

# How to integrate FIXEdge with Splunk

- [Features](#)
- [Interaction model](#)
- [Configuring](#)
  - [1. Upgrade software](#)
  - [2. Configure Logging](#)
  - [3. Configure Splunk](#)

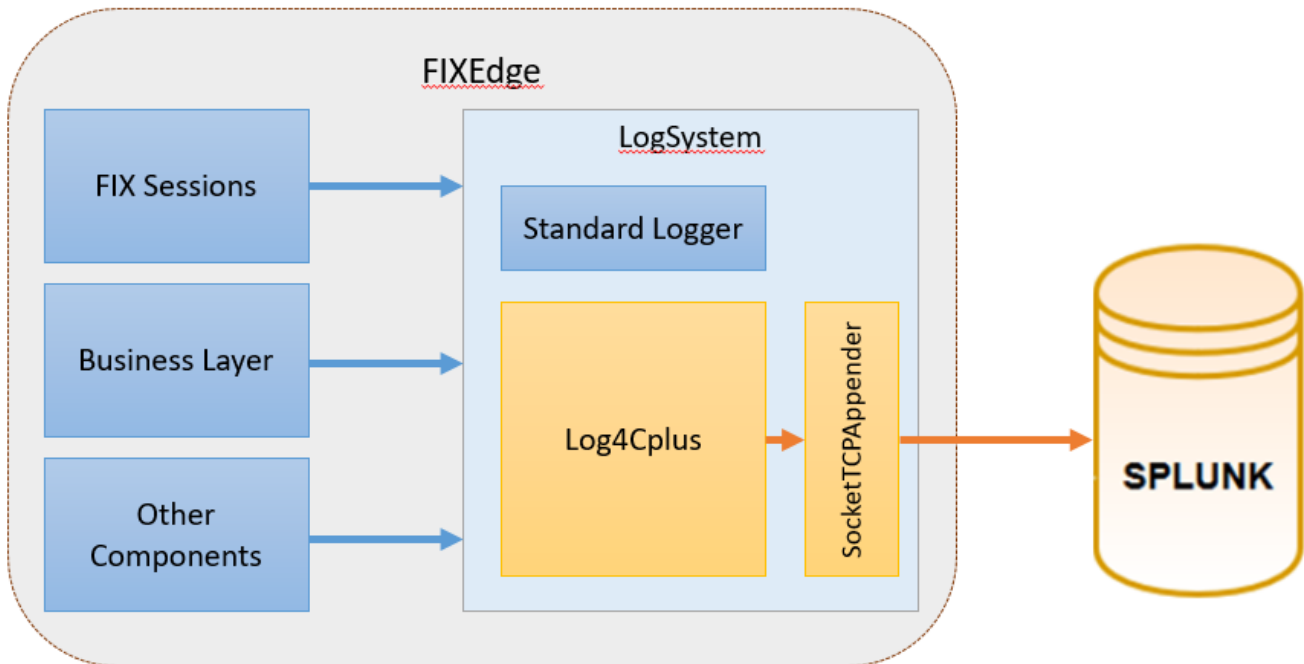
## Features


Integration with Splunk supports the following features:

- Log messages forwarding to the Splunk
- Connection with Splunk is supported over TCP
- Splunk agent can be used
- Configurable timestamp

## Interaction model

Interaction between FIX engine and Splunk/Splunk agent is maintained via [Log4Cplus library](#):



 The described functionality was successfully tested with version 7.2.0 of Splunk

## Configuring

### 1. Upgrade software

[Upgrade FEEdge](#) to version 6.7 or FA to version 2.26. If you are using FA rebuild your application with the new version of FA.

### 2. Configure Logging

To forward log messages to Splunk specify **Log4Cplus** for **Log.Device** property in *FIXEdge.properties* (for FIXEdge) or *engine.properties* (for FIXAntenna) file and configure `log4cplus` parameters as follows:

### FIXEdge.properties or engine.properties changes

```
# add Log4Cplus device for duplication logs to the log4cplus
Log.Device = File Log4Cplus

#----- configure log4plus for forwarding to the Splunk -----
log4cplus.rootLogger = TRACE,Splunk
log4cplus.appender.Splunk=log4cplus::SocketTCPAppender
#set host/port Splunk
log4cplus.appender.Splunk.port=<PORT>
log4cplus.appender.Splunk.host=<HOST>
# using pattern for add information in log messages about
log4cplus.appender.Splunk.layout=log4cplus::PatternLayout
log4cplus.appender.Splunk.layout.ConversionPattern=%d{%FT%T.%q}Z Severity=%-5p ThreadID=%t Category=%c %m%n
```

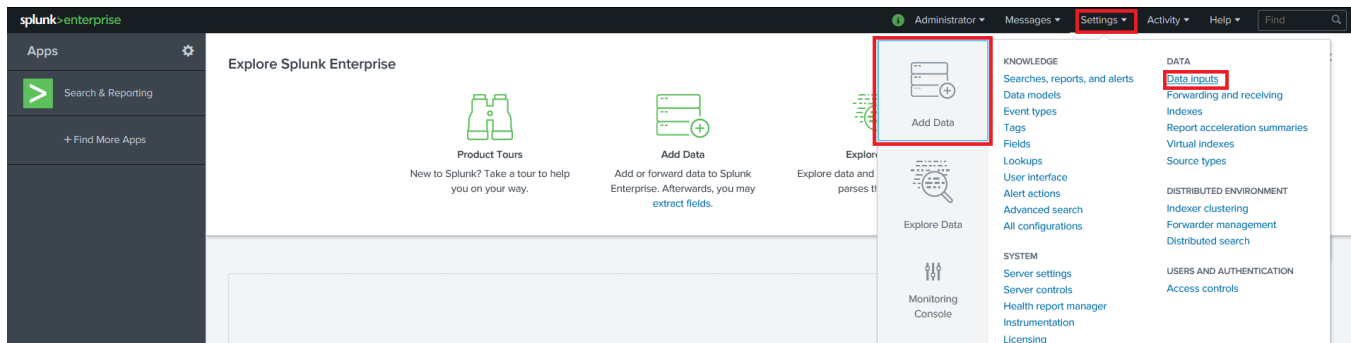
In this case logging will be performed with both creating standard log files and forwarding to Splunk (**Log.Device = File Log4Cplus** - see description of **Log.Device** parameter).

Also the example contains configuration of an extended log layout that includes severity, threadID and other additional fields (**log4cplus.appender.Splunk.layout** parameter).

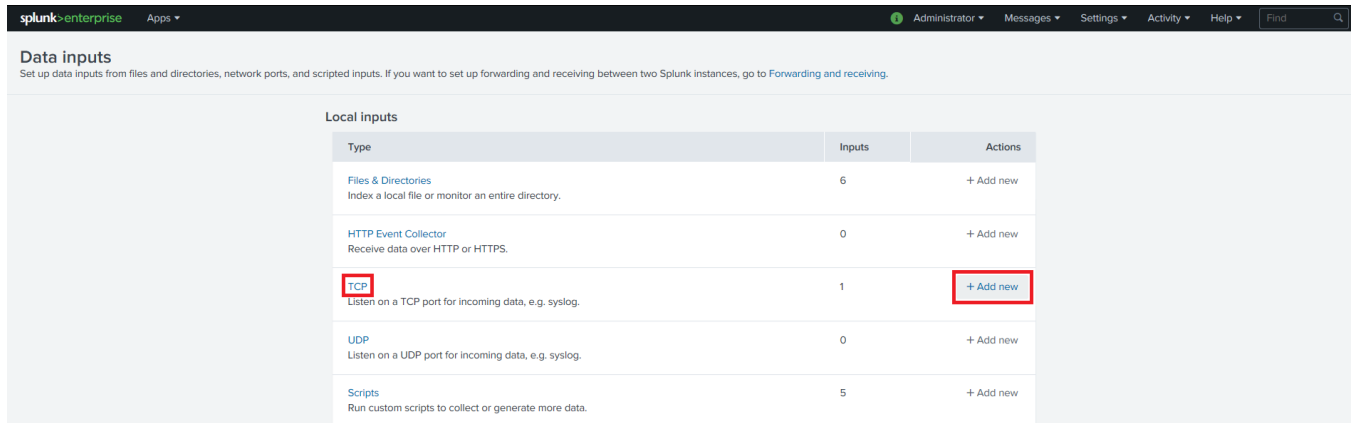
 More information about log4cplus configuration can be found here [Log4Cplus Usage](#)

## 3. Configure Splunk

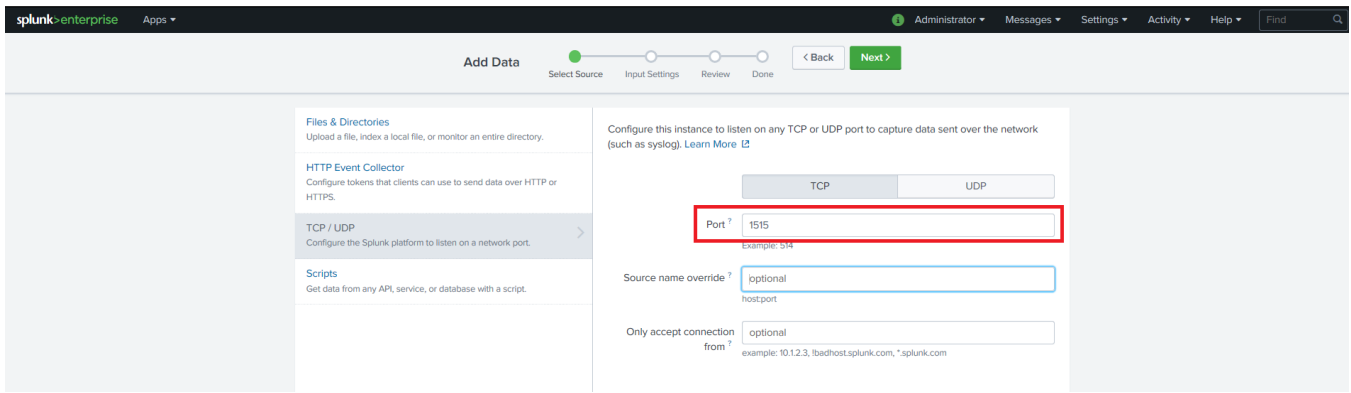
1. In Splunk Web interface configure inputs (From Splunk Home, select **Settings Add Data Data inputs**):



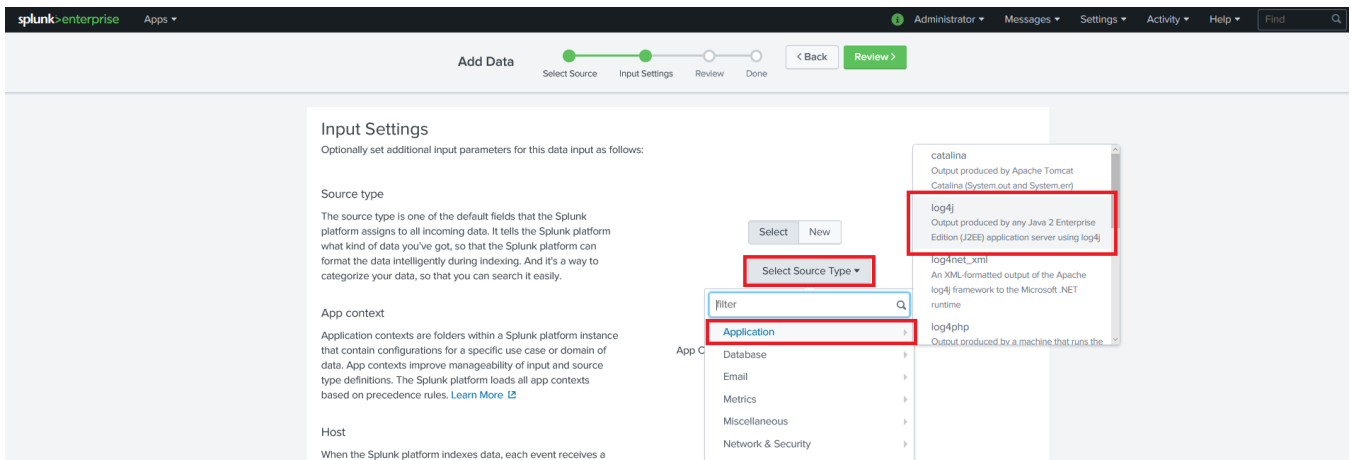
2. Add new input to TCP (From Data inputs, select **TCP Add new**):



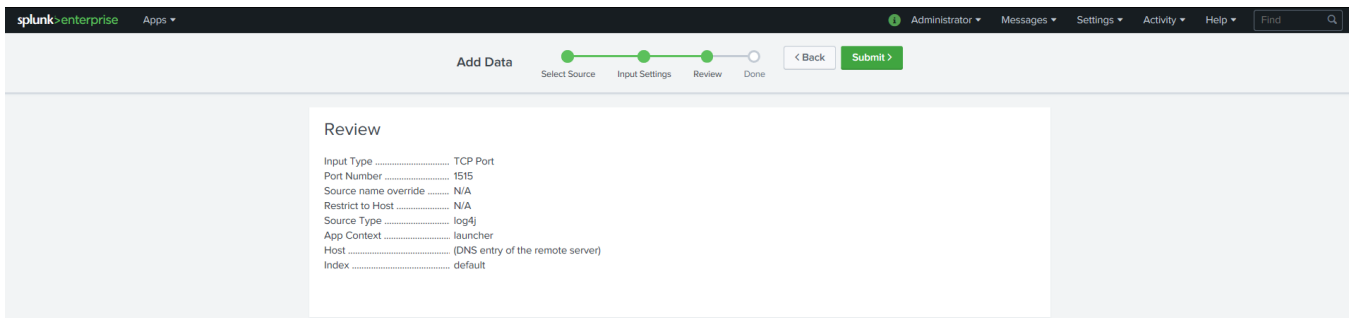
3. Select data source - choose listening port (the same port number should be set in *FIXEdge.properties* `log4cplus.appender.Splunk.port` parameter) and then click **"Next"**:



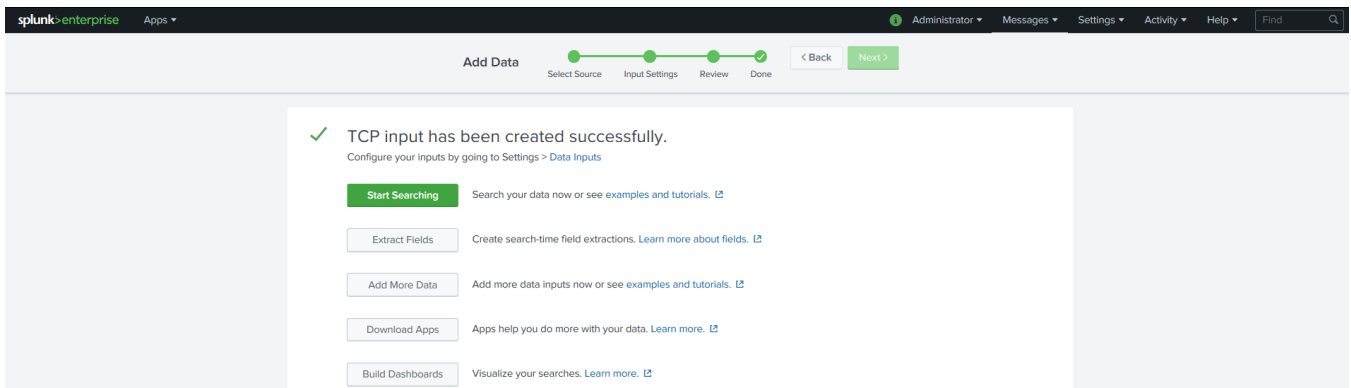
4. Configure input settings - Select source type **Application log4j** and then click "Review":



5. Check out configuration and click "Submit":



6. Click "Start Searching":



7. After starting FIXEdge session you will see FIXEdge logging in Splunk:

New Search

Save As Close

source="tcp:1514" sourcetype="log4j"

All time

544,380 of 544,380 events matched No Event Sampling

Job [Progress Icons] Smart Mode

Events (544,380) Patterns Statistics Visualization



List Format 50 Per Page

< Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields  
 # APP 1  
 # Category 30  
 # COMP 1  
 # date\_hour 24  
 # date\_mday 6  
 # Host 10000000

All Fields

i	Time	Event
>	10/25/18 5:28:40.007 AM	2018-10-25T05:28:40.007Z Severity=INFO APP=1097 COMP=1153 LogID=N/A TheardID=139817929127680 Category=Engine Session <FIXADMIN, AdminClient> : Change state: old state=NonGracefullyTerminated new state=WaitForFirstLogon host = ibc-fixedge-2.lib_cluster_network   source = tcp:1514   sourcetype = log4j
>	10/25/18 5:28:40.007 AM	2018-10-25T05:28:40.007Z Severity=DEBUG APP=1097 COMP=1153 LogID=N/A TheardID=139817929127680 Category=Engine Session <FIXADMIN, AdminClient> : InSeqNum = 3. OutSeqNum = 3 host = ibc-fixedge-2.lib_cluster_network   source = tcp:1514   sourcetype = log4j
>	10/25/18 5:28:40.007 AM	2018-10-25T05:28:40.007Z Severity=TRACE APP=1097 COMP=1153 LogID=N/A TheardID=139817442580224 Category=CCAdminApplication Admin session onLogout() processing finished. host = ibc-fixedge-2.lib_cluster_network   source = tcp:1514   sourcetype = log4j
>	10/25/18 5:28:40.007 AM	2018-10-25T05:28:40.007Z Severity=TRACE APP=1097 COMP=1153 LogID=N/A TheardID=139817442580224 Category=CCAdminApplication Clearing subscriptions. host = ibc-fixedge-2.lib_cluster_network   source = tcp:1514   sourcetype = log4j