

# FireEye Malware Protection System

## Logpoint Log Sources Configuration Guide

---

LogPoint

# logpoint

logpoint

## Table of Contents

<b>General Description</b> .....	3
<b>Functional Description</b> .....	3
<b>Configure FireEye Malware Protection System</b> .....	4
Configure FireEye from UI .....	4
Configure FireEye from command line .....	4
<b>Expected Log format</b> .....	5
<b>Sample Log</b> .....	Error! Bookmark not defined.
<b>Configuration in LogPoint</b> .....	5
<b>Importing Application</b> .....	5
<b>Adding Repos</b> .....	6
<b>Configure Normalization Policy</b> .....	7
<b>Configure Enrichment Policy</b> .....	8
<b>Configure Routing policy</b> .....	10
<b>Configure Processing Policy</b> .....	16
<b>Configure Device</b> .....	17

## General Description

With this integration LogPoint can fully extract and correlate the FireEye events and at the same time combine the results with observations from other systems. Administrators of the FireEye server can use LogPoint to provide long-term analytics.

## Functional Description

Key analytical components of the integration are ability to view event summary from FireEye devices.

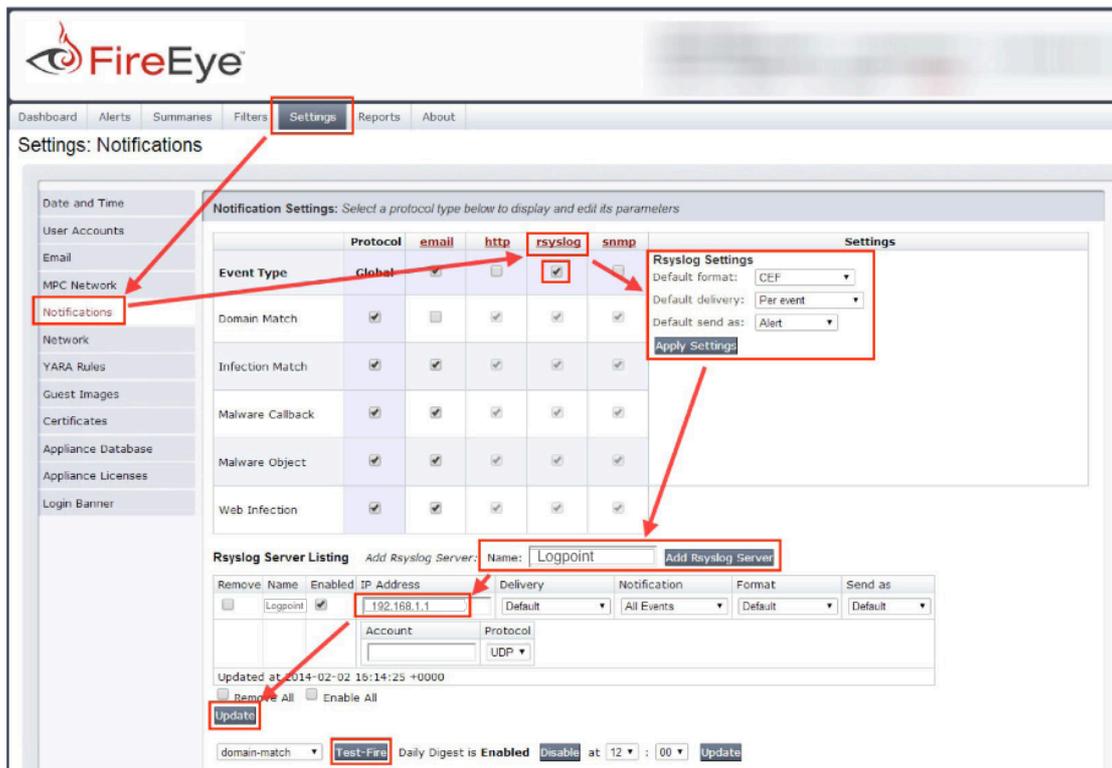
## Screen Shots



# Configuration of FireEye Malware Protection System

## Configure FireEye from UI

1. Log into the FireEye appliance with an administrator account
2. Click on **Settings**
3. Select **Notifications**
4. Click **rsyslog**
5. Check the “**Event type**” check box
6. Make sure Rsyslog settings are:
  - i. Default format: CEF
  - ii. Default delivery: Per event
  - iii. Default send as: Alert



Now, Left to Add Rsyslog Server button, type Logpoint and click on **Add Rsyslog Server** button. Then type the IP address of Logpoint server and click on **Update** button below. In the Protocol dropdown, select TCP if you want to send logs in TCP format.

## Configure FireEye from command line

See your product documentation about how to access and use the command line interface. Once you open a command line, do the following:

1. Enter following command to enter the configuration mode

```
enable
configure terminal
```

2. To activate rsyslog notification:

```
fenotify rsyslog enable
```

3. Add a remote Logpoint Server:

```
fenotify rsyslog trap-sink Logpoint
```

4. Specify the IP address for the new remote server:

```
fenotify rsyslog trap-sink Logpoint address <IP-address>
```

Where, <IP-address> is the IP address of Logpoint server

5. Set the event format:

```
fenotify rsyslog trap-sink Logpoint prefer message format cef
```

6. Save the configuration:

```
write memory
```

## Expected Log format

```
CEF:<version>|<vendor>|<product>|<device_version>|<signature_id>|<event_type>|<severity>|<key=value> <key=value> <key=value>...
```

## Log Sample

```
<164>fenotify-12903.alert: CEF:0|FireEye|MPS|1.1.0.7|WI|web-infection|4|rt=Mar 06 2013 12:52:17 Z src=10.10.0.1 shost=abc.item.com dproc=InternetExplorer 8.0.70.15 cs3Label=osinfo cs3=Microsoft Windows7 Professional 6.1 base filePath=10.10.0.1/f248706c253/q.php dvchost=ips01 dvc=1.1.0.7 smac=0:1:1:0:aa:aa cn1Label=vlan cn1=0 externalId=103 cs4Label=link cs4=https://logpoint.com/event_stream/events_for_bot?inc_id\=13 cs2Label=anomaly cs2=anomaly-tag misc-anomaly cs1Label=sname cs1=Exploit.Browser
```

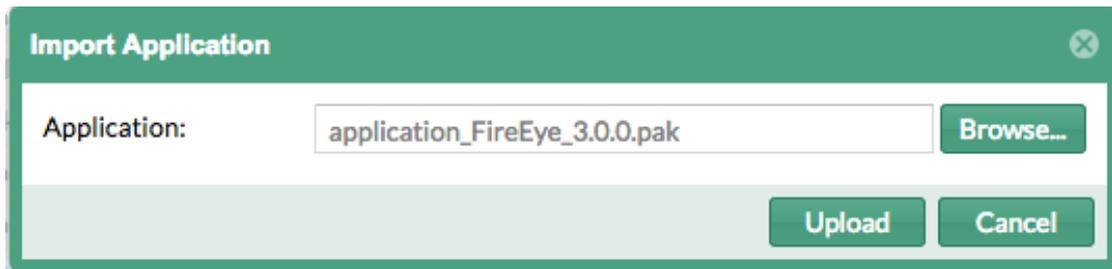
## Configuration in LogPoint

Now login to the LogPoint installation and run through the following steps to finalize.

### Importing Application

To import the Application Package follow the following steps:

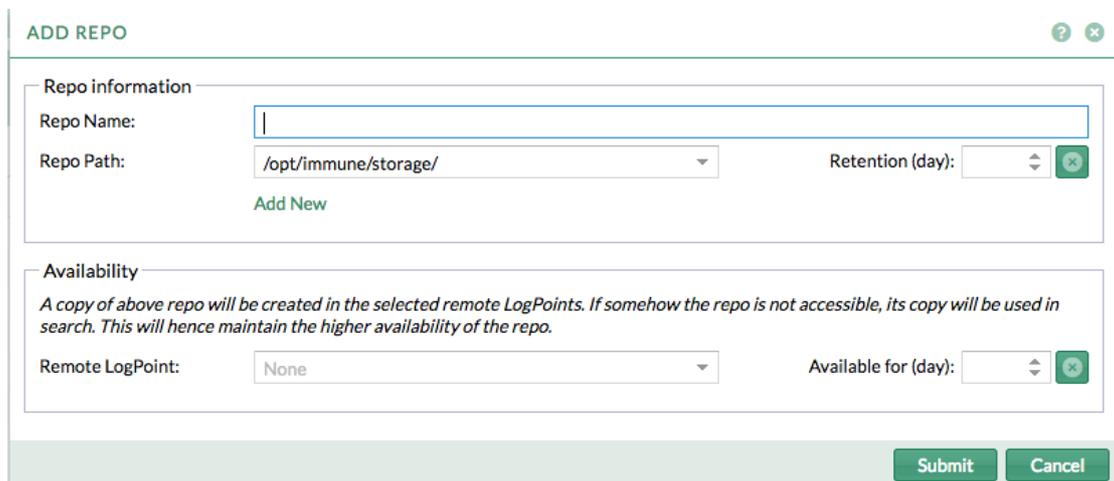
1. Go to Settings >> System >> Application.
2. Click Import.
3. Click on Browse, Choose FireEye.
4. Click on upload Button.



## Adding Repos

To add repos, follow the following steps:

1. Go to Settings >> Configuration >> Repos.
2. Click **Add Repo**. A pop-up window appears for Repo Information and Availability.



3. In the Repo Information section, provide a **Repo Name**. (The length of the Repo Name should not exceed 29 characters). Select a **Repo Path** and the preferred **Retention (day)** period.
4. Click Add New to add multiple storage locations for your repo.
5. Under the Availability section, select a **Remote LogPoint** and set up a time period for **Available for (day)**.
6. Click **Submit**.

Once after a repo has been added, it will be populated in the Repos feed along with its repo name, disk space used and retention days.

The number of days displayed under the **Retention (days)** column is the cumulative days of all the retention days associated with the different **Repo Path** for a repo.

## Configure Normalization Policy

To configure the normalization policy, follow the following steps:

1. Go to Settings >> Configuration >> Normalization Policies.
2. Click **Add**.
3. Provide a **Policy Name**.

### CREATE NORMALIZATION POLICY

Normalization Policy Information

Policy Name:

Compiled Normalizer:

Available		Selected
CEFCompiledNormalizer	↑	
CheckPointOpsecCompiledNormalizer	→	
FirstClassCompiledNormalizer	←	
FortiOSCompiledNormalizer	↓	
JSONCompiledNormalizer	⌵	

Normalization Packages:

Available		Selected
Charite_DHCP_WLAN	↑	
Charite_DHCP_Wired	↑	
Charite_Radius_WLAN	→	
Charite_Radius_Wired	←	
LP_A10 Thunder CEF	↓	
LP_Cisco ISE	↓	
LP_FreeRadius Server	⌵	
LP_FreeRadius VPN		

**Note:** Ordering of the Normalization Packages will reset the signatures order according to the packages. Either packages order or the individual signatures order can be altered at a time.

[View Signatures](#) [Submit](#) [Cancel](#)

4. Drag and drop the available **Normalization Packages** and **Compiled Normalizer** to the right-side windowpane. The selected normalization packages can now be reordered according to the requirement.
5. Click **View Signatures** to view signatures in the selected packages. You can deactivate signatures from your policy by deselecting them. You can deselect in three ways:
  - Double click the selected signatures
  - Drag and drop in the initial windowpane.
  - Press  button from the arrow buttons.
6. Click **Submit**.

## Configure Enrichment Policy

1. Go to Settings >> Configuration >> Enrichment Policies.
2. Click **Add**.

**CREATE ENRICHMENT POLICY** ✕

---

**Enrichment basic**

Policy Name:  !

Description:

**Specification**

**Enrichment Criteria**

*Enrichment rule will be applied only if all of the conditions are satisfied by log event*

Key Presents  ✕

[Add New Criterion](#)

**Enrichment Rule**

*Enrichment rule will be applied if all of the conditions below matches*

Enrichment Source:

Source	Operation	Category	
<input type="text"/>	<input type="text" value="Equals"/>	<input type="text" value="Simple"/>	<input type="text" value="Event Key"/> <span style="float: right; color: green;">✕</span>

[Add New Rule](#)

[Remove Specification](#)

[Add New Specification](#)

Submit
Cancel

3. Under Enrichment basic section, provide **Policy Name** and **Description**.
4. Under Specification section, provide **Enrichment Criteria** and **Enrichment Rule**.
5. Provide the key value after selecting the Enrichment Criterion from the dropdown menu. The key entered must be present in the log event, and the value of the key in the log event must match the value or Regular Expression specified.

**Note:** Clicking Add New Criterion will generate a new dropdown menu for Enrichment Criteria options.

6. Select the Enrichment Source from the dropdown menu. The information to be filled will be followed as per the selected Enrichment Source.
  - Choose a Source from the dropdown menu.
  - The type of Operation will be set to **Equals** by default.
  - Choose a Category from the dropdown menu.
  - If you select Simple, provide the Event Key suitable with the Source.
  - If you select Type Based, choose an Event Key Type from the dropdown menu. In this case, all the fields of the selected type are eligible to be taken into consideration.

**Enrichment Rule**

*Enrichment rule will be applied if all of the conditions below matches*

Enrichment Source:

Source	Operation	Category	
<input type="text" value="description"/>	<input type="text" value="Equals"/>	<input type="text" value="Type Based"/>	Event Key Type: <input type="text" value="String"/>

Enable prefixing ✕

[Add New Rule](#)

- Select the checkbox Enable prefixing, if you want the results to be prefixed with the event key. Unselect the checkbox if you want to obtain a particular result. In such case, LogPoint will perform the lexicographic operation, where the result will be presented in alphabetical order of the event key.

**Note:** Clicking Add New Rule will generate a new dropdown menu for Enrichment Rule options.

7. Click Submit.

**Note:** If you have a distributed LogPoint setup you cannot administer the Enrichment Policies of the remote LogPoints from the **Distributed LogPoint** dropdown menu on the **Header Bar** inside the Settings menu.

**Warning:** Using enriched field as an Enrichment Criteria for Type based enrichment is now allowed if the enrichment has been performed once previously. For example, if the field **source\_address** is an enriched field, then the user is not allowed to use that field as an enrichment criteria value.

## Configure Routing policy

Routing Policy allows the users to selectively determine what incoming data gets forwarded to a particular repository and what gets dropped. Routing is performed on the basis of "key-value-match" or "key-present" criteria.

Steps to configure Routing Policy:

1. Go to Settings >> Configuration >> Routing Policies.
2. Click **Add Policy**.

S.N.	Type	Key	Value	Repo	Operation	Actions
------	------	-----	-------	------	-----------	---------

In the Add Policy panel, click ? to open the help section for routing policy. It lists all the points to be considered while creating a routing policy.

ADD POLICY
< Back ✕

---

**Policy Name:**

- The value can be alpha numeric characters with hyphen(-), underscore(\_) and the value should not contain any spaces.
- The value should be unique.
- The policy name should not start with \_logpoint.

---

**Routing Policy:**

- Routing Policies are used to forward particular log messages to a desired repository or to drop them.

---

**Policy Information:**

- Provide a name to the routing policy. Make sure that the policy name is same as the name of an existing repository.
- Catch All acts as the target repository if any of the routing criteria is not applied.

---

**Routing Criteria:**

- Select type for the routing criteria.
- KeyPresent will only take key parameter and this key will be used to filter out the messages.
- KeyPresentValueMatches will take both key and value as parameters where value is a regular expression and the combination of both key and value will be used to filter out the messages.
- Select repository to send the message if condition is satisfied.
- Operation determines either to forward the message to specified repo or drop the message, if the condition is satisfied.
- Click on add button to create routing criteria after filling up the credentials.
- The added criteria are listed in the table below the form section.
- The routing criteria listed in the table can be re-ordered and also can be removed.
- The messages are processed in order of routing criteria specified.

- In *Policy Information* section of the panel, provide **Policy Name** for the routing policy.
  - In the same section, select a repository from the dropdown menu as **Catch All**. If any *Routing Criteria* does not match with the log messages, Catch All repository will act as the target repository.
5. In *Routing Criteria* section, select a **Type** for the routing criteria. The type may be either "KeyPresent" or "KeyPresentValueMatches".
- If KeyPresent type is selected, provide a **Key**. The routing criteria will be applied to the log messages containing the provided key.

**Policy Information**

Policy Name:

Catch All:

**Routing Criteria**

Type:

Key:

Operation:  Store raw message     Discard raw message     Discard entire event

Repository:

S.N.	Type	Key	Value	Repo	Operation	Actions

- If KeyPresentValueMatches is selected, provide a **Key** and its **Value**. The routing criteria will be applied to the log messages confirming the provided Key-Value match.

**Note:** The Key for both KeyPresent and KeyPresentValueMatches types must be a normalized field name of the log message.

6. Select the target **Repository** from the dropdown menu for the *Routing Criteria*.
7. Choose an **Operation** to:
  - Store raw message: This will store both the raw message and the normalized data in the target repository.
  - Discard raw message: This will discard raw message and store the normalized data only.
  - Discard entire event: This will discard both raw message and the normalized data.

8. Click **Add**.

### ADD POLICY

**Policy Information**

Policy Name:

Catch All:

**Routing Criteria**

Type:

Key:

Value:

Operation:  Store raw message  Discard raw message  Discard entire event

Repository:



S.N.	Type	Key	Value	Repo	Operation	Actions
1	KeyPresent	source_port	Not Applicable	routing_repo	Store message	^ v 🗑️
2	KeyPresentVal...	sig_id	12345	routing_repo	Discard raw message	^ v 🗑️

All the added criteria are listed in the table below *Policy Information* section and prioritized according to their *S.N.* with serial number 1 being the highest priority criteria. Priority of routing criteria can be changed by clicking "up arrow" and "down arrow" in *Actions* column of the table.

9. Click **Submit** to save the routing policy, or **Cancel** to abort the process.

ADD POLICY
?
✕

**Policy Information**

Policy Name:

Catch All:

**Routing Criteria**

Type:

Key:

Value:

Operation:  Store raw message  Discard raw message  Discard entire event

Repository:

Add

S.N.	Type	Key	Value	Repo	Operation	Actions
1	KeyPresent	source_port	Not Applicable	routing_repo	Store message	^ v 🗑️
2	KeyPresentVal...	sig_id	12345	routing_repo	Discard raw message	^ v 🗑️
3	KeyPresentVal...	norm_id	23456	routing_repo	Discard raw message	^ v 🗑️

Submit
Cancel

After submitting the policy, users will be redirected to the Routing Policy page where all the routing policies are listed in a table. The table also displays **Number of Repositories** that the policy is using and **Number of Devices** to which the policy is applied.

logpoint DASHBOARD SEARCH REPORT INCIDENT SETTINGS 05:11:25 admin

### Routing Policies

+ Add Policy More 0 selected Search...

S.N.	Name	Number of Repositories	Number of Devices	Catch All	Actions
1	routing_repo	2	0	default	
2	_LogPointAlerts	1	0	default	
3	default	0	1	default	
4	_logpoint	0	1	_logpoint	

Page 1 of 1 Displaying 1 - 4 of 4 Page size: 25

USER ACCOUNTS CONFIGURATION KNOWLEDGE BASE SYSTEM ROUTING POLICIES

Now, if any of the routing criteria configured in the policy is matched by an incoming log message, it will be either forwarded to the target repository or dropped as per the policy.

For example, let's configure a routing policy as shown in the figure below:

### ADD POLICY

**Policy Information**

Policy Name:

Catch All:

**Routing Criteria**

Type:

Key:

Value:

Operation:  Store raw message  Discard raw message  Discard entire event

Repository:

S.N.	Type	Key	Value	Repo	Operation	Actions
1	KeyPresent	source_port	Not Applicable	routing_repo	Store message	
2	KeyPresentVal...	sig_id	12345	routing_repo	Discard raw message	
3	KeyPresentVal...	norm_id	23456	routing_repo	Discard raw message	

So, the following log message that contains a field named `source_port` is forwarded to "routing\_repo" repository as configured in the routing policy.

```
2017/01/12 08:13:33
Connection | Deny | Firewall
action=denied | col_ts=2017/01/12 08:13:33 | col_type=filesystem | collected_at=LogPoint | destination_address=192.168.4.255 | destination_port=138 |
device_ip=127.0.0.1 | device_name=localhost | log_ts=2017/01/12 08:13:33 | logpoint_name=LogPoint | norm_id=Kernel | object=set_firewall | process=kernel |
protocol=udp | repo_name=routing_repo | sig_id=19023 | source_address=192.168.4.165 | source_name=/var/log/syslog | source_port=138 |
Jan 12 08:13:29 LogPoint kernel: [ 8964.458358] set_firewall; denied udp; IN=eth0 OUT= MAC=ff:ff:ff:ff:00:0c:29:1f:3b:d5:08:00 SRC=192.168.4.165 DST=192.168.4.2
55 LEN=242 TOS=0x00 PREC=0x00 TTL=128 ID=19110 PROTO=UDP SPT=138 DPT=138 LEN=222
```

- It is not possible to specify routing specifications for the repo "\_logpoint".
- "\_LogPointAlerts" is the default routing policy bundled with LogPoint. For the log messages whose 'norm\_id' field has 'LogPointAlerts' value, the policy routes those log messages to \_LogPointAlerts repo. Otherwise, it forwards them to default repo.

## Configure Processing Policy

A **Processing Policy** integrates Normalization Policy, Enrichment Policy, and Routing Policy into a single policy. The main purpose of the Processing Policy is to aid in the data enrichment process.

1. Go to Settings >> Configuration >> Processing Policies.
2. Click **Add**.
3. Provide **Policy Name**.
4. Select the required **Normalization Policy** from the dropdown menu.
5. Select the required **Enrichment Policy** from the dropdown menu. It is optional to add an **Enrichment Policy**.
6. Select the required **Routing Policy** from the dropdown menu.
7. Click **Submit**.

## PROCESSING POLICY



**Processing Policy**

Policy Name:

Normalization Policy:

Enrichment Policy:

Routing Policy:

Submit

Cancel

### Configure Device

1. Start by clicking through “Settings” > “Devices”
2. Click on the “Add” button, to add a new device, and fill out the fields
  - a. “Name”: Name of the device
  - b. “IP address(es)”: IP address of the device
  - c. “Device Groups”: Device groups, that this device should be part of.

## CREATE DEVICE



**Device Information**

Name:

IP address(es):

Device Groups:

Log Collection Policy:

Distributed Collector:

Time Zone:

**Risk Values**

Confidentiality:

Integrity:

Availability:

