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.

© 2016 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
Table of Contents

About this Guide .................................................................................................................................... 1
  Scope................................................................................................................................................ 1
  Audience......................................................................................................................................... 1
Introduction ........................................................................................................................................... 3
Pre-requisites ...................................................................................................................................... 3
Configuring Cisco Sourcefire ............................................................................................................. 3
EventTracker Knowledge Pack ........................................................................................................... 4
  Categories ...................................................................................................................................... 4
  Alerts ............................................................................................................................................. 5
  Flex Reports ................................................................................................................................. 5
Import Knowledge Pack into EventTracker ....................................................................................... 7
  Categories ...................................................................................................................................... 7
  Alerts ............................................................................................................................................. 9
Token Templates................................................................................................................................ 10
  Flex Reports .................................................................................................................................
  Knowledge Object ...........................................................................................................................
Verifying Cisco Sourcefire knowledge pack in EventTracker .......................................................... 15
  Cisco Sourcefire Categories ...........................................................................................................
  Cisco Sourcefire Alerts ...................................................................................................................
  Cisco Sourcefire Token Template.....................................................................................................
  Cisco Sourcefire Flex Reports ........................................................................................................
  Cisco Sourcefire Knowledge Object ................................................................................................
Create Flex Dashboards in EventTracker ........................................................................................... 19
  Schedule Reports ...........................................................................................................................
  Create Dashlets .............................................................................................................................
Sample Flex Dashboards .................................................................................................................... 25
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.
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.

![Edit Policy](image)

**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 Tracker Table](image)

**Example Alerts**


**Cisco SourceFire: Correlation events**

This report provides the information related to alert generated and the impact on system due to correlated events.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Device Name</th>
<th>Source Address</th>
<th>Source Port</th>
<th>Source Port</th>
<th>Protocol Type</th>
<th>Correlation Detail</th>
<th>Alert Name</th>
<th>Alert Type</th>
<th>Alert Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 25 03:04:02</td>
<td>Sourcefire</td>
<td>139.230.245.23</td>
<td>52076</td>
<td>7252:4:91</td>
<td>tcp</td>
<td>Open Log Forwarding/Opensoc Log Forwarding</td>
<td>MALWARE-CNC A Network Trojan was Detected</td>
<td>Unknown</td>
<td></td>
</tr>
<tr>
<td>Jun 26 05:40:29</td>
<td>Sourcefire</td>
<td>192.168.30.1</td>
<td>1.100.0.30</td>
<td></td>
<td>icmp</td>
<td>IP-priority-low-only/Syslog-Policy-01</td>
<td>PROTOCOL-ICMP PING undefined code</td>
<td>Misc Activity</td>
<td>Potentially Vulnerable</td>
</tr>
</tbody>
</table>


**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 | Role Name | Action | URI Name | URI Category | URI Reputation | URL Category | URL Reputation |
|------------------|-------------|-----------|-----------------|----------------|-------------|---------------------|-------------------|---------------------|------------------|----------------|----------|--------|-----------|--------------|---------------|--------------|---------------|---------------|
| May 07 14:34:23  | Cisco-TMPAS-| "red"     | Ingress-Off     | 172.233.3.151  | 60442      | 192.168.168.100     | 443               | HTTPS              |                  |               |          | Allow   | Default   | N/A            | High Risk       |              |               |
| May 06 04:57:19  | gpa-control-| "William" | Ingress         | 10.64.147.105  | 52818      | 173.194.93.212     | 443               | Unknown            |                  |               |          | Allow   | Default   | N/A            | Unknown         |              | Misc Activity  |

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.

![EventTracker Control Panel](image)

*Figure 3*

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

**Categories**

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

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

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

![Image of Export Import Utility](image)

**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.

![Image of success message](image)

**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 the **Import** option.

3. Click on the **Browse** button.

4. Locate **All Cisco SourceFire token templates.ettd** file, and then click the **Open** button.
5. Now select the check box and then click on 'Import' option. EventTracker displays success message.

![Template(s) imported successfully](image)

6. Click on OK button.

**Flex Reports**

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

Knowledge Object

1. Click the Admin menu, and then click Knowledge Objects.
2. Click on 'Import' option.
3. In IMPORT pane click on Browse button.

4. Locate All Cisco SourceFire knowledge object.etko file, and then click the UPLOAD button.
5. Now select the check box and then click on ‘OVERWRITE’ option. EventTracker displays success message.

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.

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

EventTracker displays message box.

![Successfully saved configuration.](image)

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.
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
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.
Create Flex Dashboards in EventTracker

Schedule Reports

1. Open EventTracker in browser and logon.

2. Navigate to Reports>Configuration.


4. Click on 'schedule' to plan a report for later execution.
5. Choose appropriate time for report execution and in Step 8 check Persist data in Eventvault explorer box.
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.
3. Navigate to Dashboard>Flex. Flex Dashboard pane is shown.

4. Fill suitable title and description and click Save button.

5. Click to configure a new flex dashlet. Widget configuration pane is shown.
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.
15. If satisfied, click **Configure** button.

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](image)

Figure 33

2. Cisco SourceFire: Correlation events

![Cisco SourceFire: Correlation events](image)

Figure 34