How to use FIXEye - Splunk integration capabilities

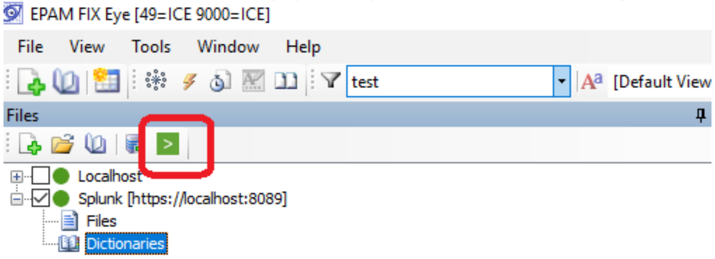
General Notes

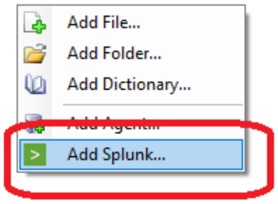
Splunk is a system for searching, monitoring, and analyzing machine-generated big data. It is often used for financial or trading information storage as well. This document is intended to describe how to configure FIXEye-Splunk connection and search for fix data in Splunk storage using FIXEye application.

Managing connections

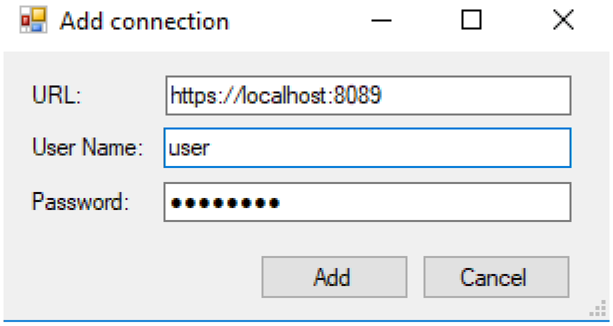
Create new connection

1. Open 'Add connection...' dialog by clicking '>' button or choose 'Add Splunk...' menu item with right-click context menu in file window.





2. Fill-in all input boxes in the dialog and presses 'Add' button. For connection to work user must be previously created in Splunk system. URL is web link to Splunk system.

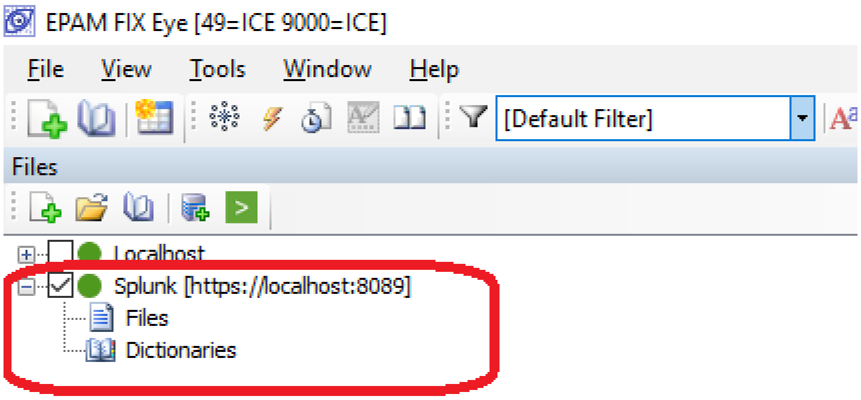


URL: https://localhost:8089

User Name: user

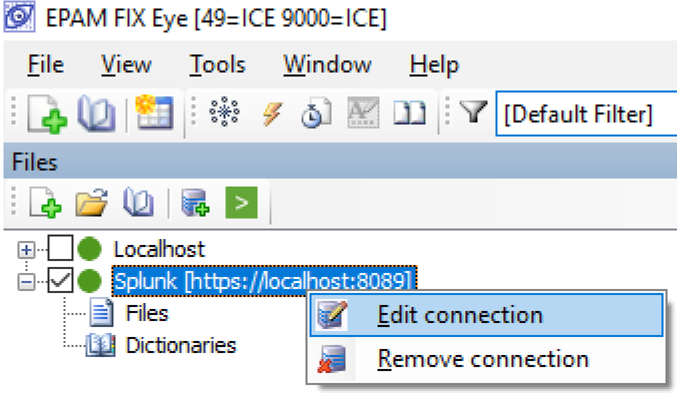
Password: ●●●●●●●●

3. The newly created connection to Splunk appears in file window.

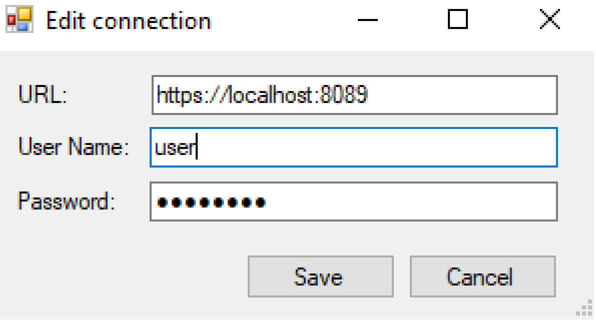

EPAM FIX Eye [49=ICE 9000=ICE]
File View Tools Window Help
[Default Filter]
Files
Localhost
Splunk [https://localhost:8089]
Files
Dictionaries

Edit connection

1. Right-click an existing Splunk connection and choose 'Edit connection'.


EPAM FIX Eye [49=ICE 9000=ICE]
File View Tools Window Help
[Default Filter]
Files
Localhost
Splunk [https://localhost:8089]
Files
Dictionaries
Edit connection
Remove connection

2. 'Edit connection...' dialog appears. Input boxes of the dialog contain corresponding values of the connection.



URL: https://localhost:8089

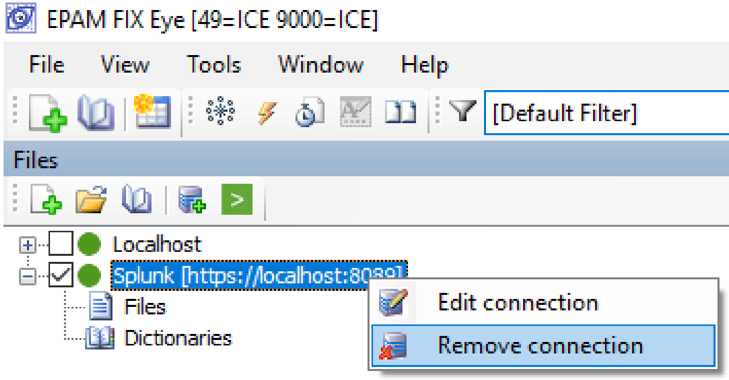
User Name: user

Password: ••••••••

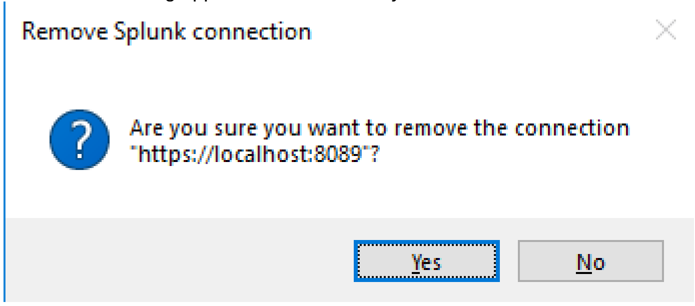
3. Change values. Presses 'Save' button if you want changes to be saved or use 'Cancel' button for changes to be discarded.

Remove connection

1. Right-clicks an existing Splunk connection and choose 'Remove connection'.



2. Confirmation dialog appears. Press "Yes" if you want to remove connection and "No" if you want to keep it.


Remove Splunk connection

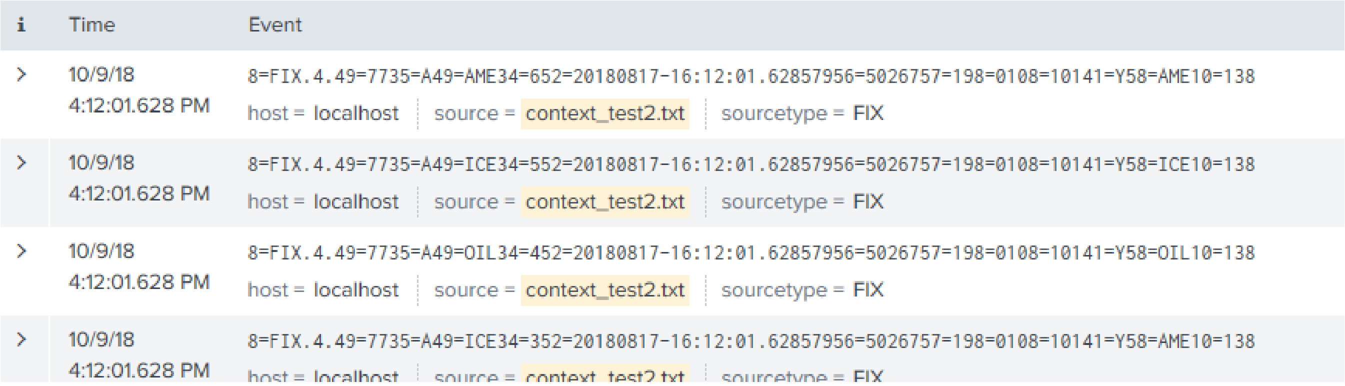
Are you sure you want to remove the connection "https://localhost:8089"?

Types of search

it is important to be aware that to search using FIXEye-Splunk connection means that all searching job is taking place on Splunk side. FIXEye sends search string to Splunk, gets the result and displays it. So FIXEye has to use splunk syntax and it is really different from FIXEye native syntax. For user convenience some simple patterns such as tag=value may be used but for more complicated searching syntax will be different and it is recommended to study splunk documentation.

Search in Raw FIX messages

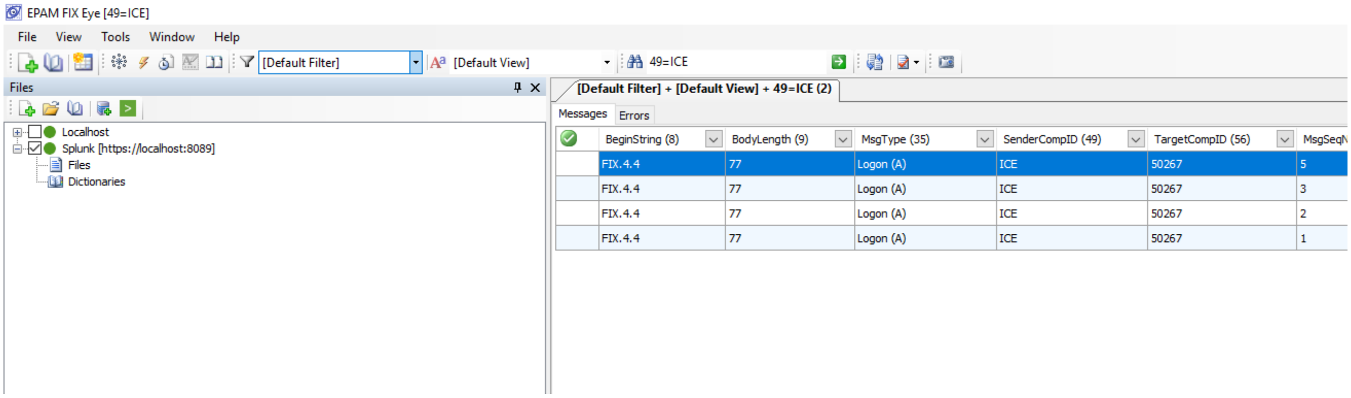
It is the case when FIX messages are imported in Splunk "as is". On the picture below it is seen that each event is a FIX message and nothing more.



i	Time	Event
>	10/9/18 4:12:01.628 PM	8=FIX.4.49=7735=A49=AME34=652=20180817-16:12:01.62857956=5026757=198=0108=10141=Y58=AME10=138 host = localhost | source = context_test2.txt | sourcetype = FIX
>	10/9/18 4:12:01.628 PM	8=FIX.4.49=7735=A49=ICE34=552=20180817-16:12:01.62857956=5026757=198=0108=10141=Y58=ICE10=138 host = localhost | source = context_test2.txt | sourcetype = FIX
>	10/9/18 4:12:01.628 PM	8=FIX.4.49=7735=A49=OIL34=452=20180817-16:12:01.62857956=5026757=198=0108=10141=Y58=OIL10=138 host = localhost | source = context_test2.txt | sourcetype = FIX
>	10/9/18 4:12:01.628 PM	8=FIX.4.49=7735=A49=ICE34=352=20180817-16:12:01.62857956=5026757=198=0108=10141=Y58=AME10=138 host = localhost | source = context_test2.txt | sourcetype = FIX

This is the main scenario of using Splunk as a back-end for FIXEye.

Example1: simple search query (49=ICE)

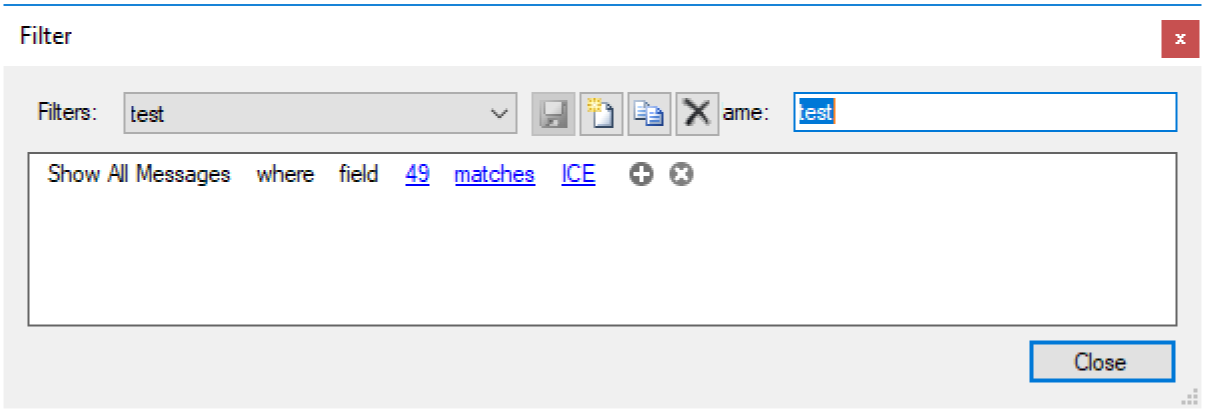


[Default Filter] [Default View] 49=ICE

[Default Filter] + [Default View] + 49=ICE (2)

BeginString (8)	BodyLength (9)	MsgType (35)	SenderCompID (49)	TargetCompID (56)	MsgSeqN
FIX.4.4	77	Logon (A)	ICE	50267	5
FIX.4.4	77	Logon (A)	ICE	50267	3
FIX.4.4	77	Logon (A)	ICE	50267	2
FIX.4.4	77	Logon (A)	ICE	50267	1

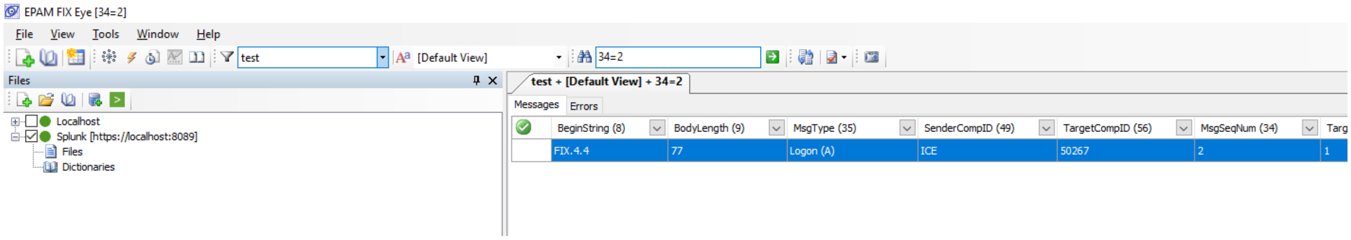
Example2: filter + search query (49=ICE in filter and 34=2 in search box)



Filters: test

ame: test

Show All Messages where field 49 matches ICE



test [Default View] 34=2

test + [Default View] + 34=2

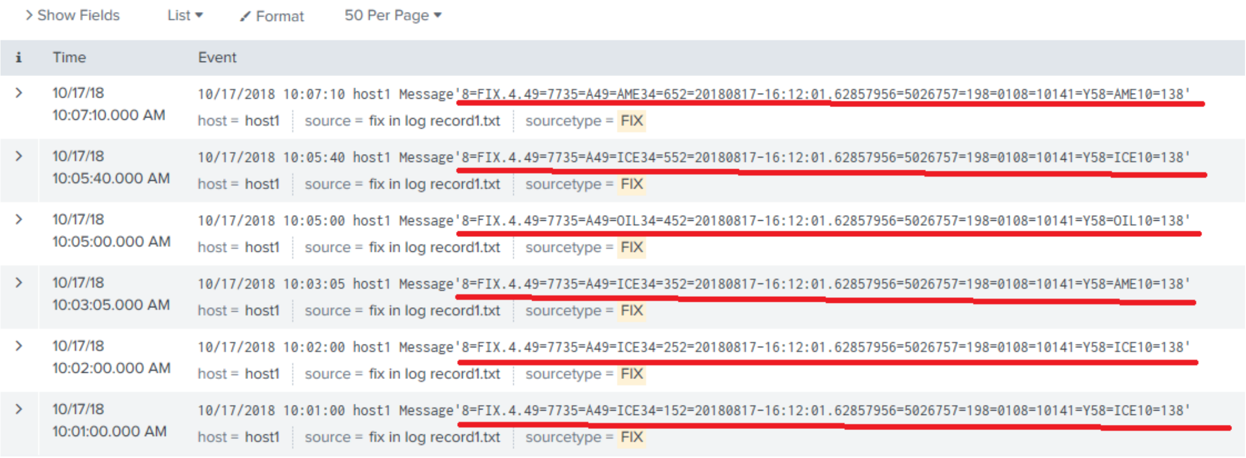
BeginString (8)	BodyLength (9)	MsgType (35)	SenderCompID (49)	TargetCompID (56)	MsgSeqNum (34)	Targ
FIX.4.4	77	Logon (A)	ICE	50267	2	1

Regular expressions work in filter but doesn't work in search queries.

Search in Log record

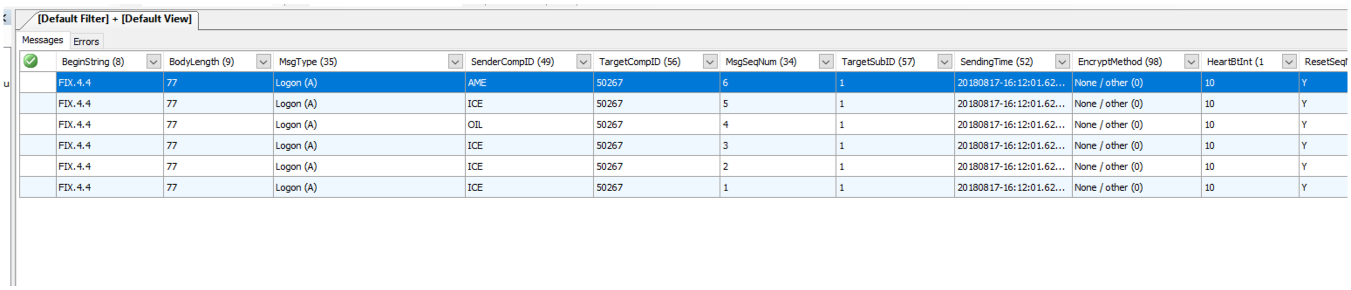
FIX messages can be a part of some log record having several fields related to a tool produced this record with one field containing raw FIX message. This can be a result when an application forwards its logs into Splunk and includes raw FIX messages in those logs.

For example let us have such records in Splunk:



i	Time	Event
>	10/17/18 10:07:10.000 AM	10/17/2018 10:07:10 host1 Message'8=FIX.4.49=7735=A49=AME34=652=20180817-16:12:01.62857956=5026757=198=0108=10141=Y58=AME10=138' host = host1 source = fix in log record1.txt sourcetype = FIX
>	10/17/18 10:05:40.000 AM	10/17/2018 10:05:40 host1 Message'8=FIX.4.49=7735=A49=ICE34=552=20180817-16:12:01.62857956=5026757=198=0108=10141=Y58=ICE10=138' host = host1 source = fix in log record1.txt sourcetype = FIX
>	10/17/18 10:05:00.000 AM	10/17/2018 10:05:00 host1 Message'8=FIX.4.49=7735=A49=OIL34=452=20180817-16:12:01.62857956=5026757=198=0108=10141=Y58=OIL10=138' host = host1 source = fix in log record1.txt sourcetype = FIX
>	10/17/18 10:03:05.000 AM	10/17/2018 10:03:05 host1 Message'8=FIX.4.49=7735=A49=ICE34=352=20180817-16:12:01.62857956=5026757=198=0108=10141=Y58=AME10=138' host = host1 source = fix in log record1.txt sourcetype = FIX
>	10/17/18 10:02:00.000 AM	10/17/2018 10:02:00 host1 Message'8=FIX.4.49=7735=A49=ICE34=252=20180817-16:12:01.62857956=5026757=198=0108=10141=Y58=ICE10=138' host = host1 source = fix in log record1.txt sourcetype = FIX
>	10/17/18 10:01:00.000 AM	10/17/2018 10:01:00 host1 Message'8=FIX.4.49=7735=A49=ICE34=152=20180817-16:12:01.62857956=5026757=198=0108=10141=Y58=ICE10=138' host = host1 source = fix in log record1.txt sourcetype = FIX

FIXEye "show all" for this pattern will be:

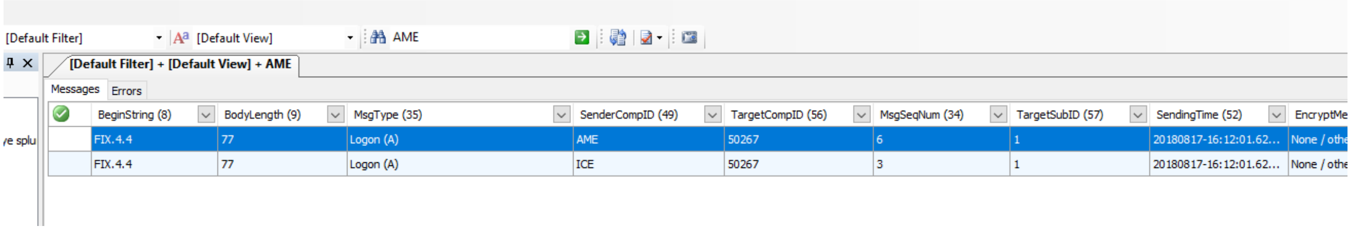


✓	BeginString (8)	BodyLength (9)	MsgType (35)	SenderCompID (49)	TargetCompID (56)	MsgSeqNum (34)	TargetSubID (57)	SendingTime (52)	EncryptMethod (98)	HeartBtInt (1	ResetSeq
	FIX.4.4	77	Logon (A)	AME	50267	6	1	20180817-16:12:01.62...	None / other (0)	10	Y
	FIX.4.4	77	Logon (A)	ICE	50267	5	1	20180817-16:12:01.62...	None / other (0)	10	Y
	FIX.4.4	77	Logon (A)	OIL	50267	4	1	20180817-16:12:01.62...	None / other (0)	10	Y
	FIX.4.4	77	Logon (A)	ICE	50267	3	1	20180817-16:12:01.62...	None / other (0)	10	Y
	FIX.4.4	77	Logon (A)	ICE	50267	2	1	20180817-16:12:01.62...	None / other (0)	10	Y
	FIX.4.4	77	Logon (A)	ICE	50267	1	1	20180817-16:12:01.62...	None / other (0)	10	Y

It can be seen that only record with fix message is displayed. It is possible to use search criteria concerning other records if you know the name of the fields or possible values.

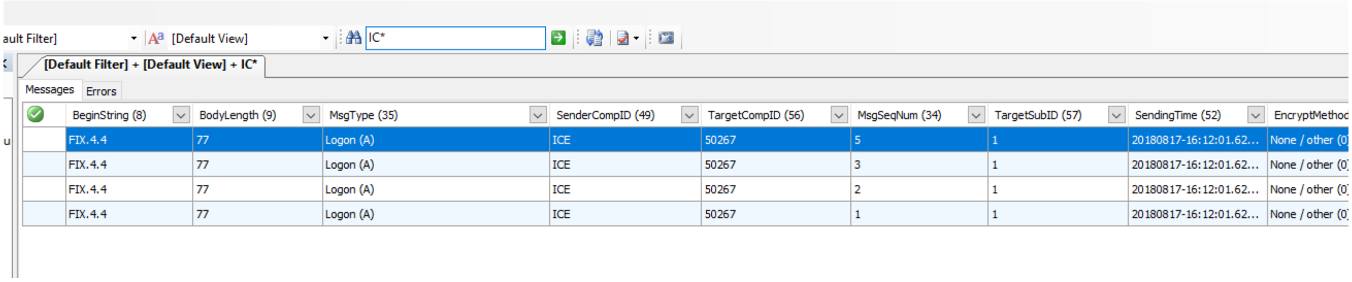
Examples:

Example3: search query = AME



✓	BeginString (8)	BodyLength (9)	MsgType (35)	SenderCompID (49)	TargetCompID (56)	MsgSeqNum (34)	TargetSubID (57)	SendingTime (52)	EncryptMe
	FIX.4.4	77	Logon (A)	AME	50267	6	1	20180817-16:12:01.62...	None / othe
	FIX.4.4	77	Logon (A)	ICE	50267	3	1	20180817-16:12:01.62...	None / othe

Example4: search query = IC* (note! to search for a part of the string * symbol must be used.)



✓	BeginString (8)	BodyLength (9)	MsgType (35)	SenderCompID (49)	TargetCompID (56)	MsgSeqNum (34)	TargetSubID (57)	SendingTime (52)	EncryptMethoc
	FIX.4.4	77	Logon (A)	ICE	50267	5	1	20180817-16:12:01.62...	None / other (0
	FIX.4.4	77	Logon (A)	ICE	50267	3	1	20180817-16:12:01.62...	None / other (0
	FIX.4.4	77	Logon (A)	ICE	50267	2	1	20180817-16:12:01.62...	None / other (0
	FIX.4.4	77	Logon (A)	ICE	50267	1	1	20180817-16:12:01.62...	None / other (0

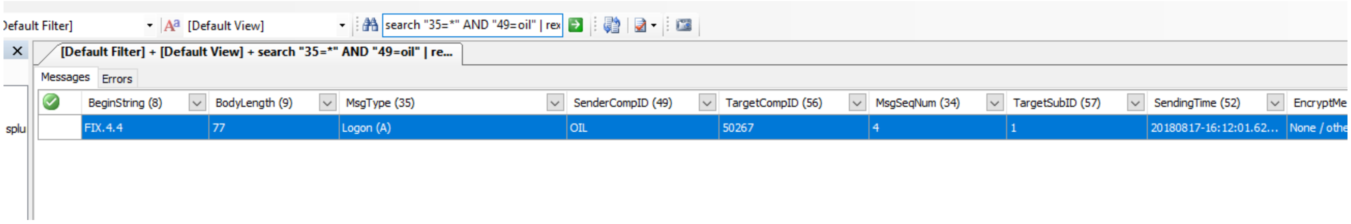
For more complicated search cases user must use splunk syntax and the search string must begin with "search". FIXEye passes this search string without any processing to Splunk and awaits raw FIX messages Splunk will return in the first field.

Example5: string "search "35=*" AND "49=oil" | rex "(?<Message>8=FIX.+\x0110=\d{3}\x01)" | search Message != '' | table Message"

Explanation:

part of expression	description
search	In splunk it is a command for search. In FIXEye it is a mandatory word meaning usage of splunk syntax in search string.
"35=*" AND "49=oil"	An expression defining what we want to find. Quotes mean that we want to search text pattern not a splunk field. * means any symbol. AND is logical conjunction. Expression means find patterns containing both 35=* and 49=oil
|	a pipeline symbol - results from the output of previous processing step are put to the input of next step
rex	field extraction command. It takes as an input a regular expression, searches in the result of previous step and puts the search result in a field
"(?<Message>8=FIX.+\x0110=\d{3}\x01)"	Input for rex command. Regular expression providing extraction of FIX message (which start with 8=FIX and ends with SOH10=any3digitsSOH sequence). <Message> is the name of a field containing extracted FIX message put in brackets.
search Message !=''	search for FIX messages that are not empty ('' is two apostrophes). Message is the name from the previous pipeline step
table Message	Pick only Message group from all groups that is in the output of previous pipeline step

The search result is shown below.



)efault Filter]
[Default View]
search "35=*" AND "49=oil" | rex
[Default Filter] + [Default View] + search "35=*" AND "49=oil" | re...
Messages
Errors
splu

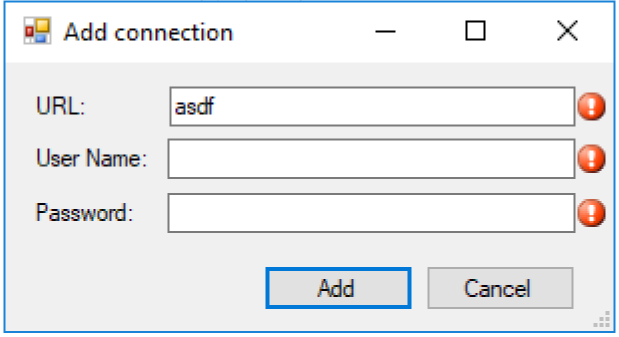
	BeginString (8)	BodyLength (9)	MsgType (35)	SenderCompID (49)	TargetCompID (56)	MsgSeqNum (34)	TargetSubID (57)	SendingTime (52)	EncryptMe
	FIX.4.4	77	Logon (A)	OIL	50267	4	1	20180817-16:12:01.62...	None / othe

Note, that FIX message must contain SOH symbols as delimiters. The space delimiters will not work!

There is a complicated way to deal with space delimiters. FIX message should be converted on the fly by adding a step into Splunk search pipeline to replace space symbol used as delimiter by SOH symbol which is supported by FIXEye. To do so please check Splunk documentation.

Troubleshooting

1. "Connection is not added" error. You can see exclamation marks on the right side of the fields. When pointer is over the mark pop-up explanations can be seen.
   Incorrect URL - change URL, it must have correct form, e.g. https://localhost:8089 for local machine.
   User name can't be empty - put in valid user name
   Password can't be empty - put in password for user

   URL: asdf
   User Name:
   Password:

2. "Error occurred while parsing messages (in Details: 401 Unauthorized Warning: login failed)" error - Check user name and password in connection properties