

Installation Instructions for FileSure Splunk integration

Install FileSure Splunk Configuration (filesure)

The first step contains the Splunk-side configuration files for FileSure configuration.

Copy the delivered folder `filesure` to `$Splunk_Home\etc\apps` on the Splunk server.

1. The file `app.conf` contains standard default Splunk attributes that come with any standard or custom Splunk “app”
2. The file `indexes.conf` defines a custom index to store the FileSure syslog data.
 - a. The default is named `syslog` but can be changed as desired. If updating, create the `local` directory, copy `indexes.conf`, update all instances of `syslog` with the preferred index name, and delete the `indexes.conf` in the `default` directory. This is not the standard process, but that’s the only way to delete the `syslog` index. Note that further updates will be required, but they will be outlined in this document.
 - b. The maximum size of the index is set to 5GB. Adjust this as needed. Once an index hits its maximum size, Splunk will automatically delete the oldest data as new data is ingested.
3. The file `macros.conf` defines a custom “macro”. All it does is simplifies searching. This will be illustrated later in the document.
4. The file `props.conf` contains the important configurations instructing Splunk how to interpret the UDP syslog FileSure data. This is the only required file on the Splunk side.
 - a. The first non-comment line is `[syslog_filesure]`. This declares the stanza that establishes the sourcetype `syslog_filesure`. All lines below it define that sourcetype.
 - b. `DATETIME_CONFIG = CURRENT`
 - i. Instructs Splunk to use the current date time when the data is received as the `_time` Splunk variable.
 - c. `LINE_BREAKER = ([\r\n]+)`
 - i. Instructs Splunk to split events on every new line (each syslog message is a one-liner).
 - d. The other fields before the `EXTRACT-` declarations are default Splunk sourcetype definitions.
 - e. The `EXTRACT-` fields extract custom fields so that they are available when searching in Splunk. They use standard python regular expressions to do so. The name immediately following `EXTRACT-` does not matter. It gives a name to each field extraction that is not visible in Splunk. The field extraction works as such: `(?<field_name>field_value_regex)`. Anything outside of those

parentheses is required to match but not assigned to any variables. The field names chosen were used in accordance with the Splunk Common Information Model. This can be googled, but all fields are later renamed to the field names outlined in the requirements.

Sample data using the latest version (05/01/2020) of FileSure:

```
> May  1 04:32:08 127.0.0.1 BYS142487722:{C3E71101-710C-4D2E-B3EE-
AEDFC5FA31DE}:EC2AMAZ-3B7MT1R:EC2AMAZ-3B7MT1R\Administrator:Splunk
Apps | C:\Program Files\Splunk\etc\apps\Splunk_TA_windows\license-
eula_rename2.rtf | 0 | 0 | File Rename | C:\Windows\explorer.exe |
Fixed Drive | 1 | C:\Program
Files\Splunk\etc\apps\Splunk_TA_windows\license-eula.rtf
> May  1 04:32:08 127.0.0.1 BYS142482220:{C3E71101-710C-4D2E-B3EE-
AEDFC5FA31DE}:EC2AMAZ-3B7MT1R:EC2AMAZ-3B7MT1R\Administrator:Splunk
Apps | C:\PROGRAM FILES\SPLUNK\ETC\APPS\SPLUNK_TA_WINDOWS\LICENSE-
EULA_RENAME2.RTF | 0 | 0 | Opened for Delete | C:\Windows\explorer.exe
| Fixed Drive | 1 |
> May  1 04:32:05 127.0.0.1 BYS114704266:{C3E71101-710C-4D2E-B3EE-
AEDFC5FA31DE}:EC2AMAZ-3B7MT1R:EC2AMAZ-3B7MT1R\Administrator:Splunk
Apps | C:\Program Files\Splunk\etc\apps\Splunk_TA_windows\license-
eula_rename.rtf | 0 | 0 | File Rename | C:\Windows\explorer.exe |
Fixed Drive | 1 | C:\Program
Files\Splunk\etc\apps\Splunk_TA_windows\license-eula_rename2.rtf
> May  1 04:32:05 127.0.0.1 BYS114668936:{C3E71101-710C-4D2E-B3EE-
AEDFC5FA31DE}:EC2AMAZ-3B7MT1R:EC2AMAZ-3B7MT1R\Administrator:Splunk
Apps | C:\PROGRAM FILES\SPLUNK\ETC\APPS\SPLUNK_TA_WINDOWS\LICENSE-
EULA_RENAME.RTF | 0 | 0 | Opened for Delete | C:\Windows\explorer.exe
| Fixed Drive | 1 |
```

- i. EXTRACT-universal-fields = `(?<src_ip>[\d\.]+)`
`BYS(?<id>\d+):\{?(?<org_id>[\w-]+)\}?:(?<dvc>[\w-]+):`
 1. `src_ip` (later renamed to `IP_Address`) is any combination of digits (`\d`) and periods (`\.`) followed by a space and `BYS`
 2. `id` (later renamed to `Message_Number`) is all of the consecutive digits (`\d+`) immediately after `BYS`
 3. `org_id` (later renamed to `Organization_ID`) is all of the A-Z, a-z, 0-9, and '-' characters immediately after `Message_Number`, ':', and an optional '{'. `Organization_ID` may have an optional '}' following it.
 4. `dvc` (later renamed to `Machine_Name`) is all of the A-Z, a-z, 0-9, and '-' characters immediately after `Organization_ID`, the optional '}', and a ':' character, and is followed by a ':' character.
 5. The fields in this regular expression are parsed for all FileSure syslog events. It applies to both 108 and 110 events.
- ii. EXTRACT-110-fields1 = `\sBYS[^:]+:[^:]+:[^:]+:(?<src_user>[^:]+):(?<rule_name>[^\\]+)\s?`
 1. This field extraction applies only to FileSure log level 110.
 2. The field extraction starts with `BYS` followed by three ':' characters with anything allowed between the ':' characters

3. `src_user` (later renamed to `User_Name`) extracts all non-':' characters between the third and fourth ':' characters after `BYS`
4. `rule_name` (later renamed to `Rule_Name`) extracts everything after `User_Name` and a ':' and has an optional space and a '|' character after it.

iii. `EXTRACT-110-fields2 =`

```
\\|s?(?<file_name>[^\|]+)\|s?\\|s?(?<FileSure_Denied>\d+
+)\|s?\\|s?(?<Windows_Denied>\d+)\|s?\\|s?(?<Operation>[
^\|]+)\|s?\\|s?(?<Executable_Name>[^\|]+)\|s?\\|s?(?<Dri
ve_Type>[^\|]+)\|s?\\|s?(?<FileSure_Type>\d+)\|s?\\|s?(?
<file_rename>.*)$
```

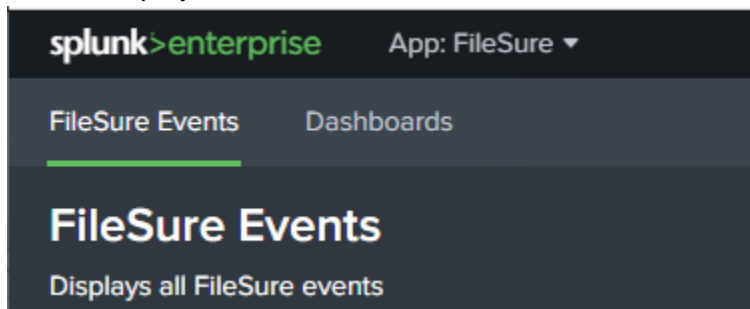
1. This field extraction applies only to FileSure log level 110 and begins with the first '|' character followed by an optional space.
2. `file_name` (later renamed to `File_Name`) is all of the characters between the first two '|' characters with leading and trailing spaces removed.
3. `FileSure_Denied` and `Windows_Denied` are one or more digits in the next two segments separated by '|' and optional space characters.
4. `Operation`, `Executable_Name`, `Drive_Type`, and `FileSure_Type` are the next segment of characters separated by '|' and optional leading and trailing spaces. `FileSure_Type` is limited to digit characters only.
5. `file_rename` (later renamed to `Rename_To`) is an optional field that matches everything after the last '|' character to the end of the message ('\$').

iv. `EXTRACT-108`

1. This is untested based on the provided data. It works similarly to the 110 fields.

f. The `FIELDALIAS-` fields simply rename the extracted fields from `EXTRACT-`. Both the original and the renamed alias are displayed in the Splunk GUI.

5. The data subfolder contains a custom navigation menu (FileSure Events and Dashboards in the screenshot below) and a sample dashboard. The navigation bar is displayed below, and the dashboard is outlined later in the document.



All of the configurations mentioned above are accessed via the GUI by navigating to: Settings > Sourcetypes > Type "syslog_filesure" (Uncheck "Show only popular")

splunk enterprise Apps Administrator Messages Settings Activity Help Find

Source Types

Source types are used to assign configurations like timestamp recognition, event breaking, and field extractions to data indexed by Splunk. [Learn more](#)

1 Source Types ☐ Show only popular Category: All App: syslog_filesure x

Name syslog_filesure

FileSure SysLog sourcetype. This sourcetype breaks on every line and extracts the _time as the current time and fields for 110 and 108 events.

- KNOWLEDGE
 - Searches, reports, and alerts
 - Data models
 - Event types
 - Tags
 - Fields
 - Lookups
 - User interface
 - Alert actions
 - Advanced search
 - All configurations
- DATA
 - Data inputs
 - Forwarding and receiving
 - Indexes
 - Report acceleration summaries
 - Source types
- DISTRIBUTED ENVIRONMENT
 - Indexer clustering
 - Forwarder management
 - Distributed search
- USERS AND AUTHENTICATION
 - Roles
 - Users
 - Tokens
 - Password Management
 - Authentication Methods
- SYSTEM
 - Server settings
 - Server controls
 - Health report manager
 - Instrumentation
 - Licensing
 - Workload management

Add Data Monitoring Console

Edit Source Type: syslog_filesure

Description: FileSure SysLog sourcetype. This sourcetype breaks on every line and extracts the _time

Destination app: FileSure

Category: Custom

Indexed Extractions: none

Event Breaks: Timestamp Advanced

Name	Value	
CHARSET	AUTO	x
DATETIME_CONFIG	CURRENT	x
EXTRACT-108-details	^[^:]+:[^:]+:[^:]+:(?<Details>.*)	x
EXTRACT-108-fields1	:(?<Sender>[^:]+):User (?<src_us	x
EXTRACT-110-fields1	\sBYS[^:]+:[^:]+:(?<src_user>	x
EXTRACT-110-fields2	\\s?(?<file_name>[^\\]+)\\s?\\s?(?	x
EXTRACT-universal-fields	(?<src_ip>[\\d\\.]+) BYS(?<id>\\d+):	x
FIELDALIAS-dvc	dvc AS Machine_Name	x
FIELDALIAS-file_rename	file_rename AS Rename_To	x
FIELDALIAS-id	id AS Message_Number	x
FIELDALIAS-org_id	org_id AS Organization_ID	x

Install FileSure Data Input (filesure_uf)

Once the Splunk configuration has been installed, the data input can be enabled. This was placed in a separate Splunk app in case the environment expands to the point where FileSure monitors are no longer on the Splunk server. If Splunk forwarders are installed on non-Splunk servers, this is the app that will need to be installed on those machines running the FileSure product.

Copy the delivered folder `filesure_uf` to `$Splunk_Home\etc\apps` on all servers running FileSure. For the initial install, this is the same server that Splunk is running on as described in the requirements.

1. The file `app.conf` contains standard default Splunk attributes that come with any standard or custom Splunk “app”
2. The file `inputs.conf` contains the input configuration to instruct Splunk to listen for UDP messages on port 514 of the local machine.
 - a. `index = syslog`
 - i. This is where Splunk is instructed to store the data. If the index was customized as mentioned previously, update this to the name of the custom index name.
 - b. `sourcetype = syslog_filesure`
 - i. This tells Splunk how to interpret the data. This ties back to the `props.conf` file installed on the Splunk server.
 - c. `connection_host = dns`
 - i. This tells Splunk how to resolve the “host” field name in Splunk (using dns instead of ip address or other options).
3. Restart the Splunk Windows Service after installation.
4. To view this in the GUI, navigate to Settings > Data Inputs > UDP
 - a. Note that the webserver (GUI) is not available for Splunk forwarders (this does not apply to the current development environment)

ork ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk

cal inputs

Type
Local event log collection Collect event logs from this machine.
Remote event log collections Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.
Files & Directories Index a local file or monitor an entire directory.
Local performance monitoring Collect performance data from local machine.
Remote performance monitoring Collect performance and event information from remote hosts. Requires domain credentials.
HTTP Event Collector Receive data over HTTP or HTTPS.
TCP Listen on a TCP port for incoming data, e.g. syslog.
UDP Listen on a UDP port for incoming data, e.g. syslog.
...

Add Data

Monitoring Console

KNOWLEDGE

Searches, reports, and alerts

Data models

Event types

Tags

Fields

Lookups

User interface

Alert actions

Advanced search

All configurations

SYSTEM

Server settings

Server controls

Health report manager

Instrumentation

Licensing

Workload management

DATA

Data inputs

Forwarding and receiving

Indexes

Report acceleration summaries

Source types

DISTRIBUTED ENVIRONMENT

Indexer clustering

Forwarder management

Distributed search

USERS AND AUTHENTICATION

Roles

Users

Tokens

Password Management

Authentication Methods

514
Data Inputs » UDP » 514

Source

Source name override

If set, overrides the default source value for your UDP entry (host:port).

Source type

Set sourcetype field for all events from this source.

Set sourcetype

Source type *

☒ More settings

Host

Set host

IP DNS Custom

"DNS" sets the host to the DNS entry of the remote server.

Index

Set the destination index for this source.

Index

Restrict to Host

Only accept requests from this host.

Cancel Save

5. Ensure the FileSure product is running and writing to syslog on UDP 514 on the server with this app installed.

(Optional) Install custom Splunk Windows inputs

This is entirely optional and has no effect on the FileSure customizations. This was used in developing the Splunk configurations to get a better overview of the server. This add-on is often used for all servers that communicate with Splunk, but as an optional option, feel free to install this

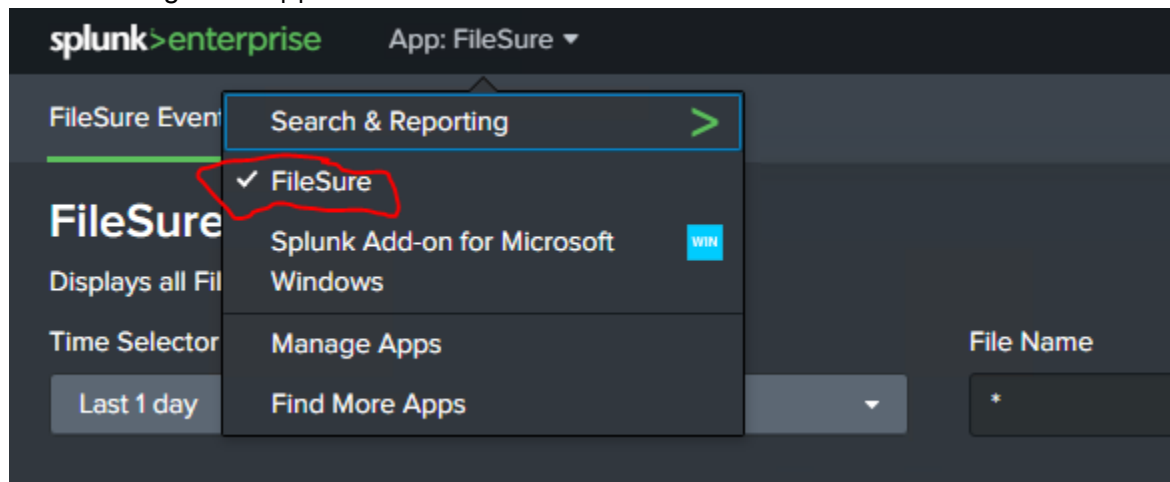
1. Download the Splunk-developed app Splunk add-on for Windows (<https://splunkbase.splunk.com/app/742/>). This add-on adds great built-in Windows monitoring, and nothing is enabled by default. SplunkBase resources are free after creating a free Splunk account.
2. Copy the folder local to \$Splunk_Home\etc\apps\Splunk_TA_Windows, and restart the Splunk service.
3. The file indexes.conf defines a custom index to store the windows event log data.
4. The file inputs.conf enables the following inputs:
 - a. Windows Application Event Log
 - b. Windows Security Event Log
 - c. Windows System Event Log
 - d. Windows PowerShell Operational Event Log
 - e. ByStorm FileSure Event Log
 - f. Default "listening ports" input (runs every 300 seconds while Splunk is running)
 - g. Windows Network Monitoring
 - h. No custom index was set for the previous two so they go to index = main (default Splunk index)

FileSure for Splunk Quick walkthrough

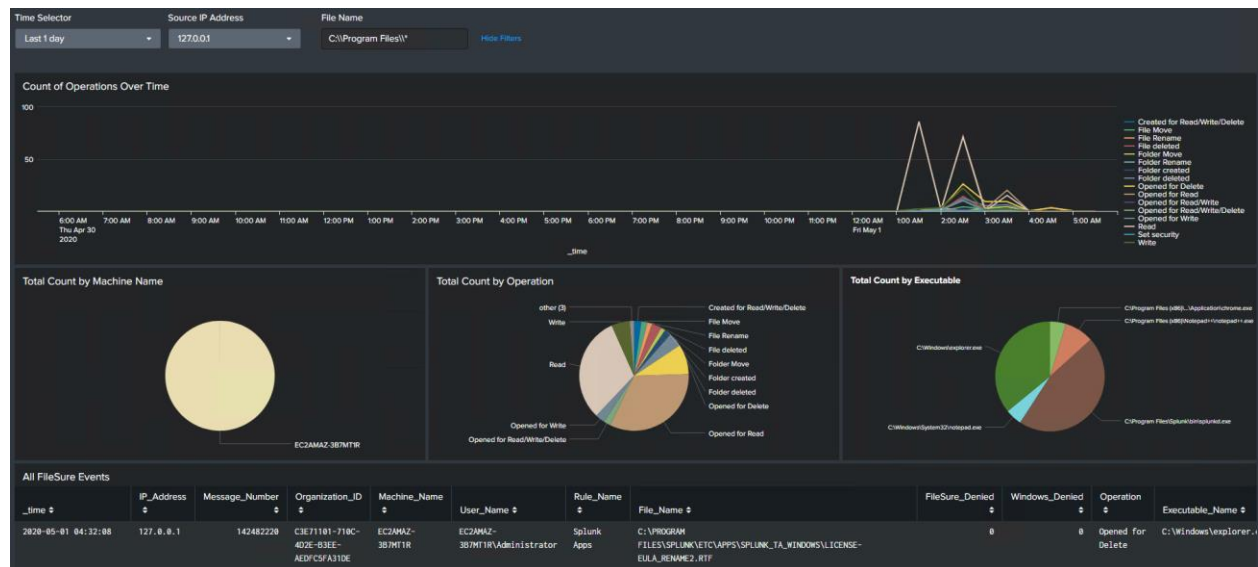
Once the first two sections have been installed, data will be available in Splunk.

1. A dashboard has been provided to give a jump-start to Splunk-side development.

Navigate to Apps > FileSure



2. This dashboard is an example of the sorts of things you can now do with your data
 - a. The “Time Selector” provides the ability to quickly switch to different points in time. By default, it searches the past one day.
 - b. The “Source IP Address” is an example of a drop-down that extracts data and allows the user to quickly select from valid options.
 - c. The “File Name” is an example of a raw text search that allows the user to enter data freely. As designed, backslashes must be escaped (use “C:\\Program Files*” instead of “C:\Program Files*”), and use * as the wild card (this is universal to Splunk searching).
 - d. The first panel shows a chart of counts of file operations over time. This can be customized to show counts, averages, etc. of any extracted fields over time.
 - e. The second row shows a few sample pie charts of counts of a few sample fields over the selected time range.



f. The bottom panel demonstrates the raw data with the field names extracted.

_time	IP_Address	Message_Number	Organization_ID	Machine_Name	User_Name	Rule_Name	File_Name	FileSure_Denied	Windows_Denied	Operation	Executable_Name	Drive
2020-05-01 04:32:08	127.0.0.1	142482228	C3E71181-718C-402E-83EE-AEDFC5FA310E	EC2AMAZ-3B7MT1R	EC2AMAZ-3B7MT1R\Administrator	Splunk Apps	C:\PROGRAM FILES\SPLUNK\ETC\APPS\SPLUNK_TA_WINDOWS\LICENCE-EULA_RENAME2.RTF	0	0	Opened for Delete	C:\Windows\explorer.exe	Fixe Drive
2020-05-01 04:32:08	127.0.0.1	142487722	C3E71181-718C-402E-83EE-AEDFC5FA310E	EC2AMAZ-3B7MT1R	EC2AMAZ-3B7MT1R\Administrator	Splunk Apps	C:\PROGRAM FILES\SPLUNK\ETC\APPS\SPLUNK_TA_WINDOWS\LICENCE-EULA_RENAME2.RTF	0	0	File Rename	C:\Windows\explorer.exe	Fixe Drive
2020-05-01 04:32:05	127.0.0.1	114704266	C3E71181-718C-402E-83EE-AEDFC5FA310E	EC2AMAZ-3B7MT1R	EC2AMAZ-3B7MT1R\Administrator	Splunk Apps	C:\PROGRAM FILES\SPLUNK\ETC\APPS\SPLUNK_TA_WINDOWS\LICENCE-EULA_RENAME2.RTF	0	0	File Rename	C:\Windows\explorer.exe	Fixe Drive
2020-05-01 04:32:05	127.0.0.1	114668936	C3E71181-718C-402E-83EE-AEDFC5FA310E	EC2AMAZ-3B7MT1R	EC2AMAZ-3B7MT1R\Administrator	Splunk Apps	C:\PROGRAM FILES\SPLUNK\ETC\APPS\SPLUNK_TA_WINDOWS\LICENCE-EULA_RENAME2.RTF	0	0	Opened for Delete	C:\Windows\explorer.exe	Fixe Drive
2020-05-01 04:32:03	127.0.0.1	94925549	C3E71181-718C-402E-83EE-AEDFC5FA310E	EC2AMAZ-3B7MT1R	EC2AMAZ-3B7MT1R\Administrator	Splunk Apps	C:\PROGRAM FILES\SPLUNK\ETC\APPS\SPLUNK_TA_WINDOWS\LICENCE-EULA_RENAME2.RTF	0	0	File Rename	C:\Windows\explorer.exe	Fixe Drive
2020-05-01 04:32:03	127.0.0.1	94921078	C3E71181-718C-402E-83EE-AEDFC5FA310E	EC2AMAZ-3B7MT1R	EC2AMAZ-3B7MT1R\Administrator	Splunk Apps	C:\PROGRAM FILES\SPLUNK\ETC\APPS\SPLUNK_TA_WINDOWS\LICENCE-EULA_RENAME2.RTF	0	0	Opened for Delete	C:\Windows\explorer.exe	Fixe Drive
2020-05-01 03:51:32	127.0.0.1	1558912484	C3E71181-718C-402E-83EE-AEDFC5FA310E	EC2AMAZ-3B7MT1R	EC2AMAZ-3B7MT1R\Administrator	Splunk Apps	C:\PROGRAM FILES\SPLUNK\ETC\APPS\SPLUNK_TA_WINDOWS\LOCAL\INDEXES.CONF	0	0	Read	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	Fixe Drive
2020-05-01 03:51:32	127.0.0.1	1558909038	C3E71181-718C-402E-83EE-AEDFC5FA310E	EC2AMAZ-3B7MT1R	EC2AMAZ-3B7MT1R\Administrator	Splunk Apps	C:\PROGRAM FILES\SPLUNK\ETC\APPS\SPLUNK_TA_WINDOWS\LOCAL\INDEXES.CONF	0	0	Opened for Read	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	Fixe Drive

g. All of the panels have the option to view the searches that generated them. Simple hover over the panel on the bottom-right part of it, and click the magnifying glass. This opens the search in a new tab.

0	0	Opened for Read	C:\Windows\System32\notepad.exe	Fixe Drive
0	0	Read	C:\Windows\System32\notepad.exe	Fixe Drive
0	0	Write	C:\Windows\System32\notepad.exe	Fixe Drive
0	0	Opened for Read/Write	C:\Windows\System32\notepad.exe	Fixe Drive

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Q 10m ago

5:59 AM

splunk>enterprise App: FileSure

FileSure Events Dashboards

New Search

```
'get_syslog_filesure'
| table _raw _time IP_Address Message_Number Organization_ID Machine_Name User_Name Rule_Name File_Name FileSure_Denied Windows_Denied Operation Executable_Name Drive_Type FileSure_Type
| rename _time _time
| sort _time | table _time IP_Address Message_Number Organization_ID Machine_Name User_Name Rule_Name File_Name FileSure_Denied Windows_Denied Operation Executable_Name Drive_Type FileSure_Type
| search IP_Address="127.0.0.1" File_Name="C:\\Program Files\\*"
```

✓ 554 events (4/30/20 6:00:09.000 AM to 5/1/20 6:00:09.000 AM) No Event Sampling

Events Patterns **Statistics (554)** Visualization

20 Per Page Format Preview

_time	IP_Address	Message_Number	Organization_ID	Machine_Name	User_Name	Rule_Name	File_Name	FileSure_Denied	Windows
2020-05-01 04:32:08	127.0.0.1	142482220	C3E71101-710C-402E-B3EE-AEDFC5FA310E	EC2AMAZ-3B7MT1R	EC2AMAZ-3B7MT1R\Administrator	Splunk Apps	C:\PROGRAM FILES\SPLUNK\ETC\APPS\SPLUNK_TA_WINDOWS\LICENSE-EULA_RENAME2.RTF	0	
2020-05-01 04:32:08	127.0.0.1	142487722	C3E71101-710C-402E-B3EE-AEDFC5FA310E	EC2AMAZ-3B7MT1R	EC2AMAZ-3B7MT1R\Administrator	Splunk Apps	C:\Program Files\Splunk\etc\apps\Splunk_TA_windows\license-eula_rename2.rtf	0	

- h. The search has extra lines in it due to how the dashboard is put together. To simplify things, delete everything after and including the fourth bar

FileSure Events Dashboards

New Search

```
'get_syslog_filesure'
| table _raw _time IP_Address Message_Number Organization_ID Machine_Name User_Name Rule_Name File_Name FileSure_Denied Windows_Denied Operation Executable_Name Drive_Type FileSure_Type
| sort _time
```

✓ 557 events (4/30/20 6:01:36.000 AM to 5/1/20 6:01:36.000 AM) No Event Sampling

Events Patterns **Statistics (557)** Visualization

20 Per Page Format Preview

_raw	_time	IP_Address	Message_Number	Organization_ID	Machine_Name	User_Name	Rule_Name	File_Name
May 1 04:32:08 127.0.0.1 BYS142482220:{C3E71101-710C-402E-B3EE-AEDFC5FA310E}:EC2AMAZ-3B7MT1R\Administrator:Splunk Apps C:\PROGRAM FILES\SPLUNK\ETC\APPS\SPLUNK_TA_WINDOWS\LICENSE-EULA_RENAME2.RTF 0 0 0 Opened for Delete C:\Windows\explorer.exe Fixed Drive 1	2020-05-01 04:32:08	127.0.0.1	142482220	C3E71101-710C-402E-B3EE-AEDFC5FA310E	EC2AMAZ-3B7MT1R	EC2AMAZ-3B7MT1R\Administrator	Splunk Apps	C:\PROGRAM FILES\SPLUNK\ETC\APPS\SPLUNK_TA_WINDOWS\LICENSE-EULA_RENAME2.RTF

- i. There is now an extra field called “_raw”. This allows you to see the actual raw data sent by FileSure. There are also two data points before the message - these are automatically extracted by Splunk (a time and a source IP address). This _raw data can be compared to the rest of the fields to verify accuracy.
- j. The text `get_syslog_filesure` is the macro mentioned previously. Macros simply resolve to other text so replace the first line with the definition of the macro
- index=syslog sourcetype=syslog_filesure

New Search

```
index=syslog sourcetype=syslog_filesure
| table _raw _time IP_Address Message_Number Organization_ID Machine_Name User_Name Rule_Name File_Name FileSure_Denied Windows_Denied Operation Executable_Name
| sort -_time
```

✓ 557 events (4/30/20 6:04:06.000 AM to 5/1/20 6:04:06.000 AM) No Event Sampling

Events Patterns **Statistics (557)** Visualization

20 Per Page Format Preview

_raw	_time	IP_Address	Message_Number	Organization_ID	Machine_Name	User_Name
May 1 04:32:08 127.0.0.1 BYS142482220:{C3E71101-710C-4D2E-B3EE-AEDFC5FA31DE}:EC2AMAZ-3B7MT1R:EC2AMAZ-3B7MT1R\Administrator: Splunk Apps C:\PROGRAM	2020-05-01 04:32:08	127.0.0.1	142482220	C3E71101-710C-4D2E-B3EE-AEDFC5FA31DE	EC2AMAZ-3B7MT1R	EC2AMAZ-3B7MT1R

