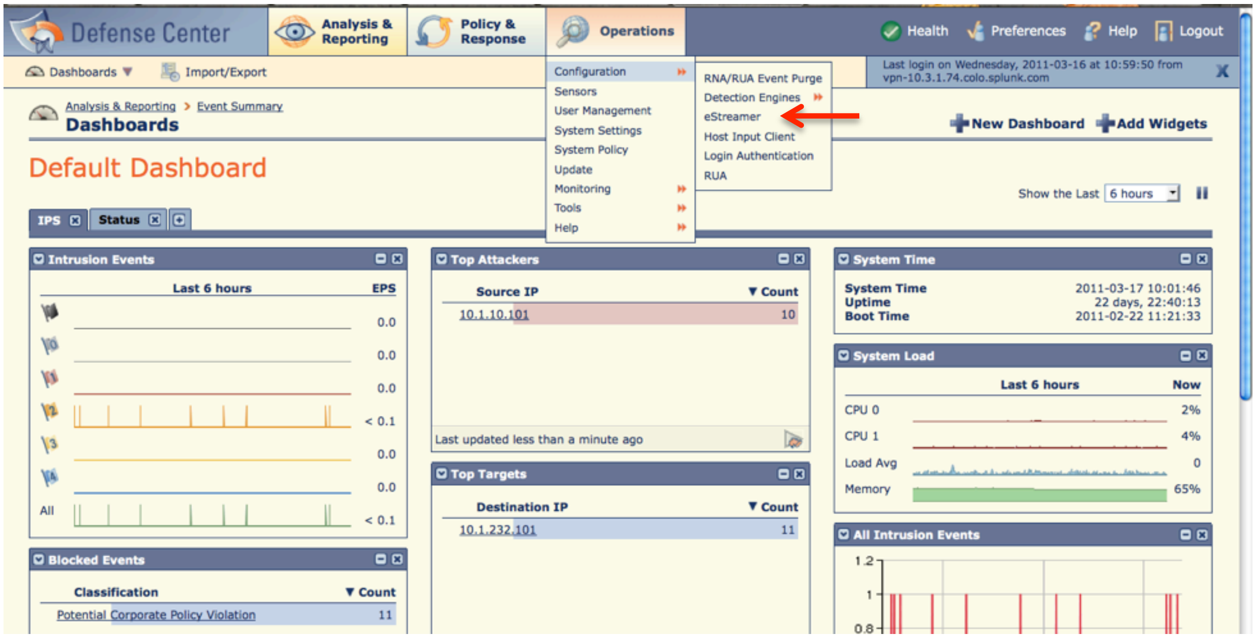
How to add an eStreamer client:

By
Andrew Thanalertvisuti, Solutions Architect, Splunk Inc.

1. Go to Operations → Configuration → eStreamer



Source IP	Count
10.1.10.101	10

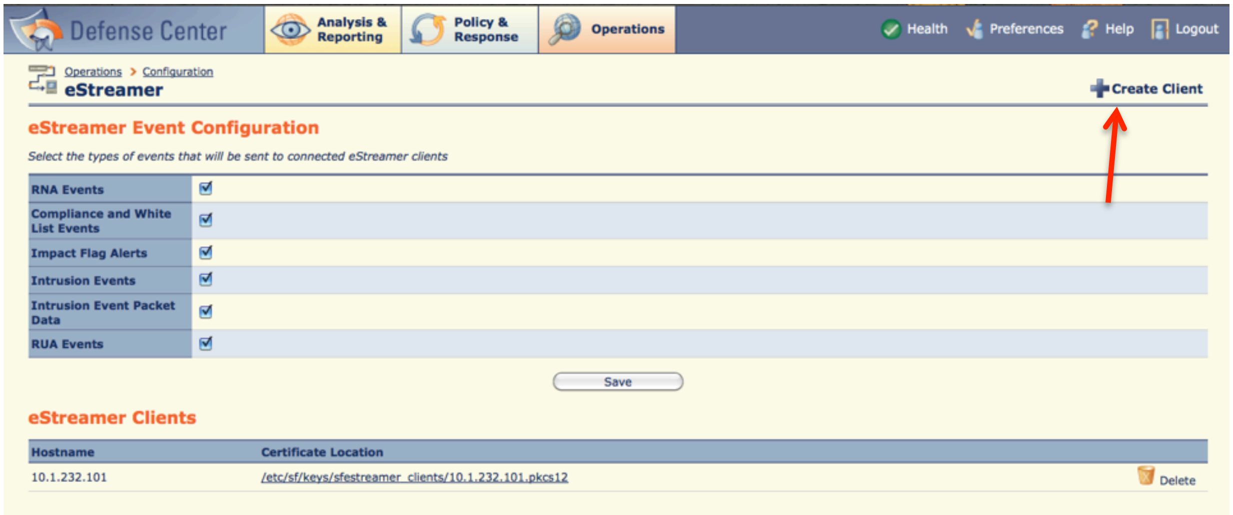
Destination IP	Count
10.1.232.101	11

System Time	2011-03-17 10:01:46
Uptime	22 days, 22:40:13
Boot Time	2011-02-22 11:21:33

	Last 6 hours	Now
CPU 0		2%
CPU 1		4%
Load Avg		0
Memory		65%

Classification	Count
Potential Corporate Policy Violation	11

2. Click on Create Client.



eStreamer Event Configuration

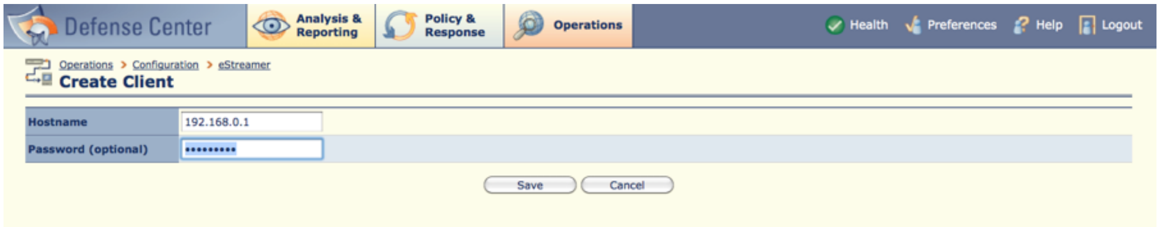
Select the types of events that will be sent to connected eStreamer clients

RNA Events	☑
Compliance and White List Events	☑
Impact Flag Alerts	☑
Intrusion Events	☑
Intrusion Event Packet Data	☑
RUA Events	☑

eStreamer Clients

Hostname	Certificate Location	
10.1.232.101	/etc/sf/keys/sfestreamer_clients/10.1.232.101.pkcs12	Delete

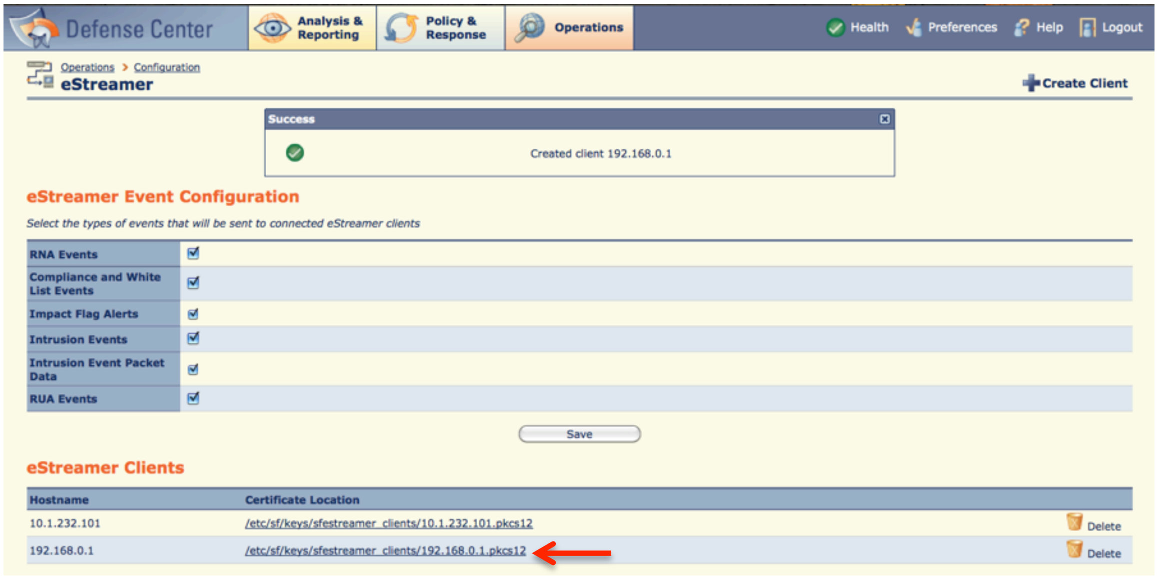
3. Enter a hostname or an IP address of the client that will connect to eStreamer server (i.e. Defense Center). Then click Save.



Create Client

Hostname	192.168.0.1
Password (optional)	•••••••••

4. Click on the created client Certificate Location.



eStreamer

Success

Created client 192.168.0.1

eStreamer Event Configuration

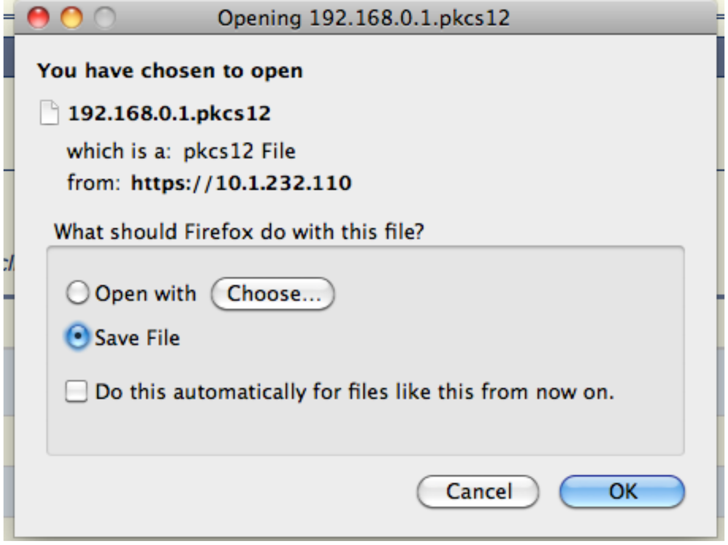
Select the types of events that will be sent to connected eStreamer clients

RNA Events	☑
Compliance and White List Events	☑
Impact Flag Alerts	☑
Intrusion Events	☑
Intrusion Event Packet Data	☑
RUA Events	☑

eStreamer Clients

Hostname	Certificate Location
10.1.232.101	/etc/sf/keys/sfestreamer_clients/10.1.232.101.pkcs12
192.168.0.1	/etc/sf/keys/sfestreamer_clients/192.168.0.1.pkcs12

5. Save the certificate.



Opening 192.168.0.1.pkcs12

You have chosen to open

192.168.0.1.pkcs12

which is a: pkcs12 File

from: **https://10.1.232.110**

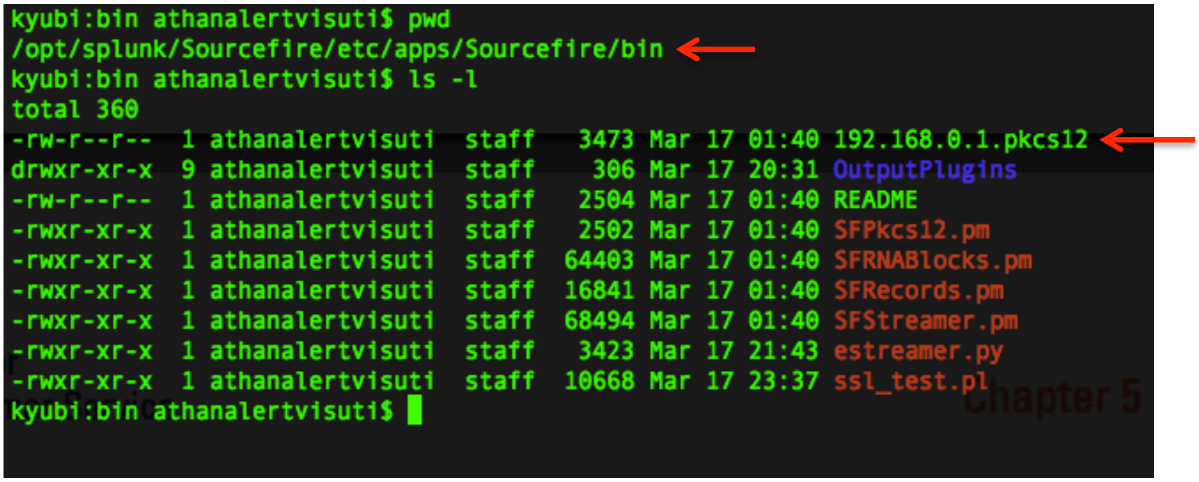
What should Firefox do with this file?

○ Open with

● Save File

☐ Do this automatically for files like this from now on.

6. Copy the certificate to the eStreamer client's system (inside Splunk for Sourcefire app's directory)



```
kyubi:bin athanalertvisuti$ pwd
/opt/splunk/Sourcefire/etc/apps/Sourcefire/bin
kyubi:bin athanalertvisuti$ ls -l
total 360
-rw-r--r--  1 athanalertvisuti  staff   3473 Mar 17 01:40 192.168.0.1.pkcs12
drwxr-xr-x  9 athanalertvisuti  staff    306 Mar 17 20:31 OutputPlugins
-rw-r--r--  1 athanalertvisuti  staff   2504 Mar 17 01:40 README
-rwxr-xr-x  1 athanalertvisuti  staff   2502 Mar 17 01:40 SFPkcs12.pm
-rwxr-xr-x  1 athanalertvisuti  staff  64403 Mar 17 01:40 SFRNABlocks.pm
-rwxr-xr-x  1 athanalertvisuti  staff  16841 Mar 17 01:40 SFRecords.pm
-rwxr-xr-x  1 athanalertvisuti  staff  68494 Mar 17 01:40 SFStreamer.pm
-rwxr-xr-x  1 athanalertvisuti  staff   3423 Mar 17 21:43 estreamer.py
-rwxr-xr-x  1 athanalertvisuti  staff  10668 Mar 17 23:37 ssl_test.pl
kyubi:bin athanalertvisuti$ 
```

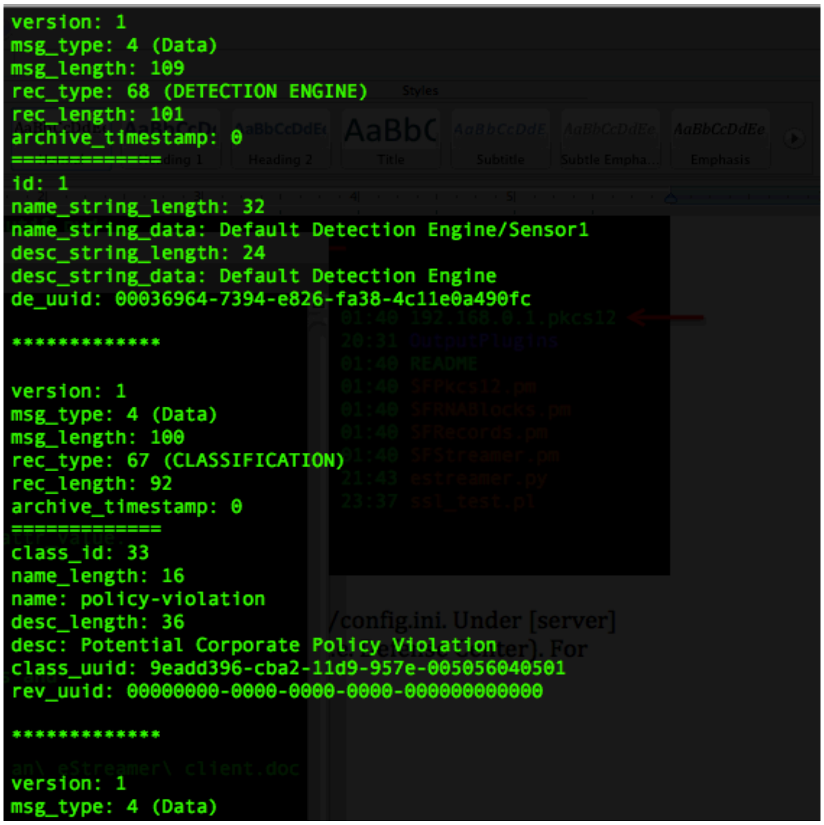
7. Edit $SPLUNK_HOME/etc/apps/Sourcefire/default/config.ini. Under [server] stanza, input the IP address of the eStreamer server (i.e. Defense Center). For example:

```
[server]
# IP address of eStreamer server
ip = 10.0.0.1
```

8. Try to test the connection from your eStreamer client to eStreamer server by running the following command (assuming the server ip is 10.0.0.1):

```
$ $SPLUNK_HOME/etc/apps/Sourcefire/bin/ssl_test.pl  10.0.0.1
```

If everything is set up correctly, the above command should return you many results from the eStreamer server, as shown in the following figure:



```
version: 1
msg_type: 4 (Data)
msg_length: 109
rec_type: 68 (DETECTION ENGINE)
rec_length: 101
archive_timestamp: 0
=============
id: 1
name_string_length: 32
name_string_data: Default Detection Engine/Sensor1
desc_string_length: 24
desc_string_data: Default Detection Engine
de_uuid: 00036964-7394-e826-fa38-4c11e0a490fc

*************

version: 1
msg_type: 4 (Data)
msg_length: 100
rec_type: 67 (CLASSIFICATION)
rec_length: 92
archive_timestamp: 0
=============
class_id: 33
name_length: 16
name: policy-violation
desc_length: 36
desc: Potential Corporate Policy Violation
class_uuid: 9eadd396-cba2-11d9-957e-005056040501
rev_uuid: 00000000-0000-0000-0000-000000000000

*************

version: 1
msg_type: 4 (Data)
```

9. Now you are ready to start using Splunk for Sourcefire App!