# Integrate Cisco Sourcefire

*EventTracker Enterprise*

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

Publication Date: April 18, 2016

# About this Guide

This guide will facilitate **Cisco Sourcefire** user to send logs to EventTracker Enterprise.

## Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise 7.x or later and Cisco Sourcefire 6.0.0**

## Audience

Administrators who want to monitor **Cisco Sourcefire** using EventTracker Enterprise.

*The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.*

*This document is for informational purposes only. Prism Microsystems MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.*

*Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.*

*Prism Microsystems may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Prism Microsystems, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.*

*The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.*

# Table of Contents

# Introduction

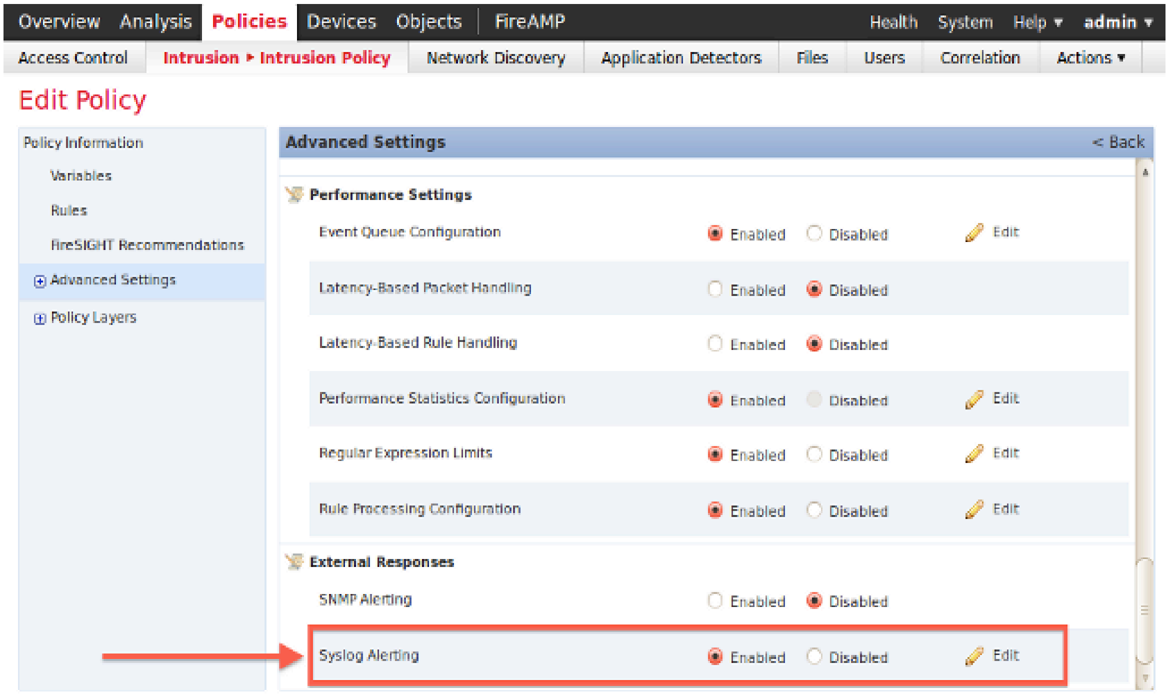
**Sourcefire, Inc** develops network security hardware and software. The company's FirePOWER network security appliances are based on Snort, an open-source Intrusion Detection System (IDS).

# Pre-requisites

- **EventTracker 7.x or later** should be installed.
- Syslog port (default is 514) must be allowed in your firewall.
- User should have administrator privileges to Cisco Sourcefire.

# Configuring Cisco Sourcefire

1. Log into the web user interface of your Sourcefire Management Center.
2. Navigate to **Policies** > **Intrusion** > **Intrusion Policy**.
3. Click **Edit** next to the policy you want to apply.
4. Click on **Advanced Settings.**
5. Locate **Syslog Alerting** in the list and set it to **Enabled**.



Performance Settings

Event Queue Configuration ● Enabled ○ Disabled Edit

Latency-Based Packet Handling ○ Enabled ● Disabled

Latency-Based Rule Handling ○ Enabled ● Disabled

Performance Statistics Configuration ● Enabled ○ Disabled Edit

Regular Expression Limits ● Enabled ○ Disabled Edit

Rule Processing Configuration ● Enabled ○ Disabled Edit

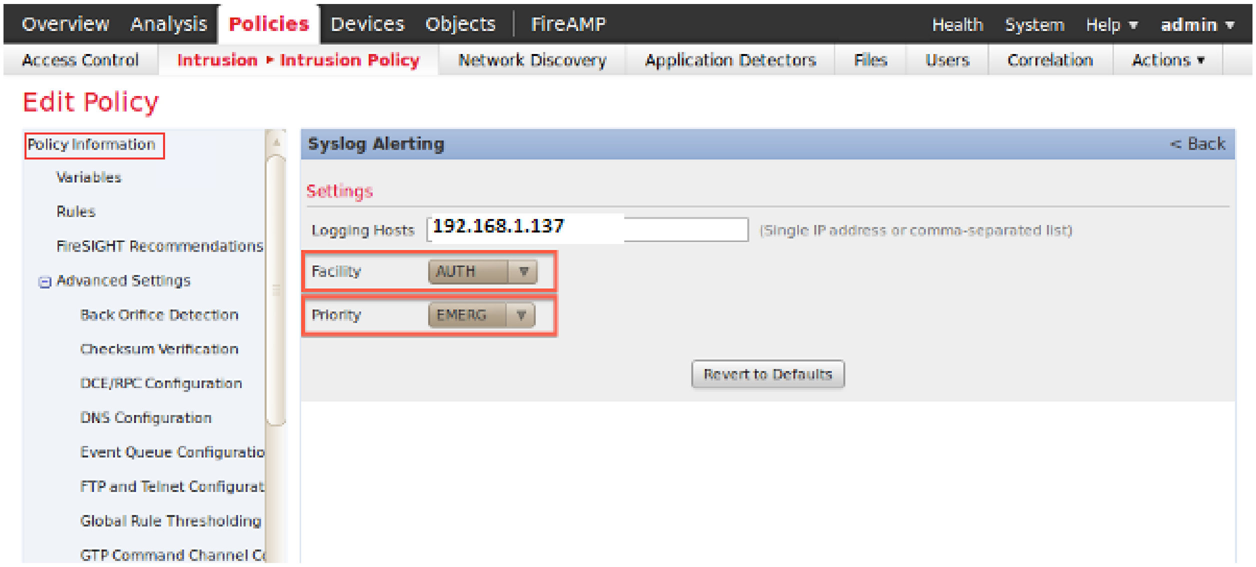
External Responses

SNMP Alerting ○ Enabled ● Disabled

Syslog Alerting ● Enabled ○ Disabled Edit

Figure 1

6. Click **Edit** next to the right of **Syslog Alerting.**
7. Type the IP address of EventTracker on the **Logging Hosts** field. Eg: 192.168.1.137
8. Choose an appropriate **Facility** and **Severity** from the drop-down menu. These can be left at the default values unless a Syslog server is configured to accept alerts for a certain facility or severity.



Logging Hosts 192.168.1.137 (Single IP address or comma-separated list)

Facility AUTH

Priority EMERG

Figure 2

9. Click on **Policy Information** near the top left of this screen.
10. Click the **Commit Changes** button.
11. Reapply your Intrusion Policy.

# EventTracker Knowledge Pack

Once Cisco Sourcefire is configured, events are received in EventTracker; Alerts and Reports can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker to support Cisco Sourcefire.

## Categories

- **Cisco SourceFire: IDS and IPS activity**
  This category provides information related to threat detection and prevention details.

- **Cisco SourceFire: Correlation events**
  This category provides information related to correlation events monitoring where several

events are tied up to pinpoint behavior of the network.

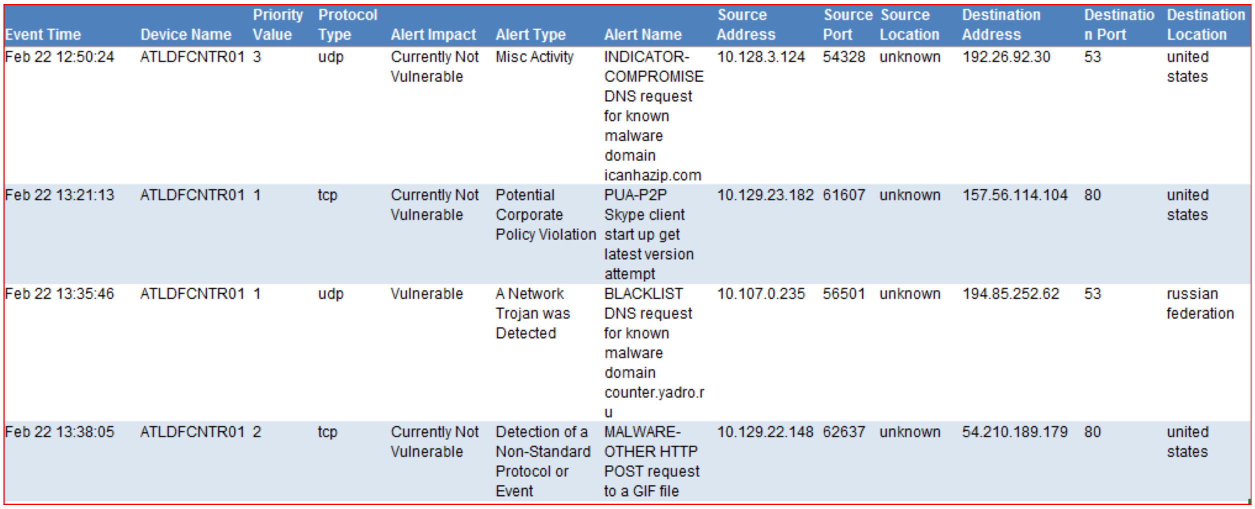
- **Cisco SourceFire: Inbound and outbound traffic**
  This category provides information related to connection type, traffic originating from, access control rule name and action defined.

# Alerts

- **Cisco SourceFire: High priority alert generated**
  This alert is generated when alert priority is highest for the detected alert type.

# Flex Reports

- **Cisco SourceFire: IDS and IPS activity**
  This report provides information related to alert type detected and its impact and location details from where traffic is being received.

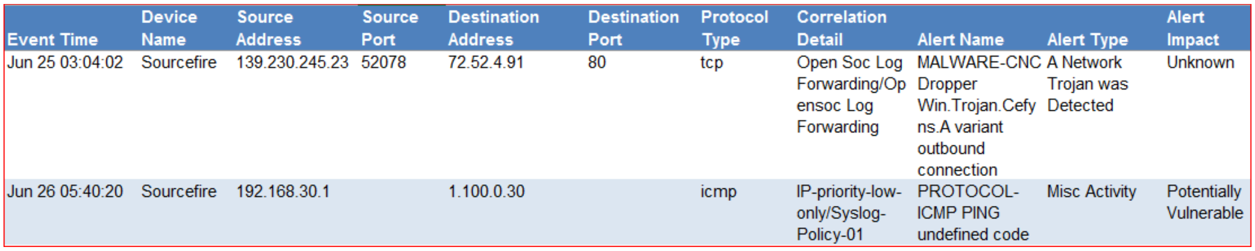


| Event Time | Device Name | Priority Value | Protocol Type | Alert Impact | Alert Type | Alert Name | Source Address | Source Port | Source Location | Destination Address | Destination Port | Destination Location |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Feb 22 12:50:24 | ATLDFCNTR01 | 3 | udp | Currently Not Vulnerable | Misc Activity | INDICATOR-COMPROMISE DNS request for known malware domain icanhazip.com | 10.128.3.124 | 54328 | unknown | 192.26.92.30 | 53 | united states |
| Feb 22 13:21:13 | ATLDFCNTR01 | 1 | tcp | Currently Not Vulnerable | Potential Corporate Policy Violation | PUA-P2P Skype client start up get latest version attempt | 10.129.23.182 | 61607 | unknown | 157.56.114.104 | 80 | united states |
| Feb 22 13:35:46 | ATLDFCNTR01 | 1 | udp | Vulnerable | A Network Trojan was Detected | BLACKLIST DNS request for known malware domain counter.yadro.ru | 10.107.0.235 | 56501 | unknown | 194.85.252.62 | 53 | russian federation |
| Feb 22 13:38:05 | ATLDFCNTR01 | 2 | tcp | Currently Not Vulnerable | Detection of a Non-Standard Protocol or Event | MALWARE-OTHER HTTP POST request to a GIF file | 10.129.22.148 | 62637 | unknown | 54.210.189.179 | 80 | united states |

```
Feb 22 13:05:47 atldfcntr01 Feb 22 18:05:47 ATLDFCNTR01 SFIMS: [1:29119:1] "BLACKLIST DNS
request for known malware domain counter.yadro.ru" [Impact: Vulnerable] From "SFOSCFIRE01"
at Mon Feb 22 18:05:46 2016 UTC [Classification: A Network Trojan was Detected] [Priority: 1]
{udp} 10.1.16.115:61131 (unknown)->194.190.124.17:53 (russian federation)

Feb 22 13:04:32 atldfcntr01 Feb 22 18:04:32 ATLDFCNTR01 SFIMS: [1:24105:9] "MALWARE-
OTHER HTTP POST request to a GIF file" [Impact: Currently Not Vulnerable] From
"SFOSCFIRE01" at Mon Feb 22 18:04:32 2016 UTC [Classification: Detection of a Non-Standard
Protocol or Event] [Priority: 2] {tcp} 10.5.101.93:49548 (unknown)->40.118.160.210:80 (united
states)
```

- **Cisco SourceFire: Correlation events**
  This report provides the information related to alert generated and the impact on system due to correlated events.

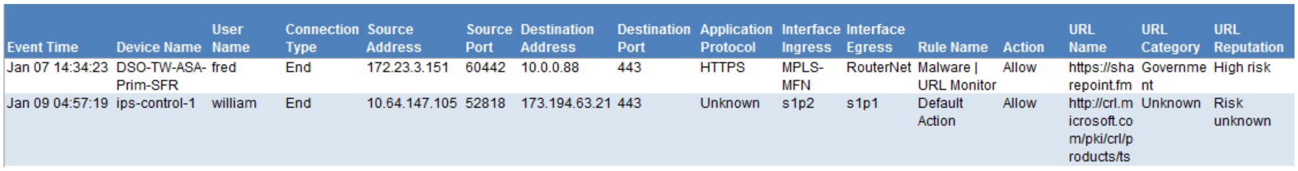


| Event Time | Device Name | Source Address | Source Port | Destination Address | Destination Port | Protocol Type | Correlation Detail | Alert Name | Alert Type | Alert Impact |
|---|---|---|---|---|---|---|---|---|---|---|
| Jun 25 03:04:02 | Sourcefire | 139.230.245.23 | 52078 | 72.52.4.91 | 80 | tcp | Open Soc Log Forwarding/Opensoc Log Forwarding | MALWARE-CNC Dropper Win.Trojan.Cefyns.A variant outbound connection | A Network Trojan was Detected | Unknown |
| Jun 26 05:40:20 | Sourcefire | 192.168.30.1 | | 1.100.0.30 | | icmp | IP-priority-low-only/Syslog-Policy-01 | PROTOCOL-ICMP PING undefined code | Misc Activity | Potentially Vulnerable |

```
 Jun 25 12:12:17 1.150.0.47 Jun 25 03:04:02 Sourcefire SFIMS: Correlation Event: Open Soc Log
Forwarding/Opensoc Log Forwarding at Thu Oct 23 04:55:39 2014 UTC: [1:19123:7] "MALWARE-
CNC Dropper Win.Trojan.Cefyns.A variant outbound connection" [Impact: Unknown] From
"172.19.50.7" at Thu Oct 23 04:55:38 2014 UTC [Classification: A Network Trojan was Detected]
[Priority: 1] {tcp} 139.230.245.23:52078->72.52.4.91:80

Jun 25 12:12:17 1.150.0.47 Jun 25 03:04:02 Sourcefire SFIMS: Correlation Event: IP-priority-low-
only/Syslog-Policy-01 at Thu Jun 25 03:04:02 2015 UTC: [1:365:11] "PROTOCOL-ICMP PING
undefined code" [Impact: Potentially Vulnerable] From "1.176.0.33" at Thu Jun 25 03:04:01 2015
UTC [Classification: Misc Activity] [Priority: 3] {icmp} 192.168.30.1->1.100.0.30
```

- **Cisco SourceFire: Inbound and outbound traffic**
  This report provides the information related to traffic established from source to destination using application protocol, rule configured and action taken by the Sourcefire.



| Event Time | Device Name | User Name | Connection Type | Source Address | Source Port | Destination Address | Destination Port | Application Protocol | Interface Ingress | Interface Egress | Rule Name | Action | URL Name | URL Category | URL Reputation |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Jan 07 14:34:23 | DSO-TW-ASA-Prim-SFR | fred | End | 172.23.3.151 | 60442 | 10.0.0.88 | 443 | HTTPS | MPLS-MFN | RouterNet | Malware \| URL Monitor | Allow | https://sharepoint.fm | Government | High risk |
| Jan 09 04:57:19 | ips-control-1 | william | End | 10.64.147.105 | 52818 | 173.194.63.21 | 443 | Unknown | s1p2 | s1p1 | Default Action | Allow | http://crl.microsoft.com/pki/crl/products/ts | Unknown | Risk unknown |

```
2015-03-17 00:01:25 Syslog.Alert 10.24.100.2 Mar 16 13:50:47 SET-ASASFR SFIMS: [Primary
Detection Engine (3fb65e80-3ea7-11e4-ae31-d6323923abe1)][Default Access Control] Connection
Type: End, User: rad2, Client: Microsoft CryptoAPI, Application Protocol: HTTP, Web App:
Microsoft, Access Control Rule Name: LogWebTraffic, Access Control Rule Action: Allow, Access
Control Rule Reasons: Unknown, URL Category: Business and Economy, URL Reputation: High
risk, URL: http://crl.microsoft.com/pki/crl/products/tspca.crl, Interface Ingress: Inside, Interface
Egress: Outside, Security Zone Ingress: N/A, Security Zone Egress: N/A, Security Intelligence
Matching IP: None, Security Intelligence Category: None, Client Version: 6.1, Number of File
Events: 0, Number of IPS Events: 0, TCP Flags: 0x0, NetBIOS Domain: (null), Initiator Packets: 17,
Responder Packets: 9, Initiator Bytes: 2799, Responder Bytes: 2083, Context: unknown {TCP}
10.24.100.91:62157 -> 74.73.232.50:80
```

# Import Knowledge Pack into EventTracker

**NOTE**: Import knowledge pack items in the following sequence

- Categories
- Alerts
- Token Templates
- Flex Reports
- Knowledge Objects

1. Launch **EventTracker Control Panel**.
2. Double click **Export/Import Utility**, and then click the **Import** tab.

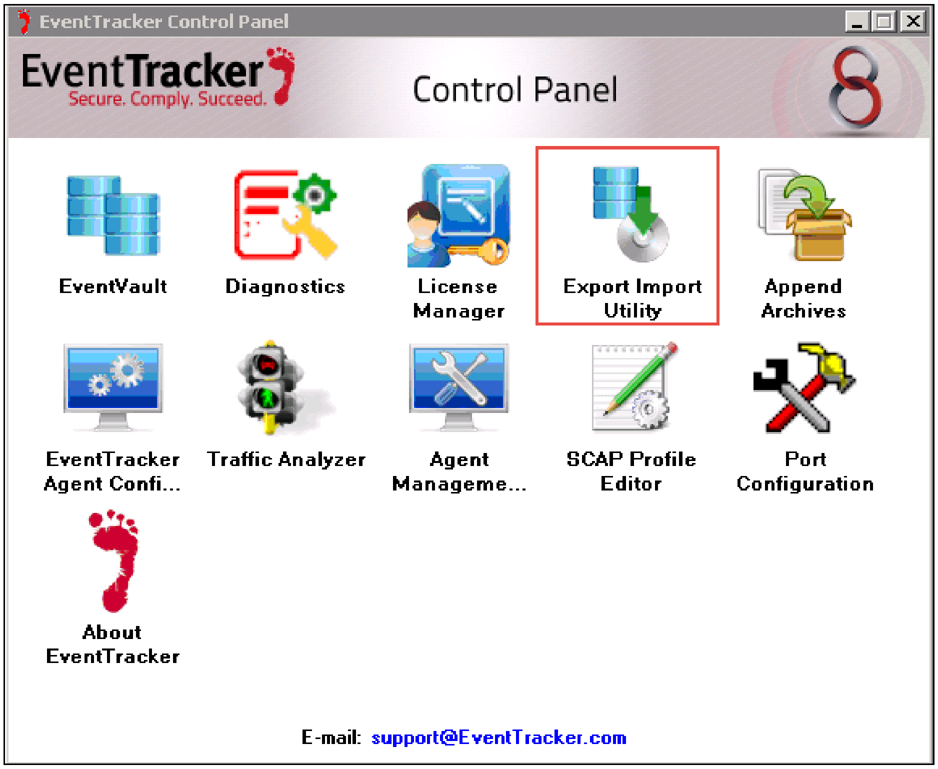
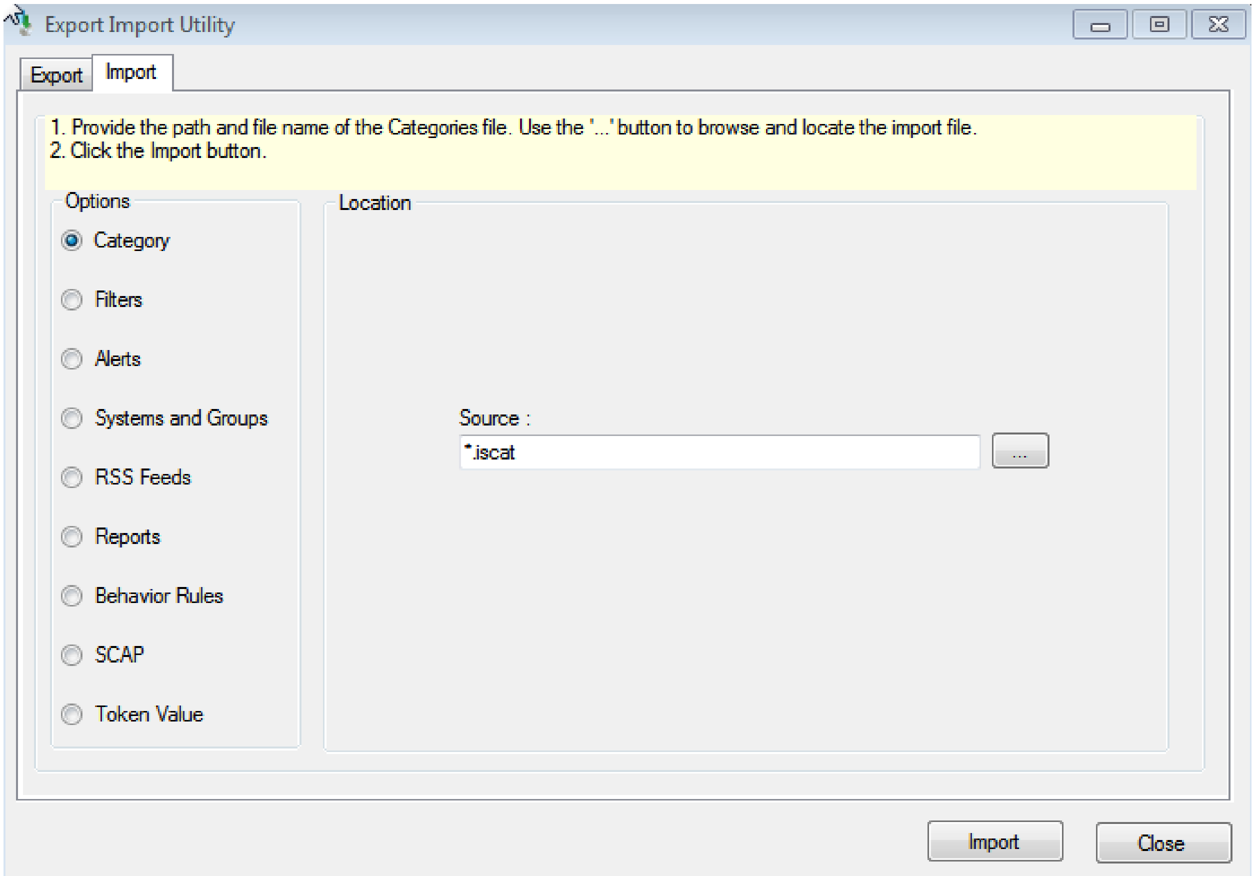


Figure 3

Import **Categories, Alerts, Flex Reports and Knowledge Objects** as given below.

# Categories

1. Click **Category** option, and then click the browse ... button.



Export Import Utility

1. Provide the path and file name of the Categories file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Options

- ● Category
- ○ Filters
- ○ Alerts
- ○ Systems and Groups
- ○ RSS Feeds
- ○ Reports
- ○ Behavior Rules
- ○ SCAP
- ○ Token Value

Location

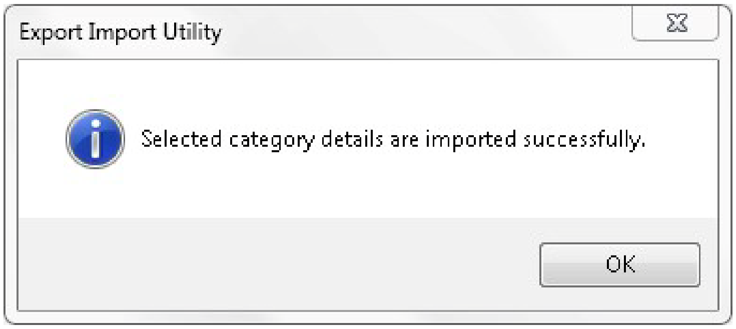
Source : *.iscat

Figure 4

2. Locate **All Cisco SourceFire categories.iscat** file, and then click the **Open** button.

3. To import categories, click the **Import** button.

   EventTracker displays success message.



Export Import Utility

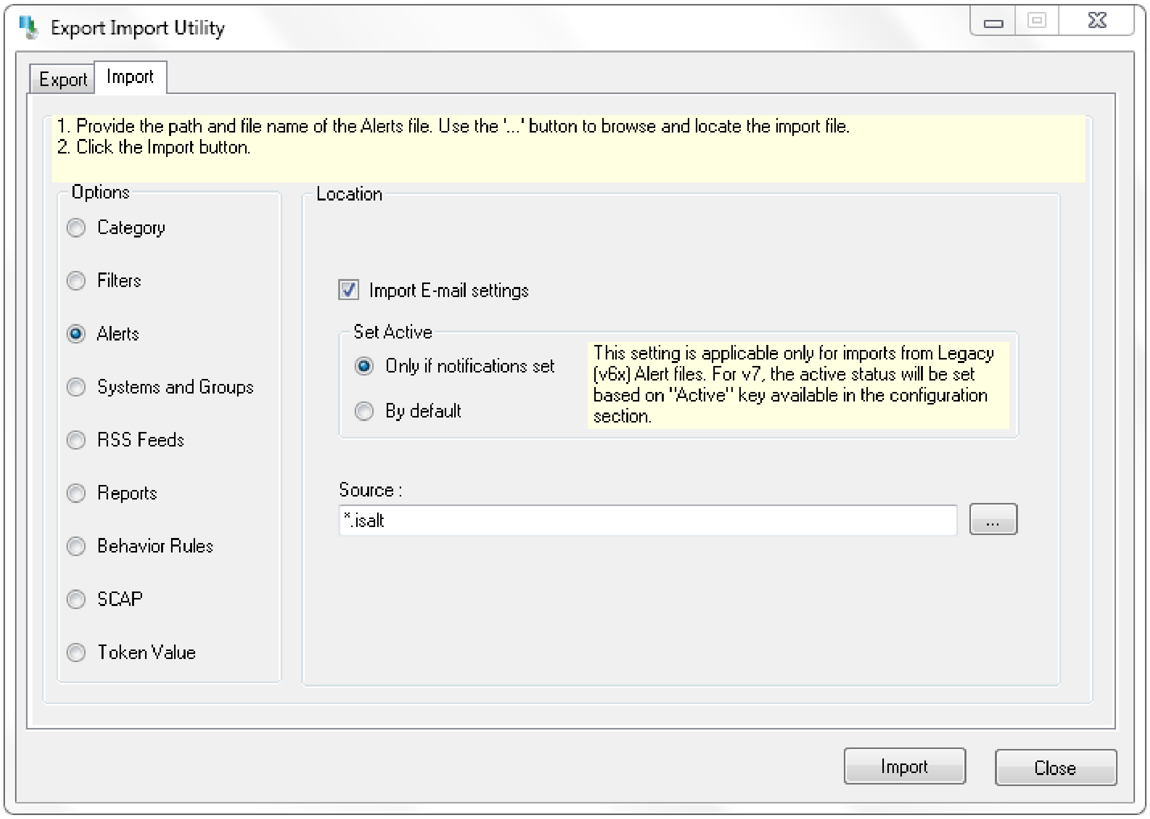
Selected category details are imported successfully.

Figure 5

4. Click **OK**, and then click the **Close** button.

# Alerts

1. Click **Alert** option, and then click the **browse** … button.



1. Provide the path and file name of the Alerts file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

☑ Import E-mail settings

Set Active

● Only if notifications set

○ By default

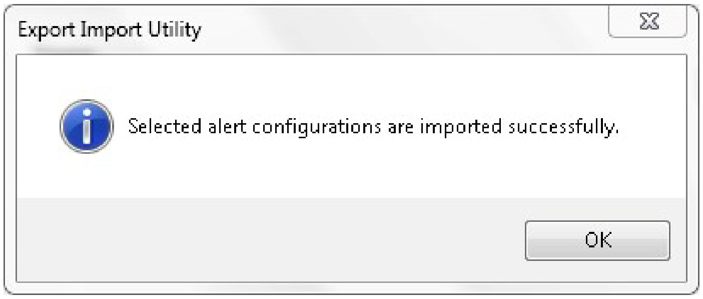
This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.

Source : *.isalt

Figure 6

2. Locate **All Cisco SourceFire alerts.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

EventTracker displays success message.



Selected alert configurations are imported successfully.

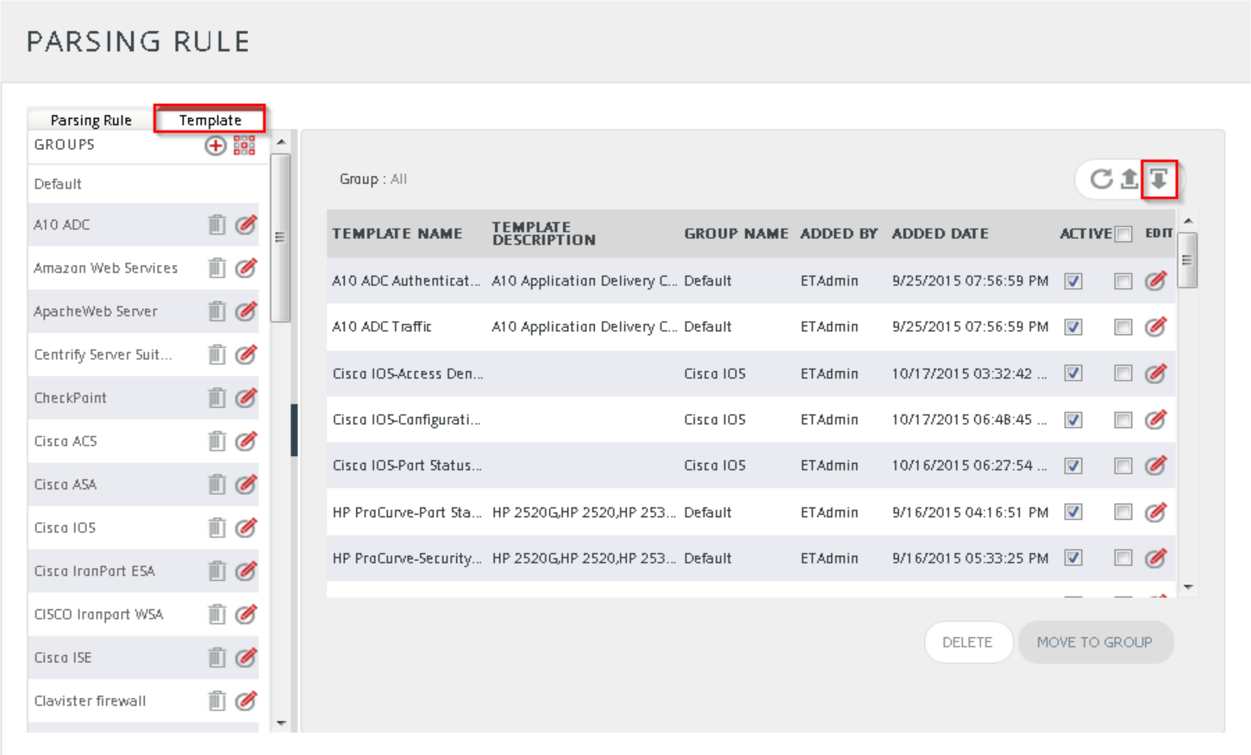
Figure 7

5. Click **OK**, and then click the **Close** button.

# Token Templates

1. Click the **Admin** menu, and then click **Parsing rule**.

2. Select **Template** tab, and then click on ⭳ '**Import**' option.



PARSING RULE

Parsing Rule | Template

GROUPS

Default

A10 ADC

Amazon Web Services

ApacheWeb Server

Centrify Server Suit...

CheckPoint

Cisco ACS

Cisco ASA

Cisco IOS

Cisco IronPort ESA

CISCO Ironport WSA

Cisco ISE

Clavister firewall

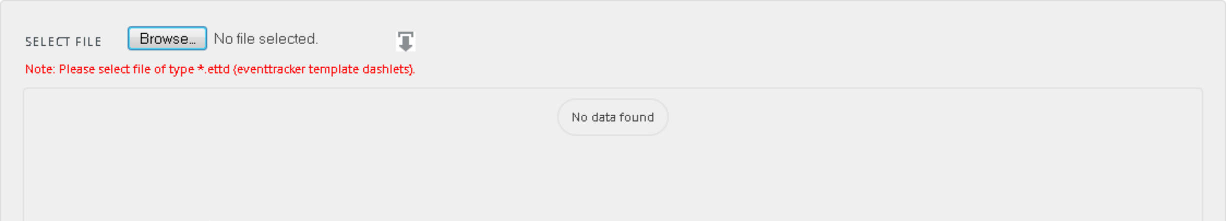
Group : All

| TEMPLATE NAME | TEMPLATE DESCRIPTION | GROUP NAME | ADDED BY | ADDED DATE | ACTIVE | □ | EDIT |
|---|---|---|---|---|---|---|---|
| A10 ADC Authenticat... | A10 Application Delivery C... | Default | ETAdmin | 9/25/2015 07:56:59 PM | ☑ | □ | |
| A10 ADC Traffic | A10 Application Delivery C... | Default | ETAdmin | 9/25/2015 07:56:59 PM | ☑ | □ | |
| Cisco IOS-Access Den... | | Cisco IOS | ETAdmin | 10/17/2015 03:32:42 ... | ☑ | □ | |
| Cisco IOS-Configurati... | | Cisco IOS | ETAdmin | 10/17/2015 06:48:45 ... | ☑ | □ | |
| Cisco IOS-Port Status... | | Cisco IOS | ETAdmin | 10/16/2015 06:27:54 ... | ☑ | □ | |
| HP ProCurve-Port Sta... | HP 2520G,HP 2520,HP 253... | Default | ETAdmin | 9/16/2015 04:16:51 PM | ☑ | □ | |
| HP ProCurve-Security... | HP 2520G,HP 2520,HP 253... | Default | ETAdmin | 9/16/2015 05:33:25 PM | ☑ | □ | |

DELETE | MOVE TO GROUP

Figure 8

3. Click on **Browse** button.



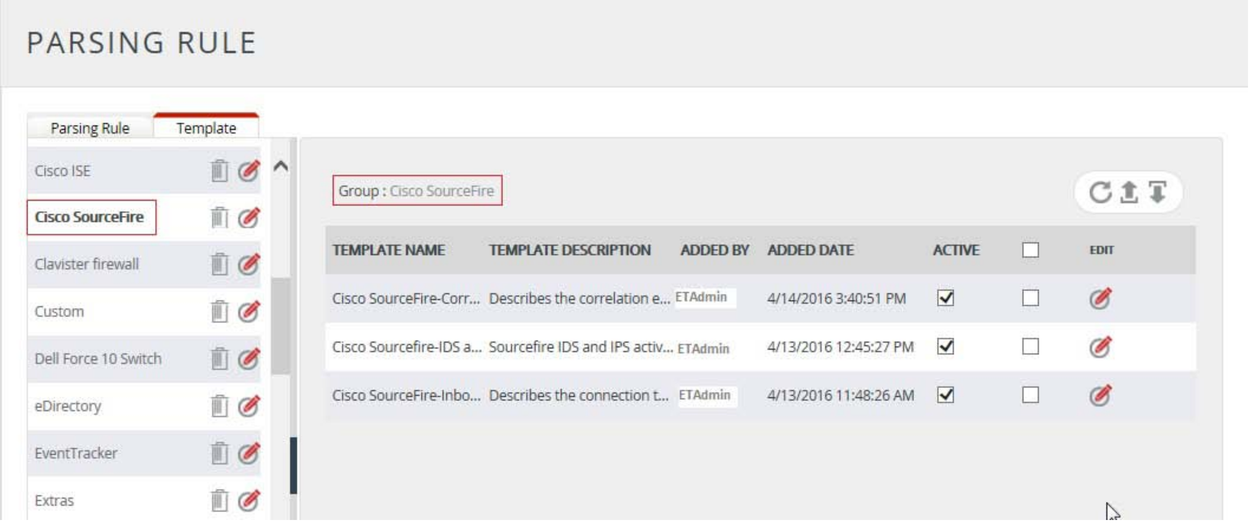
SELECT FILE Browse... No file selected.

Note: Please select file of type *.ettd (eventtracker template dashlets).

No data found

Figure 9

4. Locate **All Cisco SourceFire token templates.ettd** file, and then click the **Open** button



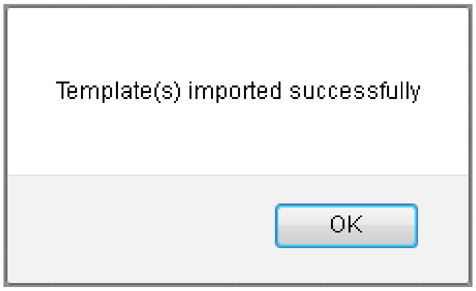
PARSING RULE

Group : Cisco SourceFire

| TEMPLATE NAME | TEMPLATE DESCRIPTION | ADDED BY | ADDED DATE | ACTIVE | □ | EDIT |
|---|---|---|---|---|---|---|
| Cisco SourceFire-Corr... | Describes the correlation e... | ETAdmin | 4/14/2016 3:40:51 PM | ☑ | □ | ✎ |
| Cisco Sourcefire-IDS a... | Sourcefire IDS and IPS activ... | ETAdmin | 4/13/2016 12:45:27 PM | ☑ | □ | ✎ |
| Cisco SourceFire-Inbo... | Describes the connection t... | ETAdmin | 4/13/2016 11:48:26 AM | ☑ | □ | ✎ |

Figure 10

5. Now select the check box and then click on ⤓ '**Import**' option.
   EventTracker displays success message.



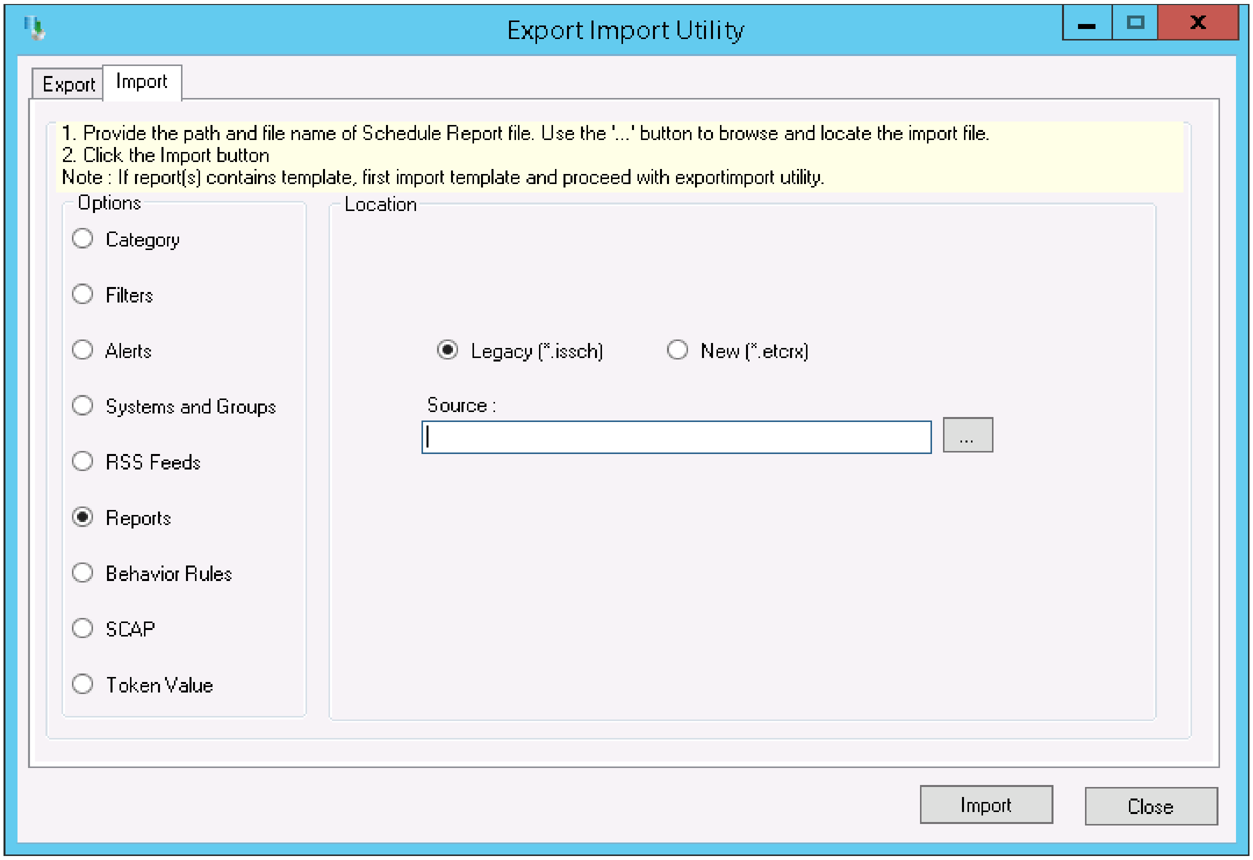
Template(s) imported successfully

Figure 11

6. Click on **OK** button.

# Flex Reports

1. Click **Report** option, and then click the browse [ … ] button



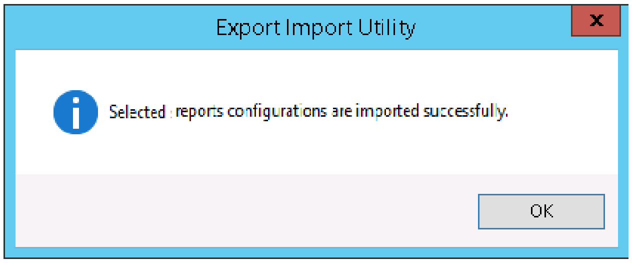
1. Provide the path and file name of Schedule Report file. Use the '...' button to browse and locate the import file.
2. Click the Import button
Note : If report(s) contains template, first import template and proceed with exportimport utility.

Options:
○ Category
○ Filters
○ Alerts
○ Systems and Groups
○ RSS Feeds
● Reports
○ Behavior Rules
○ SCAP
○ Token Value

Location:
● Legacy (*.issch) ○ New (*.etcrx)

Figure 12

2. Locate the **All Cisco SourceFire flex reports.issch** file, and then click the **Open** button.
3. Click the **Import** button to import the scheduled reports, EventTracker displays success message.



Selected reports configurations are imported successfully.

Figure 13

# Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**.
2. Click on ⬇ '**Import**' option.

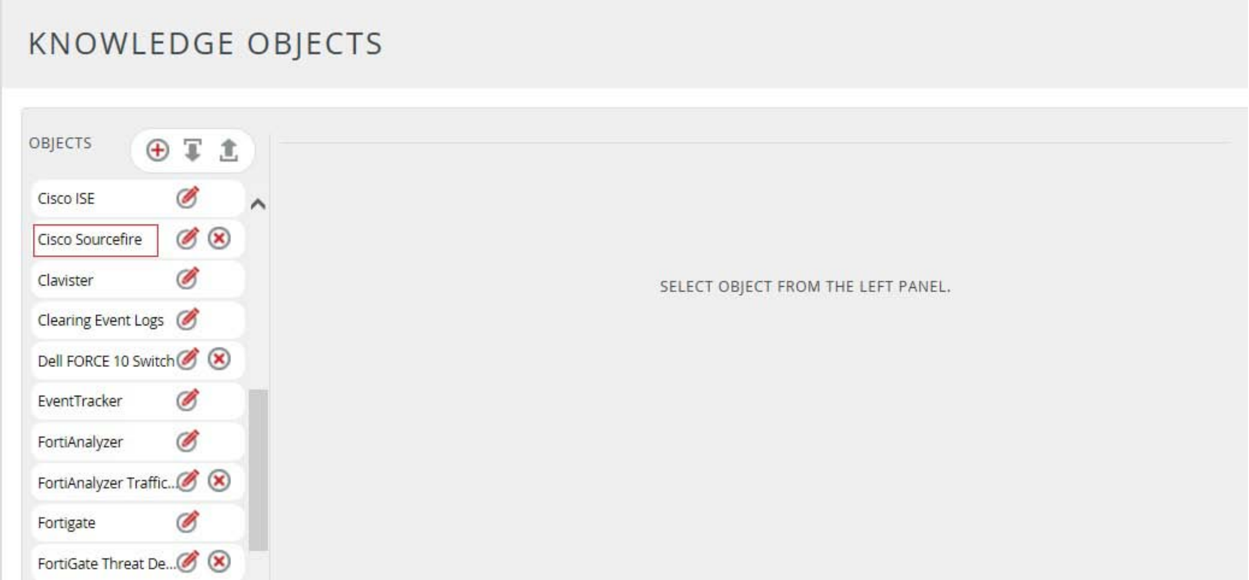


Figure 14

3. In **IMPORT** pane click on **Browse** button.

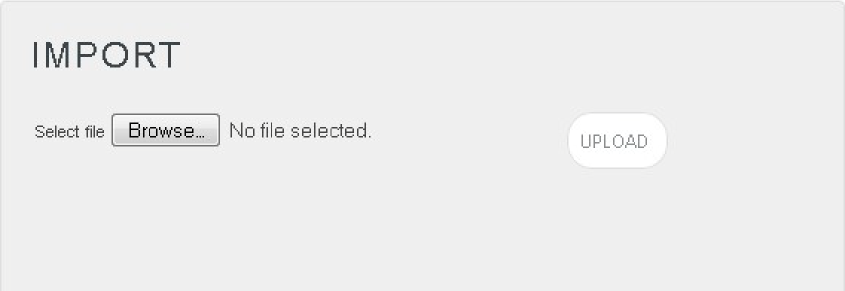
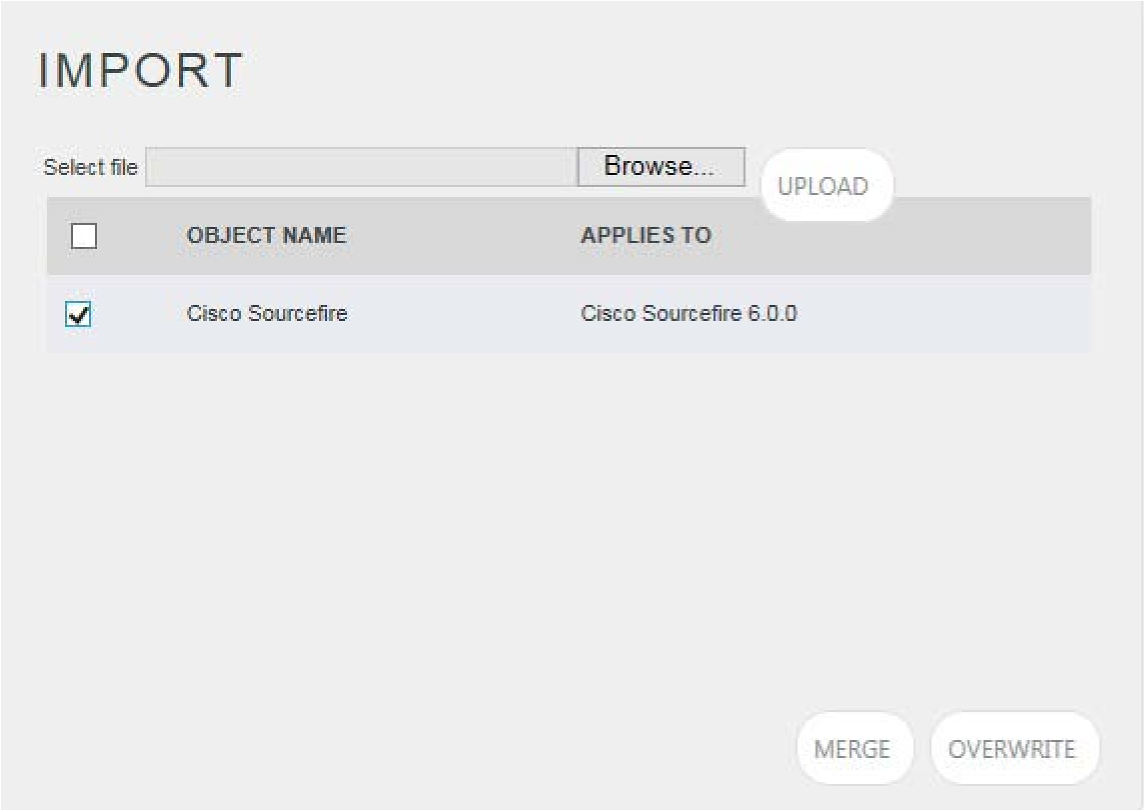


Figure 15

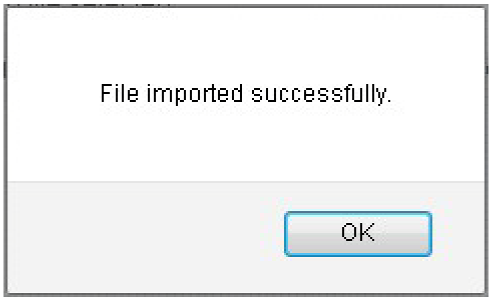
4. Locate **All Cisco SourceFire knowledge object.etko** file, and then click the **UPLOAD** button.



| □ | OBJECT NAME | APPLIES TO |
|---|---|---|
| ☑ | Cisco Sourcefire | Cisco Sourcefire 6.0.0 |

Figure 16

5. Now select the check box and then click on '**OVERWRITE**' option.
   EventTracker displays success message.



File imported successfully.

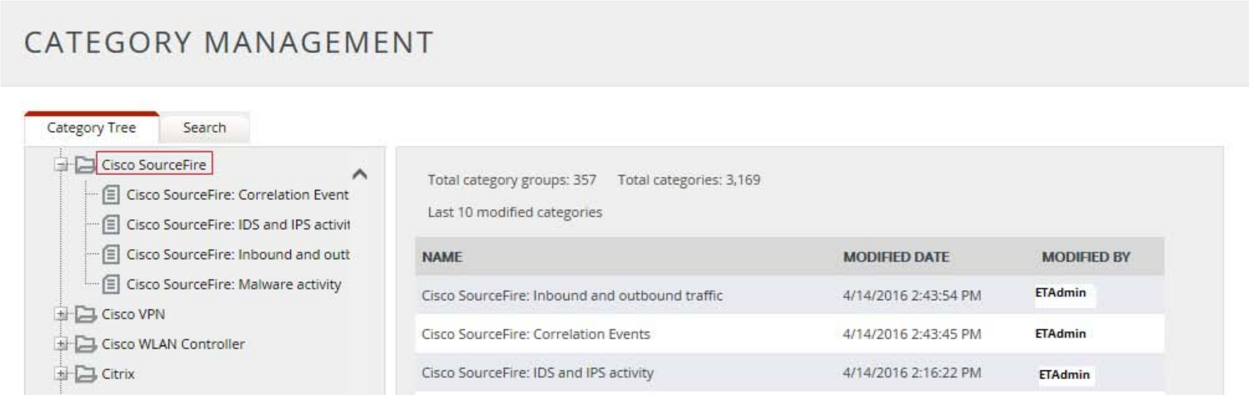
Figure 17

6. Click on **OK** button.

# Verifying Cisco Sourcefire knowledge pack in EventTracker

## Cisco Sourcefire Categories

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand **Cisco SourceFire** group folder to view the imported categories.


CATEGORY MANAGEMENT
Category Tree
Search
Cisco SourceFire
Cisco SourceFire: Correlation Event
Cisco SourceFire: IDS and IPS activit
Cisco SourceFire: Inbound and outt
Cisco SourceFire: Malware activity
Cisco VPN
Cisco WLAN Controller
Citrix

Total category groups: 357 Total categories: 3,169

Last 10 modified categories

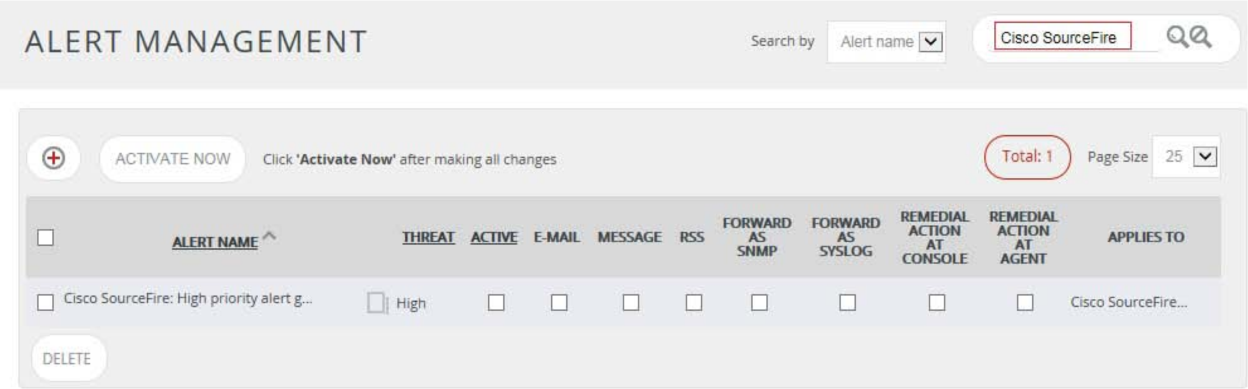
| NAME | MODIFIED DATE | MODIFIED BY |
|---|---|---|
| Cisco SourceFire: Inbound and outbound traffic | 4/14/2016 2:43:54 PM | ETAdmin |
| Cisco SourceFire: Correlation Events | 4/14/2016 2:43:45 PM | ETAdmin |
| Cisco SourceFire: IDS and IPS activity | 4/14/2016 2:16:22 PM | ETAdmin |

Figure 18

## Cisco Sourcefire Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Alerts**.
3. In **Search** field, type '**Cisco SourceFire'**, and then click the **Go** button.

   Alert Management page will display all the imported Cisco Sourcefire alerts.



ALERT MANAGEMENT

Search by Alert name Cisco SourceFire

Click **'Activate Now'** after making all changes

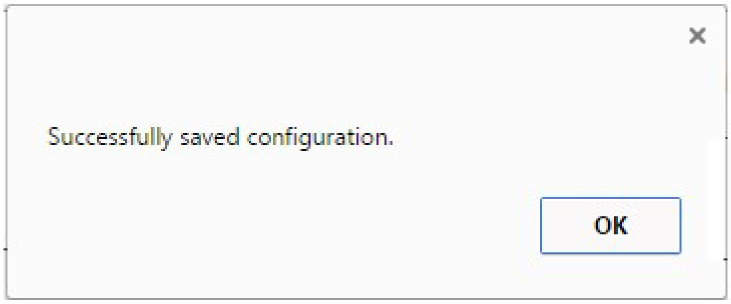
Total: 1 Page Size 25

| □ | ALERT NAME | THREAT | ACTIVE | E-MAIL | MESSAGE | RSS | FORWARD AS SNMP | FORWARD AS SYSLOG | REMEDIAL ACTION AT CONSOLE | REMEDIAL ACTION AT AGENT | APPLIES TO |
|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | Cisco SourceFire: High priority alert g... | High | □ | □ | □ | □ | □ | □ | □ | □ | Cisco SourceFire... |

Figure 19

4. To activate the imported alerts, select the respective checkbox in the **Active** column.

   EventTracker displays message box.



Successfully saved configuration.

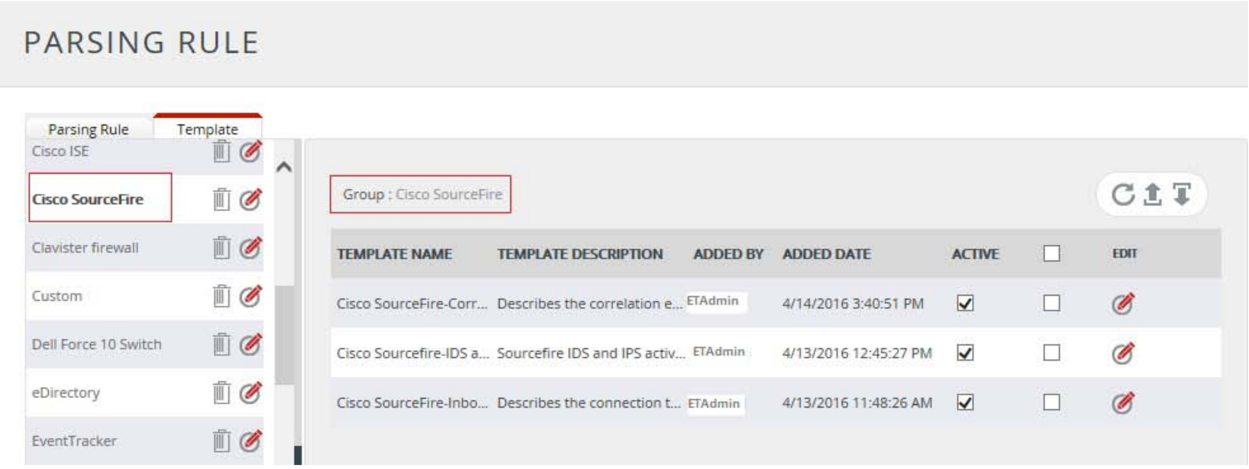
Figure 20

5. Click **OK**, and then click the **Activate Now** button.

   **NOTE:**
   You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.

# Cisco Sourcefire Token Template

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Parsing Rules**.



Group : Cisco SourceFire

| TEMPLATE NAME | TEMPLATE DESCRIPTION | ADDED BY | ADDED DATE | ACTIVE | □ | EDIT |
|---|---|---|---|---|---|---|
| Cisco SourceFire-Corr... | Describes the correlation e... | ETAdmin | 4/14/2016 3:40:51 PM | ☑ | □ | |
| Cisco Sourcefire-IDS a... | Sourcefire IDS and IPS activ... | ETAdmin | 4/13/2016 12:45:27 PM | ☑ | □ | |
| Cisco SourceFire-Inbo... | Describes the connection t... | ETAdmin | 4/13/2016 11:48:26 AM | ☑ | □ | |

Figure 21

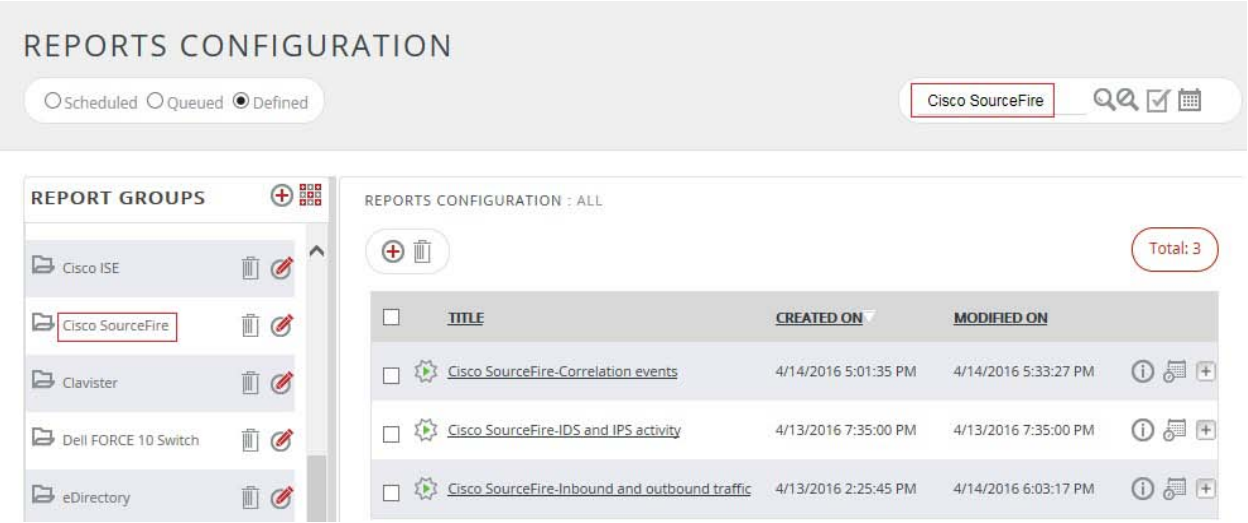
# Cisco Sourcefire Flex Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports** menu, and then select **Configuration**.
3. In **Reports Configuration** pane, select **Defined** option.

   EventTracker displays **Defined** page.

4. In search box enter '**Cisco Sourcefire'**, and then click the **Search** button.

   EventTracker displays Flex reports of Cisco SourceFire

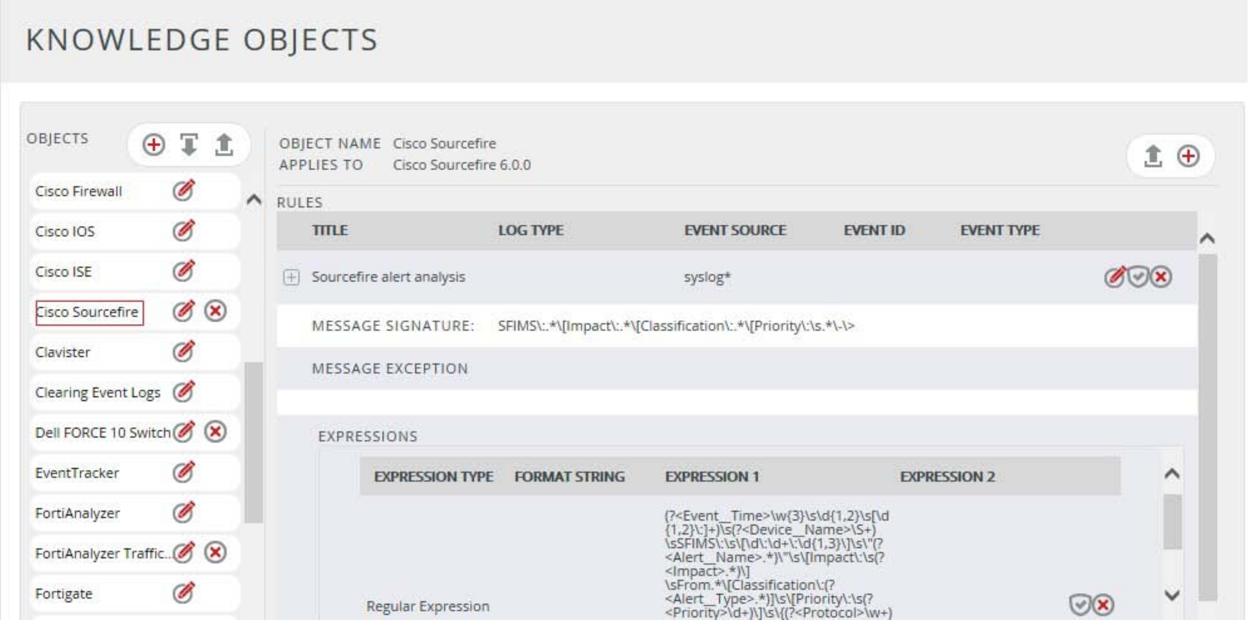


| □ | TITLE | CREATED ON | MODIFIED ON |
|---|---|---|---|
| □ | Cisco SourceFire-Correlation events | 4/14/2016 5:01:35 PM | 4/14/2016 5:33:27 PM |
| □ | Cisco SourceFire-IDS and IPS activity | 4/13/2016 7:35:00 PM | 4/13/2016 7:35:00 PM |
| □ | Cisco SourceFire-Inbound and outbound traffic | 4/13/2016 2:25:45 PM | 4/14/2016 6:03:17 PM |

Figure 22

# Cisco Sourcefire Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**
2. Scroll down and select **Cisco Sourcefire** in **Objects** pane. Imported **Cisco SourceFire** object details are shown.



OBJECT NAME Cisco Sourcefire
APPLIES TO Cisco Sourcefire 6.0.0

RULES

| TITLE | LOG TYPE | EVENT SOURCE | EVENT ID | EVENT TYPE |
|---|---|---|---|---|
| Sourcefire alert analysis | | syslog* | | |

MESSAGE SIGNATURE: SFIMS\:.*\[Impact\:.*\[Classification\:.*\[Priority\:\s.*\-\>

MESSAGE EXCEPTION

EXPRESSIONS

| EXPRESSION TYPE | FORMAT STRING | EXPRESSION 1 | EXPRESSION 2 |
|---|---|---|---|
| Regular Expression | | (?<Event__Time>\w{3}\s\d{1,2}\s[\d{1,2}\:]+)\s(?<Device__Name>\S+)\sSFIMS\:\s\[\d\:\d+\:\d{1,3}\]\s\"(?<Alert__Name>.*)\"\s\[Impact\:\s(?<Impact>.*)\]\sFrom.*\[Classification\:(?<Alert__Type>.*)]\s\[Priority\:\s(?<Priority>\d+)\]\s\{(?<Protocol>\w+) | |

Figure 23

# Create Flex Dashboards in EventTracker

## Schedule Reports

1. Open **EventTracker** in browser and logon.

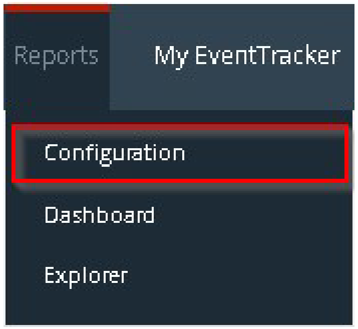
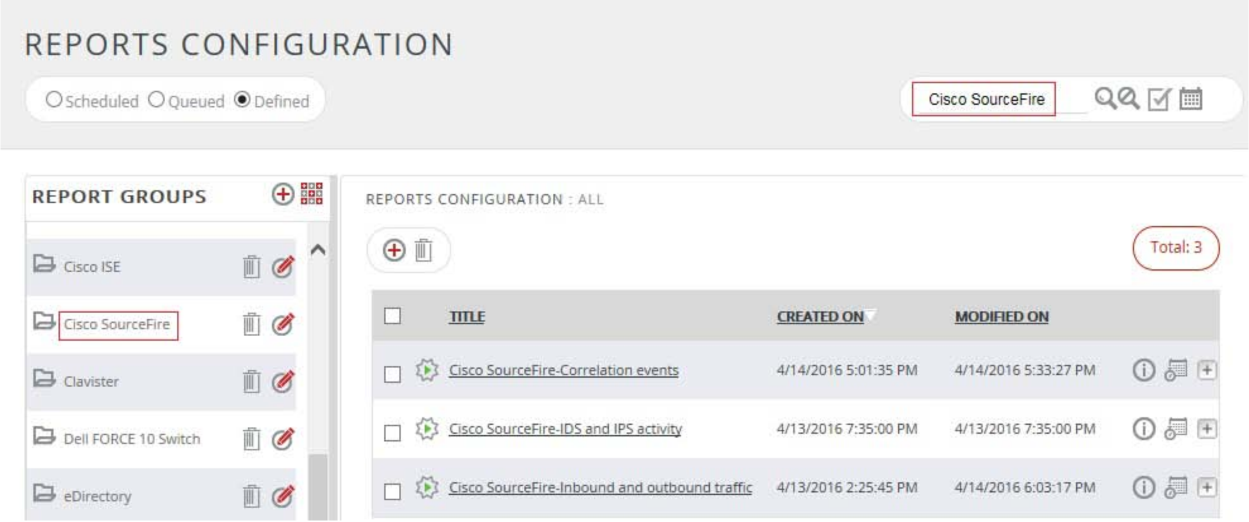


Figure 24

2. Navigate to **Reports>Configuration**.

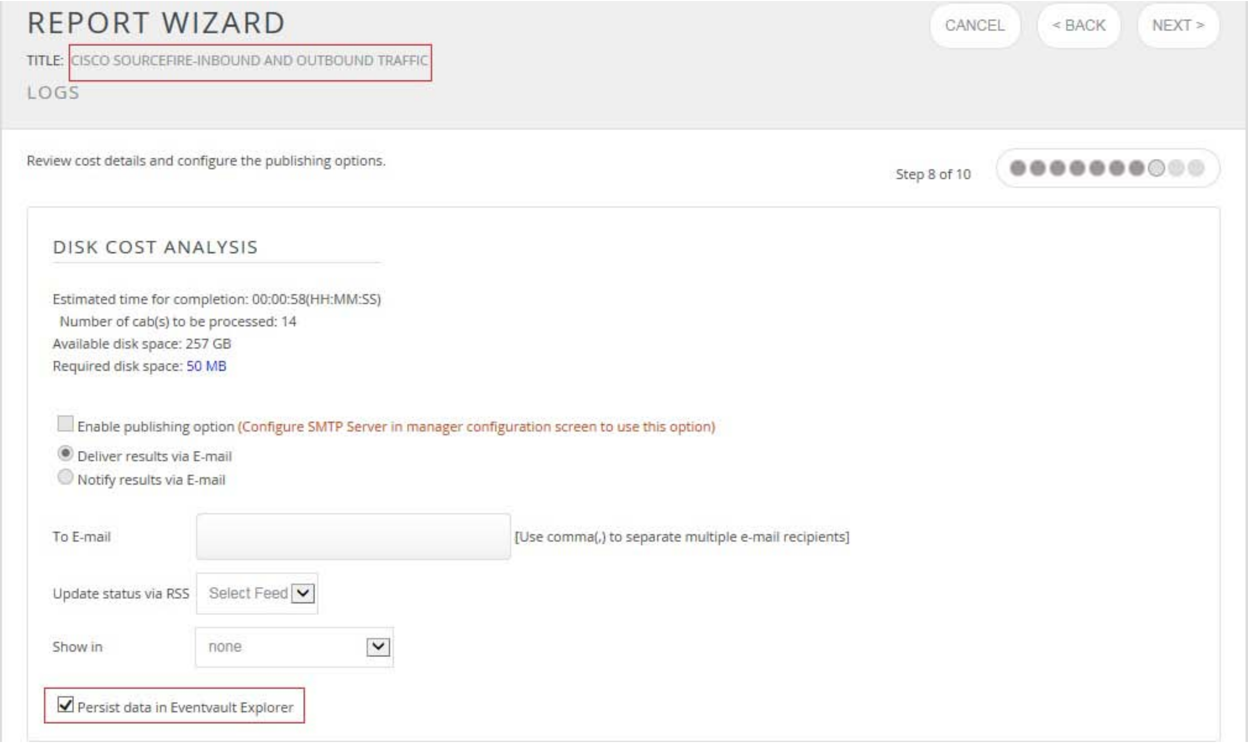


| □ | TITLE | CREATED ON | MODIFIED ON |
|---|---|---|---|
| □ | Cisco SourceFire-Correlation events | 4/14/2016 5:01:35 PM | 4/14/2016 5:33:27 PM |
| □ | Cisco SourceFire-IDS and IPS activity | 4/13/2016 7:35:00 PM | 4/13/2016 7:35:00 PM |
| □ | Cisco SourceFire-Inbound and outbound traffic | 4/13/2016 2:25:45 PM | 4/14/2016 6:03:17 PM |

Figure 25

3. Select **Cisco SourceFire** in report groups. Check **Defined** dialog box.

4. Click on '**schedule**' to plan a report for later execution.



TITLE: CISCO SOURCEFIRE-INBOUND AND OUTBOUND TRAFFIC

LOGS

Review cost details and configure the publishing options.

Step 8 of 10

DISK COST ANALYSIS

Estimated time for completion: 00:00:58(HH:MM:SS)
Number of cab(s) to be processed: 14
Available disk space: 257 GB
Required disk space: 50 MB

□ Enable publishing option (Configure SMTP Server in manager configuration screen to use this option)
● Deliver results via E-mail
○ Notify results via E-mail

To E-mail [Use comma(,) to separate multiple e-mail recipients]

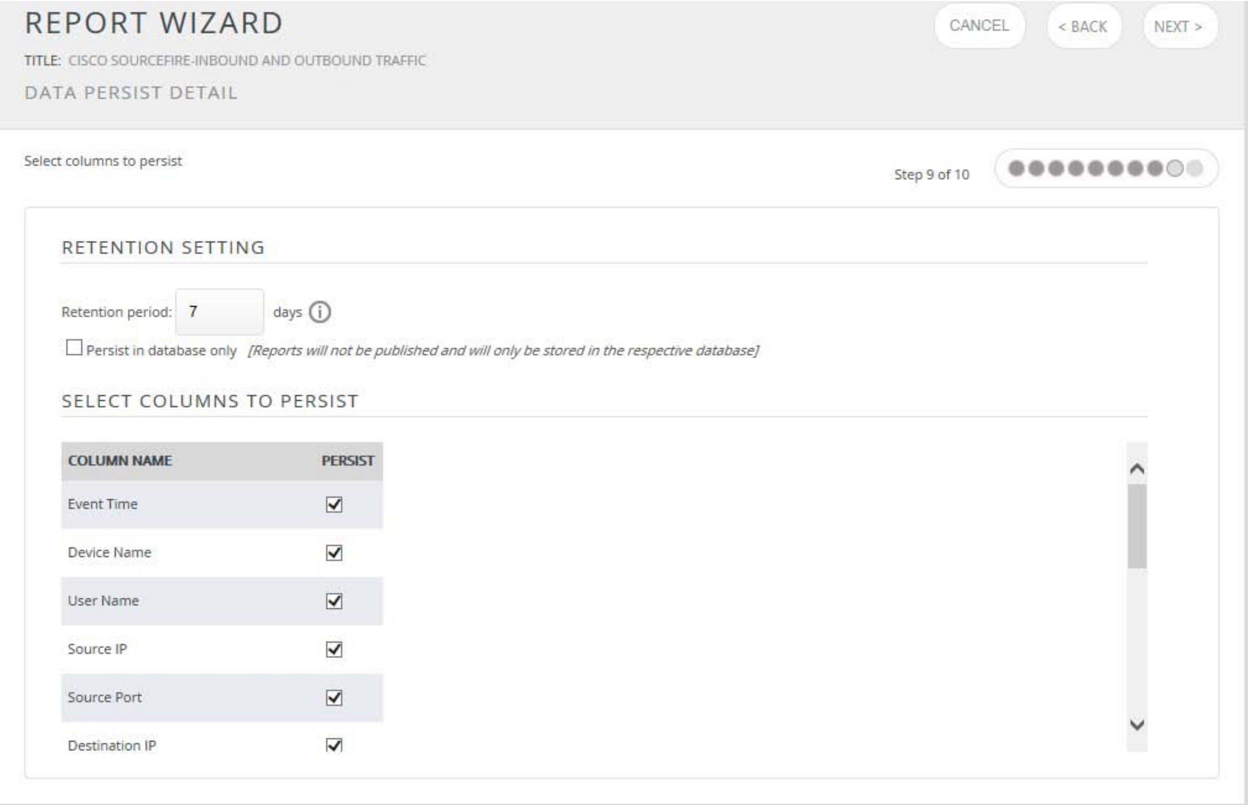
Update status via RSS: Select Feed

Show in: none

☑ Persist data in Eventvault Explorer

Figure 26

5. Choose appropriate time for report execution and in **Step 8** check **Persist data in Eventvault explorer** box.



REPORT WIZARD

TITLE: CISCO SOURCEFIRE-INBOUND AND OUTBOUND TRAFFIC

DATA PERSIST DETAIL

Select columns to persist

Step 9 of 10

RETENTION SETTING

Retention period: 7 days

☐ Persist in database only *[Reports will not be published and will only be stored in the respective database]*

SELECT COLUMNS TO PERSIST

| COLUMN NAME | PERSIST |
|---|---|
| Event Time | ☑ |
| Device Name | ☑ |
| User Name | ☑ |
| Source IP | ☑ |
| Source Port | ☑ |
| Destination IP | ☑ |

Figure 27

6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.
7. Proceed to next step and click **Schedule** button.
8. Wait for scheduled time or generate report manually.

# Create Dashlets

1. **EventTracker 8** is required to configure flex dashboard.
2. Open **EventTracker** in browser and logon.

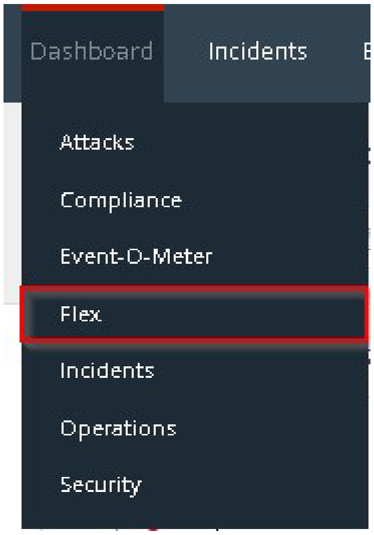
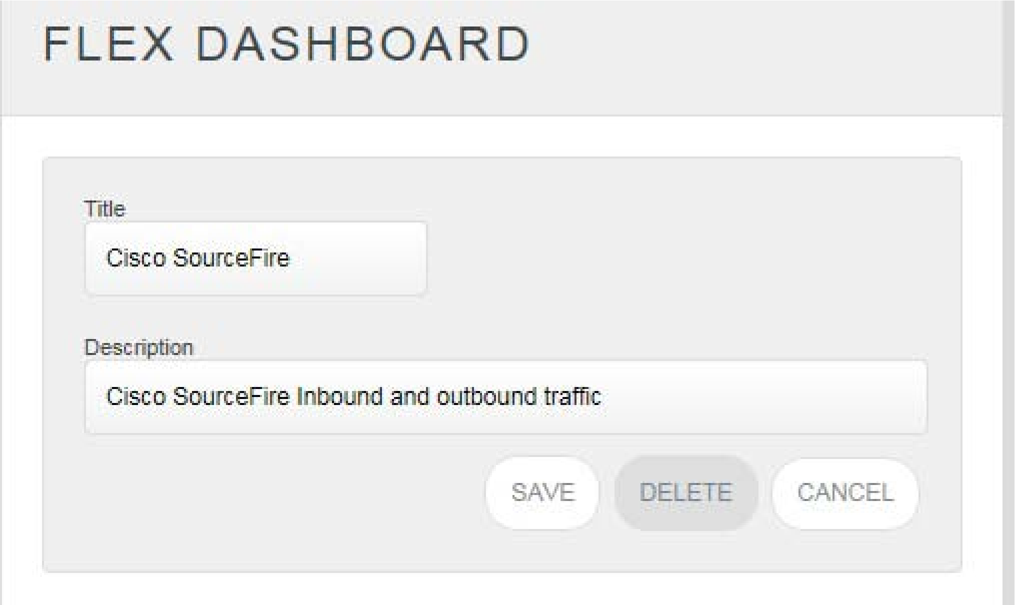


Figure 28

3. Navigate to **Dashboard>Flex**.
   Flex Dashboard pane is shown.



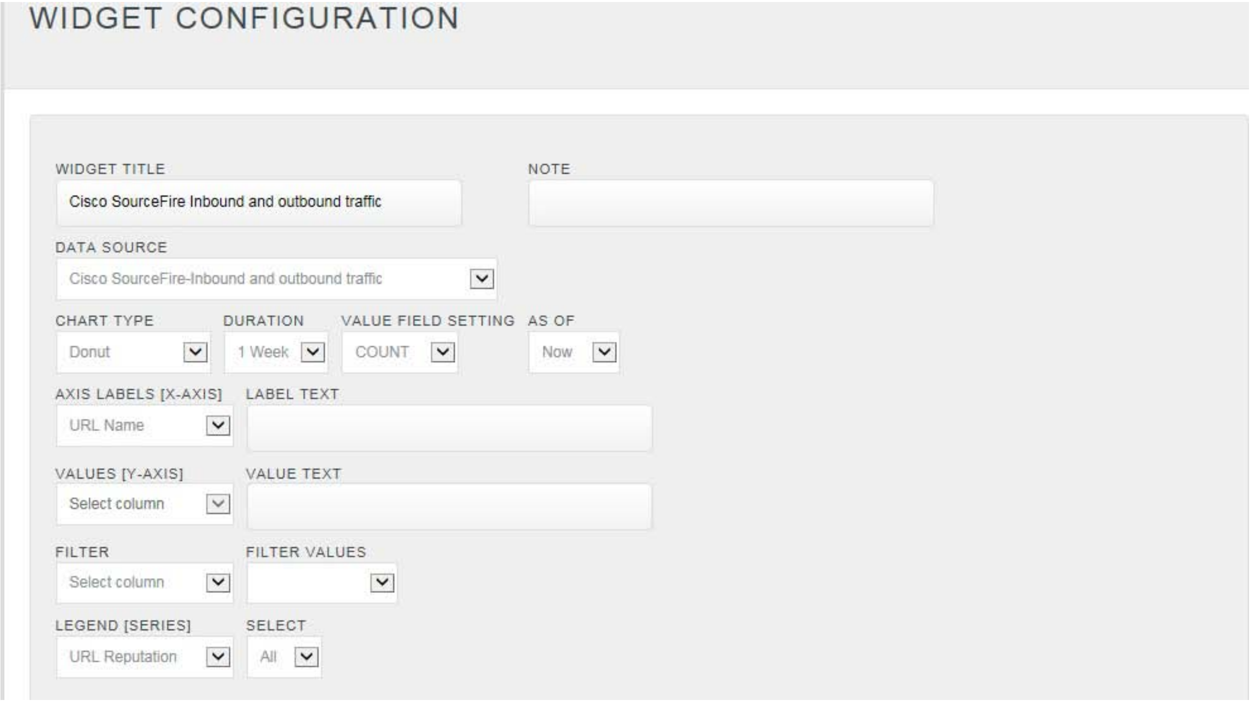
FLEX DASHBOARD

Title: Cisco SourceFire

Description: Cisco SourceFire Inbound and outbound traffic

Figure 29

4. Fill suitable title and description and click **Save** button.
5. Click ⚙ to configure a new flex dashlet. Widget configuration pane is shown.



WIDGET CONFIGURATION

WIDGET TITLE: Cisco SourceFire Inbound and outbound traffic

NOTE:

DATA SOURCE: Cisco SourceFire-Inbound and outbound traffic

CHART TYPE: Donut

DURATION: 1 Week

VALUE FIELD SETTING: COUNT

AS OF: Now

AXIS LABELS [X-AXIS]: URL Name

LABEL TEXT:

VALUES [Y-AXIS]: Select column

VALUE TEXT:

FILTER: Select column

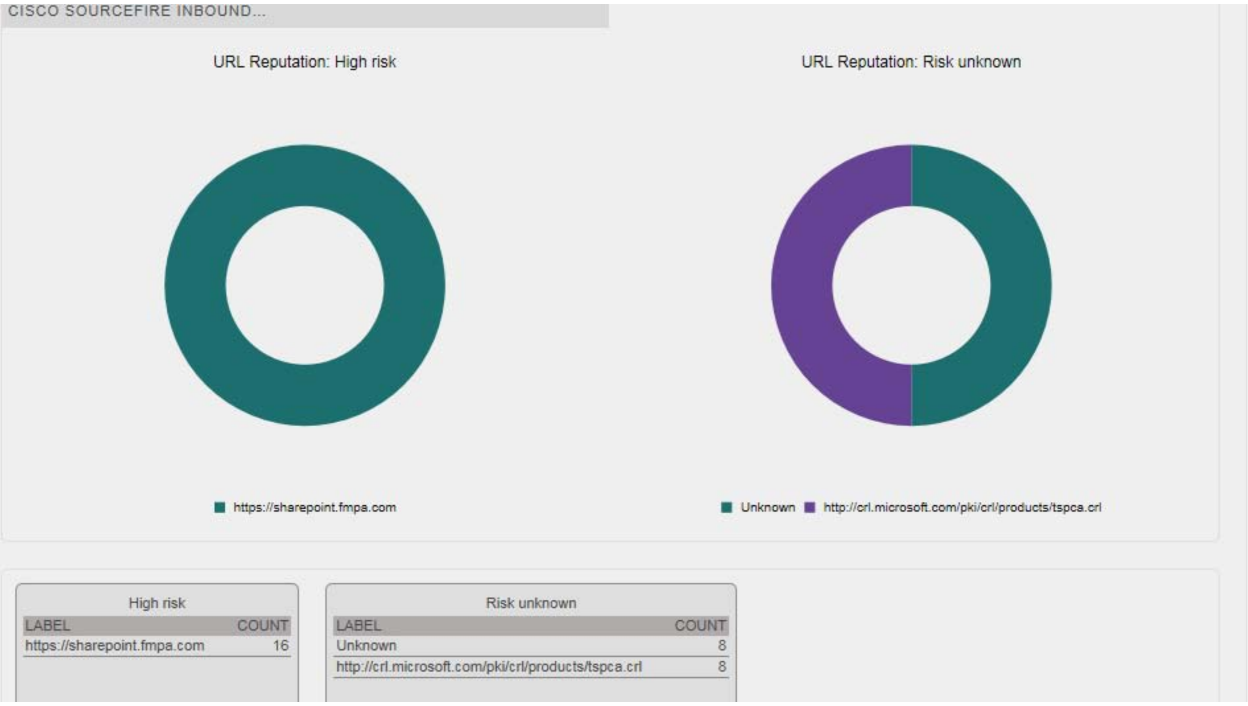
FILTER VALUES:

LEGEND [SERIES]: URL Reputation

SELECT: All

Figure 30

6. Locate earlier scheduled report in **Data Source** dropdown.
7. Select **Chart Type** from dropdown.
8. Select extent of data to be displayed in **Duration** dropdown.
9. Select computation type in **Value Field Setting** dropdown.
10. Select evaluation duration in **As Of** dropdown.
11. Select comparable values in **X Axis** with suitable label.
12. Select numeric values in **Y Axis** with suitable label.
13. Select comparable sequence in **Legend**.
14. Click **Test** button to evaluate. Evaluated chart is shown.


CISCO SOURCEFIRE INBOUND...
URL Reputation: High risk
URL Reputation: Risk unknown
🟩 https://sharepoint.fmpa.com
🟩 Unknown
🟪 http://crl.microsoft.com/pki/crl/products/tspca.crl

High risk

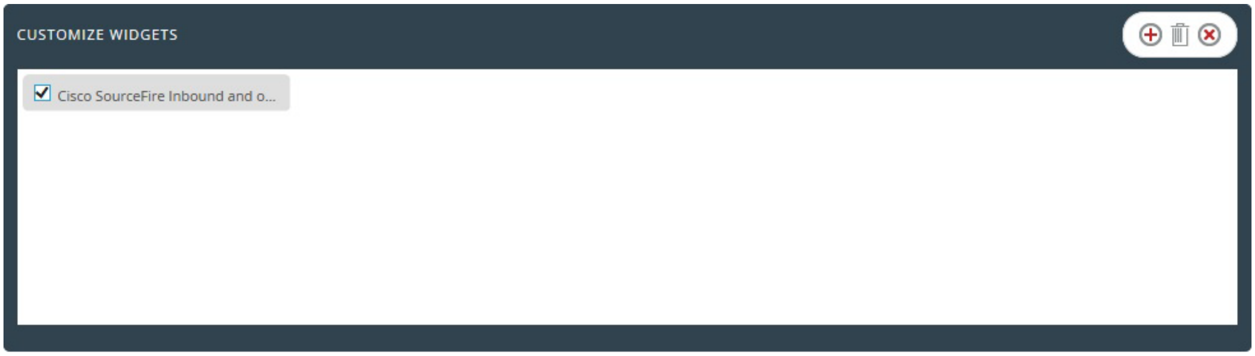
| LABEL | COUNT |
|---|---|
| https://sharepoint.fmpa.com | 16 |

Risk unknown

| LABEL | COUNT |
|---|---|
| Unknown | 8 |
| http://crl.microsoft.com/pki/crl/products/tspca.crl | 8 |

Figure 31

15. If satisfied, click **Configure** button.



☑ Cisco SourceFire Inbound and o...

Figure 32

16. Click 'customize' ⚙ to locate and choose created dashlet.
17. Click ⊕ to add dashlet to earlier created dashboard.

# Sample Flex Dashboards

### 1. Cisco SourceFire: Inbound and outbound traffic

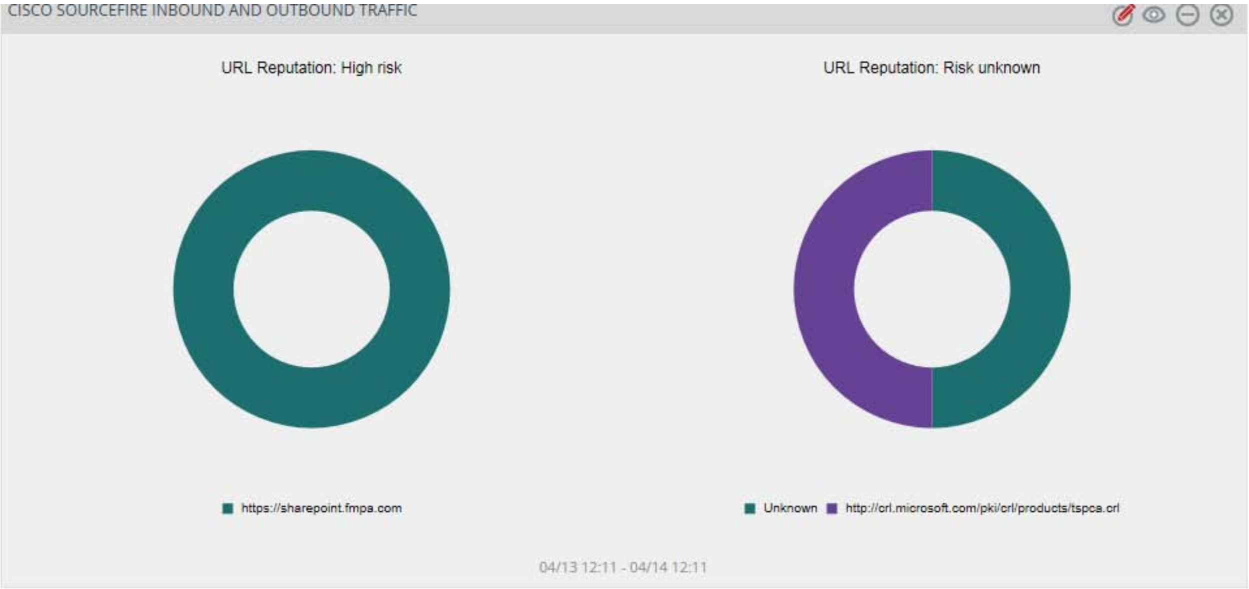

CISCO SOURCEFIRE INBOUND AND OUTBOUND TRAFFIC
URL Reputation: High risk
URL Reputation: Risk unknown
https://sharepoint.fmpa.com
Unknown
http://crl.microsoft.com/pki/crl/products/tspca.crl
04/13 12:11 - 04/14 12:11

Figure 33

### 2. Cisco SourceFire: Correlation events

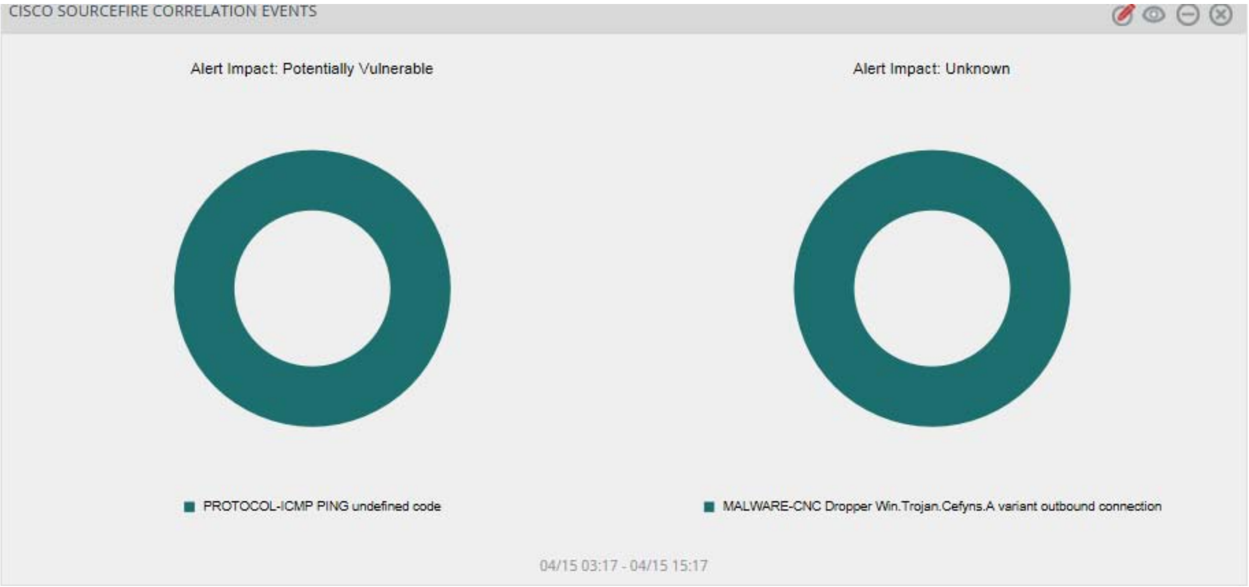

CISCO SOURCEFIRE CORRELATION EVENTS
Alert Impact: Potentially Vulnerable
Alert Impact: Unknown
PROTOCOL-ICMP PING undefined code
MALWARE-CNC Dropper Win.Trojan.Cefyns.A variant outbound connection
04/15 03:17 - 04/15 15:17

Figure 34