

Integrate FairWarning® Patient Privacy Monitoring

Abstract

The purpose of this document is to help user 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.

MANAGER CONFIGURATION

CONFIGURATION syslog / VIRTUAL COLLECTION POINT **DIRECT LOG ARCHIVER / NETFLOW RECEIVER** AGENT SETTINGS

E-MAIL CONFIGURATION STATUSTRACKER

Direct log file archiving from external sources Purge files after days ASSOCIATED VIRTUAL COLLECTION POINT: 14505

LOG FILE FOLDER	CONFIGURATION NAME	LOG FILE EXTENSION	FIELD SEPARATOR	LOG TYPE

ADD EDIT REMOVE

Figure 1

EventTracker displays Direct Archiver Configuration window.

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.

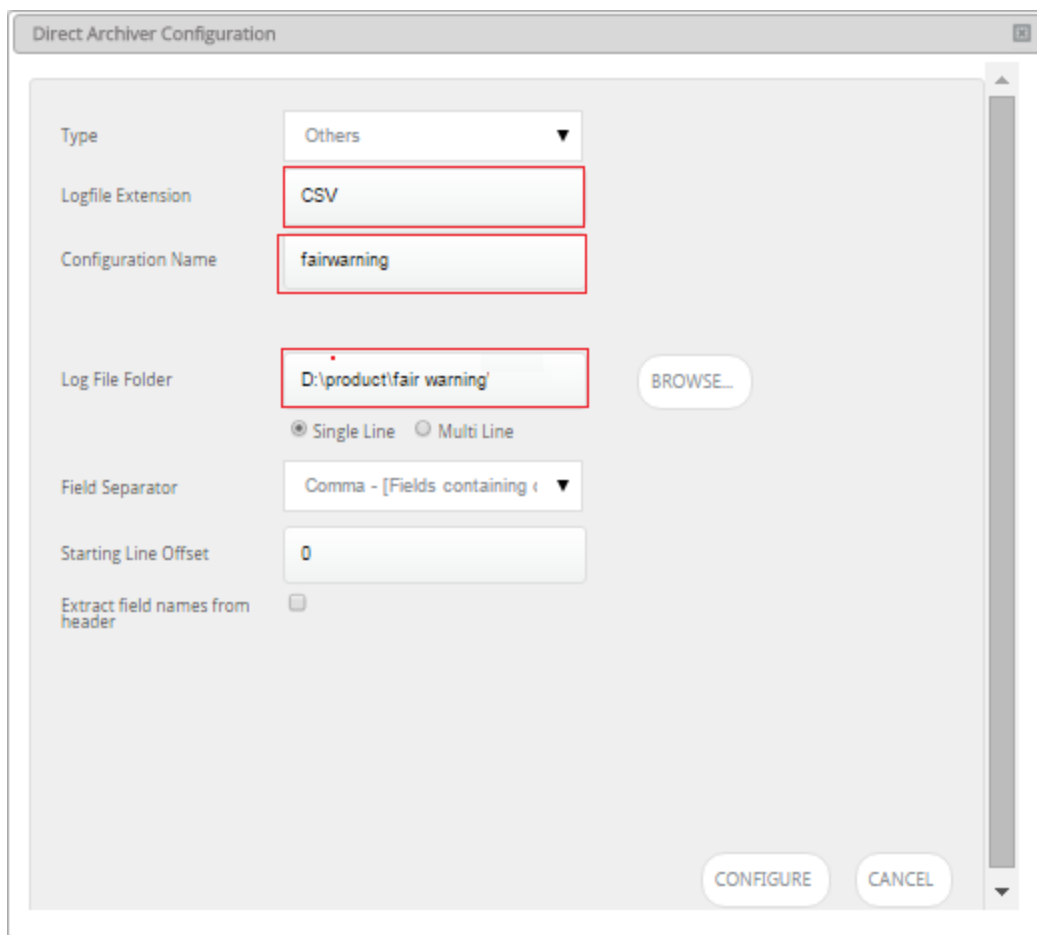


Figure 2

NOTE: Please copy FairWarning® logs into **Log File Folder**.

9. Click the **Configure** button.
Log file configuration pane is displayed.

Direct Archiver Configuration

Log file configuration

Configuration Name: D:\Current\product\fair warning\logs\fairwarn

Log Source: Fairwarning

Computer Name: Contoso-FairWarning

Computer IP: 192.168.1.254 [GET IP]

System Type: Unknown

System Description:

Comment Line Token:

Entire Row as Description Formatted Description

Log File Format: Custom Log File Format

Message Fields: [ADD]

Alert Time Stamp
Alert ID
Alert Name
Event Source
Category

[REMOVE]

Select Event Date and Time Fields Select Date Time Format Fields Select Column Mapping

Figure 3

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

- l. 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.

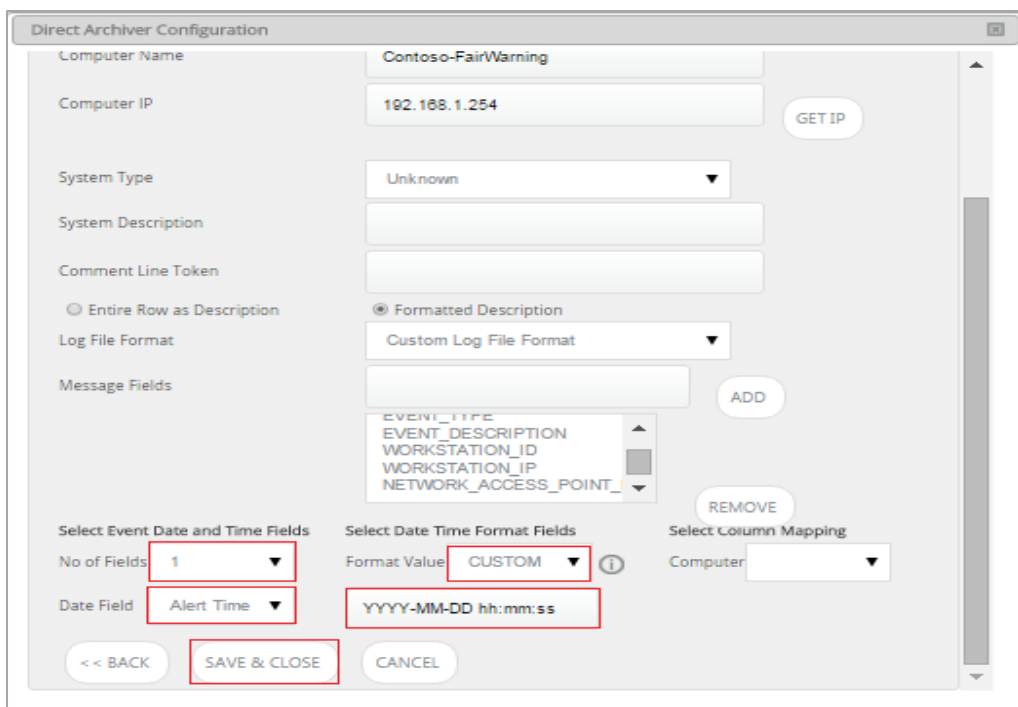


Figure 4

16. Click the **Save & Close** button.
The relevant folder is configured in the DLA folder.

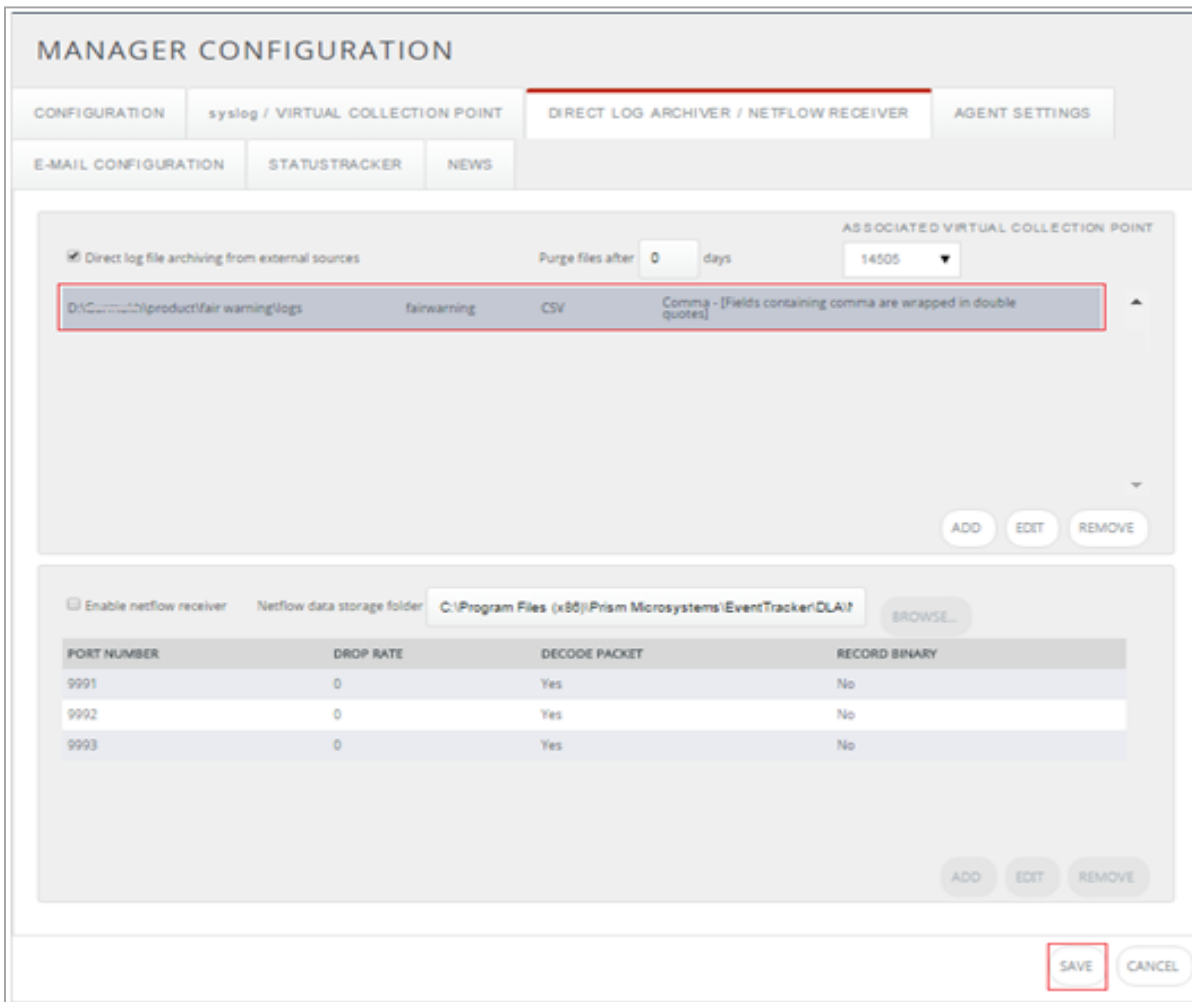


Figure 5

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.

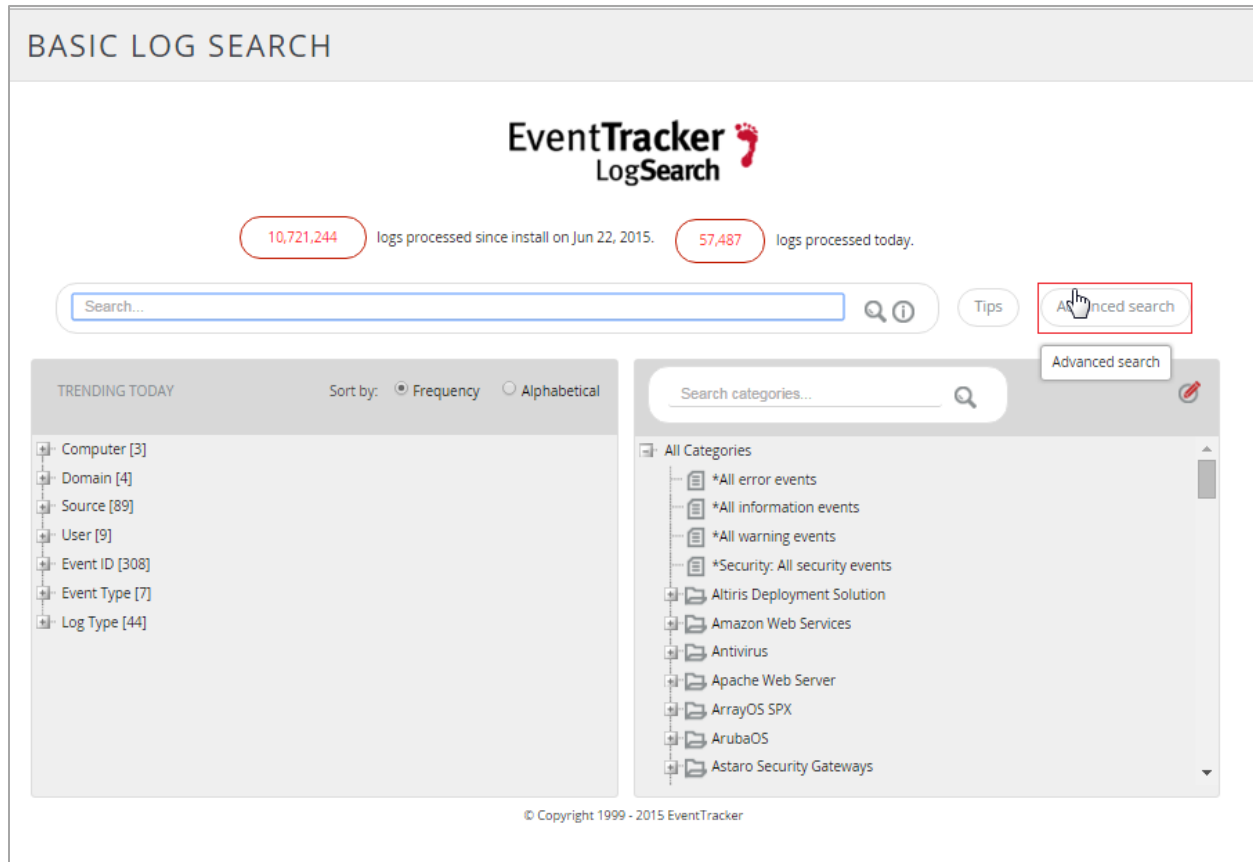


Figure 6

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.

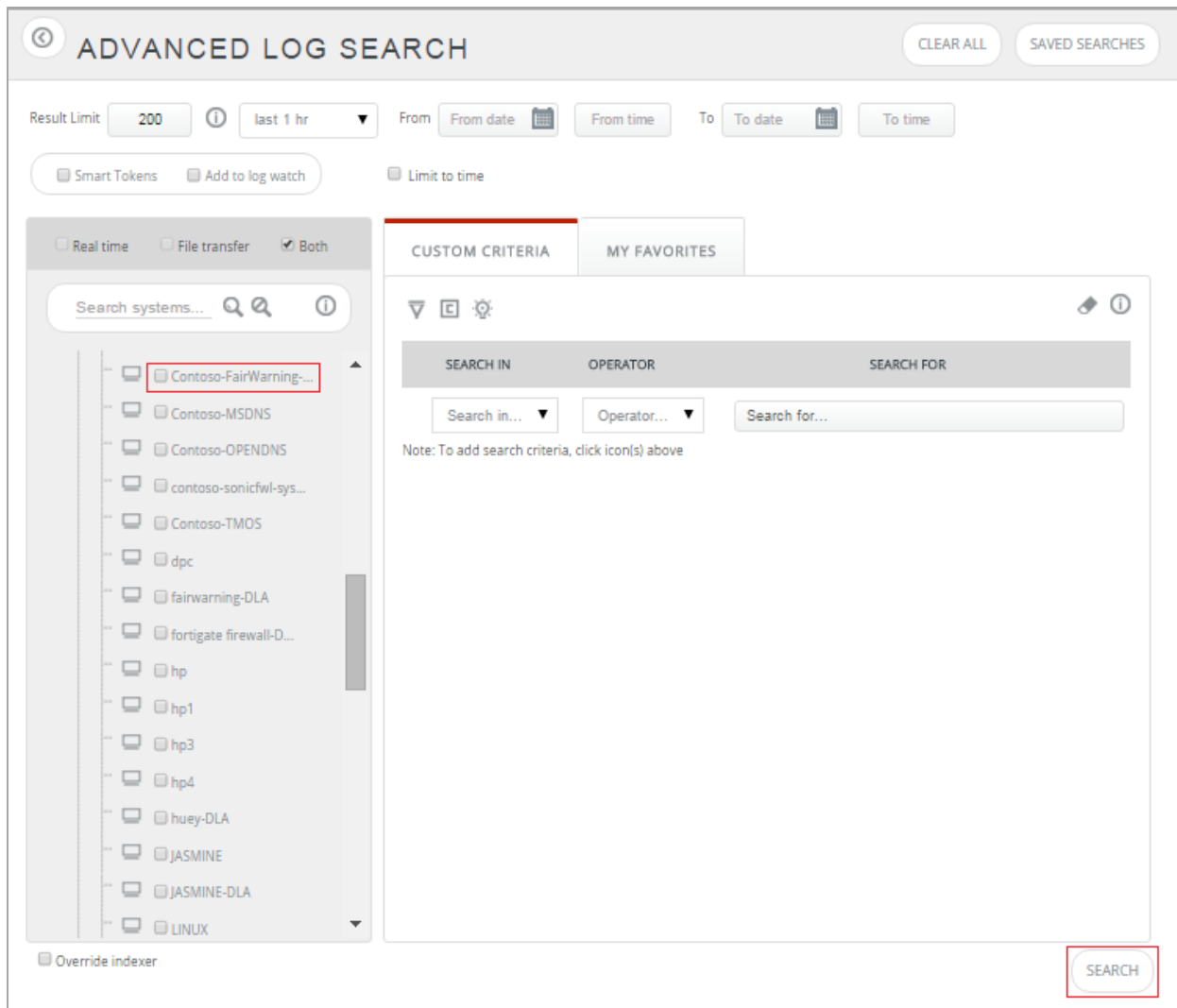


Figure 7

Log Search results display.

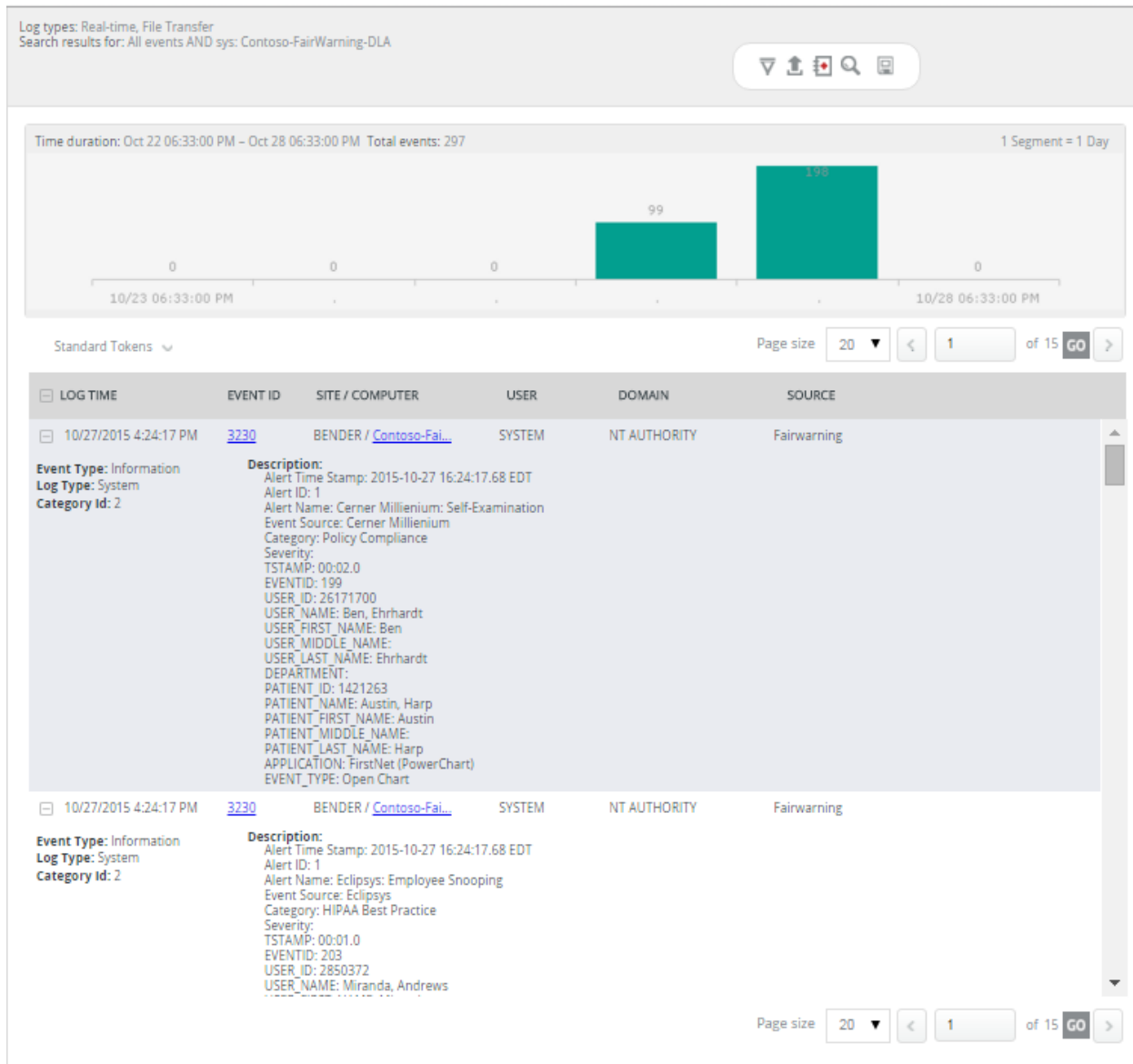


Figure 8

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.

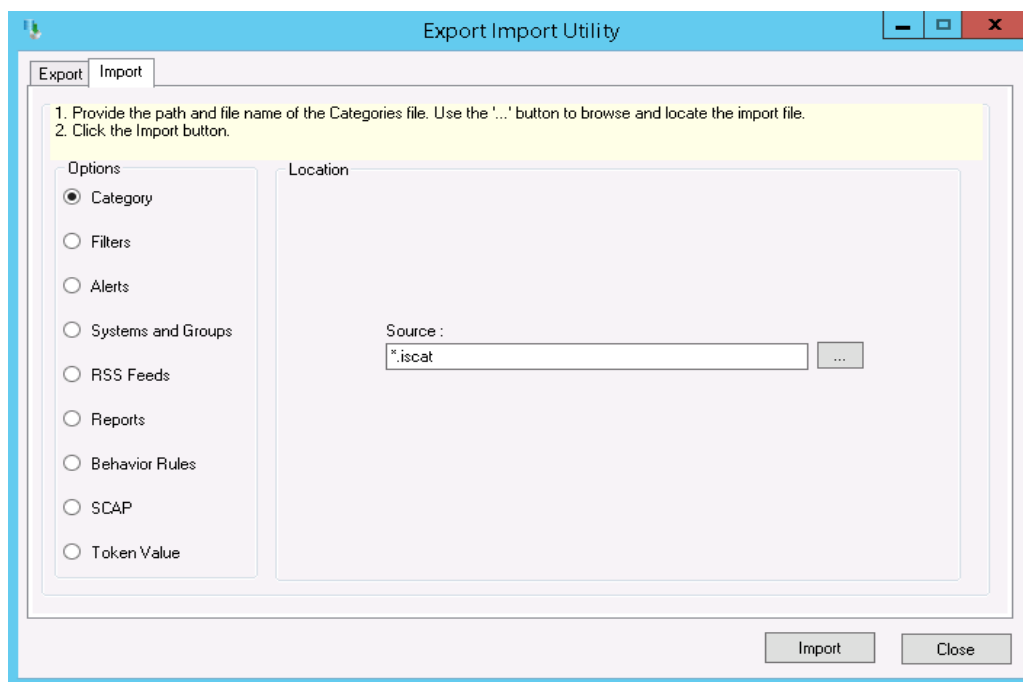


Figure 9

- 2. Locate **.iscat** file, and then click the **Open** button.
- 3. To import categories, click the **Import** button.
EventTracker displays success message.

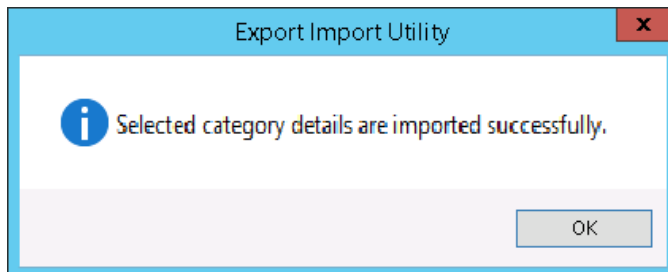



Figure 10

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

To import Tokens

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

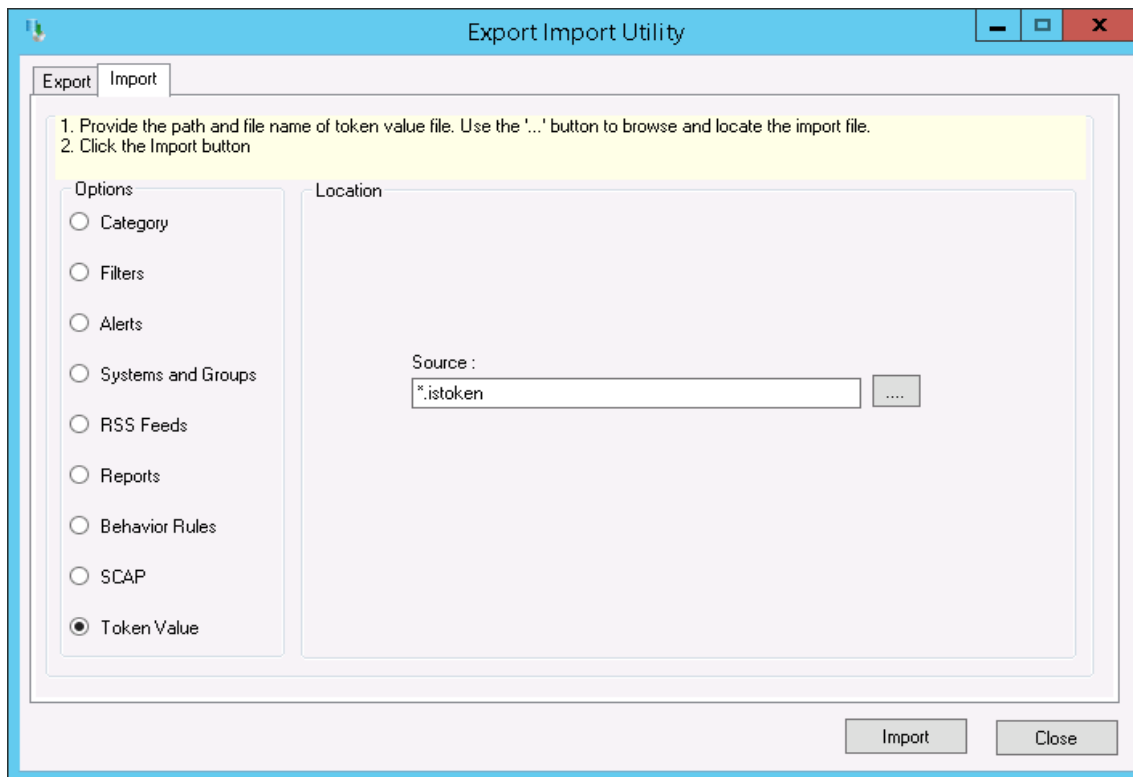


Figure 11

2. Locate the **.istoken** file, and then click the **Open** button.
3. To import tokens, click the **Import** button.
EventTracker displays success message.

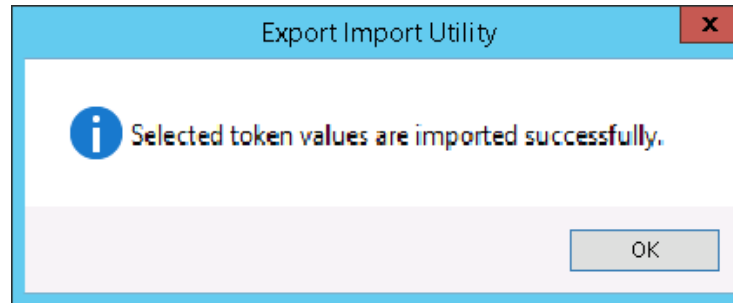



Figure 12

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

To import Flex Reports

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

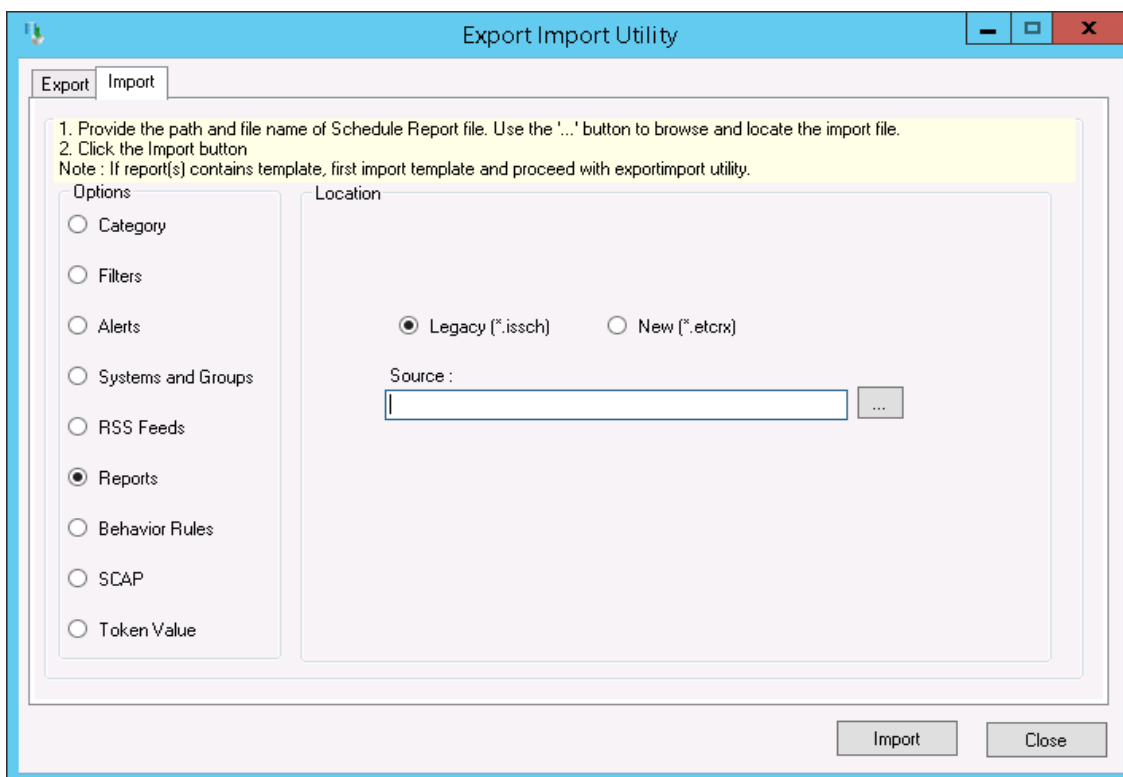


Figure 13

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.

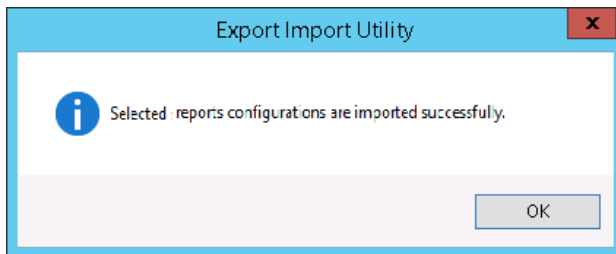


Figure 14

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.

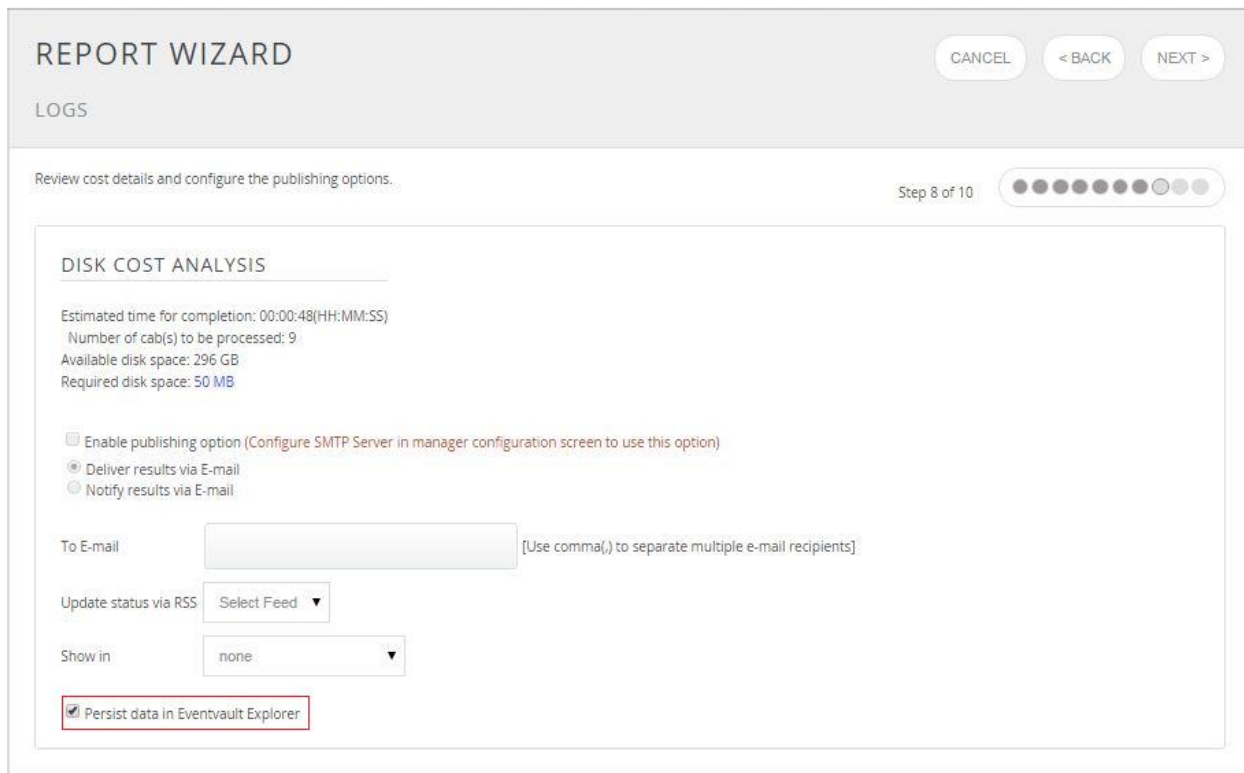


Figure 15

REPORT WIZARD
TITLE: FAIRWARNING-ALL ALERT REPORT
DATA PERSIST DETAIL

Cancel < BACK NEXT >

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
Alert Time Stamp	<input checked="" type="checkbox"/>
Alert Name	<input checked="" type="checkbox"/>
Category	<input checked="" type="checkbox"/>
User Name	<input checked="" type="checkbox"/>
User First Name	<input checked="" type="checkbox"/>
Patient Name	<input checked="" type="checkbox"/>

Figure 16

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.


FLEX DASHBOARD

Title
FairWarning

Description
FairWarning

SAVE DELETE CANCEL

Figure 17

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

WIDGET TITLE

DATA SOURCE

CHART TYPE **DURATION** **VALUE FIELD SETTING** **AS OF**

AXIS LABELS [X-AXIS] **LABEL TEXT**

VALUES [Y-AXIS] **VALUE TEXT**

FILTER **FILTER VALUES**

LEGEND [SERIES] **SELECT**

NOTE

<input type="checkbox"/> HIPAA Best Practice	<input type="checkbox"/> Policy Compliance	<input type="checkbox"/> FTC Best Practice
400	260	200
<input type="checkbox"/> Medical Identity Theft	130	

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.

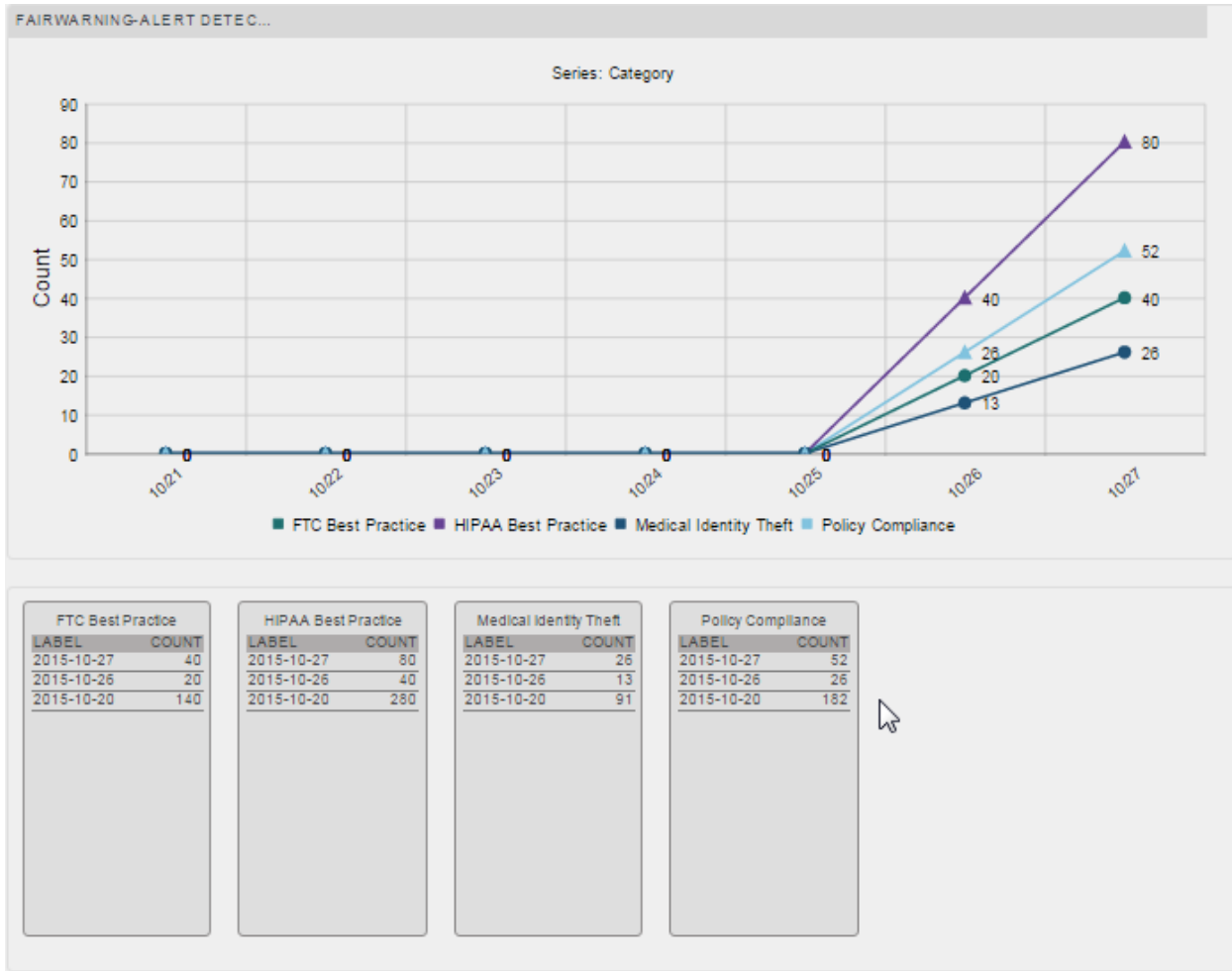


Figure 19

- After creation of Dashlet for FairWarning®, click on **Customize flex dashlet** .
- Select FairWarning®-Alert Detected usage dashlet and click on **ADD** button .



Figure 20

- Now, you can see the Dashlet on Dashboard.

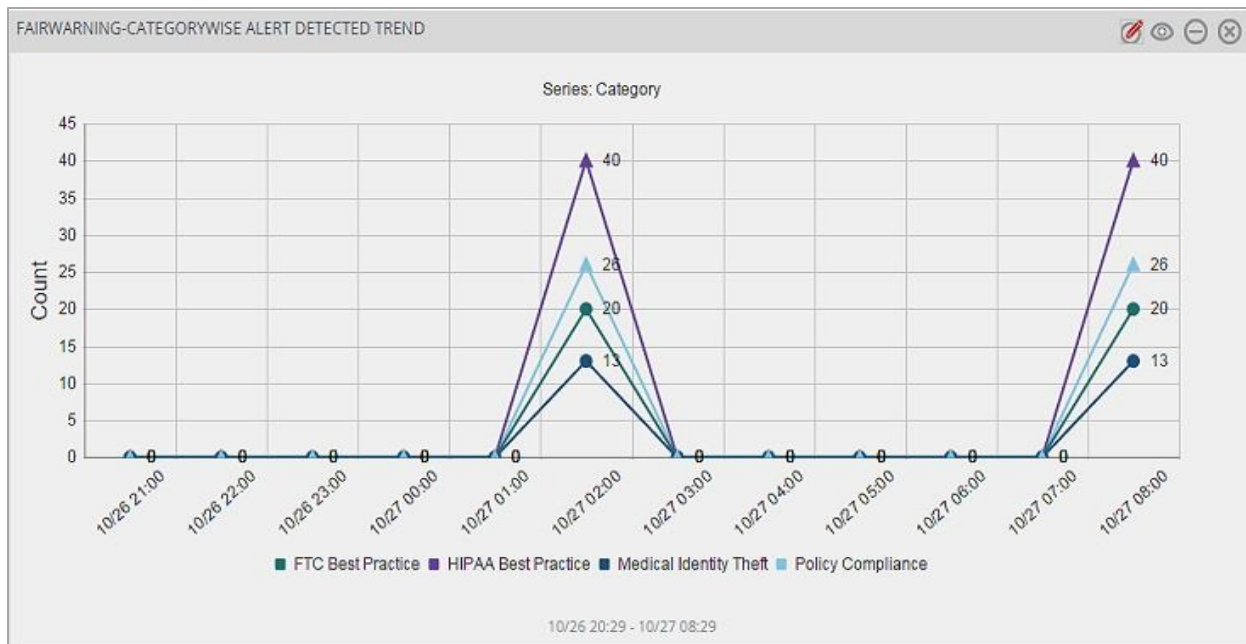


Figure 21

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.

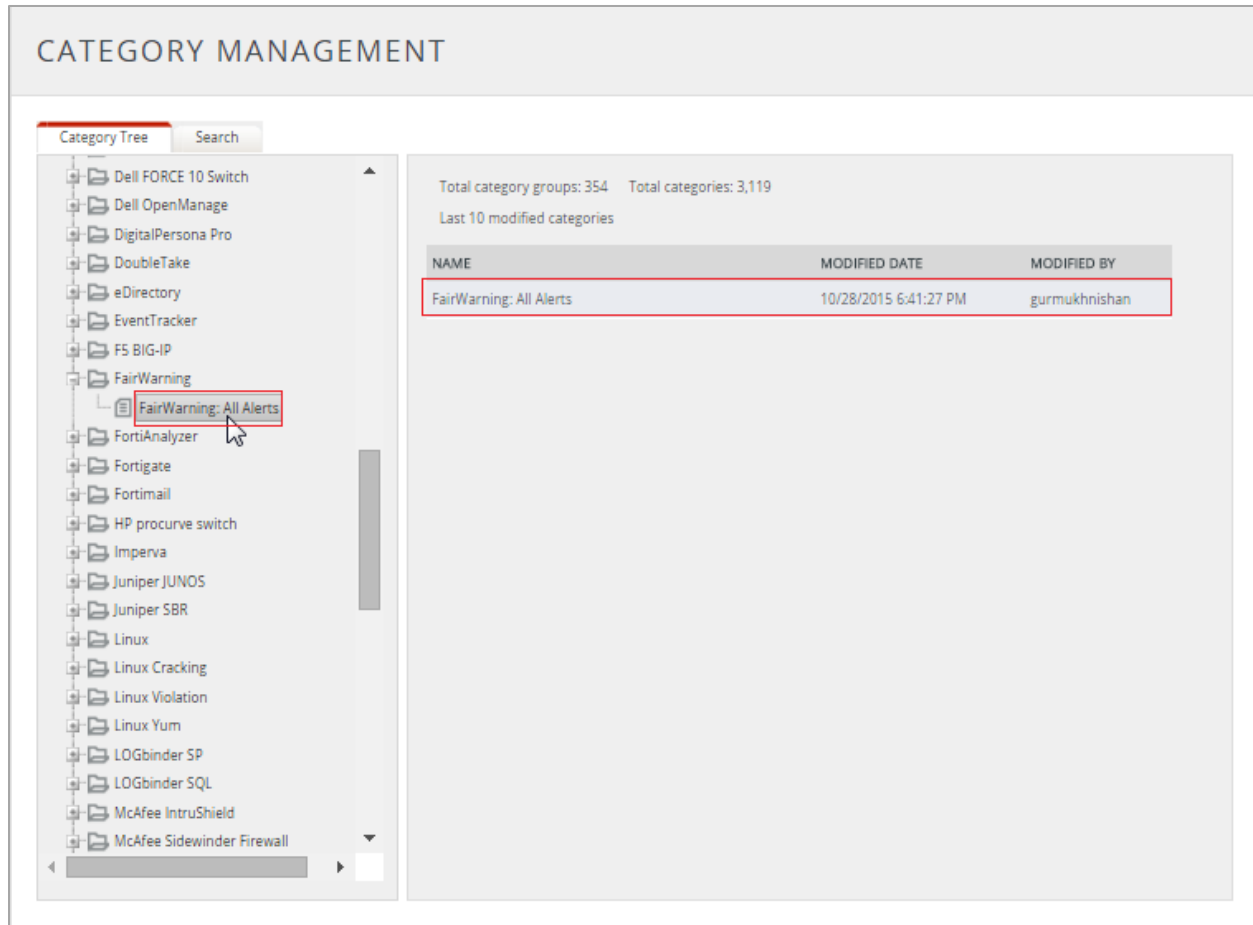


Figure 22

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).

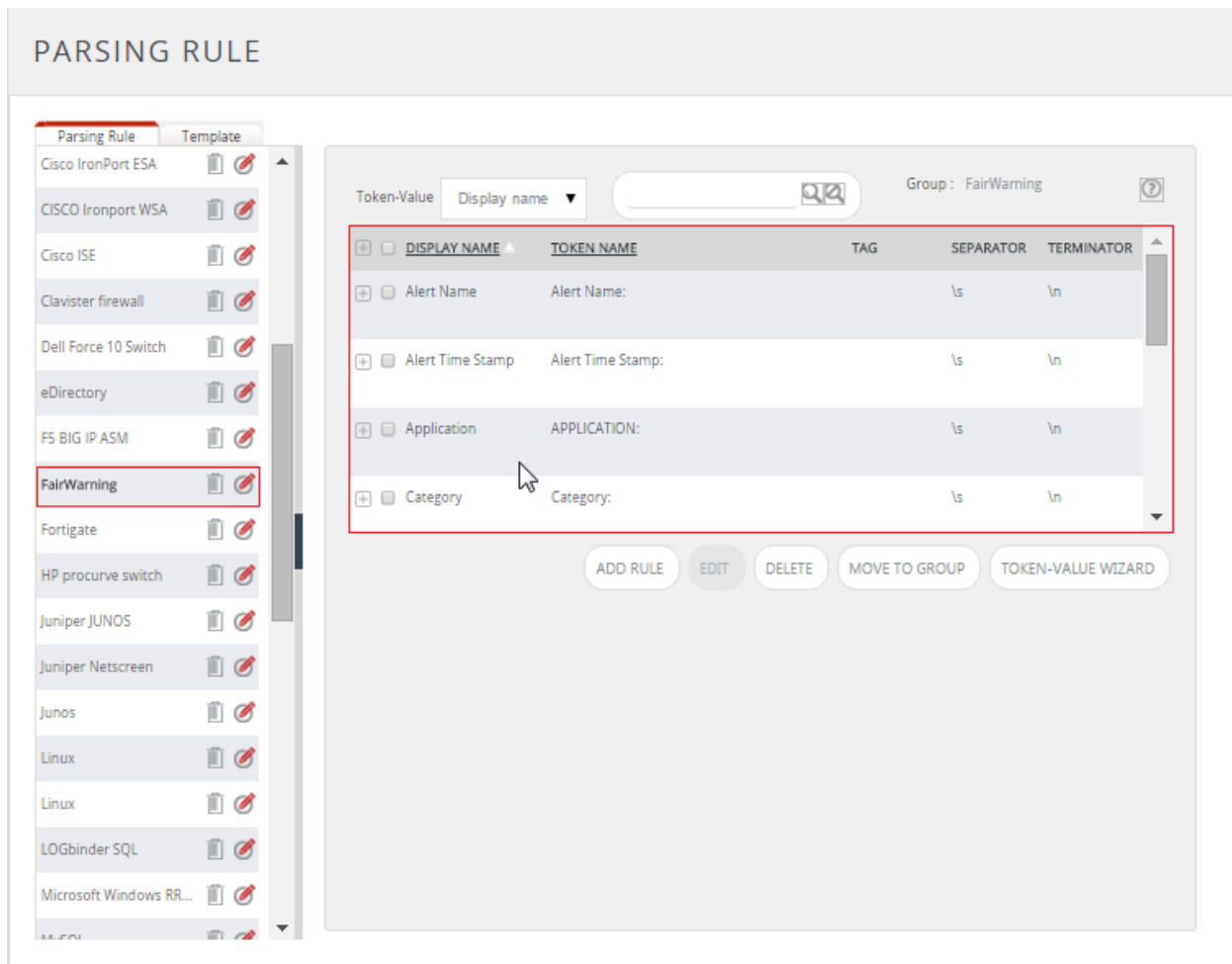


Figure 23

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®.

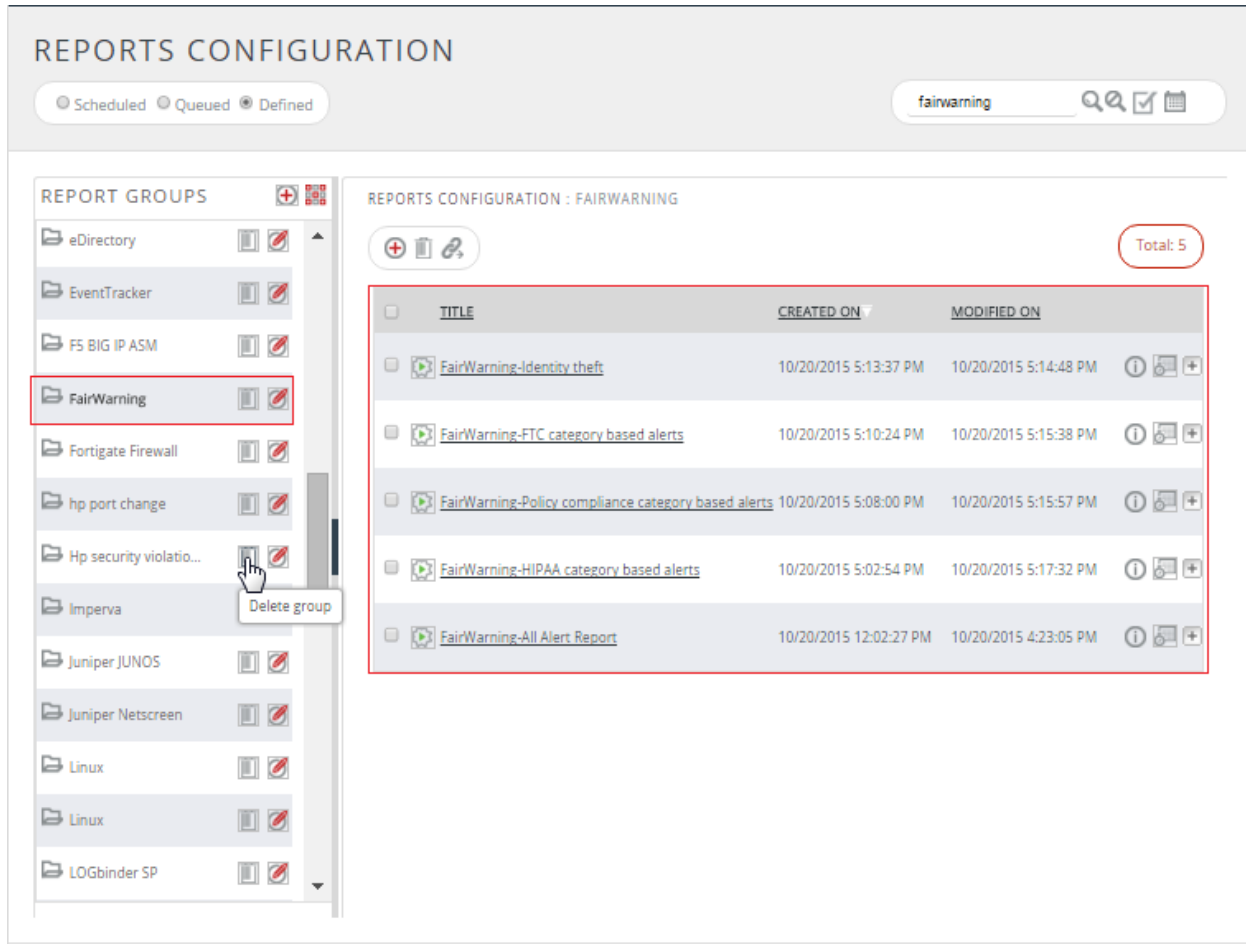


Figure 24

Here you can find imported defined reports such as FairWarning®-Identity theft.

Sample Dashboard

1) FairWarning-Category wise alert detected

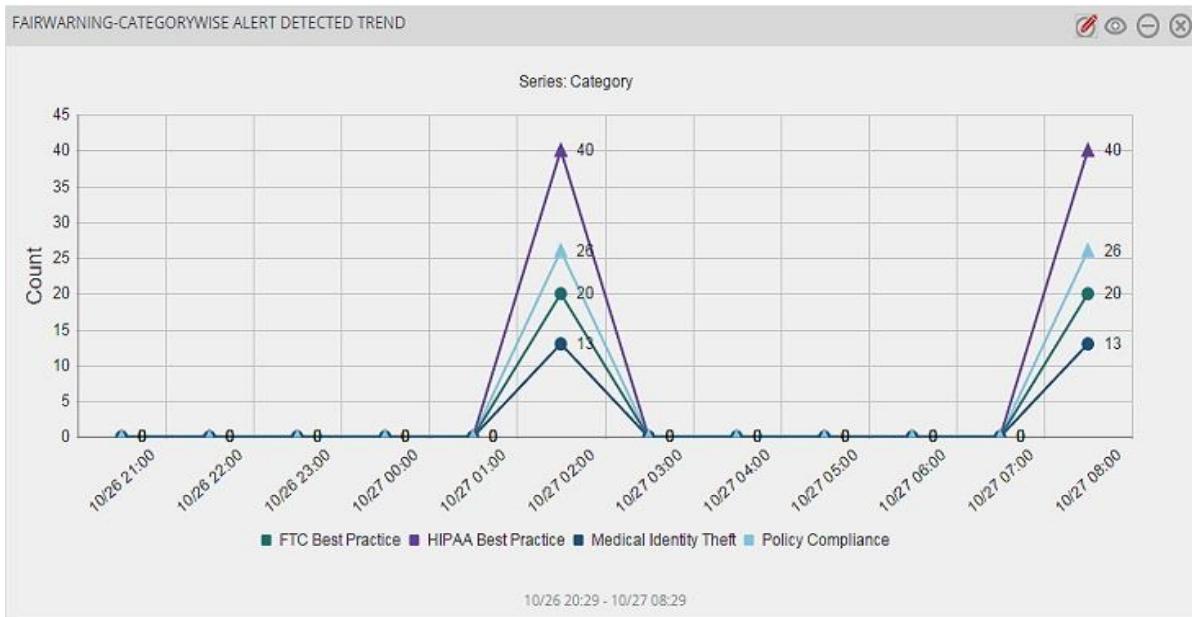


Figure 25

2) FairWarning-Suspicious user

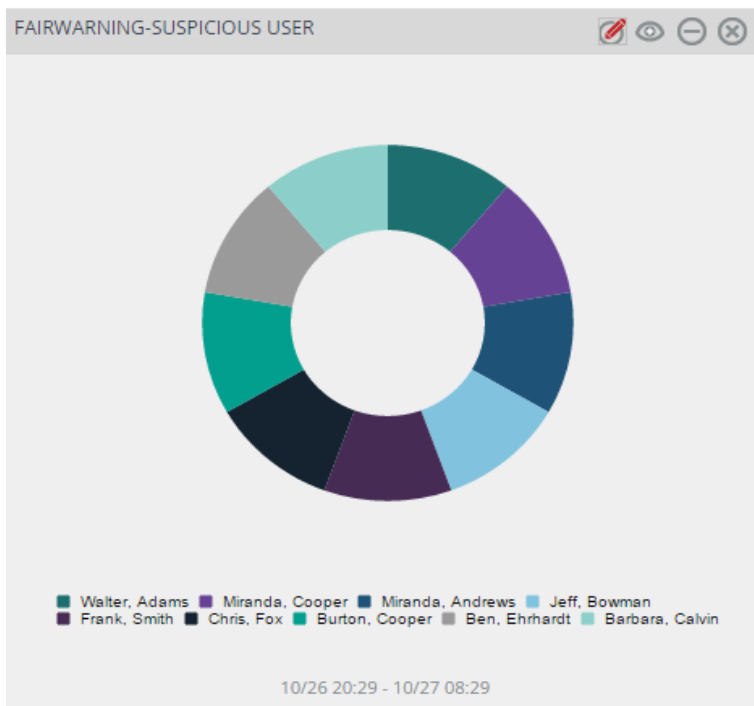


Figure 26

Sample Reports

1) FairWarning-All Alerts

FairWarning-All Alert						
Alert Time Stamp	Alert Name	Category	User Name	User First Name	Patient Name	Application
2015-04-10 16:01:04.0 EDT	Cerner Millennium: Self-Examination	Policy Compliance	Ben, Ehrhardt	Ben	Jay, Meyer	HNA: Powerchart
2015-04-10 16:03:10.02 EDT	Cerner Millennium: VIP Snooping	HIPAA Best Practice	Jeff, Bowman	Jeff	Percy, Shock	Ascent Capture Index Validation
2015-04-10 16:05:40.04 EDT	Cerner Millennium: Fuction Code (Search) + Filter (Remote user)	FTC Best Practice	Walter, Adams	Walter	Lisa, Andrews	HNA: Powerchart
2015-04-10 16:08:50.12 EDT	Cerner Millennium: Employee Snooping	HIPAA Best Practice	Chris, Fox	Chris	Ellen, Brewer	HNA: Powerchart
2015-04-10 16:11:09.768 EDT	Eclipsys: Self-Examination	Policy Compliance	Miranda, Cooper	Miranda	Percy, Shock	Ascent Capture Index Validation
2015-04-10 16:15:07.999 EDT	Eclipsys: VIP Snooping	HIPAA Best Practice	Burton, Cooper	Burton	Lisa, Andrews	Ascent Capture Index Validation
2015-04-10 16:30:59.0 EDT	Eclipsys: Fuction Code (Search) + Filter (Remote user)	FTC Best Practice	Frank, Smith	Frank	Ellen, Brewer	Ascent Capture Index Validation
2015-04-10 16:32:14.109 EDT	Eclipsys: Employee Snooping	HIPAA Best Practice	Miranda, Andrews	Miranda	Misty, Smith	Ascent Capture Index Validation
2015-04-10 16:40:10.18 EDT	Cerner Millennium: payroll access	Medical Identity Theft	Barbara, Calvin	Barbara	William, Sankovic	Ascent Capture Index Validation
2015-04-10 16:42:17.74 EDT	Cerner Millennium: Self-Examination	Policy Compliance	Ben, Ehrhardt	Ben	Austin, Harp	FirstNet (PowerChart)
2015-04-10 16:43:18.876 EDT	Cerner Millennium: VIP Snooping	HIPAA Best Practice	Jeff, Bowman	Jeff	Allen, Bowman	
2015-04-10 16:45:54.387 EDT	Cerner Millennium: Fuction Code (Search) + Filter (Remote user)	FTC Best Practice	Walter, Adams	Walter	Jay, Meyer	
2015-04-10 16:55:56.376 EDT	Cerner Millennium: Employee Snooping	HIPAA Best Practice	Chris, Fox	Chris	Percy, Shock	
2015-04-10 16:56:14.47 EDT	Mckesson Care Manager: Fuction Code (delete patient demographics)	Medical Identity Theft	Miranda, Cooper	Miranda	Lisa, Andrews	HNA: Powerchart
2015-04-10 16:59:12.97 EDT	Mckesson Care Manager: Specific Patient Investigation	Policy Compliance	Burton, Cooper	Burton	Ellen, Brewer	HNA: Powerchart
2015-04-10 16:59:16.387 EDT	Mckesson Care Manager: Self-Examination	Policy Compliance	Frank, Smith	Frank	Misty, Smith	HNA: Powerchart
2015-04-10 17:01:17.36 EDT	Mckesson Care Manager: VIP Snooping	HIPAA Best Practice	Miranda, Andrews	Miranda	William, Sankovic	HNA: Powerchart
2015-04-10 17:03:30.30 EDT	Mckesson Care Manager: Fuction Code (Search) + Filter (Remote user)	FTC Best Practice	Barbara, Calvin	Barbara	Austin, Harp	HNA: Powerchart
2015-04-10 17:05:34.18 EDT	Mckesson Care Manager: Employee Snooping	HIPAA Best Practice	Ben, Ehrhardt	Ben	Allen, Bowman	HNA: Powerchart

Figure 27

2) FairWarning-FTC category based alerts

FairWarning-FTC category based alerts				
Alert Time Stamp	Alert Name	User Name	Patient Name	Application
2015-04-10 16:01:04.0 EDT	Cerner Millenium: Fuction Code (Search) + Filter (Remote user)	Walter, Adams	Lisa, Andrews	HNA: Powerchart
2015-04-10 16:03:10.02 EDT	Eclipsys: Fuction Code (Search) + Filter (Remote user)	Frank, Smith	Ellen, Brewer	Ascent Capture Index Validation
2015-04-10 16:05:40.04 EDT	Cerner Millenium: Fuction Code (Search) + Filter (Remote user)	Walter, Adams	Jay, Meyer	
2015-04-10 16:08:50.12 EDT	Mckesson Care Manager: Fuction Code (Search) + Filter (Remote user)	Barbara, Calvin	Austin, Harp	HNA: Powerchart
2015-04-10 16:11:09.768 EDT	Eclipsys: Fuction Code (Search) + Filter (Remote user)	Chris, Fox	Lisa, Andrews	2004 Release Main Application
2015-04-10 16:15:07.999 EDT	Cerner Millenium: Fuction Code (Search) + Filter (Remote user)	Barbara, Calvin	Allen, Bowman	Ascent Capture Index Validation
2015-04-10 16:30:59.0 EDT	Mckesson Care Manager: Fuction Code (Search) + Filter (Remote user)	Burton, Cooper	William, Sankovic	Ascent Capture Index Validation
2015-04-10 16:32:14.109 EDT	Eclipsys: Fuction Code (Search) + Filter (Remote user)	Ben, Ehrhardt	Percy, Shock	Ascent Capture Index Validation
2015-04-10 16:40:10.18 EDT	Cerner Millenium: Fuction Code (Search) + Filter (Remote user)	Burton, Cooper	Austin, Harp	Ascent Capture Index Validation
2015-04-10 16:42:17.74 EDT	Mckesson Care Manager: Fuction Code (Search) + Filter (Remote user)	Walter, Adams	Misty, Smith	HNA: Powerchart
2015-04-10 16:43:18.876 EDT	Eclipsys: Fuction Code (Search) + Filter (Remote user)	Frank, Smith	Jay, Meyer	Ascent Capture Index Validation
2015-04-10 16:45:54.387 EDT	Cerner Millenium: Fuction Code (Search) + Filter (Remote user)	Walter, Adams	William, Sankovic	Ascent Capture Index Validation
2015-04-10 16:55:56.376 EDT	Mckesson Care Manager: Fuction Code (Search) + Filter (Remote user)	Barbara, Calvin	Ellen, Brewer	Ascent Capture Index Validation
2015-04-10 16:56:14.47 EDT	Eclipsys: Fuction Code (Search) + Filter (Remote user)	Chris, Fox	Allen, Bowman	HNA: Powerchart
2015-04-10 16:59:12.97 EDT	Cerner Millenium: Fuction Code (Search) + Filter (Remote user)	Barbara, Calvin	Misty, Smith	HNA: Powerchart

Figure 28