FireEye
SECURITY REIMAGINED

SPECIAL REPORT

FIREEYE APP FOR SPLUNK ENTERPRISE 6.X

Configuration Guide Version 1.3

CONTENTS

Welcome

This document provides instructions on installing the FireEye App for Splunk Enterprise and configuring the devices to communicate.

Supported FireEye Event Formats

Explanation of protocols

Easiest to configure

#	Protocol	Enc	Reason
1	SYSLOG - TCP CEF	No	TCP does not require command-line configuration on FireEye Appliance
2	SYSLOG - UDP CEF	No	Provides more data than CSV
3	SYSLOG - TCP CSV	No	TCP does not require command-line configuration on FireEye Appliance
4	SYSLOG - UDP CSV	No	JSON provides more data than CEF and CSV

Requires more effort to configure

#	Protocol	Enc	Reason
1	SYSLOG - TCP XML	No	TCP does not require command-line configuration on FireEye Appliance
2	SYSLOG - UDP XML	No	XML provides more data than CEF and CSV
3	SYSLOG - TCP JSON	No	TCP does not require command-line configuration on FireEye Appliance
4	SYSLOG - UDP JSON	No	Last resort - May not send protocol field

Most effort to configure

#	Protocol	Enc	Reason
1	HTTPS JSON	Yes	Encrypted, lighter than XML
2	HTTPS XML	Yes	Encrypted

General notes

- When sending JSON or XML to EX, use concise alerting
- For everything else, use normal alerting
- Try the easiest to configure first. Then progress to most effort if necessary.

Warning

Preference is to use TCP, but if UDP is necessary -- set FireEye UDP syslog to max chunk-size of 4096:

```
ssh admin@<FireEyeBox> en conf t
fenotify rsyslog trap-sink <splunk_connector> chunk-size 4096
```

Original Build Environment

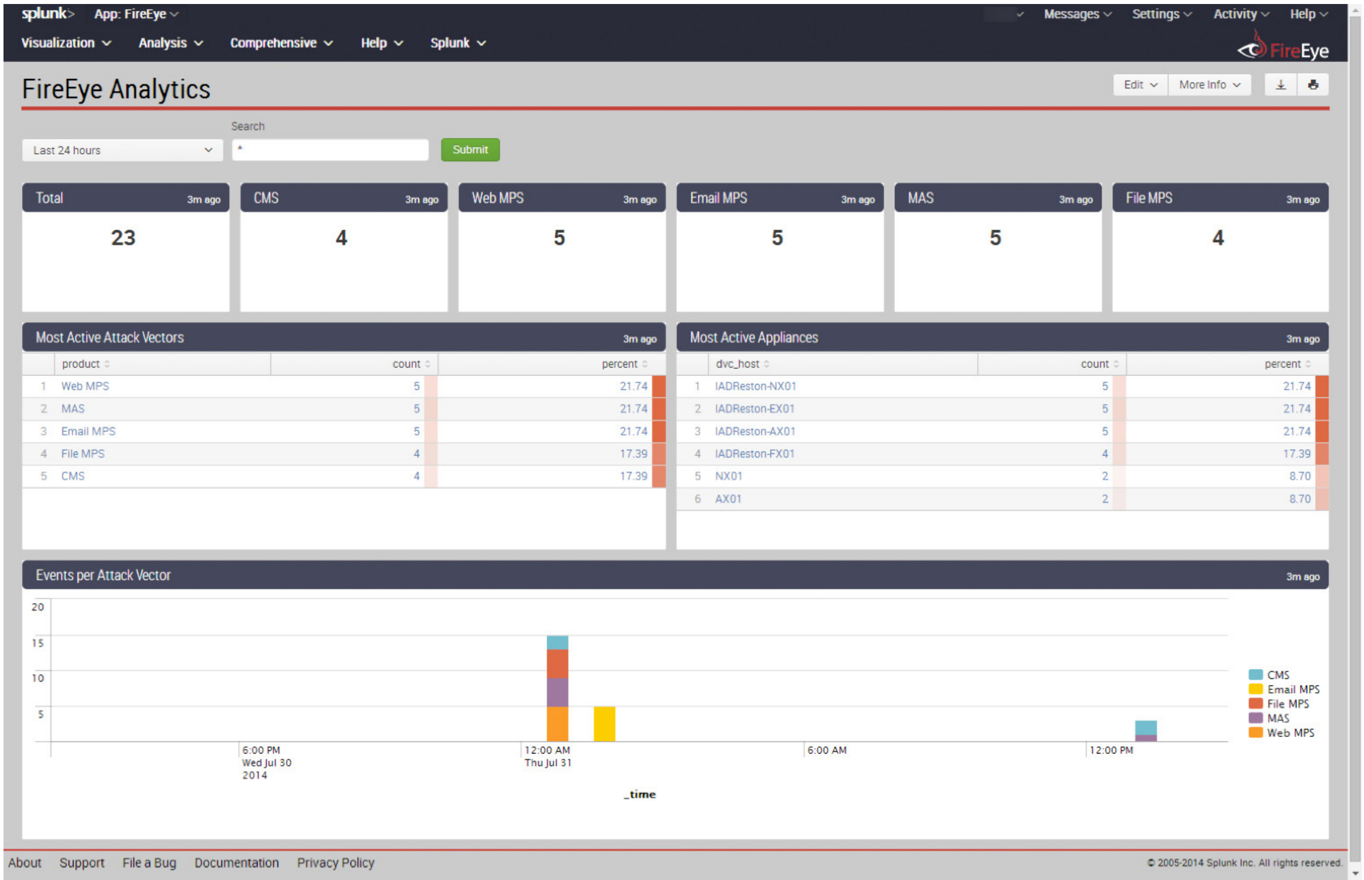
- Linux base OS
- Splunk 6.X - Non-distributed environment

Possible Dashboard Configurations

- Analytics: User-provided content. Feel free to contribute favorite dashboards via the feedback link within the app.
- Visualization: Intended as a heads-up display for a NOC/SOC. GeoIP, trends, and charts.
- Analysis: Analyst dashboard contains more detailed event data
- Comprehensive: All panels displayed on one screen--Visualization + Comprehensive
- Toolbox: Useful tools for investigators that include third-party lookups

Screenshots

The screenshots below provide default dashboards included in the FireEye App for Splunk Enterprise.



FireEye Analytics

Last 24 hours

Search

*

Total	CMS	Web MPS	Email MPS	MAS	File MPS
23	4	5	5	5	4

Most Active Attack Vectors — 3m ago

	product	count	percent
1	Web MPS	5	21.74
2	MAS	5	21.74
3	Email MPS	5	21.74
4	File MPS	4	17.39
5	CMS	4	17.39

Most Active Appliances — 3m ago

	dvc_host	count	percent
1	IADReston-NX01	5	21.74
2	IADReston-EX01	5	21.74
3	IADReston-AX01	5	21.74
4	IADReston-FX01	4	17.39
5	NX01	2	8.70
6	AX01	2	8.70

Events per Attack Vector — 3m ago

Figure 1: Analytics Dashboard

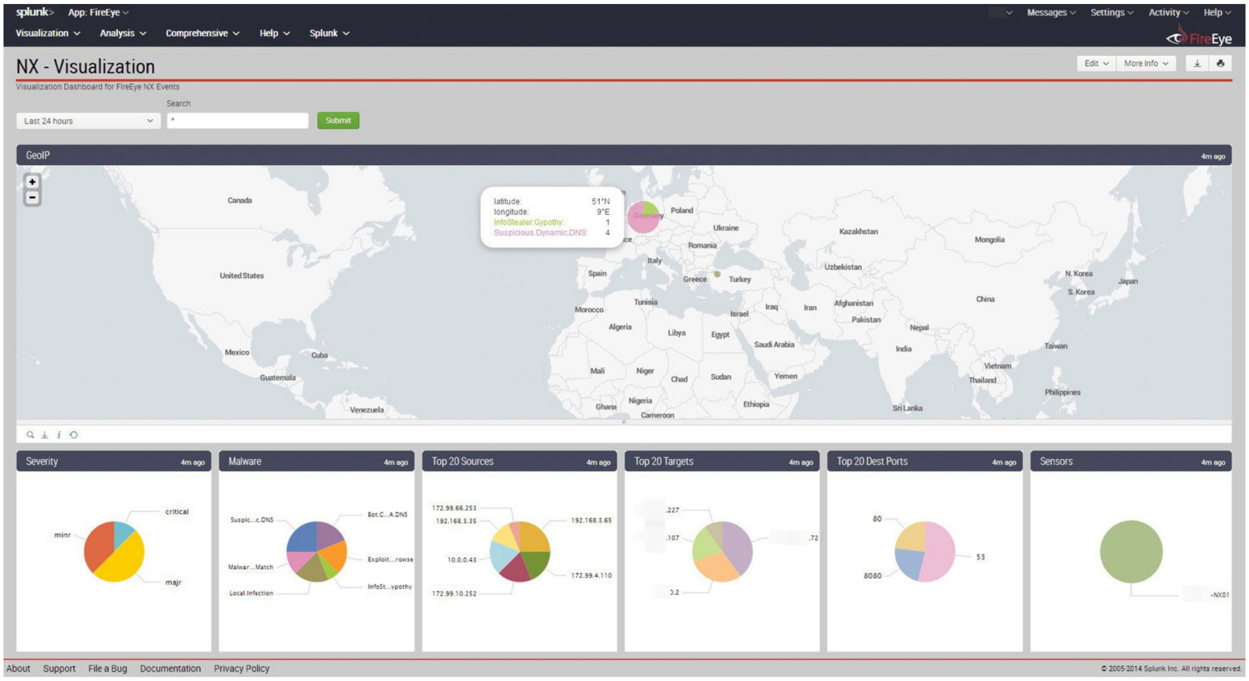
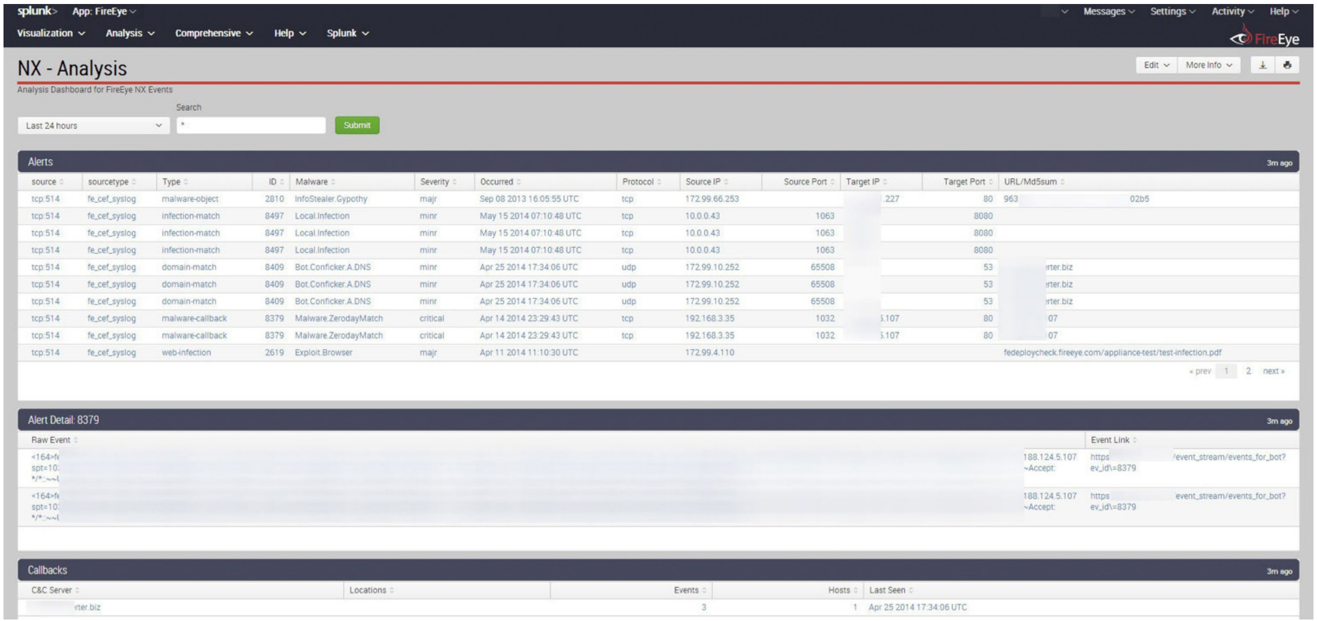


Figure 2: FireEye NX Visualization



NX - Analysis

Analysis Dashboard for FireEye NX Events

Alerts

source	sourcetype	Type	ID	Malware	Severity	Occurred	Protocol	Source IP	Source Port	Target IP	Target Port	URL/Md5sum
tcp:514	fe_cef_syslog	malware-object	2810	InfoStealer.Gypothy	majr	Sep 08 2013 16:05:55 UTC	tcp	172.99.66.253		[redacted].227	80	963[redacted]02b5
tcp:514	fe_cef_syslog	infection-match	8497	Local.Infection	minr	May 15 2014 07:10:48 UTC	tcp	10.0.0.43	1063	[redacted]	8080	
tcp:514	fe_cef_syslog	infection-match	8497	Local.Infection	minr	May 15 2014 07:10:48 UTC	tcp	10.0.0.43	1063	[redacted]	8080	
tcp:514	fe_cef_syslog	infection-match	8497	Local.Infection	minr	May 15 2014 07:10:48 UTC	tcp	10.0.0.43	1063	[redacted]	8080	
tcp:514	fe_cef_syslog	domain-match	8409	Bot.Conficker.A.DNS	minr	Apr 25 2014 17:34:06 UTC	udp	172.99.10.252	65508	[redacted]	53	[redacted]rter.biz
tcp:514	fe_cef_syslog	domain-match	8409	Bot.Conficker.A.DNS	minr	Apr 25 2014 17:34:06 UTC	udp	172.99.10.252	65508	[redacted]	53	[redacted]rter.biz
tcp:514	fe_cef_syslog	domain-match	8409	Bot.Conficker.A.DNS	minr	Apr 25 2014 17:34:06 UTC	udp	172.99.10.252	65508	[redacted]	53	[redacted]rter.biz
tcp:514	fe_cef_syslog	malware-callback	8379	Malware.ZerodayMatch	critical	Apr 14 2014 23:29:43 UTC	tcp	192.168.3.35	1032	[redacted].107	80	[redacted]07
tcp:514	fe_cef_syslog	malware-callback	8379	Malware.ZerodayMatch	critical	Apr 14 2014 23:29:43 UTC	tcp	192.168.3.35	1032	[redacted].107	80	[redacted]07
tcp:514	fe_cef_syslog	web-infection	2619	Exploit.Browser	majr	Apr 11 2014 11:10:30 UTC		172.99.4.110				fedeploycheck.fireeye.com/appliance-test/test-infection.pdf

Alert Detail: 8379

Raw Event	Event Link
<164>f[redacted] spt=10[redacted]188.124.5.107 */*:~~[redacted]~Accept:	https[redacted]/event_stream/events_for_bot? ev_id\=8379
<164>f[redacted] spt=10[redacted]188.124.5.107 */*:~~[redacted]~Accept:	https[redacted]event_stream/events_for_bot? ev_id\=8379

Callbacks

C&C Server	Locations	Events	Hosts	Last Seen
[redacted]rter.biz		3	1	Apr 25 2014 17:34:06 UTC

Figure 3: FireEye NX Analysis

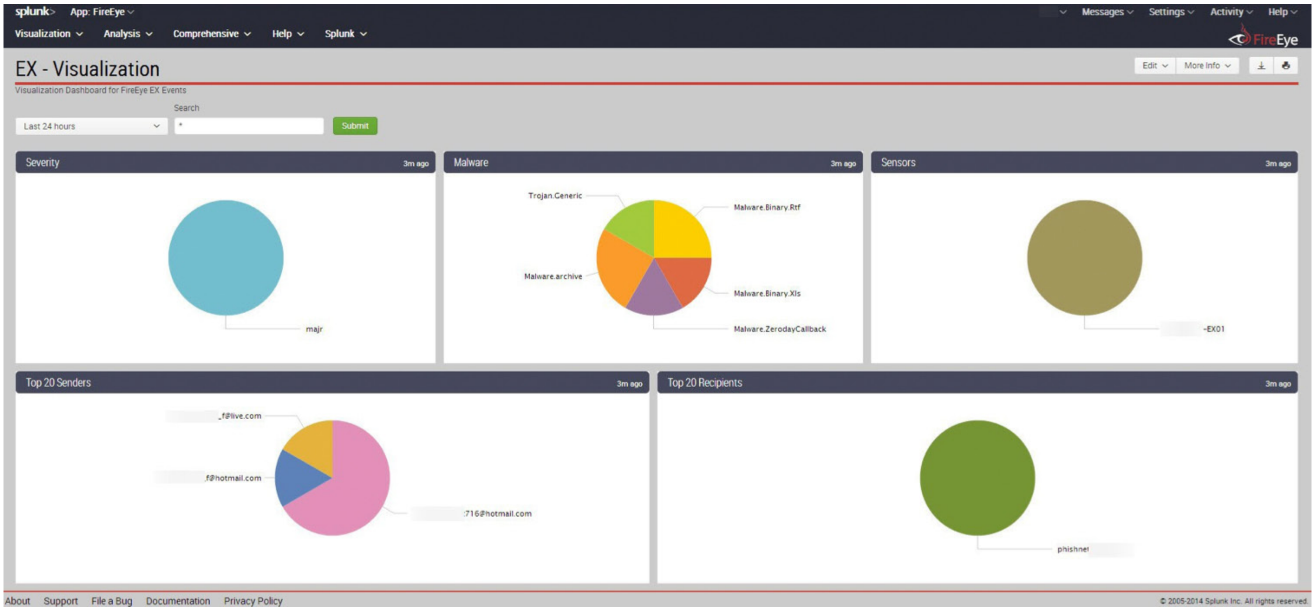
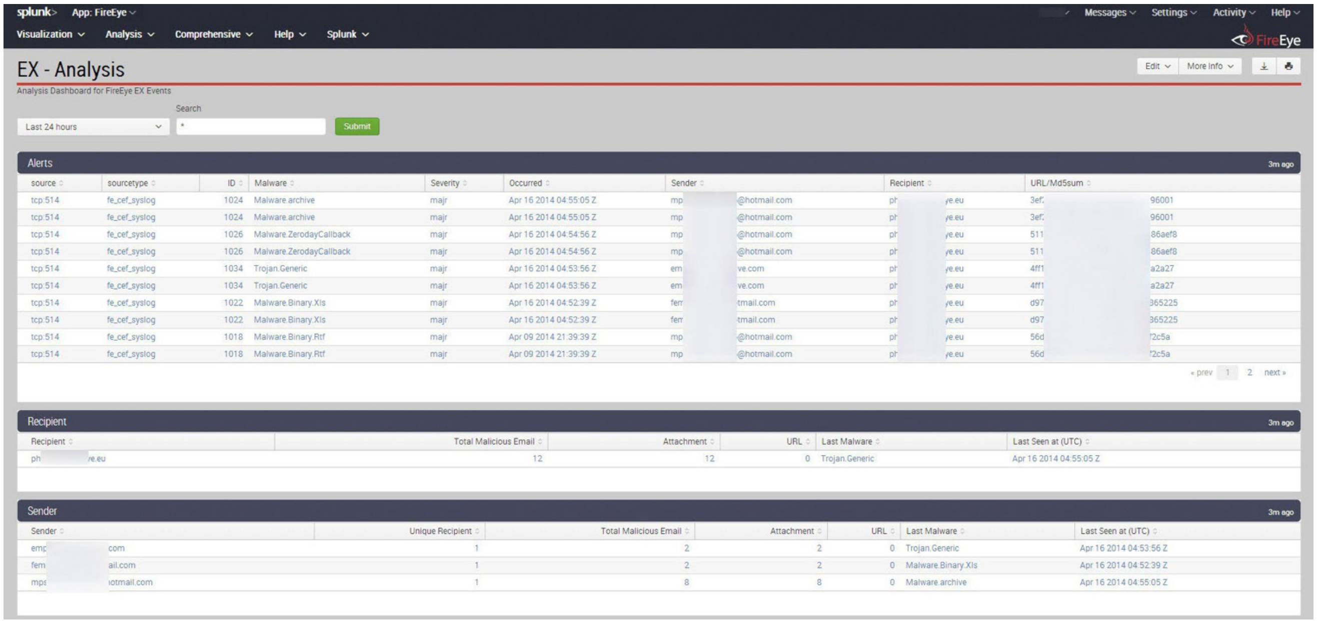


Figure 4: FireEye EX Visualization


splunk> App: FireEye
Messages Settings Activity Help
Visualization Analysis Comprehensive Help Splunk
FireEye
Edit More Info

EX - Analysis

Analysis Dashboard for FireEye EX Events

Search: Last 24 hours | * | Submit

Alerts — 3m ago

source	sourcetype	ID	Malware	Severity	Occurred	Sender	Recipient	URL/Md5sum
tcp:514	fe_cef_syslog	1024	Malware.archive	majr	Apr 16 2014 04:55:05 Z	mp[redacted]@hotmail.com	ph[redacted]ye.eu	3ef[redacted]96001
tcp:514	fe_cef_syslog	1024	Malware.archive	majr	Apr 16 2014 04:55:05 Z	mp[redacted]@hotmail.com	ph[redacted]ye.eu	3ef[redacted]96001
tcp:514	fe_cef_syslog	1026	Malware.ZerodayCallback	majr	Apr 16 2014 04:54:56 Z	mp[redacted]@hotmail.com	ph[redacted]ye.eu	511[redacted]86aef8
tcp:514	fe_cef_syslog	1026	Malware.ZerodayCallback	majr	Apr 16 2014 04:54:56 Z	mp[redacted]@hotmail.com	ph[redacted]ye.eu	511[redacted]86aef8
tcp:514	fe_cef_syslog	1034	Trojan.Generic	majr	Apr 16 2014 04:53:56 Z	em[redacted]ve.com	ph[redacted]ye.eu	4ff1[redacted]a2a27
tcp:514	fe_cef_syslog	1034	Trojan.Generic	majr	Apr 16 2014 04:53:56 Z	em[redacted]ve.com	ph[redacted]ye.eu	4ff1[redacted]a2a27
tcp:514	fe_cef_syslog	1022	Malware.Binary.Xls	majr	Apr 16 2014 04:52:39 Z	fem[redacted]tmail.com	ph[redacted]ye.eu	d97[redacted]365225
tcp:514	fe_cef_syslog	1022	Malware.Binary.Xls	majr	Apr 16 2014 04:52:39 Z	fem[redacted]tmail.com	ph[redacted]ye.eu	d97[redacted]365225
tcp:514	fe_cef_syslog	1018	Malware.Binary.Rtf	majr	Apr 09 2014 21:39:39 Z	mp[redacted]@hotmail.com	ph[redacted]ye.eu	56d[redacted]f2c5a
tcp:514	fe_cef_syslog	1018	Malware.Binary.Rtf	majr	Apr 09 2014 21:39:39 Z	mp[redacted]@hotmail.com	ph[redacted]ye.eu	56d[redacted]f2c5a

« prev 1 2 next »

Recipient — 3m ago

Recipient	Total Malicious Email	Attachment	URL	Last Malware	Last Seen at (UTC)
ph[redacted]ye.eu	12	12	0	Trojan.Generic	Apr 16 2014 04:55:05 Z

Sender — 3m ago

Sender	Unique Recipient	Total Malicious Email	Attachment	URL	Last Malware	Last Seen at (UTC)
emp[redacted]com	1	2	2	0	Trojan.Generic	Apr 16 2014 04:53:56 Z
fem[redacted]ail.com	1	2	2	0	Malware.Binary.Xls	Apr 16 2014 04:52:39 Z
mps[redacted]otmail.com	1	8	8	0	Malware.archive	Apr 16 2014 04:55:05 Z

Figure 5: FireEye EX Analysis

Installing the FireEye App for Splunk Enterprise

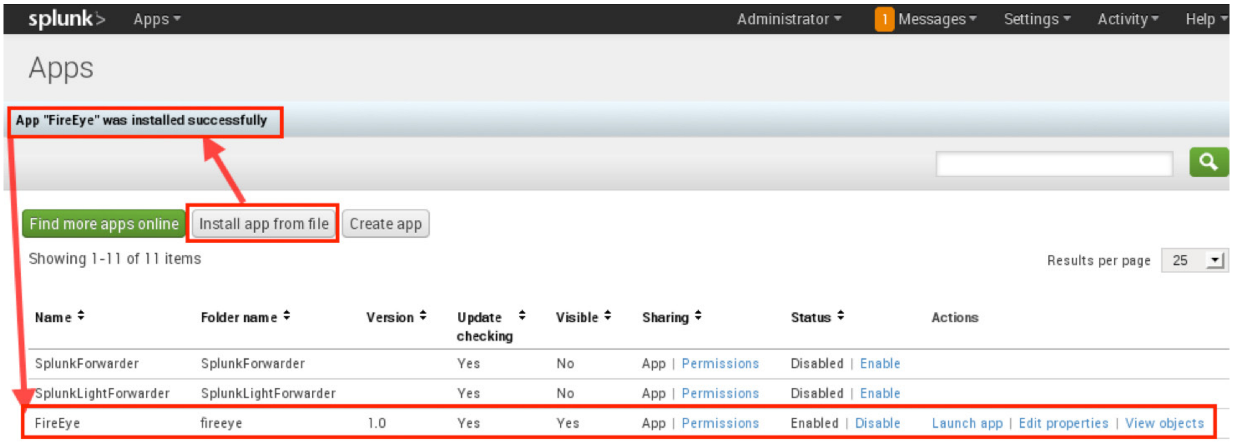
Use the App Manager within Splunk or follow the manual installation instructions below:

Manual Installation Procedures

1. Download the .spl or .tgz file.
2. Navigate to "Apps" -> "Manage Apps".
3. Click on "Install app from file".
4. Upload the downloaded file using the form provided.
5. Restart if the app requires it.

```
$SPLUNK_HOME/bin/splunk restart
```

Upon successful installation, the following screen will be present:



App "FireEye" was installed successfully

Showing 1-11 of 11 items

Results per page 25

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App | Permissions	Disabled | Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App | Permissions	Disabled | Enable	
FireEye	fireeye	1.0	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties | View objects

Figure 6: Successful Installation Message

Configuring the FireEye App for Splunk Enterprise

FireEye realizes that every customer may not own the entire suite of appliances, thus the FireEye app allows the user to customize their menu options to only contain the necessary appliances. This can be done by performing the following actions:

1. Log into Splunk using an Administrator account

2. We have made it easy to setup and change the menus by going to Help -> Configure App

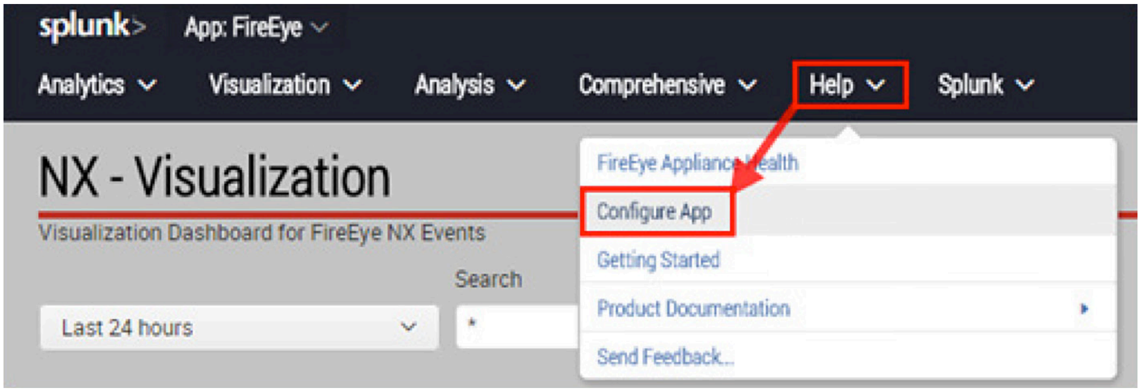
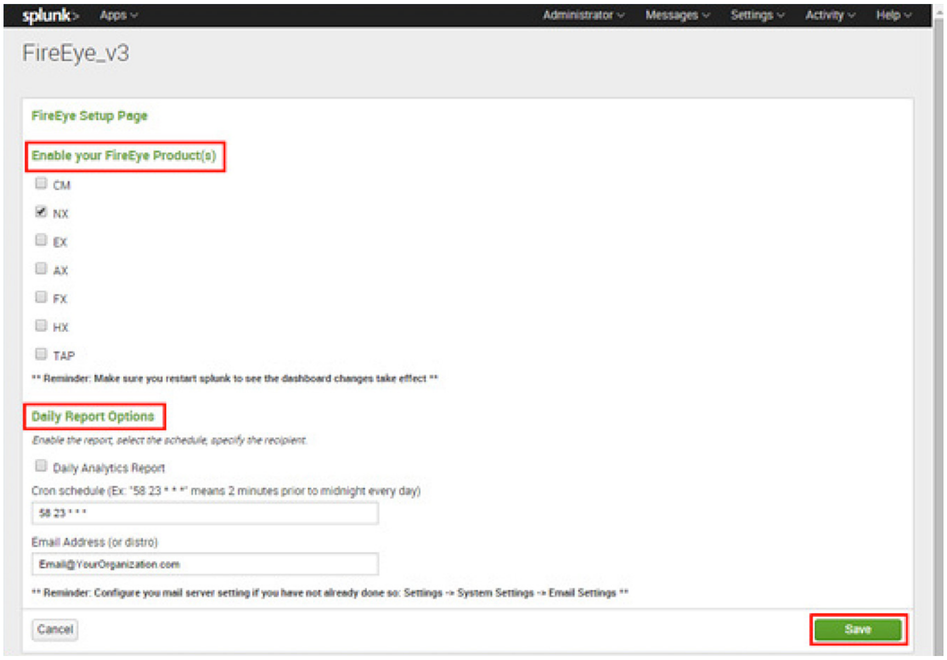


Figure 7: Help menu shows option to configure the application

3. In the next screen, users can enable certain FireEye products and optionally Daily Reports



FireEye_v3

FireEye Setup Page

Enable your FireEye Product(s)

□ CM
☑ NX
□ EX
□ AX
□ FX
□ HX
□ TAP

** Reminder: Make sure you restart splunk to see the dashboard changes take effect **

Daily Report Options

Enable the report, select the schedule, specify the recipient.

□ Daily Analytics Report

Cron schedule (Ex: "58 23 * * *" means 2 minutes prior to midnight every day)

58 23 * * *

Email Address (or distro)

Email@YourOrganization.com

** Reminder: Configure you mail server setting if you have not already done so: Settings -> System Settings -> Email Settings **

Cancel Save

Figure 8: FireEye App for Splunk Enterprise configuration screen

4. Restart Splunk when the following message appears: "Successfully updated FireEye_v3" in the top left hand corner of the screen.

```
$SPLUNK_HOME/bin/splunk restart
```

Configuring Splunk

There are many options for configuring Splunk, but the main options are listed below. You choice will depend on the constraints in your environment.

Explanation of Protocols:

#	Protocol	Enc	Reason
1	SYSLOG - TCP	No	Easier to send large amounts of data than UDP
2	SYSLOG - UDP	No	Last resort - requires shell configuration of FireEye devices
3	HTTPS via Splunk RESTful API	Yes	Encrypted, flexible sending large amounts of data

SYSLOG - TCP & UDP

The steps below should assist in the setup. The instructions below show TCP, but can easily be changed if UDP is required.

Creating Connectors

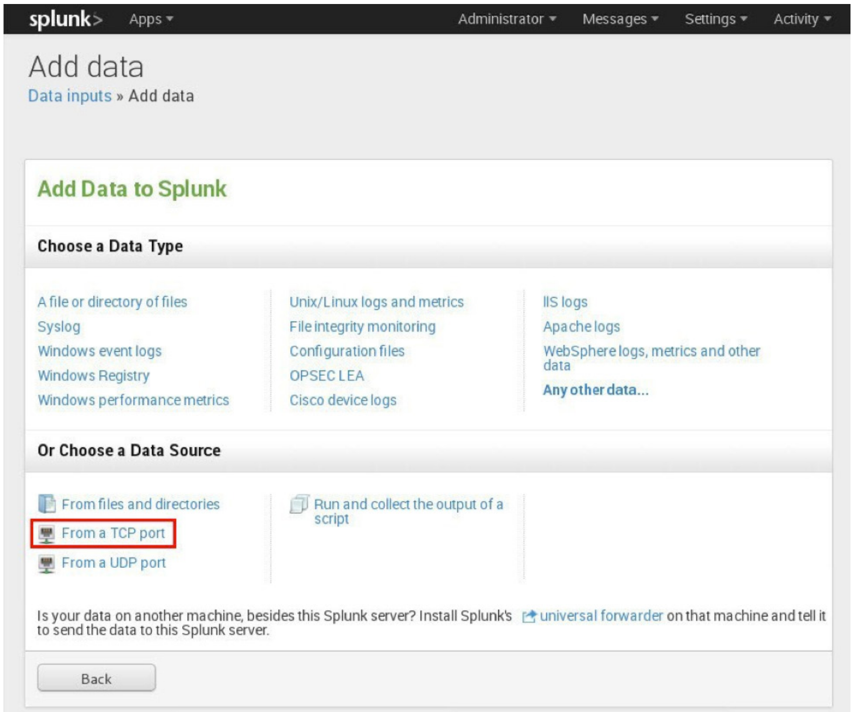
Now that we have Splunk ready to go, we have to create the connection between the FireEye and Splunk devices. This involves creating a Splunk listener and configuring the FireEye device to send the data.

Splunk Listener

The Splunk listener needs to be configured so it can receive data from other devices. Perform the following steps to create the listener:

- Again, log into the Splunk web UI with an admin account
- Click “Settings -> Data inputs -> Add data button”
- Click “From a TCP port”
- Enter “514” for the port
- Set Source Type: From list
- Select source type from list: syslog
- Click the “Save” button
- Click the “Back to home” link

Both FireEye and Splunk allow syslog over TCP. Using TCP, there are fewer concerns with data that is too large for SYSLOG—thus it is recommended.



Add data

Data inputs » Add data

Add Data to Splunk

Choose a Data Type

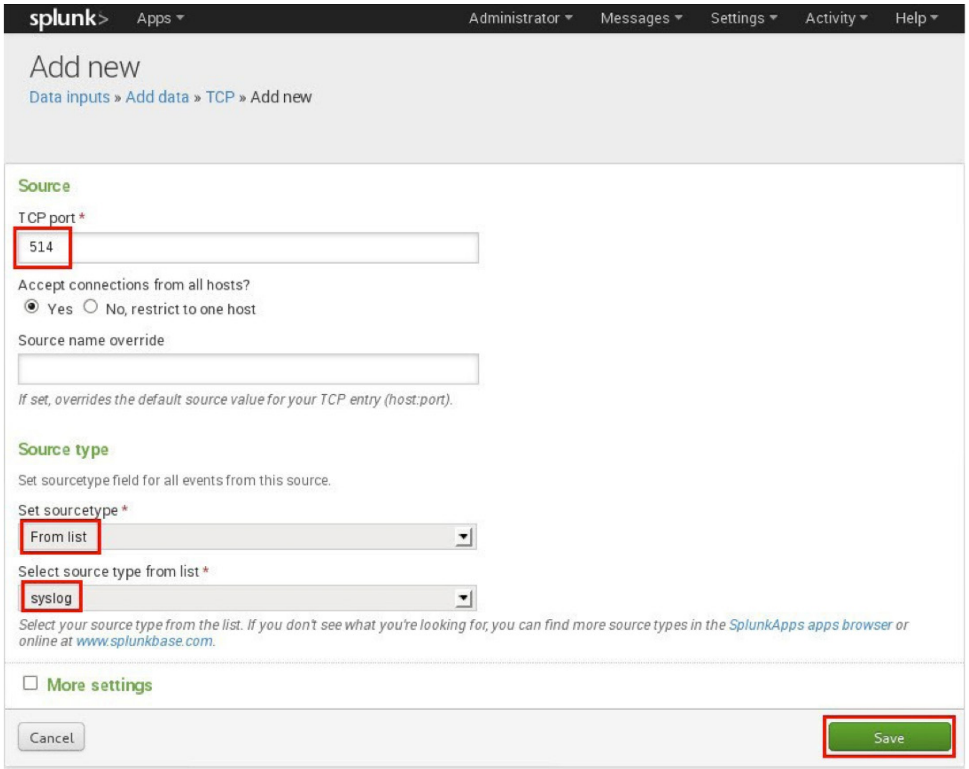
A file or directory of files
Syslog
Windows event logs
Windows Registry
Windows performance metrics
Unix/Linux logs and metrics
File integrity monitoring
Configuration files
OPSEC LEA
Cisco device logs
IIS logs
Apache logs
WebSphere logs, metrics and other data
Any other data...

Or Choose a Data Source

From files and directories
From a TCP port
From a UDP port
Run and collect the output of a script

Is your data on another machine, besides this Splunk server? Install Splunk's universal forwarder on that machine and tell it to send the data to this Splunk server.

Figure 9: Adding a data connector in Splunk



Add new

Data inputs » Add data » TCP » Add new

Source

TCP port *
514

Accept connections from all hosts?
● Yes ○ No, restrict to one host

Source name override

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

Source type

Set sourcetype field for all events from this source.

Set sourcetype *
From list

Select source type from list *
syslog

Select your source type from the list. If you don't see what you're looking for, you can find more source types in the SplunkApps apps browser or online at www.splunkbase.com.

☐ More settings

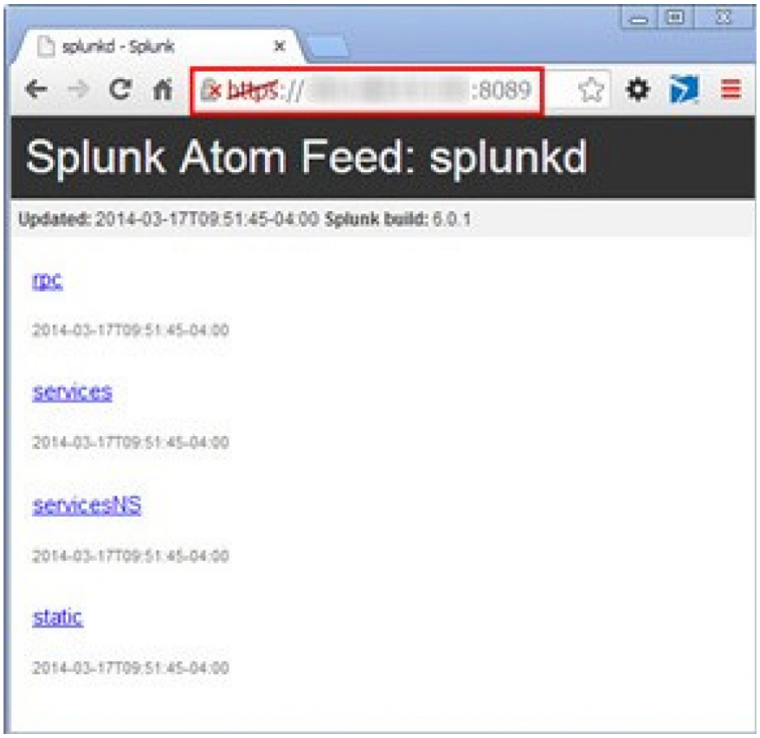
Figure 10: Adding a data connector in Splunk

HTTPS via Splunk RESTful API

The steps below should assist in the setup.

Splunk Listener

A default installation of Splunk 6.0 or later should automatically be listening via the RESTful API on port 8089. However, this can be verified by navigating to this API using a standard web browser: https://<SplunkBox>:8089



Splunk Atom Feed: splunkd

Updated: 2014-03-17T09:51:45-04:00 Splunk build: 6.0.1

rpc

2014-03-17T09:51:45-04:00

services

2014-03-17T09:51:45-04:00

servicesNS

2014-03-17T09:51:45-04:00

static

2014-03-17T09:51:45-04:00

Figure 11: Splunk RESTful API is available on the default port 8089

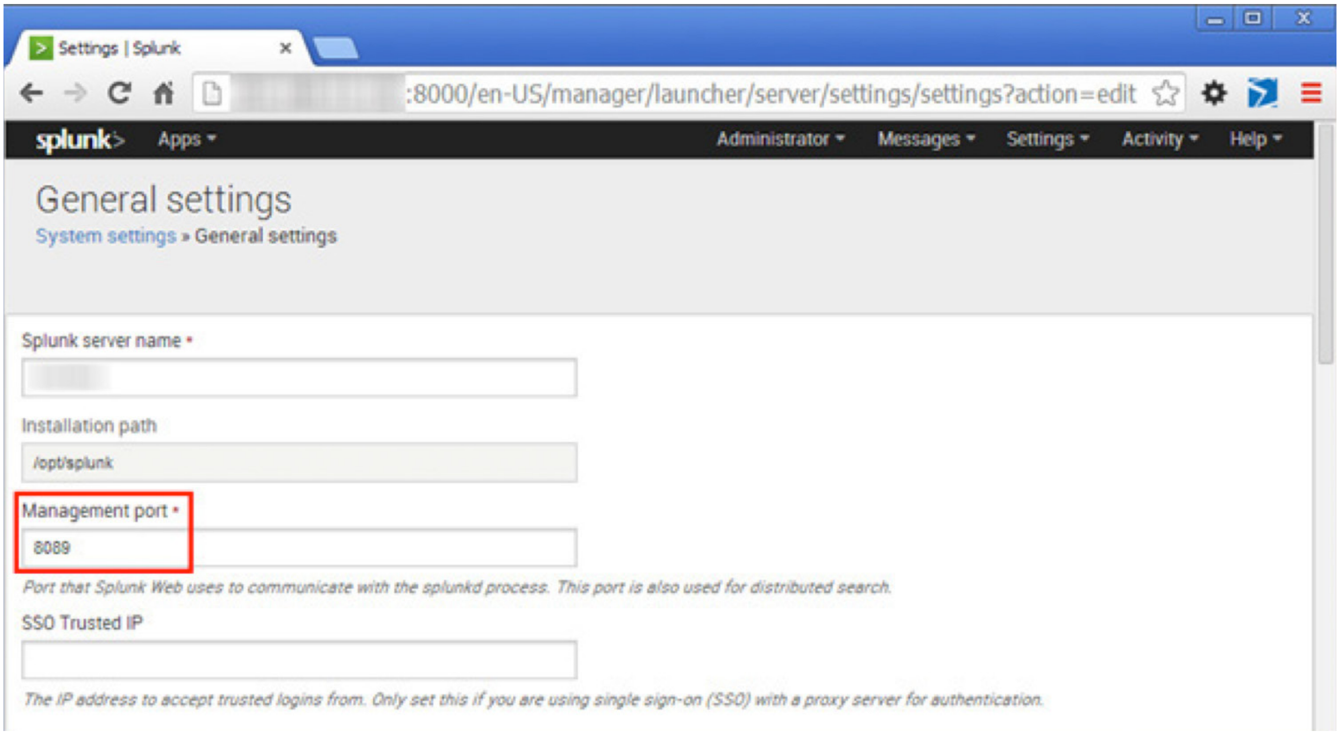
If for whatever reason, you are not able to connect to this port, you can verify the service and port number using the following steps:

Using a web browser, log in to the web interface: http://<SplunkBox>:8000

- Username: <admin account>
- Password: <password>

Set up the Splunk listener:

- Click the "Settings" hyperlink in the top right hand corner of Splunk
- Under "System", click "System settings"
- Click "General Settings"
- Note the value in the "Management port" field


Settings | Splunk
[redacted]:8000/en-US/manager/launcher/server/settings/settings?action=edit
splunk>
Apps
Administrator
Messages
Settings
Activity
Help

General settings

System settings » General settings

Splunk server name *

[redacted]

Installation path

/opt/splunk

Management port *

8089

Port that Splunk Web uses to communicate with the splunkd process. This port is also used for distributed search.

SSO Trusted IP

The IP address to accept trusted logins from. Only set this if you are using single sign-on (SSO) with a proxy server for authentication.

Figure 12: The port that Splunk uses for its RESTful API

Splunk Role

We now want to create a user in Splunk that will be used for passing the RESTful API data. However, there is currently no predefined Splunk role that can perform the job while adhering to the principle of least privilege. We could just assign our new user the "admin" role, but this would create a more severe situation should this account ever become compromised.

The following instructions will create a Splunk role that has only the ability to accept data via the RESTful API:

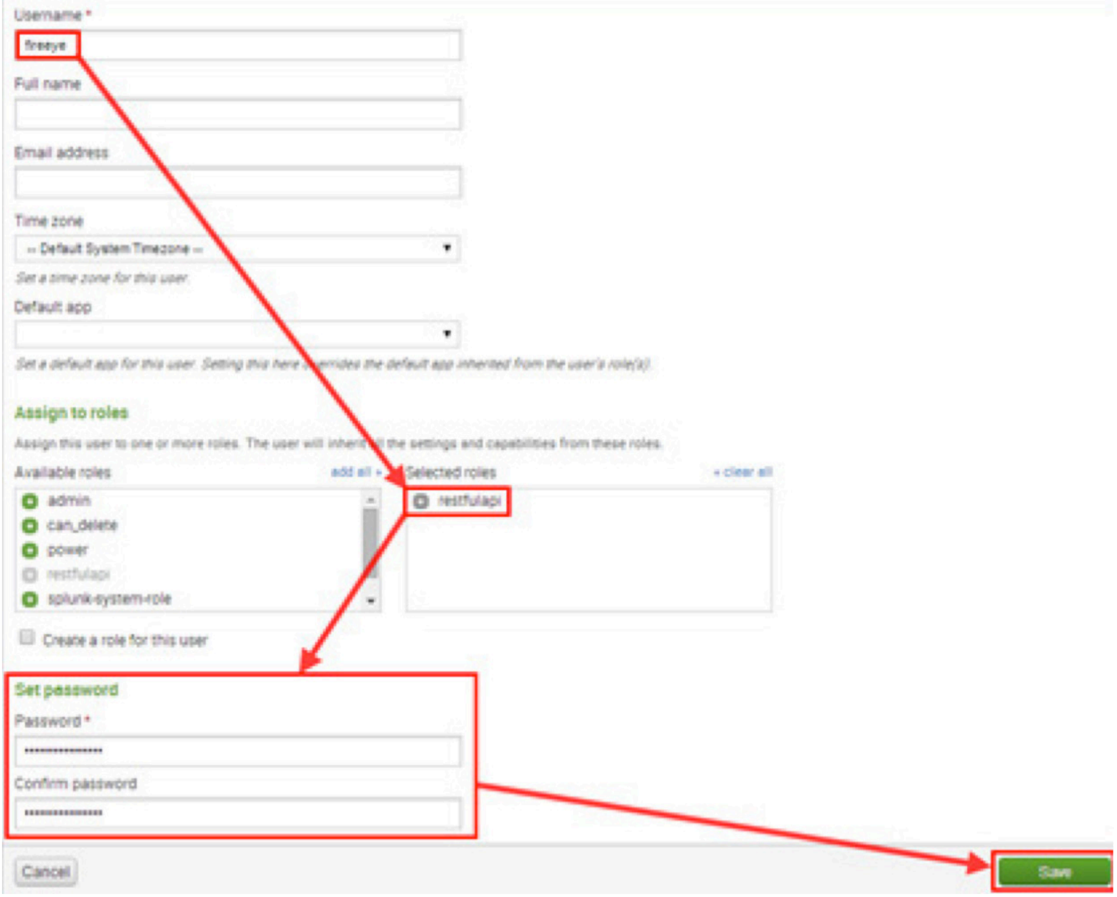
- Log into the Splunk web UI with an admin account
- Click "Settings -> Users and authentication -> Access controls"
- Click "Roles" -> Click the "New" button
- Role Name: RESTfulAPI
- Capabilities: edit_tcp

Splunk User

Now that we have created a secure role, we need to create an account that will be used for authentication to post our event data.

Note:

- Make sure the account name is alphanumeric only (no whitespaces)
- Make sure password is 17 characters or less
    - Example username: fireeye
- Again, log into the Splunk web UI with an admin account
- Click "Settings -> Users and authentication -> Access controls"
- Click "Users" -> Click the "New" button
- Fill in the required data
- Privilege Note: Remember to use our newly created restfulapi role
- Click the "Save" button



Username *
fireeye

Full name

Email address

Time zone
-- Default System Timezone --
Set a time zone for this user.

Default app

Set a default app for this user. Setting this here overrides the default app inherited from the user's role(s).

Assign to roles

Assign this user to one or more roles. The user will inherit all the settings and capabilities from these roles.

Available roles
- admin
- can_delete
- power
- restfulapi
- splunk-system-role

Selected roles
- restfulapi

□ Create a role for this user

Set password

Password *
•••••••••••••••

Confirm password
•••••••••••••••

Figure 13: Creating the Splunk admin account that will accept our HTTP POST messages.

Configuring FireEye (NX, EX, AX, FX)

There are many options for installation, but the most reliable options are listed below in order of preference. You choice will depend on the constraints in your environment.

Explanation of protocols

Easiest to configure

#	Protocol	Enc	Reason
1	SYSLOG - TCP CEF	No	TCP does not require command-line configuration on FireEye Appliance
2	SYSLOG - UDP CEF	No	Provides more data than CSV
3	SYSLOG - TCP CSV	No	TCP does not require command-line configuration on FireEye Appliance
4	SYSLOG - UDP CSV	No	Last resort - May not send protocol field

Requires more effort to configure

#	Protocol	Enc	Reason
1	SYSLOG - TCP XML	No	TCP does not require command-line configuration on FireEye Appliance
2	SYSLOG - UDP XML	No	XML provides more data than CEF and CSV
3	SYSLOG - TCP JSON	No	TCP does not require command-line configuration on FireEye Appliance
4	SYSLOG - UDP JSON	No	JSON provides more data than CEF and CSV

Most effort to configure

#	Protocol	Enc	Reason
1	HTTPS JSON	Yes	Encrypted, lighter than XML
2	HTTPS XML	Yes	Encrypted

General notes

- When sending JSON or XML to EX, use concise alerting
- For everything else, use normal alerting
- Try the easiest to configure first. Then progress to most effort if necessary.

Warning:

Preference is to use TCP, but if UDP is necessary -- set FireEye UDP syslog to max chunk-size of 4096:

```
ssh admin@<FireEyeBox>
en
conf t
fenotify rsyslog trap-sink <splunk_connector> chunk-size 4096
```

Two examples are provided below, **First for SYSLOG** and **Second for HTTPS.**

CEF over SYSLOG (TCP)

The first option we will show is how to configure the FireEye device to send CEF over SYSLOG. We understand that sending data via HTTPS may not work for everyone.

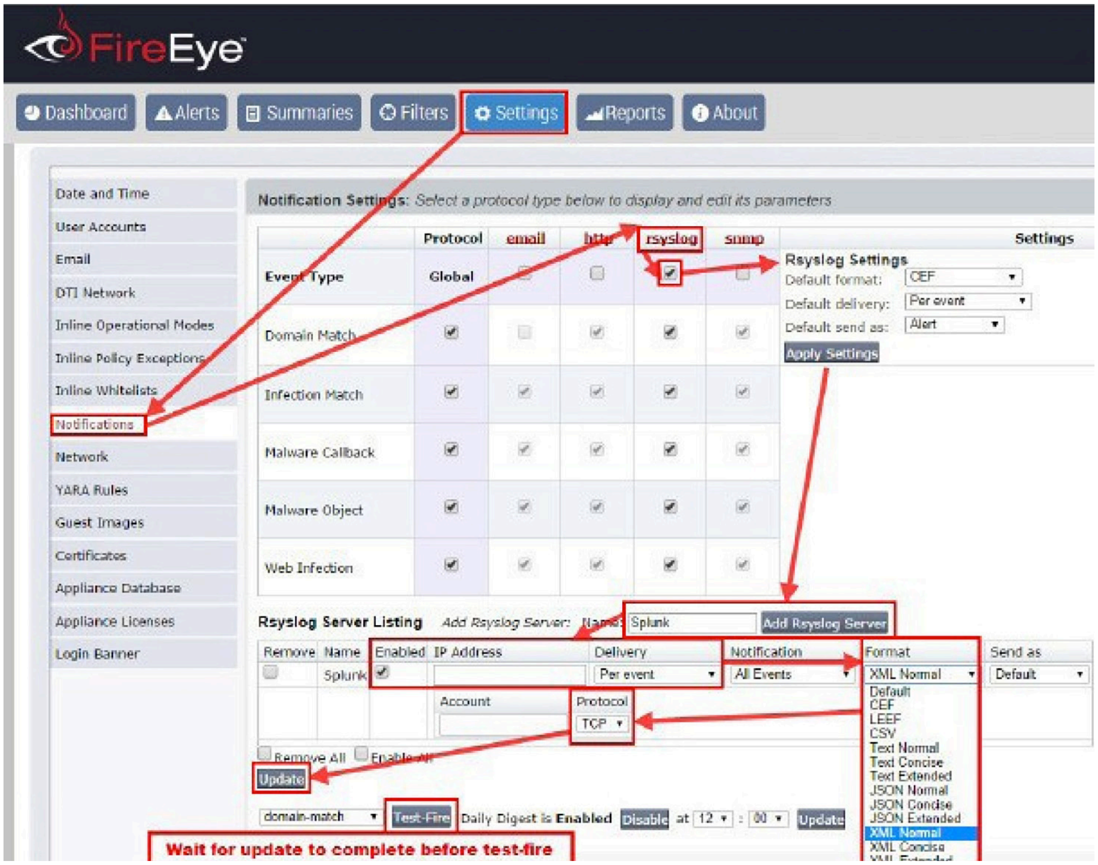
Complete the following steps to send data to Splunk using CEF over SYSLOG (TCP):

- Log into the FireEye appliance with an administrator account
- Click Settings
- Click Notifications
- Click rsyslog
- Check the “Event type” check box
- Next to the “Add Rsyslog Server” button, type “Splunk_CEF_SYSLOG”.
- Then click the “Add Rsyslog Server” button.
- Enter the IP address of the Splunk server in the “IP Address” field.

Make sure rsyslog settings are:

- Format: XML concise for EX, XML normal for everything else
- Delivery: Per event
- Send as: Alert
- Change the protocol dropdown to TCP (or use the special max chunk-size for UDP to 4096)

Remember to click the “Update” button when finished.



Notification Settings: *Select a protocol type below to display and edit its parameters*

	Protocol	email	http	rsyslog	snmp
Event Type	Global	☐	☐	☑	☐
Domain Match	☑	☐	☑	☑	☑
Infection Match	☑	☑	☑	☑	☑
Malware Callback	☑	☑	☑	☑	☑
Malware Object	☑	☑	☑	☑	☑
Web Infection	☑	☑	☑	☑	☑

Settings

Rsyslog Settings
Default format: CEF
Default delivery: Per event
Default send as: Alert
Apply Settings

Rsyslog Server Listing *Add Rsyslog Server:* Name: Splunk Add Rsyslog Server

Remove	Name	Enabled	IP Address	Delivery	Notification	Format	Send as
☐	Splunk	☑		Per event	All Events	XML Normal	Default
			Account	Protocol: TCP			

☐ Remove All ☐ Enable All
Update

domain-match Test-Fire Daily Digest is **Enabled** Disable at 12 : 00 Update

Wait for update to complete before test-fire

Figure 14: Steps to set up SYSLOG

JSON over HTTPS

The second option we will show is how to configure the FireEye device to send JSON over HTTPS. HTTPS can be a good option if you are required or prefer to send data over an encrypted channel.

Complete the following steps to send data to Splunk using extended JSON via HTTPS Post:

- Log into the FireEye appliance with an administrator account
- Click "Settings"
- Click "Notifications"
- Click the "http" hyperlink
- Under the http hyperlink, make sure the "Event type" check box is selected
- HTTP settings should be:
- Default delivery: Per event
- Default provider: Generic
- Default format: JSON concise for EX, JSON normal for everything else
- Click the "Apply Settings" button

Next to the "Add HTTP Server" button, type "SplunkHTTPS".
Then click the "Add HTTP Server" button.

Next to the newly created SplunkHTTPS entry:
Select "Enabled", "Auth", and "SSL Enable" check boxes.

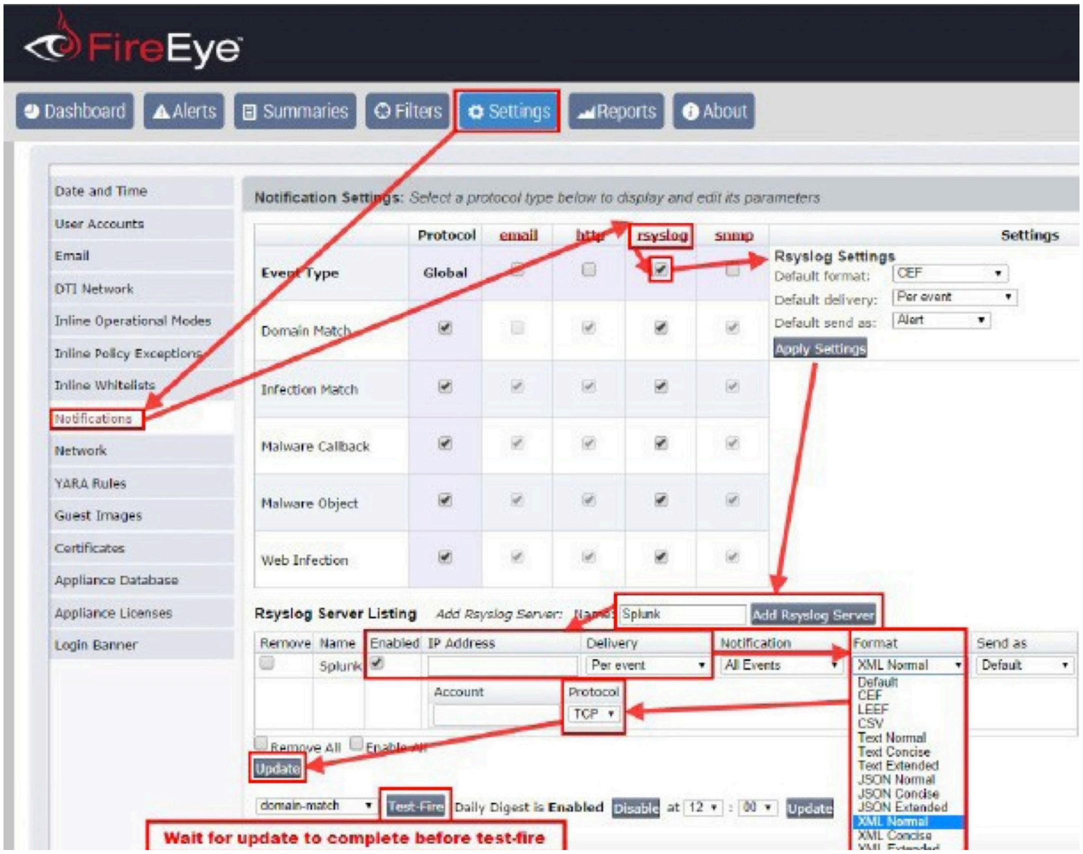
Enter the following settings:

- Server URL: https://<SplunkAD.DR.ESS>:<PORT>/services/receivers/simple?host=<FireEyeA ddress>&source=fe_alert&sourcetype=fe_json
- Username: fireeye (or username you created in Splunk)
- Password: <password you created above in Splunk>

Note: The default port used above is 8089--unless it has been changed.

Ex: https://192.168.33.152:8089/services/receivers/simple?host=192.168.33.131&source=fe_ alert&sourcetype=fe_json

Remember to click the "Update" button when finished.



Notification Settings: *Select a protocol type below to display and edit its parameters*

	Protocol	email	http	rsyslog	snmp
Event Type	**Global**	☐	☐	☑	☐
Domain Match	☑	☐	☑	☑	☑
Infection Match	☑	☑	☑	☑	☑
Malware Callback	☑	☑	☑	☑	☑
Malware Object	☑	☑	☑	☑	☑
Web Infection	☑	☑	☑	☑	☑

Settings

Rsyslog Settings

Default format: CEF

Default delivery: Per event

Default send as: Alert

Rsyslog Server Listing *Add Rsyslog Server:* Name: Splunk

Remove	Name	Enabled	IP Address	Delivery	Notification	Format	Send as
☐	Splunk	☑		Per event	All Events	XML Normal	Default
			Account	Protocol			
				TCP			

Format: Default, CEF, LEEF, CSV, Text Normal, Text Concise, Text Extended, JSON Normal, JSON Concise, JSON Extended, XML Normal, XML Concise, XML Extended

☐ Remove All ☐ Enable All

domain-match

Daily Digest is **Enabled** at 12 : 00

Wait for update to complete before test-fire

Figure 15: Steps to configure the FireEye appliance to send data to Splunk

Optional Indexing

Note: Separate indexing may not work in all environments--such as complex distributed Splunk indexing and searching.

Upon installation, the FireEye App for Splunk Enterprise stores all alert data in Splunk's default index called "main". Depending on the size of the deployment and the amount of data already stored in the main Index, this could cause a significant performance issue. You have the option to store this data in its own index to improve search performance, however at the current time this change is unsupported. That said, some clients have reported significant improvements in search time when using a separate index. One real-world example is shown below along with the required modification to enable separate indexing:

Customer Results: Year to date search takes **9 minutes 15 second**s to populate the main dashboard from the main index. After the change to a separate index, it was reduced to **20 seconds**.

Steps:

Remember to first create the index:
Settings -> Data -> Indexes -> New -> Index name: fireeye ->   Save

Out of the box configuration: eventtypes.conf is:

```
[fe]
search = sourcetype=fe_* OR sourcetype=hx_*
```

Modified configuration to support separate "fireeye" index: Change eventtypes.conf to:

```
[fe]
search = index=fireeye sourcetype=fe_* OR sourcetype=hx_*
```

Props.conf change: Remove the red hash (#) symbol below

```
# Uncomment the next line to send FireEye data to a separate index called "fireeye"
#TRANSFORMS-updateFireEyeIndex = fix_FireEye_CEF_in, fix_FireEye_CSV_in, fix_
FireEye_XML_in, fix_FireEye_JSON_st, fix_HX_CEF_in, fix_HX2_CEF_in
```

Note: If the infex is not going to be called fireeye, then transforms.conf needs to be modified.

Change RESTful string in the FireEye appliance:
https://xx.xx.xx.xx:8089/services/receivers/simple?host=xx.xx.xx. xx&source=fe_alert&index=fireeye&sourcetype=fe_json

(Special thanks to Richard Griffith for the research and solution.)

Integrating FireEye PX

Follow the steps below to integrate FireEye PX with the FireEye App for Splunk Enterprise.

1. Run the setup within the app (Help -> Setup) and select the appliances

2. Add your PX appliance IP addresses in the following file: $SPLUNK_HOME/etc/apps/FireEye_v3/lookups/px_appliances.csv

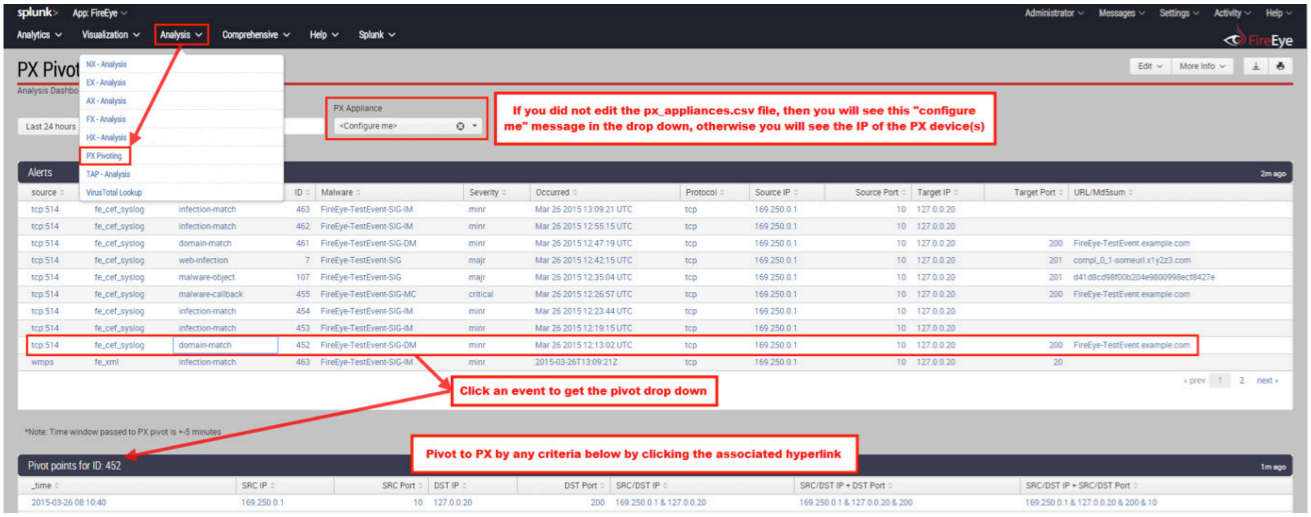
Original config:

```
system
<Configure me>
<Read the config guide>
```

After you are done (assuming your PX appliance is 192.168.5.100):

```
system
192.168.5.100
```

If the setup file is configured with the PX check box checked, a PX Pivoting menu will be available in the drop down. If the px_appliances.csv file is not configured, then <Configure me> will appear in the PX appliance drop down. If it is configured, the IP of the appliance will be in the drop down.



PX Appliance

<Configure me>

If you did not edit the px_appliances.csv file, then you will see this "configure me" message in the drop down, otherwise you will see the IP of the PX device(s)

source			ID	Malware	Severity	Occurred	Protocol	Source IP	Source Port	Target IP	Target Port	URL/Md5sum
tcp:514	fe_cef_syslog	infection-match	463	FireEye-TestEvent-SIG-IM	minr	Mar 26 2015 13:09:21 UTC	tcp	169.250.0.1	10	127.0.0.20		
tcp:514	fe_cef_syslog	infection-match	462	FireEye-TestEvent-SIG-IM	minr	Mar 26 2015 12:55:15 UTC	tcp	169.250.0.1	10	127.0.0.20		
tcp:514	fe_cef_syslog	domain-match	461	FireEye-TestEvent-SIG-DM	minr	Mar 26 2015 12:47:19 UTC	tcp	169.250.0.1	10	127.0.0.20	200	FireEye-TestEvent.example.com
tcp:514	fe_cef_syslog	web-infection	7	FireEye-TestEvent-SIG	majr	Mar 26 2015 12:42:15 UTC	tcp	169.250.0.1	10	127.0.0.20	201	compl_0_1-someurl.x1y2z3.com
tcp:514	fe_cef_syslog	malware-object	107	FireEye-TestEvent-SIG	majr	Mar 26 2015 12:35:04 UTC	tcp	169.250.0.1	10	127.0.0.20	201	d41d8cd98f00b204e9800998ecf8427e
tcp:514	fe_cef_syslog	malware-callback	455	FireEye-TestEvent-SIG-MC	critical	Mar 26 2015 12:26:57 UTC	tcp	169.250.0.1	10	127.0.0.20	200	FireEye-TestEvent.example.com
tcp:514	fe_cef_syslog	infection-match	454	FireEye-TestEvent-SIG-IM	minr	Mar 26 2015 12:23:44 UTC	tcp	169.250.0.1	10	127.0.0.20		
tcp:514	fe_cef_syslog	infection-match	453	FireEye-TestEvent-SIG-IM	minr	Mar 26 2015 12:19:15 UTC	tcp	169.250.0.1	10	127.0.0.20		
tcp:514	fe_cef_syslog	domain-match	452	FireEye-TestEvent-SIG-DM	minr	Mar 26 2015 12:13:02 UTC	tcp	169.250.0.1	10	127.0.0.20	200	FireEye-TestEvent.example.com
wmps	fe_xml	infection-match	463	FireEye-TestEvent-SIG-IM	minr	2015-03-26T13:09:21Z	tcp	169.250.0.1	10	127.0.0.20	20	

Click an event to get the pivot drop down

*Note: Time window passed to PX pivot is +-5 minutes

Pivot to PX by any criteria below by clicking the associated hyperlink

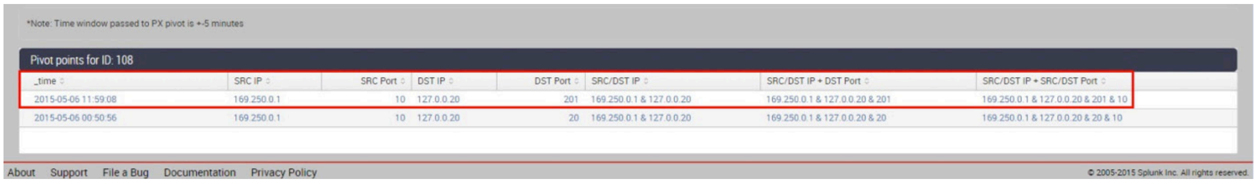
Pivot points for ID: 452

_time	SRC IP	SRC Port	DST IP	DST Port	SRC/DST IP	SRC/DST IP + DST Port	SRC/DST IP + SRC/DST Port
2015-03-26 08:10:40	169.250.0.1	10	127.0.0.20	200	169.250.0.1 & 127.0.0.20	169.250.0.1 & 127.0.0.20 & 200	169.250.0.1 & 127.0.0.20 & 200 & 10

Figure 16: Error message displayed when the PX is not configured

Once set up, the dashboard can be used to pivot based on any of the following data (as shown in the screenshot below):

- Time
- Source IP
- Source Port
- Destination IP
- Destination Port
- Source and Destination IP
- Source and Destination IP and Destination Port
- Source and Destination IP and Source and Destination Port



*Note: Time window passed to PX pivot is +-5 minutes

Pivot points for ID: 108

_time	SRC IP	SRC Port	DST IP	DST Port	SRC/DST IP	SRC/DST IP + DST Port	SRC/DST IP + SRC/DST Port
2015-05-06 11:59:08	169.250.0.1	10	127.0.0.20	201	169.250.0.1 & 127.0.0.20	169.250.0.1 & 127.0.0.20 & 201	169.250.0.1 & 127.0.0.20 & 201 & 10
2015-05-06 00:50:56	169.250.0.1	10	127.0.0.20	20	169.250.0.1 & 127.0.0.20	169.250.0.1 & 127.0.0.20 & 20	169.250.0.1 & 127.0.0.20 & 20 & 10

Figure 17: Fields that can be used to pivot

Integrating FireEye HX

Follow the steps below to integrate FireEye HX with the FireEye App for Splunk Enterprise.

1. Ensure that HX is selected as an option in the FireEye app under Help -> Configure App. (For more details, please see the section called:

"Configuring the FireEye App for Splunk Enterprise")

2. Log into FireEye with an Administrator account

3. Navigate to FireEye -> Administration

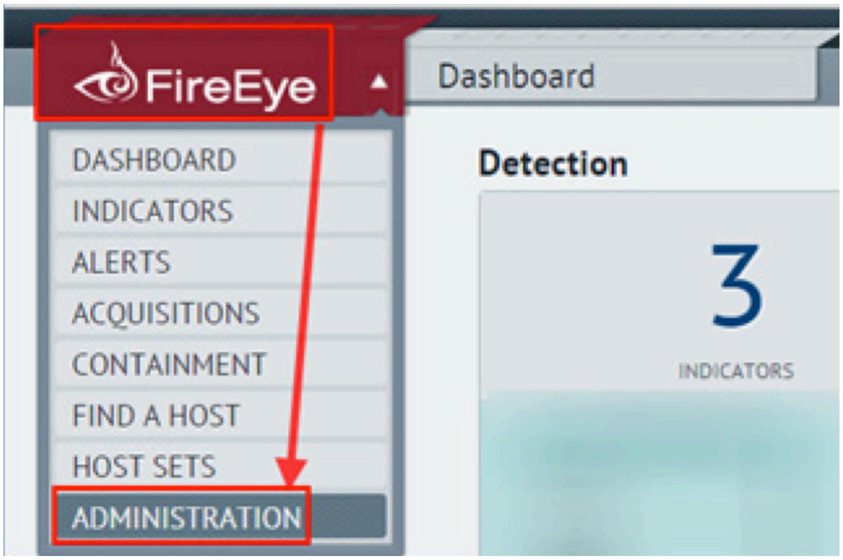


Figure 18: Administration menu in HX

4. Click the drop down and then Logging

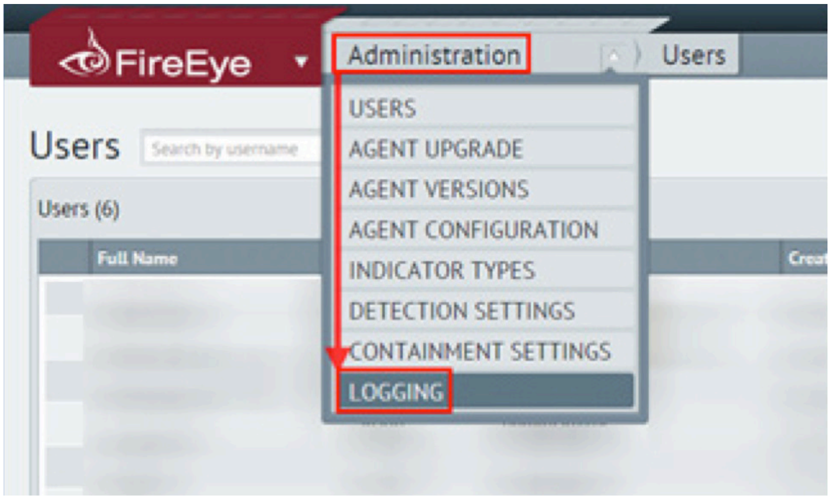
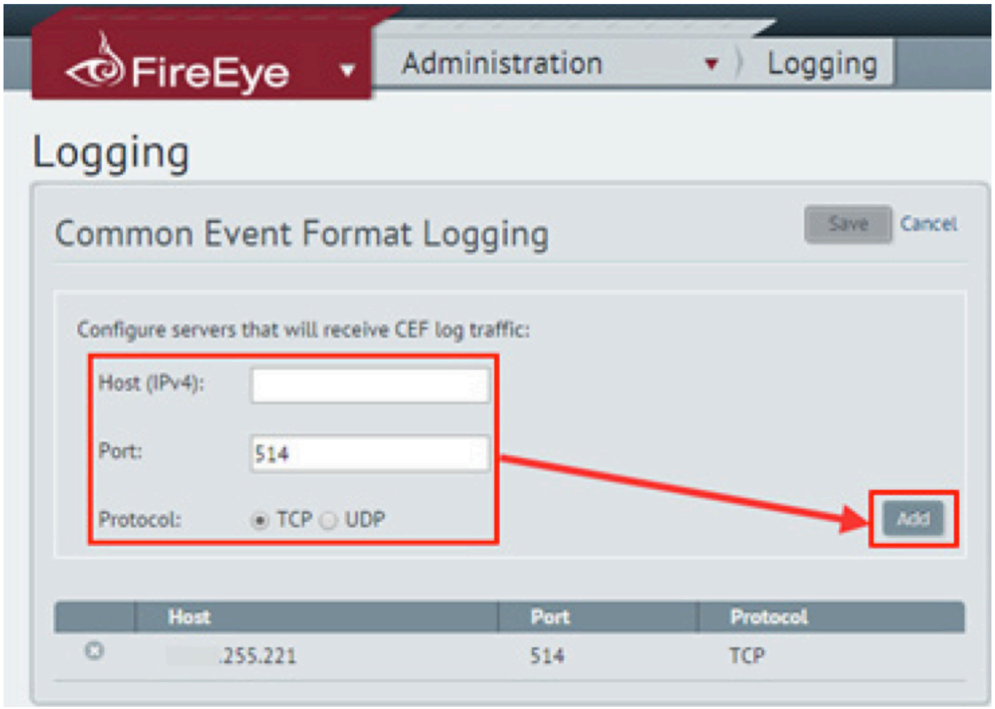


Figure 19: Logging option

5. Enter the Splunk server IP, Port, and Select TCP as the protocol. Then click the Save button.



Logging

Common Event Format Logging

Configure servers that will receive CEF log traffic:

Host (IPv4):

Port: 514

Protocol: ● TCP ○ UDP

	Host	Port	Protocol
⊗	.255.221	514	TCP

Figure 20: Entering syslog information

Integrating FireEye Threat Analytics Platform (TAP)

This section will outline how to integrate FireEye TAP into the FireEye App for Splunk Enterprise.

How it works

The diagram below is designed to show one possible use case. It also helps to illustrate data flow options between Splunk and FireEye products.

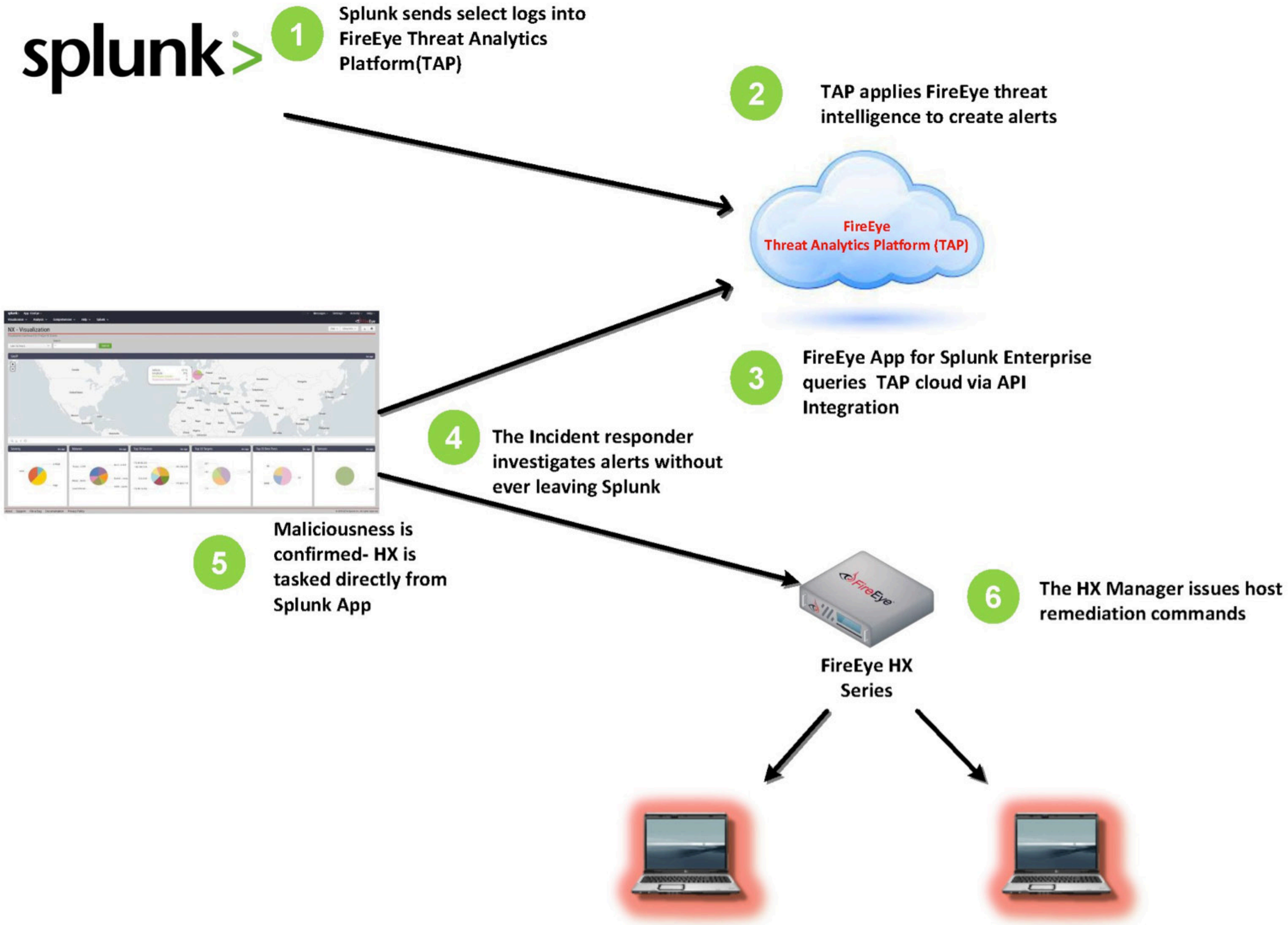

splunk>
1 Splunk sends select logs into FireEye Threat Analytics Platform(TAP)
2 TAP applies FireEye threat intelligence to create alerts
FireEye Threat Analytics Platform (TAP)
3 FireEye App for Splunk Enterprise queries TAP cloud via API Integration
4 The Incident responder investigates alerts without ever leaving Splunk
5 Maliciousness is confirmed- HX is tasked directly from Splunk App
6 The HX Manager issues host remediation commands
FireEye HX Series

Figure 21: One possible use case for TAP / Splunk integration

Requirements

- FireEye TAP is setup and receiving proper logs to generate events
- Third party Splunk App - Rest API Module Input (Big thanks to: Damien Dallimore)
  - https://apps.splunk.com/app/1546/

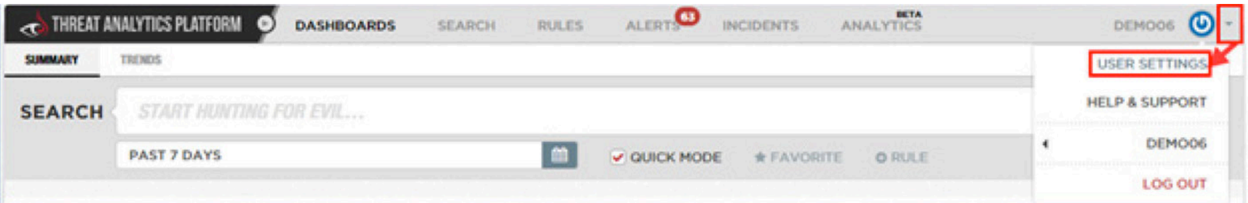
Configuring the FireEye TAP API

The instructions below will outline how to configure the TAP API.

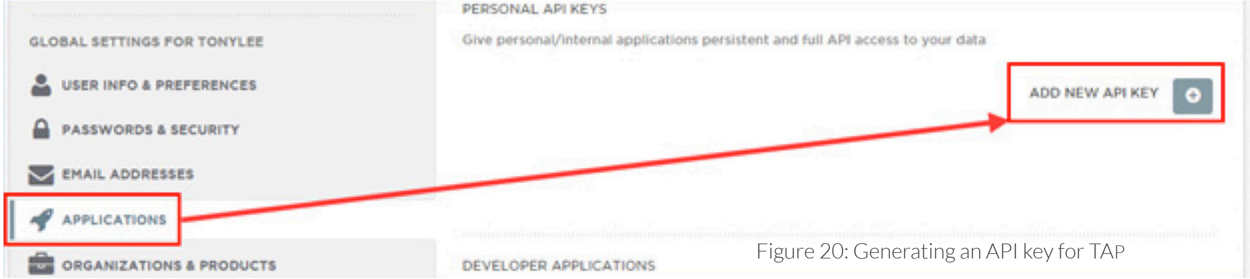
Create an API key

1. Log into the Threat Analytics Platform

2. Go to User settings by clicking the drop down arrow in the top right hand corner and then selecting "USER SETTINGS"



3. Select Applications and click "ADD NEW API KEY"

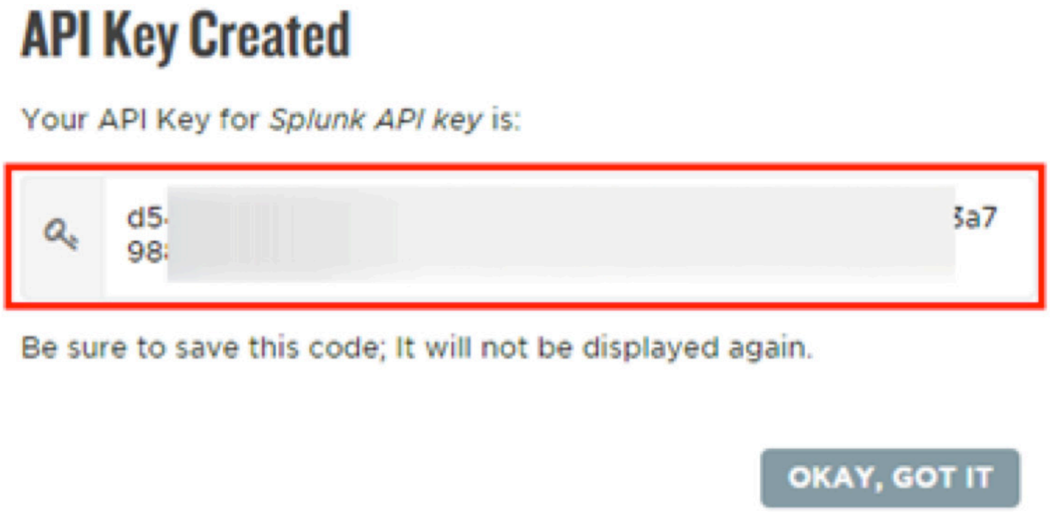


Give personal/internal applications persistent and full API access to your data

Figure 20: Generating an API key for TAP

4. Name the API key. Ex: Splunk API key

5. Save the API key in a secure place -- It will not be displayed again.



API Key Created

Your API Key for *Splunk API key* is:

d5 [redacted] 3a7 98

Be sure to save this code; It will not be displayed again.

Figure 22: API key provided

Discover the TAP Instance ID

The requirements for this step are the following:

1. URL of the TAP instance
2. API key from previous step

Using curl execute the following one-liner to retrieve the TAP Instance ID

Syntax:

```
curl -H "x-mansfield-key:INSERT_KEY_HERE" https://INSERT_URL_HERE/tap/ api/v1/users/instance
```

Example:

```
curl -H "x-mansfield-key:eb5123456789" https://yours.fireeyeapps.com/ tap/api/v1/users/instance
```

Expected response:

```
[{"id":"1234-123-123-123-123456789","name":"demo06","active":true}]
```

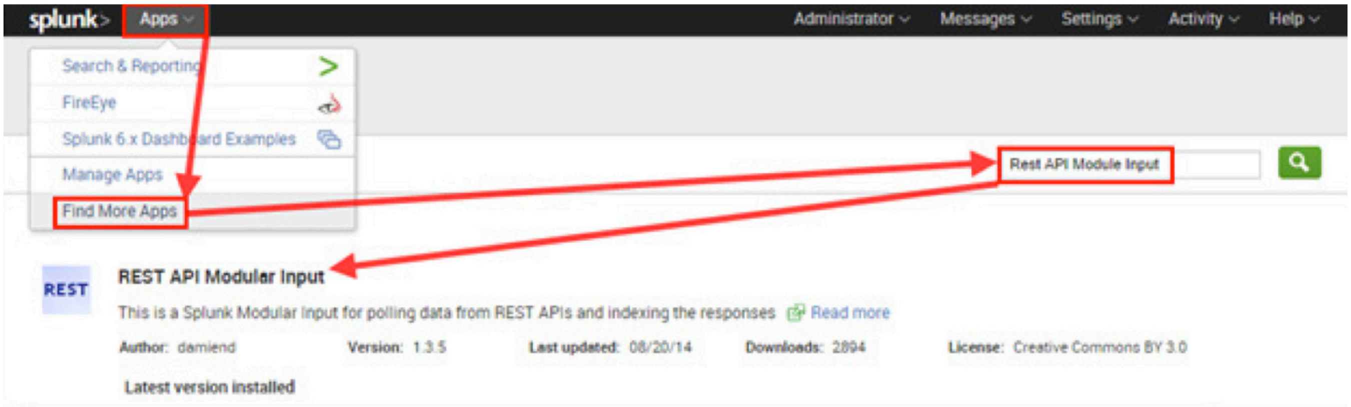
Be sure to copy down the TAP instance id that was returned from your query.

Now you have three pieces of vital information:

- URL of the TAP instance
- API key from previous step
- TAP instance ID

Install the Splunk Rest API Module Input

Use the App Manager within Splunk to search for “Rest API Module Input”



Rest API Module Input

REST API Modular Input

This is a Splunk Modular Input for polling data from REST APIs and indexing the responses Read more

Author: damiend Version: 1.3.5 Last updated: 08/20/14 Downloads: 2894 License: Creative Commons BY 3.0

Latest version installed

Figure 22: Installing Splunk REST API module Input

Or follow the manual installation instructions below:

1. Download the .spl or .tgz file from: https://apps.splunk.com/app/1546/
2. Navigate to “Apps” -> “Manage Apps”.
3. Click on “Install app from file”.
4. Upload the downloaded file using the form provided.
5. Restart if the app requires it: `$SPLUNK_HOME/bin/splunk restart splunk`

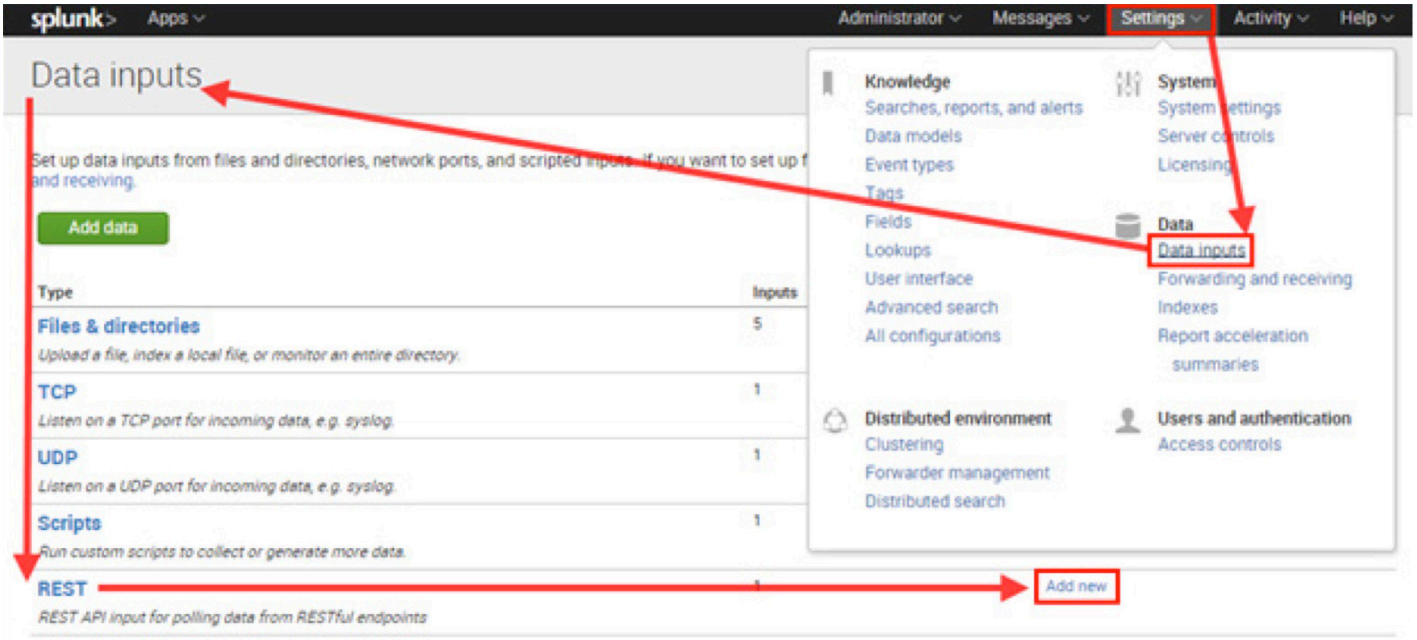
Configure the Splunk Rest API Module Input

1. 1. Add the following custom handlers:

```
$SPLUNK_HOME/etc/apps/rest_ta/bin/responsehandlers.py

class FireEyeAlertHandler:

     def  init  (self,**args): pass

     def  call  (self, response_object,raw_response_output,response_ type,req_
     args,endpoint):

          if response_type == "json":

               output = json.loads(response_object.content) last_display_id = -1

               for alert in output["alerts"]: print_xml_
               stream(json.dumps(alert)) if "displayId" in alert:

                         display_id = alert["displayId"] if
                         display_id > last_display_id:

                              last_display_id = display_id if not
                              "params" in req_args:

                    req_args["params"] = {}

if last_display_id > -1: req_args["params"]["offset"] = last_display_id

else:

     print_xml_stream(raw_response_output)

class FireEyeIncidentHandler:


     def  init  (self,**args): pass

     def  call  (self, response_object,raw_response_output,response_ type,req_
     args,endpoint):

          if response_type == "json":

               output = json.loads(response_object.content) last_display_id = -1

for incident in output["incidents"]:
    print_xml_stream(json.dumps(incident)) if "displayId" in incident:

        display_id = incident["displayId"] if display_id > last_
        display_id:

            last_display_id = display_id if not "params" in req_
            args:

    req_args["params"] = {}


if last_display_id > -1: req_args["params"]["offset"] = last_display_id

else:

print_xml_stream(raw_response_output)
```

2. Within Splunk, go to Settings -> Data -> Data Inputs

3. Next to REST, click on Add new



Data inputs

Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up f
and receiving.

Type	Inputs
Files & directories *Upload a file, index a local file, or monitor an entire directory.*	5
TCP *Listen on a TCP port for incoming data, e.g. syslog.*	1
UDP *Listen on a UDP port for incoming data, e.g. syslog.*	1
Scripts *Run custom scripts to collect or generate more data.*	1
REST *REST API input for polling data from RESTful endpoints*	1

Figure 23: Configuring the RESTful query options

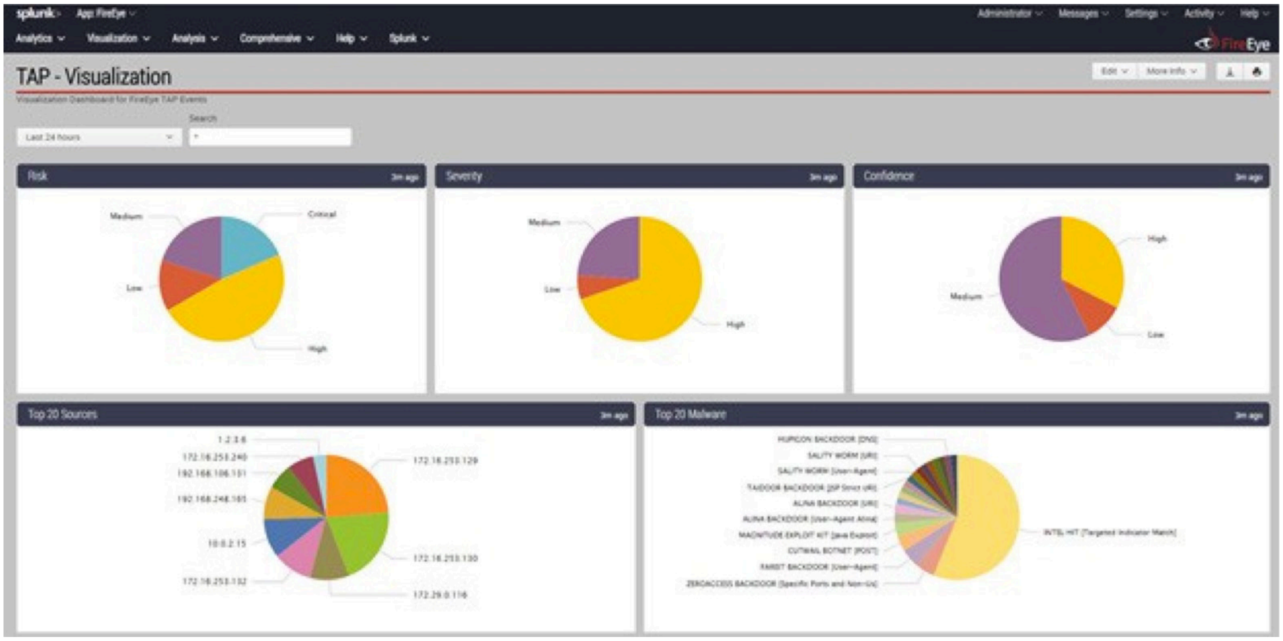
4. To set up TAP alerts, fill in the following data fields and click the save button

a. REST API Input Name: TAP-Alerts
b. Endpoint URL: https://INSERT_URL_HERE/tap/api/v1/alerts
c. HTTP Method: GET
d. Authentication Type: None
e. HTTP Header Properties: x-mansfield-key=INSERT_KEY_HERE,X-FireEye-Tap-Instance=INSERT_TAP_ID_HERE
f. URL Arguments: offset=0
g. Response type: json
h. Response Handler: FireEyeAlertHandler
i. Polling Interval: 30
j. Set Sourcetype: “Manual”
k. Select source type from list: fe_tap_json

5. To set up TAP incidents, fill in the following data fields and click the save button

a. REST API Input Name: TAP-Incidents
b. Endpoint URL: https://INSERT_URL_HERE/tap/api/v1/incidents
c. HTTP Method: GET
d. Authentication Type: None
e. HTTP Header Properties: x-mansfield-key=INSERT_KEY_HERE,X-FireEye-Tap-Instance=INSERT_TAP_ID_HERE
f. URL Arguments: offset=0
g. Response type: json
h. Response Handler: FireEye**Incident**Handler
i. Polling Interval: 30
j. Set Sourcetype: “Manual”
k. Select source type from list: fe_tap_json

6. Upon saving, Splunk should attempt a query, thus if there are TAP events, they will show up in the FireEye App for Splunk Enterprise under Visualization -> Tap Visualization and Analysis -> Tap Analysis



TAP - Visualization

Visualization Dashboard for FireEye TAP Events

Risk

Severity

Confidence

Top 20 Sources

Top 20 Malware

Figure 24: TAP visualization

Troubleshooting

There are many methods that can be used to troubleshoot connection issues.

Using Curl

Using any Linux host, or Cygwin on Windows perform the following:

Step 1) echo test > test.xml
Step 2) curl -k -g --user <username>:<password> --data-binary @test.xml

Example:

curl -k -g --user fireeye:1qaz@WSX --data-binary @oneline.txt “https://192.168.33.152:8089/services/receivers/simple?host=1 92.168.33.153&source=fe_alert&sourcetype=fe_xml”

Result:

You should see something similar to the following response from Splunk after issuing the command above:

```
<?xml version=”1.0” encoding=”UTF-8”?>
    <response>
 <results>
      <result>
<field k=”_index”>
<value>
 <text>default</text>
 </value>
</field>
<field k=”bytes”>
<value>
 <text>4</text>
 </value>
</field>
<field k=”host”>
<value>
 <text>Source IP Address here</text>
</value>
</field>
<field k=”source”>
 <value>
```

```
  <text>fe_alert</text>
 </value>
</field>
<field k=”sourcetype”>
<value>
 <text>fe_xml</text>
        </value>
       </field>
       </result>
      </results>
</response>
```

Splunk Search

After the data is successfully sent to Splunk, you should be able to search for it using the following search term: source=fe_alert

You should see “test” as the message body because it was in the body of test.xml

About the Author

Tony Lee has more than ten years of professional experience pursuing his passion in all areas of information security. He is currently a Technical Director at Mandiant, a FireEye Company, advancing many of the network penetration testing service lines. His interests of late are kiosk hacking, post exploitation tactics, and malware research. As an avid educator, Tony has instructed thousands of students at many venues worldwide, including government, universities, corporations, and conferences such as Black Hat. He takes every opportunity to share knowledge as a contributing author to Hacking Exposed 7, frequent blogger, and a lead instructor for a series of classes. He holds a Bachelor of Science degree in computer engineering from Virginia Polytechnic Institute and State University and a Master of Science degree in security informatics from The Johns Hopkins University.

Email: Tony.Lee -at-FireEye.com

Linked-in: http://www.linkedin.com/in/tonyleevt

Special Thanks

Dennis Hanzlik
Dan Dumond
Ian Ahl
Dave Pany
Karen Kukoda
Leianne Lamb
Brian Stoner
Gunpreet Singh
Kate Scott

About FireEye, Inc.

FireEye protects the most valuable assets in the world from those who have them in their sights. Our combination of technology, intelligence, and expertise — reinforced with the most aggressive incident response team — helps eliminate the impact of security breaches. We find and stop attackers at every stage of an incursion. With FireEye, you'll detect attacks as they happen. You'll understand the risk these attacks pose to your most valued assets. And you'll have the resources to quickly respond and resolve security incidents. FireEye has over 3,100 customers across 67 countries, including over 200 of the Fortune 500.

To learn more about
how FireEye can help you focus
on the alerts that matter,

visit: www.fireeye.com

FireEye

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**