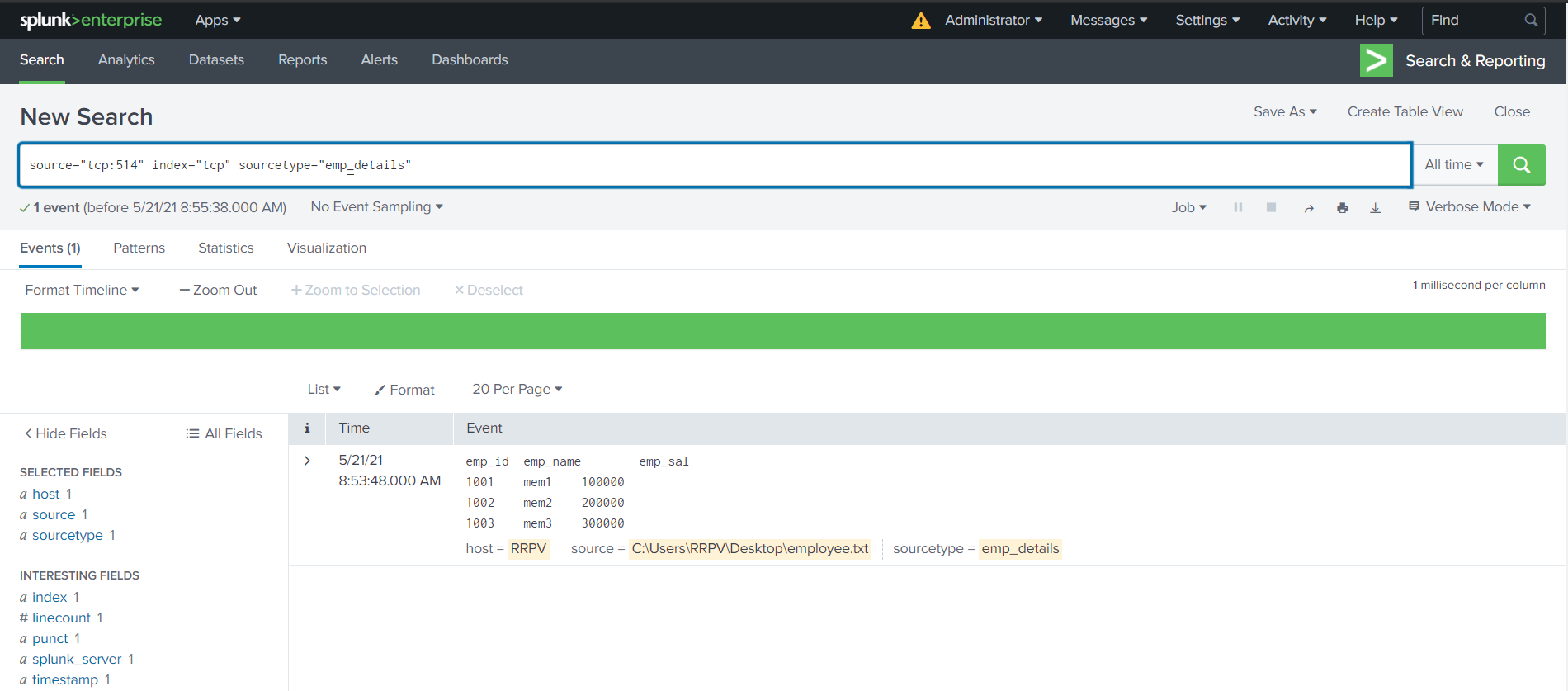
To send input using Netcat:

1. Open terminal
2. Type command

$ nc -t ip\_address\_of\_splunk\_server port < file\_to\_send\_splunk

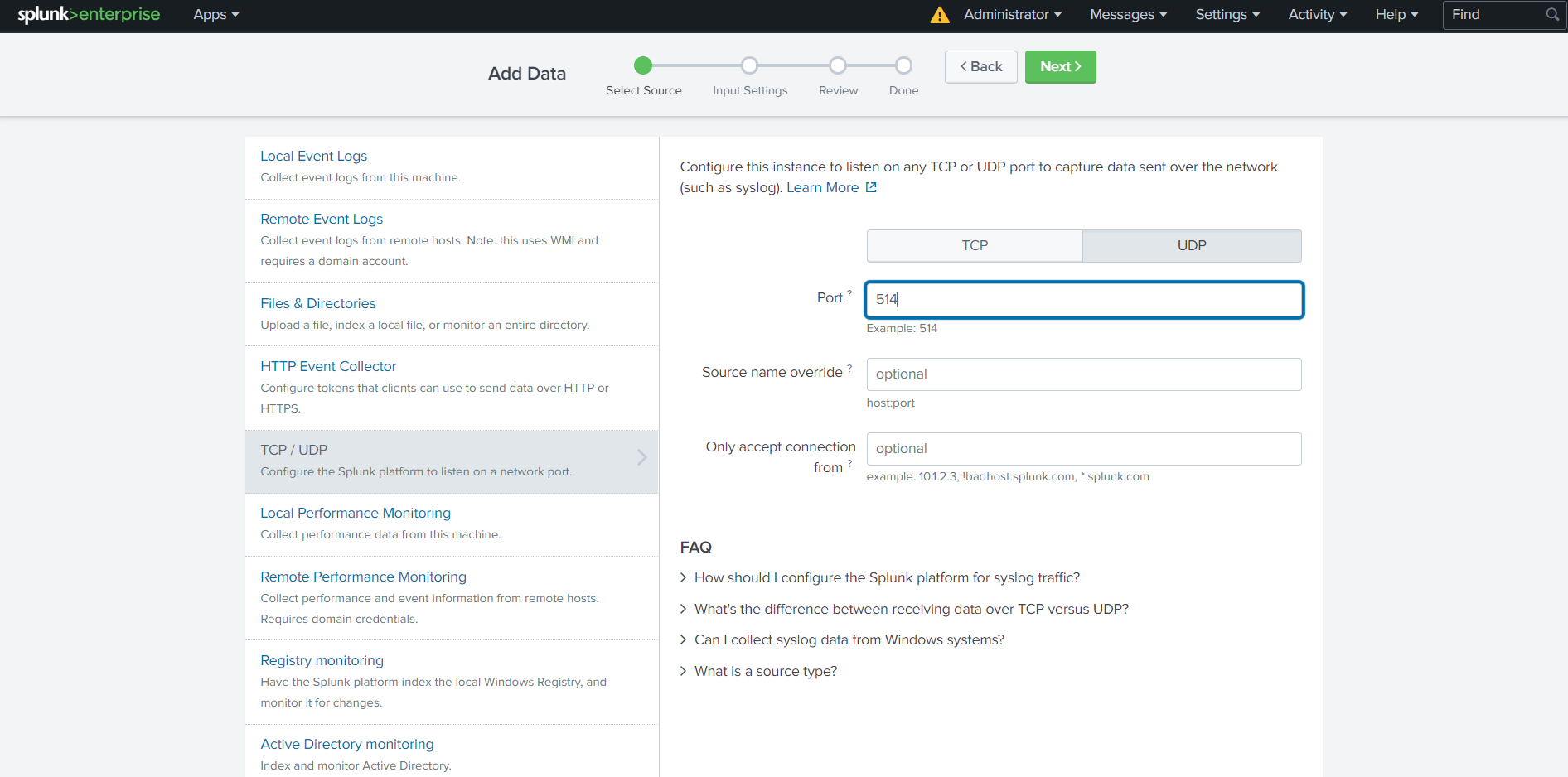
Example:

$ nc -t 127.0.0.1 154 < employee.txt



**UDP input Splunk**

1. Login splunk
2. Settings -> Data (data inputs)
3. Select UDP (Add new)
4. Enter UDP parameters
5. Click submit



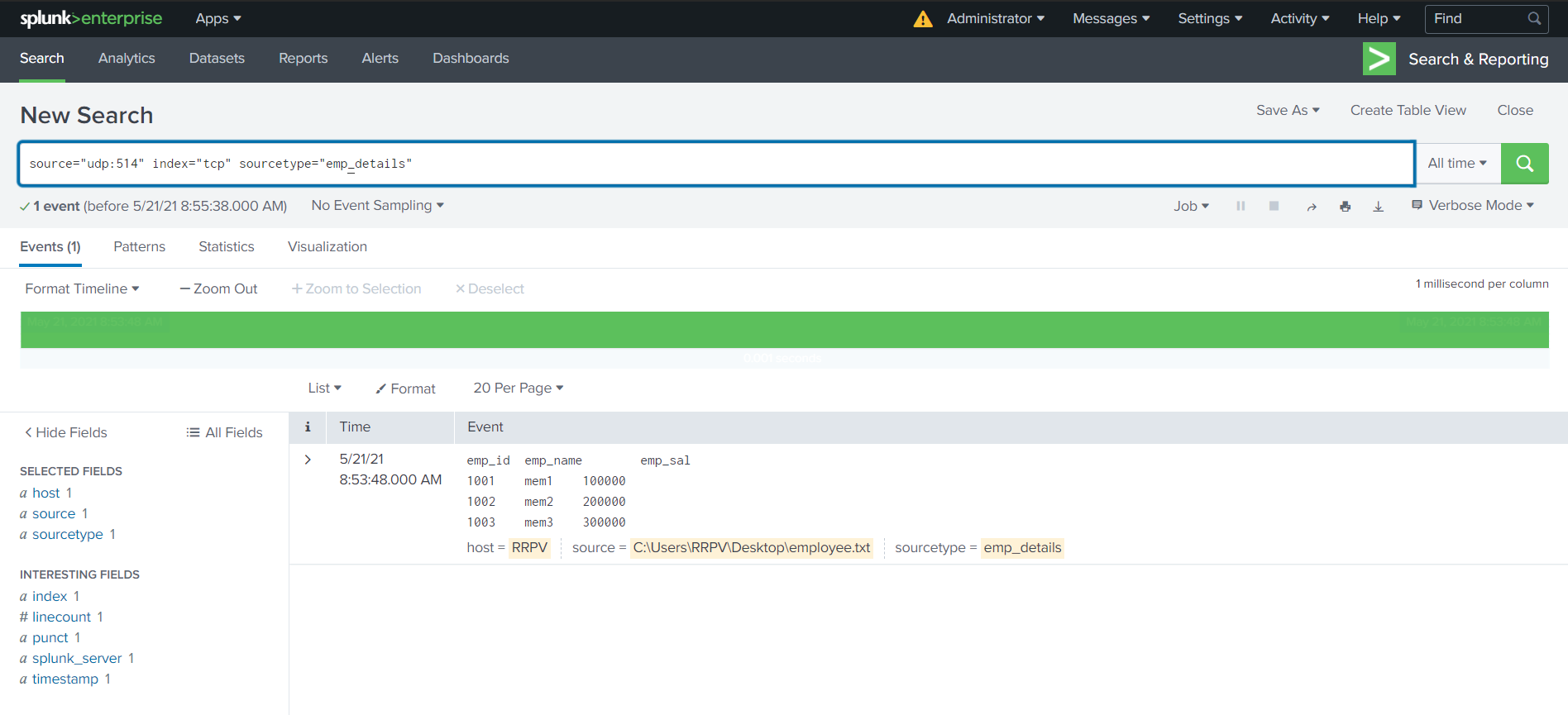
To send input using Netcat:

1. Open terminal
2. Type command

$ nc -u ip\_address\_of\_splunk\_server port < file\_to\_send\_splunk

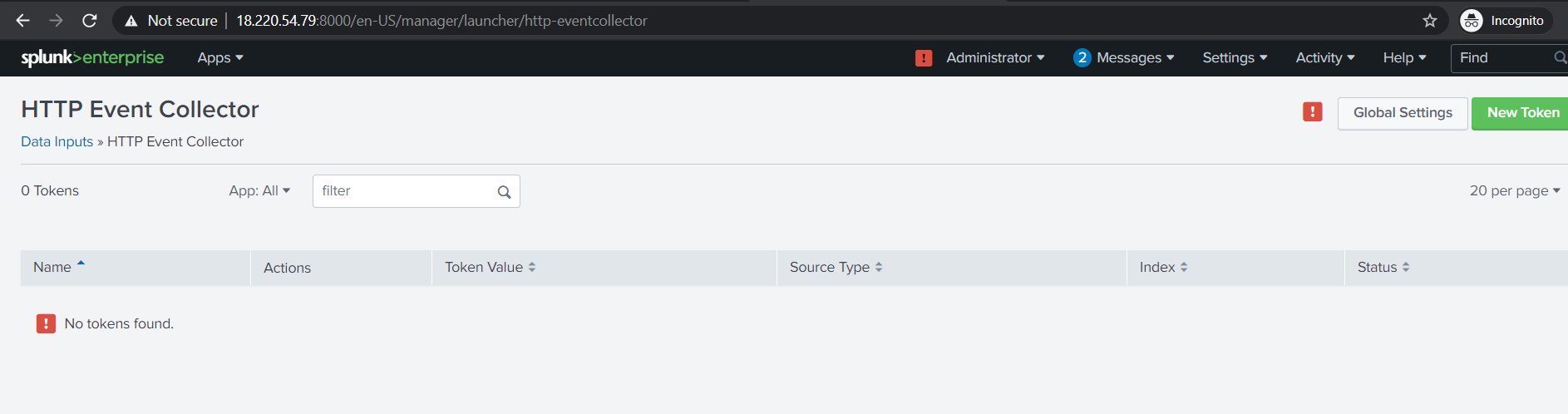
Example:

$ nc -u 127.0.0.1 154 < employee.txt

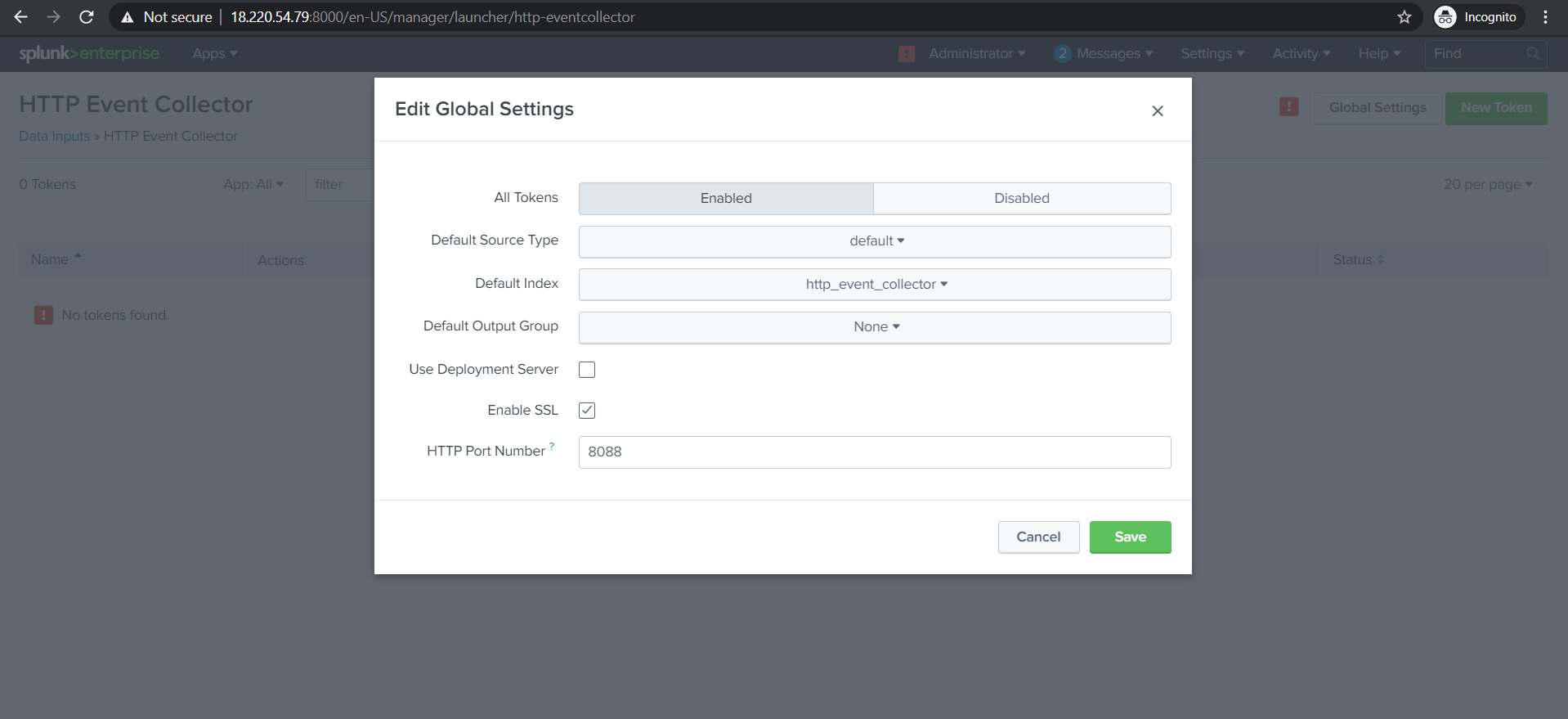


**Splunk HTTP event collector**

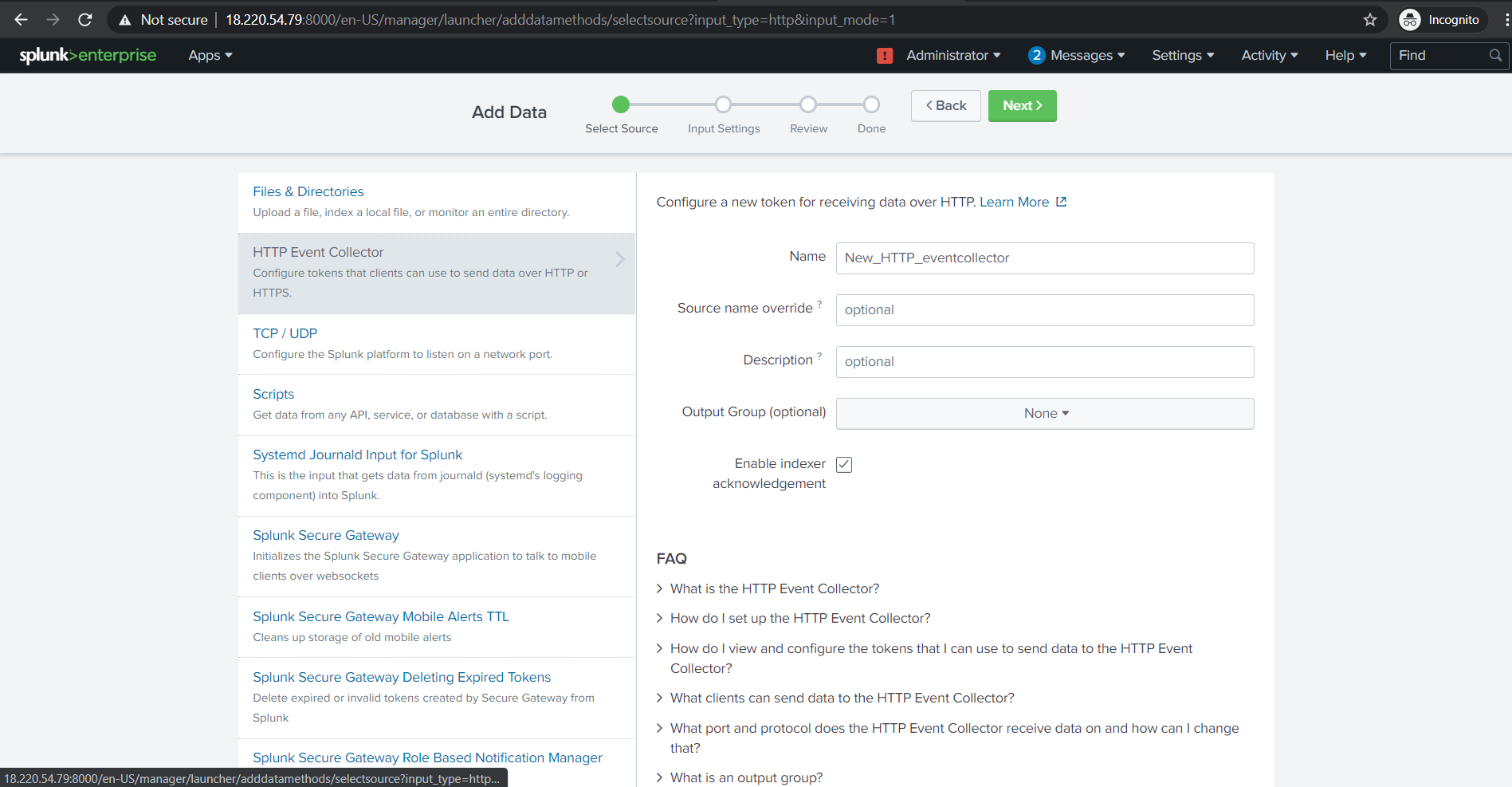
1. Login Splunk
2. Go to settings -> Data(data inputs)
3. Select HTTP event collector



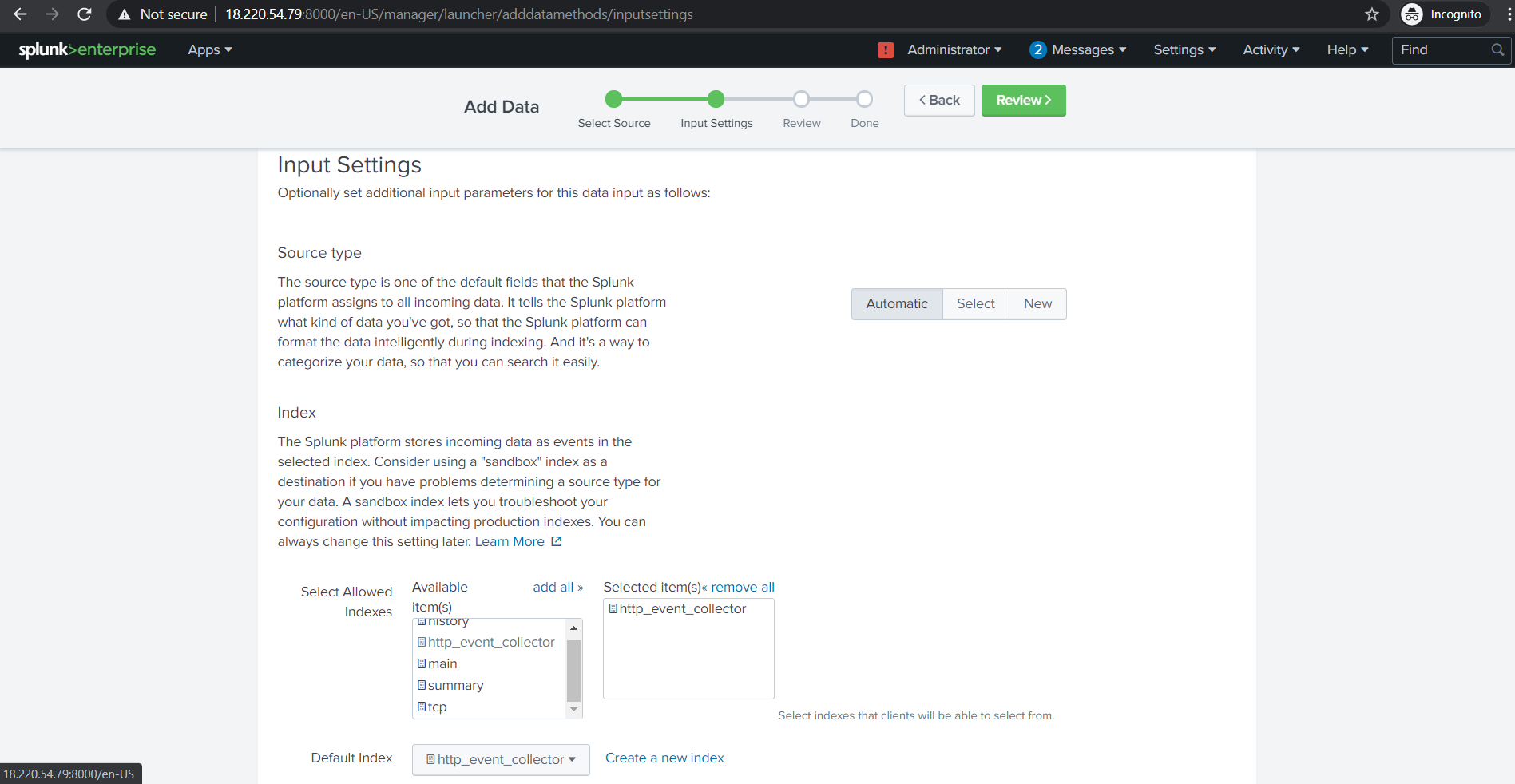
1. Go to Global settings
2. Set parameters and save



1. Go to new token

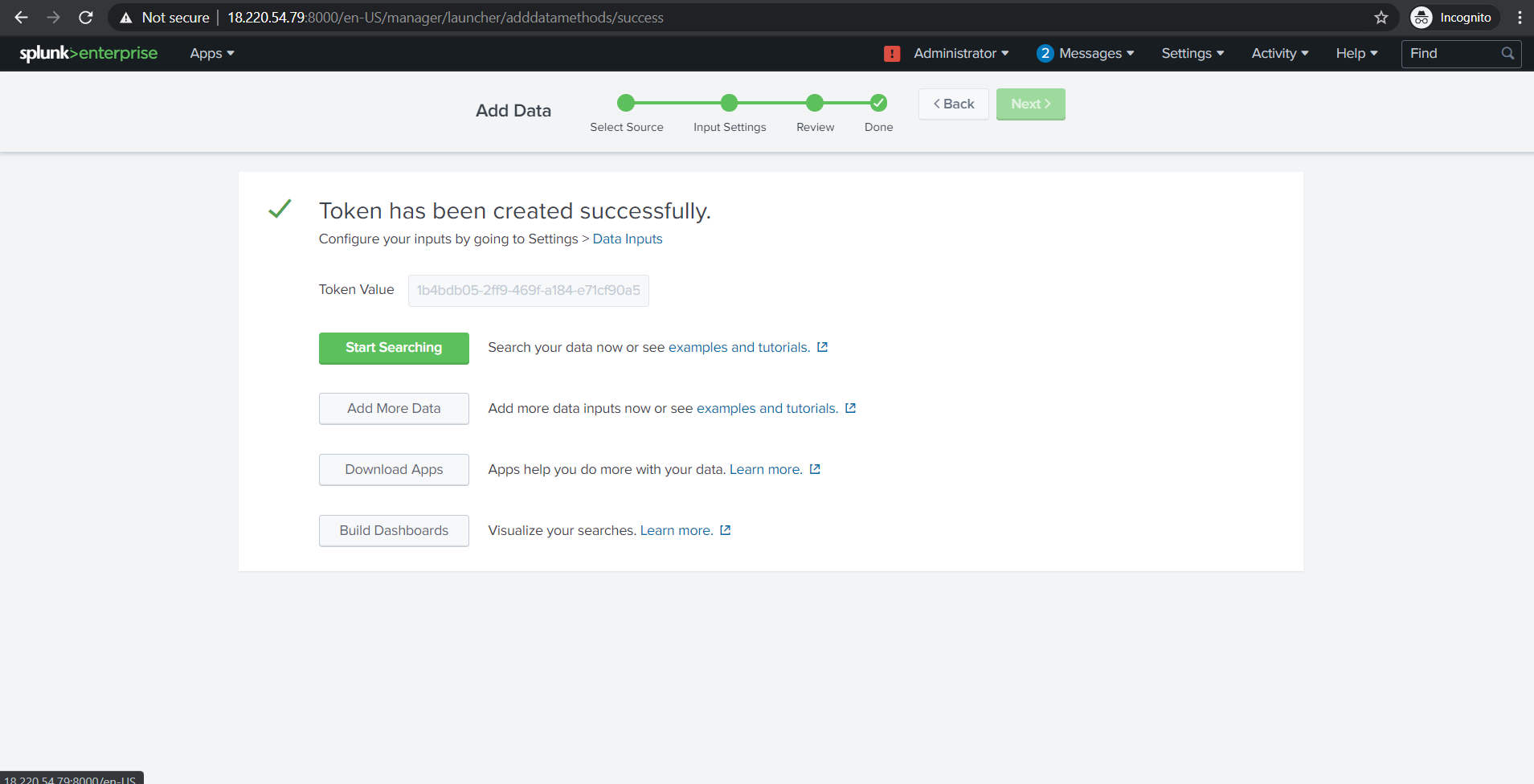


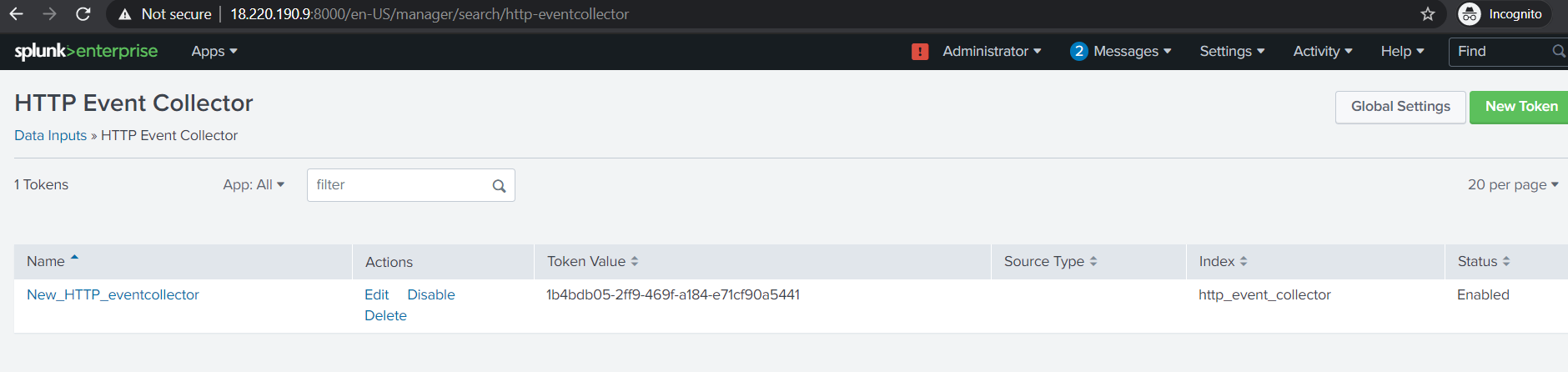
1. Set input settings



1. Review the settings
2. Click save and get **token value**

**Ex: 1b4bdb05-2ff9-469f-a184-e71cf90a5441**





**Sending data using curl**

**Example:**

1. **Token authorization**

Curl -k <http://18.220.190.9:8088/services/collector> -H “Authorization:Splunk 1b4bdb05-2ff9-469f-a184-e71cf90a5441” -d “{\”sourcetype\”: \”trail\”,\”event\”:\”hello world!\”}”

1. **Basic authorization**

Curl -k <http://18.220.190.9:8088/services/collector> -u “admin:1b4bdb05-2ff9-469f-a184-e71cf90a5441” -d “{\”sourcetype\”: \”trail\”,\”event\”:\”hello world!\”}”

1. **Multiple events**

Curl -k <http://18.220.190.9:8088/services/collector> -u “admin:1b4bdb05-2ff9-469f-a184-e71cf90a5441” -d “{\”sourcetype\”: \”trail\”,\”event\”:\”hello world!\”}{ \”sourcetype\”: \”trail\”,\”event\”:\”how are you!\”}”

1. **Raw text**

Curl -k “<http://18.220.190.9:8088/services/collector>/raw?sourcetype=trail” -H “Authorization:Splunk1b4bdb05-2ff9-469f-a184-e71cf90a5441” -d “1, 2, 3……Hello, World!”

1. **Indexer acknowledgement**

Curl -k <http://18.220.190.9:8088/services/collector?channel=1b4bdb05-2ff9-469f-a184-e71cf90a5441> -H “Authorization:Splunk 1b4bdb05-2ff9-469f-a184-e71cf90a5441” -d “{\”sourcetype\”: \”trail\”,\”event\”:\”helloworld!\”}”

To get ack

Curl -k <http://18.220.190.9:8088/services/collector/ack?channel=1b4bdb05-2ff9-469f-a184-e71cf90a5441> -H “Authorization:Splunk 1b4bdb05-2ff9-469f-a184-e71cf90a5441” -d “{\”acks\”: [0]}”

