Integrate FairWarning® Patient Privacy Monitoring
Abstract

The purpose of this document is to help users in monitoring FairWarning®.

Scope

The configurations detailed in this guide are consistent with EventTracker version 7.x and later, and FairWarning® patient privacy monitoring.

Audience

Administrators who are assigned the task to monitor and manage FairWarning® patient privacy monitoring events using EventTracker.

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

This document is for informational purposes only. EventTracker 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 EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.

EventTracker 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 EventTracker, 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.

© 2017 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
# Table of Contents

Abstract .................................................................................................................................................. 1  
Scope .................................................................................................................................................. 1  
Audience ............................................................................................................................................... 1  
Overview .............................................................................................................................................. 3  
Prerequisites ......................................................................................................................................... 3  
Forwarding FairWarning® logs into EventTracker Locally via DLA: ....................................................... 3  
EventTracker Knowledge Pack (KP) ....................................................................................................... 12  
  Categories ........................................................................................................................................... 12  
  Reports ............................................................................................................................................... 12  
  Dashboards ......................................................................................................................................... 13  
Import knowledge pack into EventTracker ............................................................................................. 13  
  To import Category ................................................................................................................................. 13  
  To import Tokens ................................................................................................................................. 14  
  To import Flex Reports .......................................................................................................................... 15  
  To Configure Flex Dashboard ................................................................................................................ 16  
Verify knowledge pack in EventTracker ............................................................................................... 20  
  Verify Categories ............................................................................................................................... 20  
  Verify Tokens ..................................................................................................................................... 21  
  Verify Flex Reports ............................................................................................................................ 22  
Sample Dashboard ................................................................................................................................... 24  
Sample Reports ...................................................................................................................................... 25
Overview

FairWarning® allows healthcare organizations to detect suspicious activity and policy violations, including privileged user access to patient healthcare information.

The EventTracker Enterprise supports FairWarning® Patient privacy monitoring. It monitors logs for triggered alerts which configured in FairWarning®. It generates reports for triggering alerts and you can also generate reports based on categories of alerts. It shows this reports data in more informative ways in dashboard which gives information about the categories of alerts, suspicious user and victim patient for whom alerts are triggered.

Prerequisites

Prior to configuring FairWarning® patient privacy monitoring and EventTracker and later, ensure that you meet the following prerequisites:

- Administrative access on EventTracker.
- User should have log files for FairWarning® patient privacy monitoring
- Firewall between FairWarning® patient privacy monitoring and EventTracker should have exception for EventTracker ports.

Forwarding FairWarning® logs into EventTracker Locally via DLA:

1. Login to EventTracker Enterprise.
2. Click Admin dropdown, and then click Manager.
3. Click Direct Log Archiver /NetFlow Receiver tab.
4. Click Direct log file archiving from external sources option.
5. Click the Add button.
6. In Type dropdown, select the type as Others.
7. Enter Configuration Name.
8. Click the Browse button to select the Log File Folder path.
   (OR)
   Type the Log File Folder path in the text box.
NOTE: Please copy FairWarning® logs into Log File Folder.

9. Click the **Configure** button.
   Log file configuration pane is displayed.
10. Enter Log Source, Computer Name, Computer IP, System Type, System Description.
11. Select Formatted Description option if not selected.
12. Select Custom Log File Format option in Log File Format
13. ADD the following in Message Fields:
   a. Alert Time Stamp
   b. Alert ID
   c. Alert Name
   d. Event Source
   e. Category
   f. Severity
   g. TSTAMP
   h. EVENTID
   i. USER_ID
   j. USER_NAME
   k. USER_FIRST_NAME
Integrate FairWarning Patient Privacy Monitoring

1. USER_MIDDLE_NAME
m. USER_LAST_NAME
n. DEPARTMENT
o. PATIENT_ID
p. PATIENT_NAME
q. PATIENT_FIRST_NAME
r. PATIENT_MIDDLE_NAME
s. PATIENT_LAST_NAME
t. APPLICATION
u. EVENT_TYPE
v. EVENT_DESCRIPTION
w. WORKSTATION_ID
x. WORKSTATION_IP
y. NETWORK_ACCESS_POINT_IP

14. Under **Event Date and Time Fields** select **No. of Fields** as 1 and select **Date Field** as Alert Time Stamp
15. Under **Select Date Time Format Fields** select **Format Value** as Custom and type YYYY-MM-DD hh:mm:ss in Custom field.

![Figure 4](image-url)
16. Click the **Save & Close** button.
   The relevant folder is configured in the DLA folder.

![Manager Configuration](image)

**Figure 5**

17. Click the **Save** button.
   Now Direct Log Archiver (DLA) has been created successfully. Check the logs in search option of EventTracker.

18. Click the **Search** menu, and then select **Advanced Search**.
   Advanced Log Search window displays.
19. Select the required systems.
20. In Custom Criteria pane, select Add custom criteria.
21. In Search in drop down, select Description.
22. In Operator drop down, select contains.
23. In Search for box, enter EventName, and then click the Search button.
Log Search results display.

Figure 7
## Integrate FairWarning Patient Privacy Monitoring

### Figure 8

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Event ID</th>
<th>Site / Computer</th>
<th>User</th>
<th>Domain</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/27/2015 4:24:17 PM</td>
<td>7720</td>
<td>BENDER / ContosoFal</td>
<td>SYSTEM</td>
<td>NT AUTHORITY</td>
<td>Fairwarning</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Event ID</th>
<th>Site / Computer</th>
<th>User</th>
<th>Domain</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/27/2015 4:24:17 PM</td>
<td>3230</td>
<td>BENDER / ContosoFal</td>
<td>SYSTEM</td>
<td>NT AUTHORITY</td>
<td>Fairwarning</td>
</tr>
<tr>
<td>Description:</td>
<td>Alert Time Stamp: 2015-10-27 16:24:17 EDT Alert ID: 1 Alert Name: Syslog: Employee Shopping Event Source: E/S/Log Category: HRM/Best Practice Severity: TTSACCP C0.01.0 EVENTID: 263 USER ID: 22072072 USER NAME: Miranda, Andrea</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
EventTracker Knowledge Pack (KP)

Once logs are received into EventTracker, Categories reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support FairWarning®.

Categories

- **FairWarning: All alerts** - This category based report provides information related to triggering of configurable alerts in FairWarning®.

Reports

- **FairWarning-All alerts** – This report provides information related to triggering of configured alerts in FairWarning® which contains Alert information (Alert time, alert name and its category), user information (Username), victim information (Patient Name and department), system and network information (Workstation ID, Workstation IP and Network access point IP).
- **FairWarning-Identify theft** - This report provides information related to triggering of Medical identity theft category based alerts in FairWarning® which contains Alert information (Alert time and alert name), user information (Username), victim information (Patient Name and department), system and network information (Workstation ID, Workstation IP and Network access point IP).
- **FairWarning-FTC category based alerts** - This report provides information related to triggering of FTC category based alerts in FairWarning® which contains Alert information (Alert time and alert name), user information (Username), victim information (Patient Name and department), system and network information (Workstation ID, Workstation IP and Network access point IP).
- **FairWarning-Policy compliance category based alerts** - This report provides information related to triggering of Policy compliance category based alerts in FairWarning® which contains Alert information (Alert time and alert name), user information (Username), victim information (Patient Name and department), system and network information (Workstation ID, Workstation IP and Network access point IP).
- **FairWarning-HIPAA category based alerts** - This report provides information related to triggering of HIPAA category based alerts in FairWarning® which contains Alert information (Alert time and alert name), user information (Username), victim information (Patient Name and department), system and network information (Workstation ID, Workstation IP and Network access point IP).
Dashboards

- **FairWarning-Category wise Alert Detected**: This dash board gives us the information about the triggered alerts which is configured in FairWarning®.
- **FairWarning-Suspicious User**: This dash board gives us the information about the User for which alerts are triggered.
- **FairWarning-Victim Patient**: This dash board gives us the information about the Patient for which alerts are triggered.
- **FairWarning-Categories Detected**: This dash board gives us the information about the categories of the alerts that are triggered.

**Import knowledge pack into EventTracker**

1. Launch EventTracker Control Panel.
2. Double click Export Import Utility. Click Import tab.
   Import Alerts/Category/Tokens/ Flex Reports as given below.

To import Category

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

![Figure 9](image-url)
2. Locate `.iscat` file, and then click the **Open** button.
3. To import categories, click the **Import** button. EventTracker displays success message.

![Figure 10](image)

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

**To import Tokens**

1. Click **Token value** option, and then click the browse `...` button.

![Figure 11](image)
2. Locate the `.istoken` file, and then click the **Open** button.

3. To import tokens, click the **Import** button.
   
   EventTracker displays success message.

![Figure 12](image12.png)

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

To import Flex Reports

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

![Figure 13](image13.png)
2. Locate the .issch file, and then click the **Open** button.
3. Click the **Import** button to import the scheduled reports.
   EventTracker displays success message.

   ![Image of Export Import Utility dialog box displaying successful import message](image1)

   **Figure 14**

4. Click the **OK** button. Click the **Close** button.

**To Configure Flex Dashboard**

1. Scheduled flex reports (FairWarning®: All Alerts) after importing them.
2. During scheduling, please check persist data and select all the columns to persist.
3. Now, wait for report to run as per schedule time.
4. After generating report, click on **Dashboard > Flex**.
5. Click on **Add Dashboard** button and fill **Title** and **Description** box and save it.
6. Now, create Dashlet for FairWarning® by clicking on **Configure flex dashlet**.

7. Fill **WIDGET TITLE**, select **DATA SOURCE**, select **CHART TYPE** and select **AXIS LABELS [X-AXIS]**.

![Widget Configuration](image)

**Figure 18**

8. After selecting and filling all options, click on the **TEST** button to check the Dashlet. If data are coming properly, then click on **CONFIGURE** button.
9. After creation of Dashlet for FairWarning®, click on **Customize flex dashlet**.

10. Select FairWarning®-Alert Detected usage dashlet and click on **ADD** button.

11. Now, you can see the Dashlet on Dashboard.
Verify knowledge pack in EventTracker

Verify Categories

1. Logon to **EventTracker Enterprise.**
2. Click **Admin** dropdown, and then click **Categories.**
3. In **Category Tree** to view imported categories, scroll down and expand FairWarning® group folder to view the imported categories.
Verify Tokens

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and then click **Parsing rule**.
3. Imported FairWarning® tokens added in Token-Value Groups list at left side of **Parsing rule** tab of EventTracker Enterprise (as shown in below figure).
Verify Flex Reports

1. Logon to EventTracker Enterprise.
2. Click the Reports.
3. Select the Configuration.
4. In the Reports Configuration, select Defined from radio button. EventTracker displays Defined page.
5. In search box enter FairWarning®, EventTracker displays flex reports of FairWarning®.
Here you can find imported defined reports such as FairWarning®-Identity theft.
Sample Dashboard

1) FairWarning-Category wise alert detected

![Figure 25](image1)

2) FairWarning-Suspicious user

![Figure 26](image2)
### Sample Reports

1) **FairWarning-All Alerts**

<table>
<thead>
<tr>
<th>Alert Time Stamp</th>
<th>Alert Name</th>
<th>Category</th>
<th>User Name</th>
<th>User First Name</th>
<th>Patient Name</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-04-10 10:01:04 EDT</td>
<td>Corner Millennium: Self-Examination</td>
<td>Policy Compliance</td>
<td>Ben, Ehmardt</td>
<td>Ben</td>
<td>Jay, Neely</td>
<td>IMA: Powerchart</td>
</tr>
<tr>
<td>2015-04-10 10:03:13 EDT</td>
<td>Corner Millennium: VIP Snooping</td>
<td>HIPAA Best Practice</td>
<td>Jeff, Bowman</td>
<td>Jeff</td>
<td>Percy, Shock</td>
<td>Ascent Capture Index Valuation</td>
</tr>
<tr>
<td>2015-04-10 10:00:32 EDT</td>
<td>Corner Millennium: Employee Snooping</td>
<td>HIPAA Best Practice</td>
<td>Chris, Fox</td>
<td>Chris</td>
<td>Ellis, Brewer</td>
<td>IMA: Powerchart</td>
</tr>
<tr>
<td>2015-04-10 15:11:09 EDT</td>
<td>Edcysys: Self-Examination</td>
<td>Policy Compliance</td>
<td>Miranda, Cooper</td>
<td>Miranda</td>
<td>Percy, Shock</td>
<td>Ascent Capture Index Valuation</td>
</tr>
<tr>
<td>2015-04-10 15:15:07 EDT</td>
<td>Edcysys: VIP Snooping</td>
<td>HIPAA Best Practice</td>
<td>Burton, Cooper</td>
<td>Burton</td>
<td>Lisa, Andrews</td>
<td>Ascent Capture Index Valuation</td>
</tr>
<tr>
<td>2015-04-10 15:35:53 EDT</td>
<td>Edcysys: Function Code (Search) + Filter (Remote user)</td>
<td>FTC Best Practice</td>
<td>Frank, Smith</td>
<td>Frank</td>
<td>Ellis, Brewer</td>
<td>Ascent Capture Index Valuation</td>
</tr>
<tr>
<td>2015-04-10 16:32:11 EDT</td>
<td>Edcysys: Employee Snooping</td>
<td>HIPAA Best Practice</td>
<td>Miranda, Andrews</td>
<td>Miranda</td>
<td>Nity, Smith</td>
<td>Ascent Capture Index Valuation</td>
</tr>
<tr>
<td>2015-04-10 16:40:10 EDT</td>
<td>Corner Millennium: payroll access</td>
<td>Medical Identity Theft</td>
<td>Barbara, Calvin</td>
<td>Barbara</td>
<td>William, Saniov</td>
<td>Ascent Capture Index Valuation</td>
</tr>
<tr>
<td>2015-04-10 16:42:17 EDT</td>
<td>Corner Millennium: Self-Examination</td>
<td>Policy Compliance</td>
<td>Ben, Ehmardt</td>
<td>Ben</td>
<td>Austin, Hargg</td>
<td>FirstNet (PowerChart)</td>
</tr>
<tr>
<td>2015-04-10 16:42:13 EDT</td>
<td>Corner Millennium: VIP Snooping</td>
<td>HIPAA Best Practice</td>
<td>Jeff, Bowman</td>
<td>Jeff</td>
<td>Allen, Bowman</td>
<td>IMA: Powerchart</td>
</tr>
<tr>
<td>2015-04-10 16:45:04 EDT</td>
<td>Corner Millennium: Function Code (Search) + Filter (Remote user)</td>
<td>FTC Best Practice</td>
<td>Walter, Adams</td>
<td>Walter</td>
<td>Jay, Neely</td>
<td>IMA: Powerchart</td>
</tr>
<tr>
<td>2015-04-15 16:58:17 EDT</td>
<td>Monesson Care Manager: Specfic Patient investigation</td>
<td>Policy Compliance</td>
<td>Burton, Cooper</td>
<td>Burton</td>
<td>Ellis, Brewer</td>
<td>IMA: Powerchart</td>
</tr>
<tr>
<td>2015-04-17 01:37 EDT</td>
<td>Monesson Care Manager: VIP Snooping</td>
<td>HIPAA Best Practice</td>
<td>Miranda, Andrews</td>
<td>Miranda</td>
<td>William, Saniov</td>
<td>IMA: Powerchart</td>
</tr>
<tr>
<td>2015-04-17 03:30 EDT</td>
<td>Monesson Care Manager: Function Code (Search) + Filter (Remote user)</td>
<td>FTC Best Practice</td>
<td>Barbara, Calvin</td>
<td>Barbara</td>
<td>Austin, Hargg</td>
<td>IMA: Powerchart</td>
</tr>
<tr>
<td>2015-04-17 05:34:15 EDT</td>
<td>Monesson Care Manager: Continuous Commitment</td>
<td>HIPAA Best Practice</td>
<td>Ben, Ehmardt</td>
<td>Ben</td>
<td>Allen, Bowman</td>
<td>IMA: Powerchart</td>
</tr>
</tbody>
</table>

Figure 27
2) FairWarning-FTC category based alerts

<table>
<thead>
<tr>
<th>Alert Time Stamp</th>
<th>Alert Name</th>
<th>User Name</th>
<th>Patient Name</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013-04-10 18:01:34.0 EDT</td>
<td>Centric Millennium: Function Code (Search) + Filter (Remote user)</td>
<td>Walter, Adams</td>
<td>Lisa, Andrews</td>
<td>HINA: Powerchart</td>
</tr>
<tr>
<td>2013-04-10 18:03:19.02 EDT</td>
<td>Eclipse: Function Code (Search) + Filter (Remote user)</td>
<td>Frank, Smith</td>
<td>Ellen, Brewer</td>
<td>Ascent Capture Index Validation</td>
</tr>
<tr>
<td>2013-04-10 18:08:59.12 EDT</td>
<td>Melrose Care Manager: Function Code (Search) + Filter (Remote user)</td>
<td>Barbara, Calvin</td>
<td>Austin, Kemp</td>
<td>HINA: Powerchart</td>
</tr>
<tr>
<td>2013-04-10 18:15:07.999 EDT</td>
<td>Centric Millennium: Function Code (Search) + Filter (Remote user)</td>
<td>Barbara, Calvin</td>
<td>Allen, Bowman</td>
<td>Ascent Capture Index Validation</td>
</tr>
<tr>
<td>2013-04-10 18:30:59.03 EDT</td>
<td>Melrose Care Manager: Function Code (Search) + Filter (Remote user)</td>
<td>Burton, Cooper</td>
<td>William, Sanlivo</td>
<td>Ascent Capture Index Validation</td>
</tr>
<tr>
<td>2013-04-10 18:40:19.15 EDT</td>
<td>Centric Millennium: Function Code (Search) + Filter (Remote user)</td>
<td>Burton, Cooper</td>
<td>Austin, Kemp</td>
<td>Ascent Capture Index Validation</td>
</tr>
<tr>
<td>2013-04-10 18:45:54.387 EDT</td>
<td>Centric Millennium: Function Code (Search) + Filter (Remote user)</td>
<td>Walter, Adams</td>
<td>William, Sanlivo</td>
<td>Ascent Capture Index Validation</td>
</tr>
<tr>
<td>2013-04-10 18:58:58.379 EDT</td>
<td>Melrose Care Manager: Function Code (Search) + Filter (Remote user)</td>
<td>Barbara, Calvin</td>
<td>Ellen, Brewer</td>
<td>Ascent Capture Index Validation</td>
</tr>
</tbody>
</table>