

# Splunk FixEdgeViewer -- Quick Start

## Quick start

This way presumes that you have got splunk package for your FixEdge installation ([FixEdgeViewer.Linux.tar.gz](#), [FixEdgeViewer.Windows.tar.gz](#)).

## Install Splunk package

do the following steps:

- Go to splunk instance's home page <http://localhost:8000/>
- Go to splunk's menu "Apps->Manage apps"
- Click a button "Install app from file"
- Click a button "Browse" then navigate through dialog window to the folder with splunk application package
- Choose a file FixEdgeViewer.\*.tar.gz (in place of \* should be suffix appropriate to your system - such as Windows or Linux) then click "Open"
- Click "Upload" to install application into splunk server

or

- unpack app package into splunk application directory like %SPLUNK\_HOME%\etc\app or \$SPLUNK\_HOME/etc/app
- restart splunk instance.

## Configure FIXEdgeViewer

- Find in unpacked directory and edit inputs.conf: you should correct here your hostname with FixEdge installation and path to log file to monitor by splunk
- For windows installation:

```
[default]
host = WINDOWSHOSTNAME
[monitor://C:\B2BITS\FIXEdge\v.5.7.0.62202\FixEdge1\log\FixEdge.log]
```

- For Linux installation:

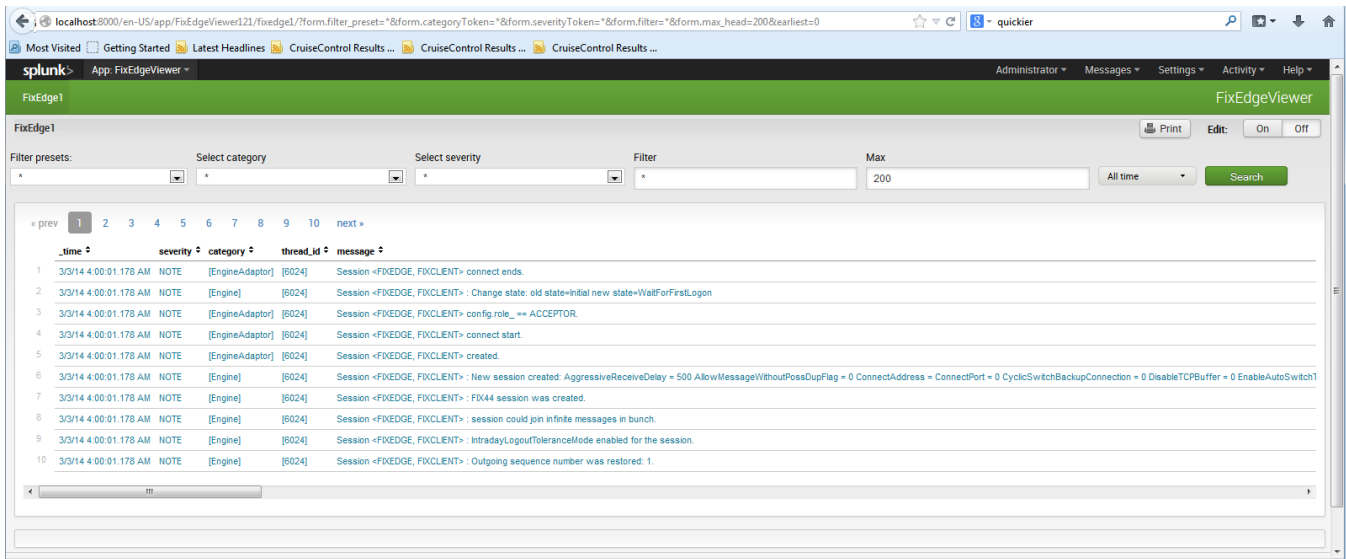
```
[default]
host = LINUXHOSTNAME
[monitor:///opt/FIXEdge/v.5.7.0.62202/FixEdge1/log/FixEdge.log]
```

- restart Splunk

## Run FIXEdgeViewer

Now you can go to Splunk instance's home page. There should be button named "FixEdgeViewer".

By clicking it you now can view FixEdge.log of your FixEdge instance:



This app allows you to filter log events by criteria such as category, severity, their combinations or custom filter expression. Also you can set maximum amount of records to see in search result and time period you look up through. Also for convenience this app has some filter presets (predefined criteria combinations). You can further inspect the context of some event by clicking on a row in a selection table.

