EventTracker
Secure. Comply. Succeed.

Integrating Cyberoam UTM

EventTracker Enterprise

Publication Date: Jan 6, 2016

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

Abstract

This guide helps you in configuring **Cyberoam UTM** and EventTracker to receive Cyberoam UTM events. You will find the detailed procedures required for monitoring Cyberoam UTM Appliance.

Intended audience

Administrators, who are assigned the task to monitor and manage events using EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 7.X and **Cyberoam UTM CR500i, Version 9.5.4 and later.**

Table of Contents

Cyberoam UTM Appliance

The Cyberoam Unified Threat Management hardware appliances offer comprehensive security to organizations, ranging from large enterprises to small and branch offices. Multiple security features integrated over a single, Layer 8 Identity-based platform make security simple, yet highly effective. Cyberoam's Extensible Security Architecture (ESA) and multi-core technology carry the ability to combat future threats for organization's security.

Overview

To monitor Cyberoam UTM Appliance in EventTracker, configure Cyberoam UTM Appliance to send all events as Syslog to the EventTracker system.

Pre-requisite

- **EventTracker v7.x and later** should be installed.
- **Cyberoam UTM** should be installed.

Configure Cyberoam UTM to forward all logs to EventTracker

Configure Syslog logging

1. Login to Cyberoam Web console using administrator credentials.
2. Select **Logs & Reports**, select **Configuration**. In **Syslog Servers** tab click '**Add**" button.

Figure 1

3. In the **Name*** filed, type the name of the server.
4. In the **IP address*** field, type the IP address of the EventTracker Manager.
5. In the **Port*** field, type the remote port number.

   The port 514 is the standard syslog port.
6. Select the required **Facility***, **Severity Level***, and **Format*** option.
7. Select the **OK** button.

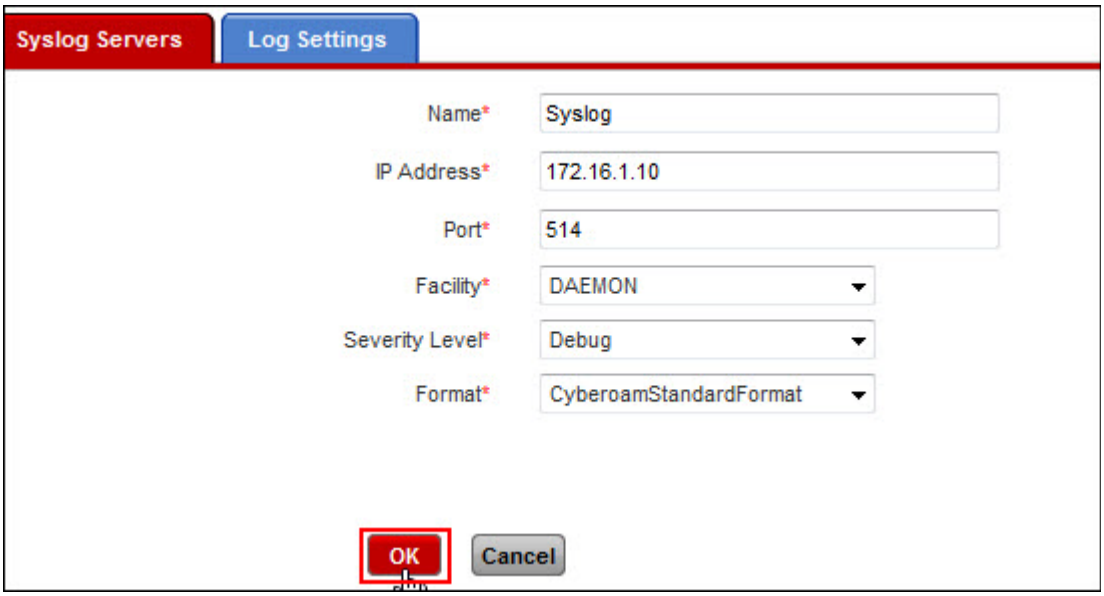
Syslog Servers
Log Settings
Name*
Syslog
IP Address*
172.16.1.10
Port*
514
Facility*
DAEMON
Severity Level*
Debug
Format*
CyberoamStandardFormat
OK
Cancel

Figure 2

EventTracker Knowledge Pack

Once Cyberoam UTM events are enabled and Cyberoam UTM events are received in EventTracker, Alerts and Reports can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker to support Cyberoam UTM monitoring.

Categories

- **Cyberoam UTM: Attack detected -** This category based report provides information related to attack detected.
- **Cyberoam UTM: Attack dropped -** This category based report provides information related to attack dropped.
- **Cyberoam UTM: DOS attack denied -** This category based report provides information related to DOS attack denied.
- **Cyberoam UTM: Firewall traffic allowed -** This category based report provides information related to firewall traffic allowed.
- **Cyberoam UTM: Firewall traffic denied -** This category based report provides information related to firewall traffic denied.
- **Cyberoam UTM: Fragmented traffic dropped -** This category based report provides information related to fragmented traffic dropped.
- **Cyberoam UTM: ICMP redirection traffic denied -** This category based report provides information related to ICMP redirection traffic denied.
- **Cyberoam UTM: Invalid traffic denied -** This category based report provides information related to invalid traffic denied.
- **Cyberoam UTM: Local ACL traffic allowed -** This category based report provides information related to local ACL traffic allowed.
- **Cyberoam UTM: Local ACL traffic blocked -** This category based report provides information related to local ACL traffic blocked.
- **Cyberoam UTM: Source routed traffic denied -** This category based report provides information related to source routed traffic denied.

- **Cyberoam UTM: Spam mail accepted -** This category based report provides information related to spam mail accepted.
- **Cyberoam UTM: Spam mail clean -** This category based report provides information related to spam mail clean.
- **Cyberoam UTM: Spam mail dropped -** This category based report provides information related to spam mail dropped.
- **Cyberoam UTM: Spam mail modified and forwarded -** This category based report provides information related to spam mail modified and forwarded.
- **Cyberoam UTM: Spam mail rejected -** This category based report provides information related to spam mail rejected.
- **Cyberoam UTM: Virus infected FTP data transfer allowed -** This category based report provides information related to virus infected FTP data transfer allowed.
- **Cyberoam UTM: Virus infected FTP data transfer blocked -** This category based report provides information related to virus infected FTP data transfer blocked.
- **Cyberoam UTM: Virus infected mail detected -** This category based report provides information related to virus infected mail detected.
- **Cyberoam UTM: Virus infected URL blocked -** This category based report provides information related to virus infected URL blocked.
- **Cyberoam UTM: Website access allowed -** This category based report provides information related to website access allowed.
- **Cyberoam UTM: Website access blocked -** This category based report provides information related to website access blocked.
- **Cyberoam UTM: All events -** This category based report provides information related to all events of Cyberoam UTM.

Alerts

- **Cyberoam UTM: Attack detected -** This alert is generated when attack is detected.
- **Cyberoam UTM: Spam detected -** This alert is generated when spam is detected.
- **Cyberoam UTM: Spam mail rejected-** This alert is generated when spam mail is rejected.

- **Cybroam UTM: Admin operations –** This alert is generated when address object, firewall rule, application and web filter policy, antivirus or spam filter policy is added, deleted or modified

- **Cyberoam UTM: User authentication failed –** This alert is generated when user failed to authentication with firewall more than 5 time in 10 second.

- **Cyberoam UTM: Virus detected -** This alert is generated when virus is detected.

Reports

- **Cyberoam UTM-Admin operations -** This report provides information related to admin operations like addition, deletion and updating of address object, firewall rules, antivirus and antispam policy which contains parameter(e.g. address object, firewall rules, policy,etc) details, Source IP, changes status and console information (GUI, CLI or central management)

- **Cyberoam UTM-User account management-** This report provides information related to user management like addition, deletion and modification of user or group and it's setting which contains user or group information, what operations happen on it, by whom changes are happened.

- **Cyberoam UTM-Antispam activity –** This report provides information related to Antispam activity like blocking of SMTP, POP3 or IMAP traffic due to spam which contains source information (e.g. source mail id, source domain name, source IP and port, source country code), destination information (e.g. Destination mail id, destination domain name, destination IP and port, destination country code), message information (message subject, mail size) and action on spam (like allow or deny).

- **Cyberoam UTM-Antivirus activity –** This report provides information related to Antivirus activity like bocking of SMTP, ftp or http traffic due to virus which contains Protocol information (SMPT, FTP or HTTP), virus details (name of virus), soruce information (source IP and port, source country code, domain name, URL Details, file name) and destination information (Destination IP and port, destination country code).

- **Cyberoam UTM-Application and web filtering –** This report provides information related to allowed and blocked traffic due to application and web filtering policy which contains URL and application information, Source information (source IP and port, source country code), destination information (Destination IP and port, Destination country code), web and application filter policy ID and status of traffic (allowed or blocked)

- **Cyberoam UTM-Firewall traffic allowed and denied –** This report provides information related to allowed or blocking of traffic due to web and application filter, IPS, antivirus or antispam which contains source information (Source IP and port, source country code, internal interface, source zone), destination information (Destination IP and port, destination country code, outer interaface, destination zone), traffic details (SMTP, FTP, HTTP,etc), status of traffic (allowed or blocked) and reason why it is blocked (DOS attack, web or application filter policy).

- **Cyberoam UTM-User authentication failed –** This report provides information related to user failed to authenticate with firewall which contains user information (username and group name), Source IP and reason why it is failed.

- **Cyberoam UTM-User authentication success –** This report provides information related to user successfully authenticate with firewall which contains user information (username and group name) and source IP information.

Dashboards

- **Cyberoam UTM-Top protocol used:** This dash board gives us the information about the top protocol used in the network.

- **Cyberoam UTM-Top source:** This dashboard gives us the information about the source IP address having high traffic.

- **Cyberoam UTM-Top Destination:** This dashboard gives us the information about the destination having high traffic.

- **Cyberoam UTM-Top user usage:** This dashboard gives us the information about the top user having high usage

- **Cyberoam UTM-Top virus detected:** This dashboard gives us the information about the top virus detected in the network

- **Cyberoam UTM-Top application used:** This dashboard gives us the information about the top application usage in the network.

Import Cyberoam UTM knowledge pack into EventTracker

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

   Import **Category/Alert** as given below.

Import Category

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

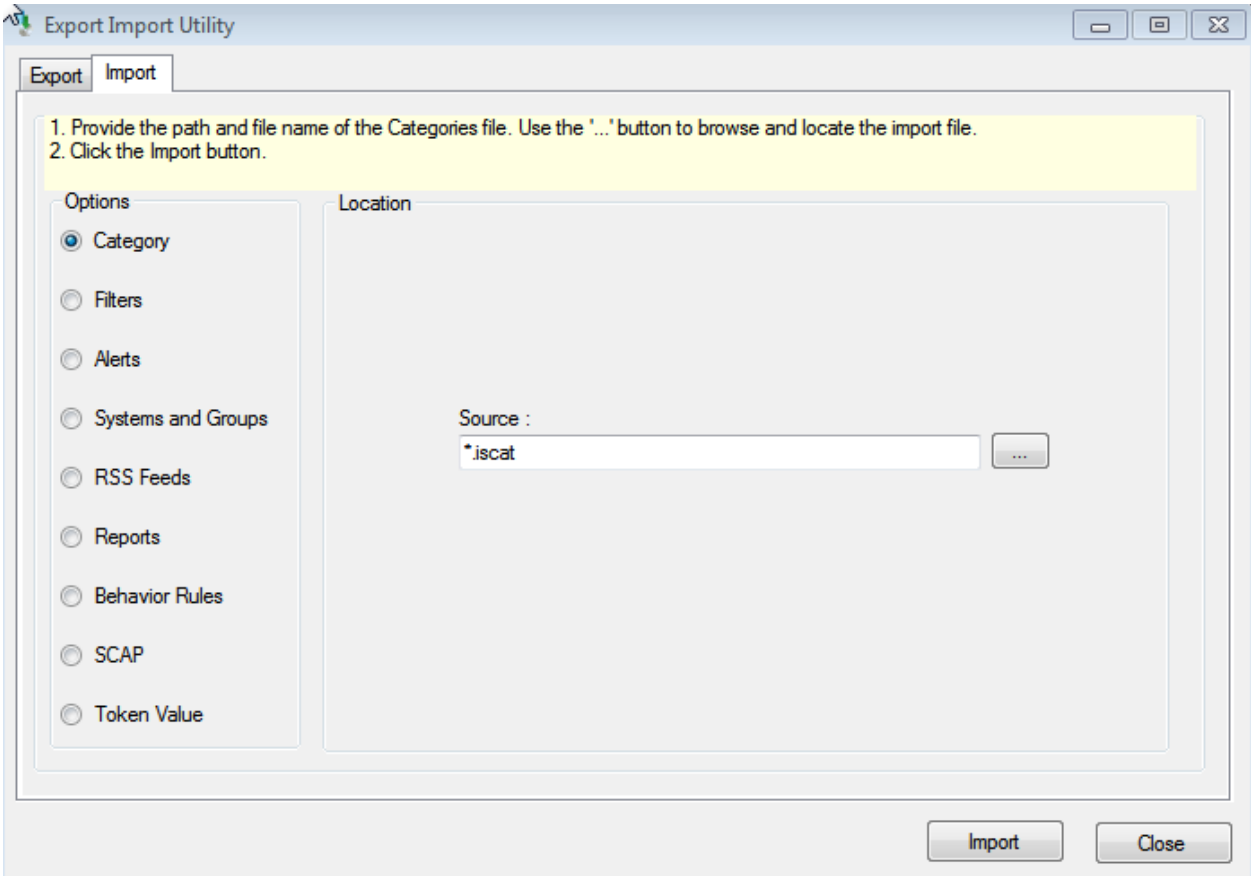

Figure 3

2. Locate **All Cyberoam UTM group of Categories.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.

   EventTracker displays success message.

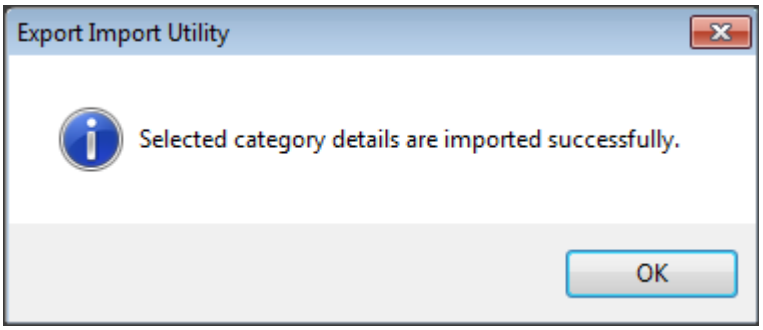

Figure 4

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

Import Alerts

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

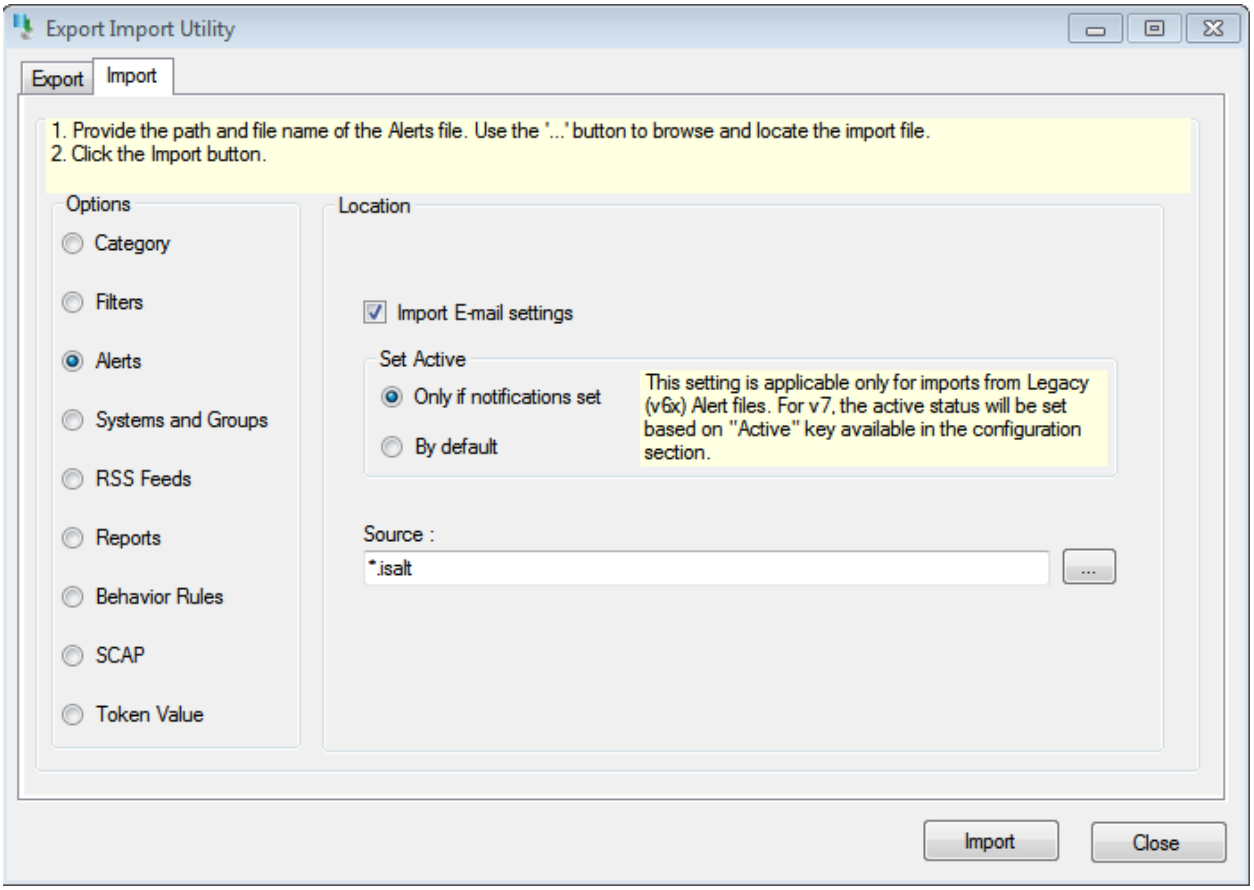

Figure 5

2. Locate **All Cyberoam UTM group of Alerts.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

   EventTracker displays success message.

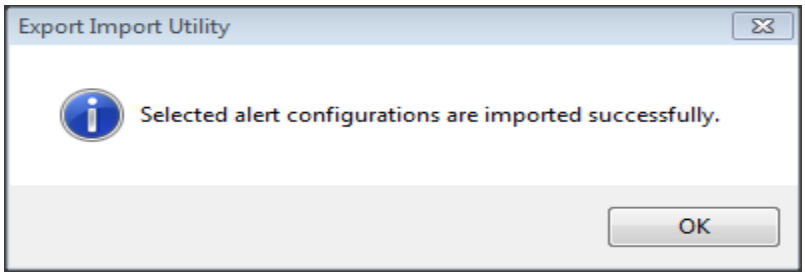

Figure 6

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

Import Flex Reports

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

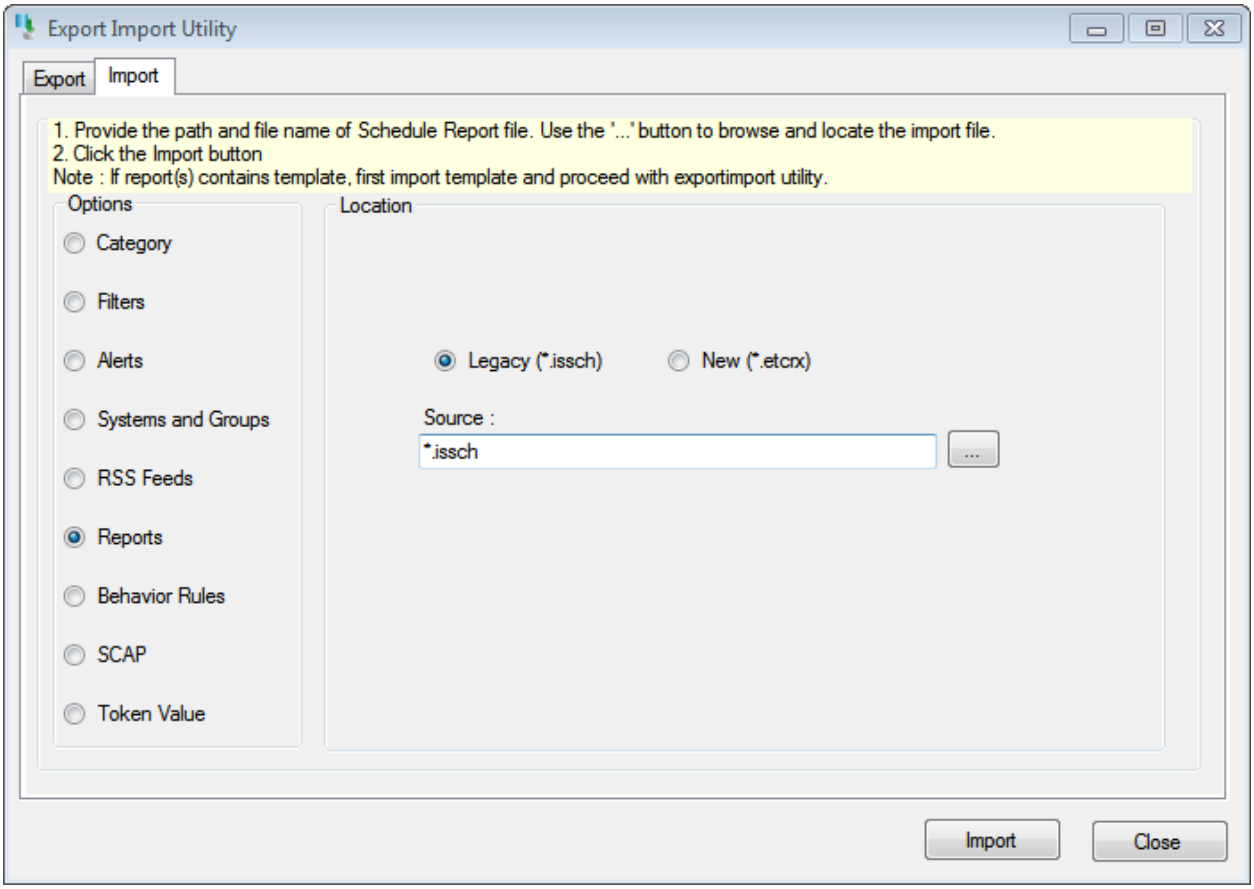

Figure 7

2. Locate the **All Cyberoam UTM group of Flex Report.issch** file, and then click the **Open** button.

3. Click the **Import** button to import the scheduled reports.

   EventTracker displays success message.

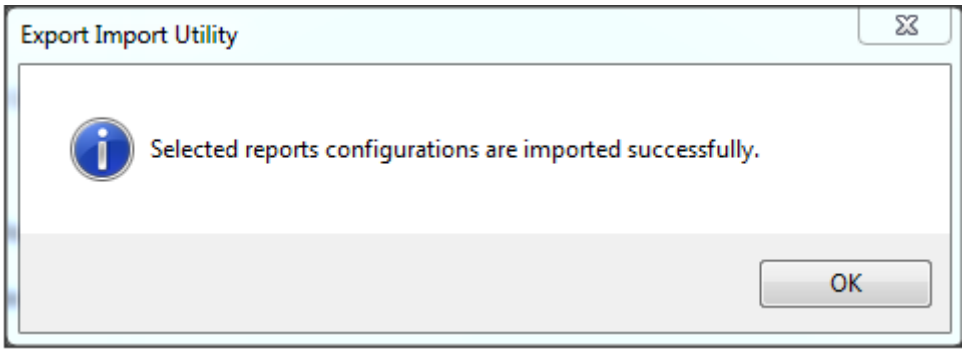

Figure 8

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

Import Tokens

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

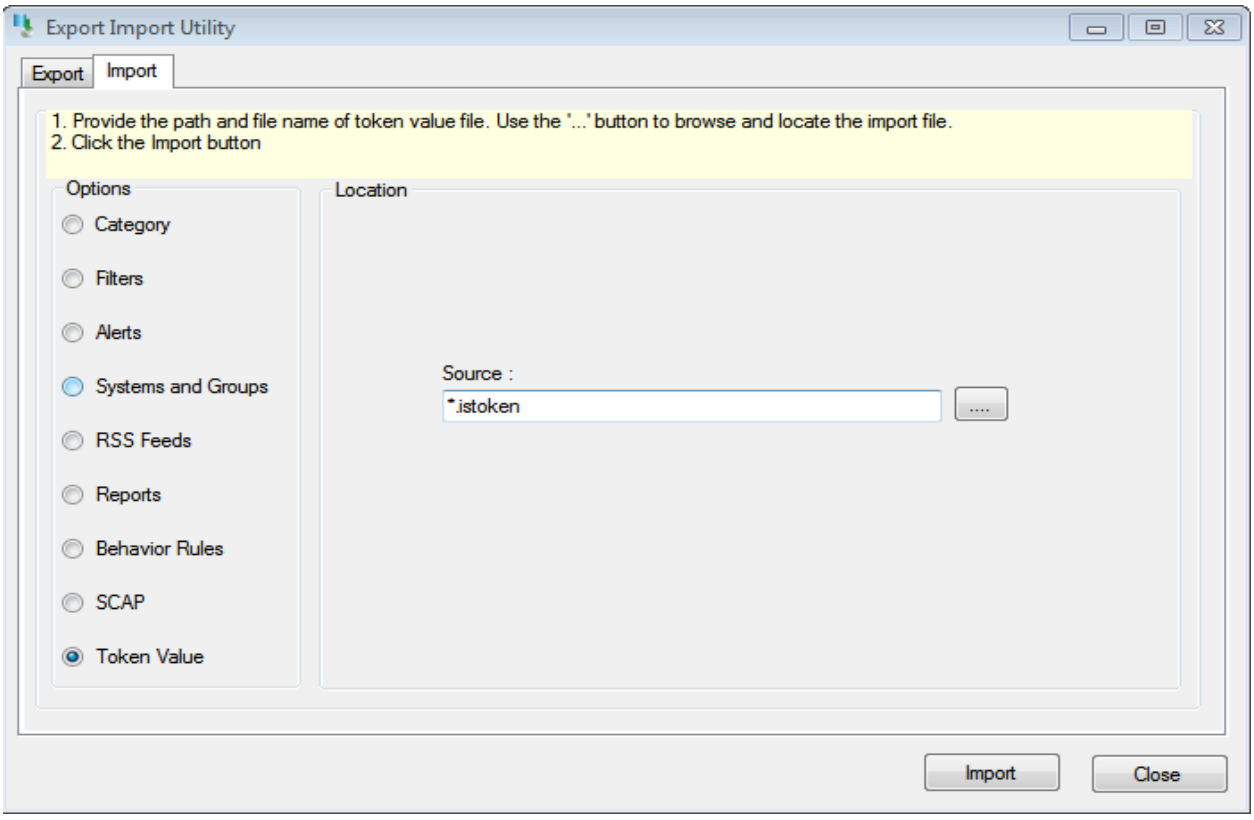

Figure 9

2. Locate the **All Cyberoam UTM group of token.istoken** file, and then click the **Open** button.

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

   EventTracker displays success message.

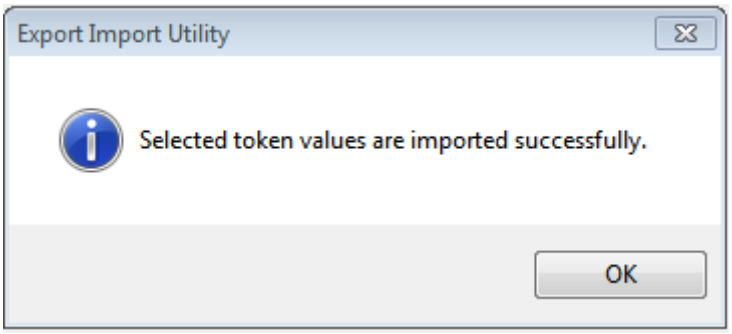

Figure 10

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

Import Template

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu and then click the **Parsing rule**.
3. Click the **Template** tab.
4. Click the **Import** button, it will open new window. (**Note**: Make sure pop-up is enable for EventTracker)

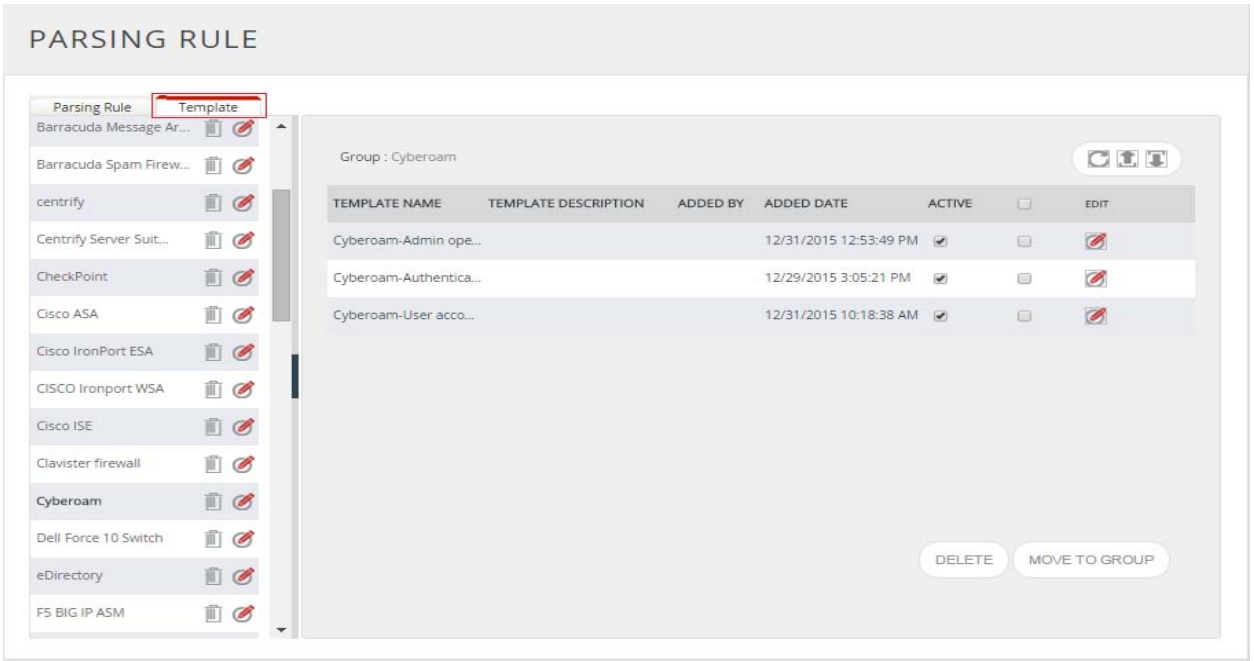

Figure 11

5. Locate and Chose **All Cyberoam UTM group of template.ETTD** file and then click the **Open** button.

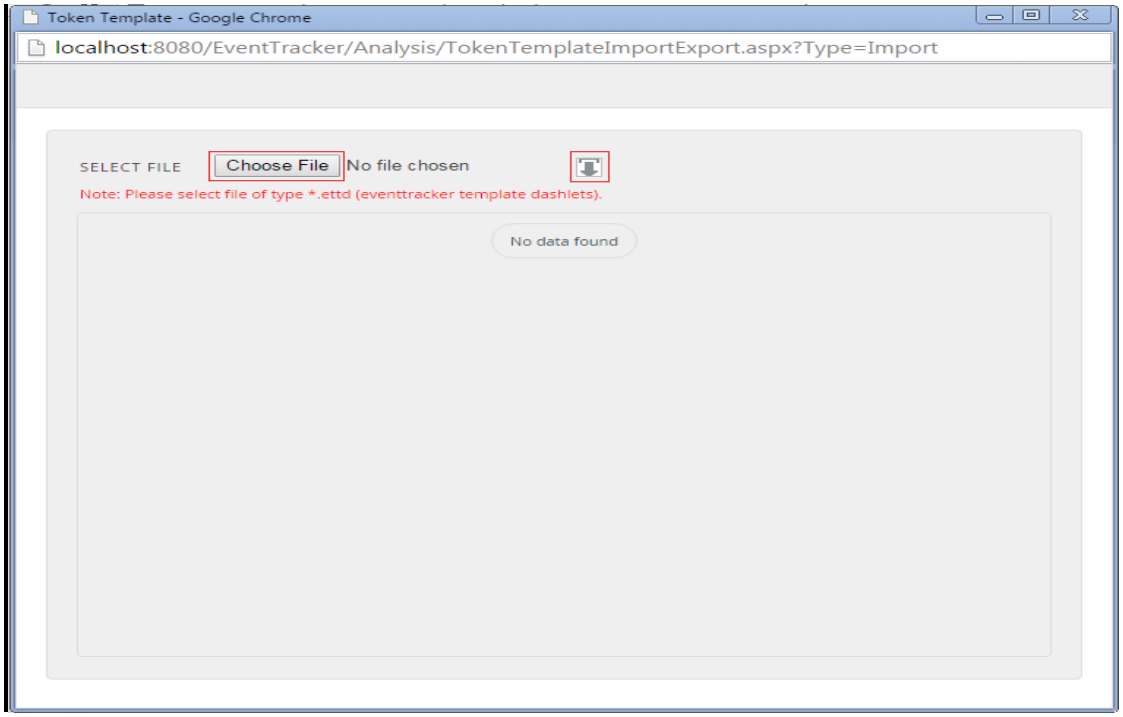

Figure 12

6. Select the template you want to upload.
7. Then click on **Import configuration** button.

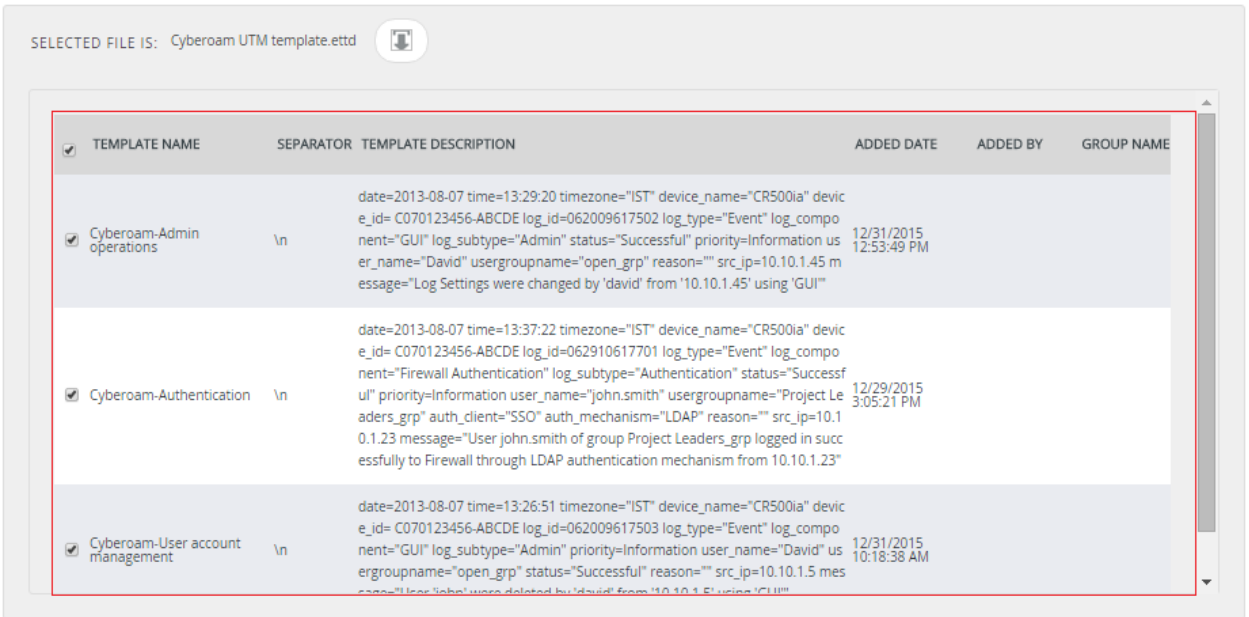

Figure 13

EventTracker displays success message.

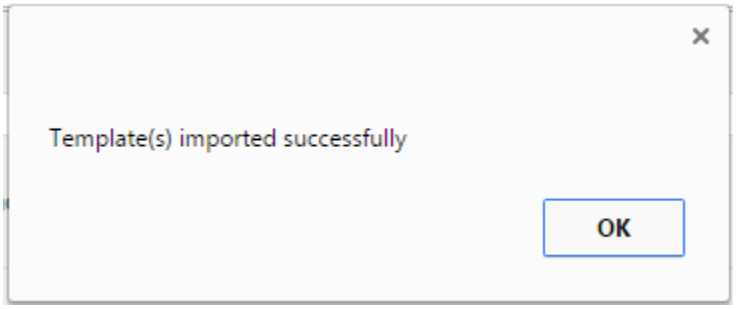

Figure 14

8. Click **OK** and it will automatically close the window.

Import Knowledge Object

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu and then click the **Knowledge Objects**.
3. Click the **Import** button, it will open new window. (**Note**: Make sure pop-up is enable for EventTracker.)

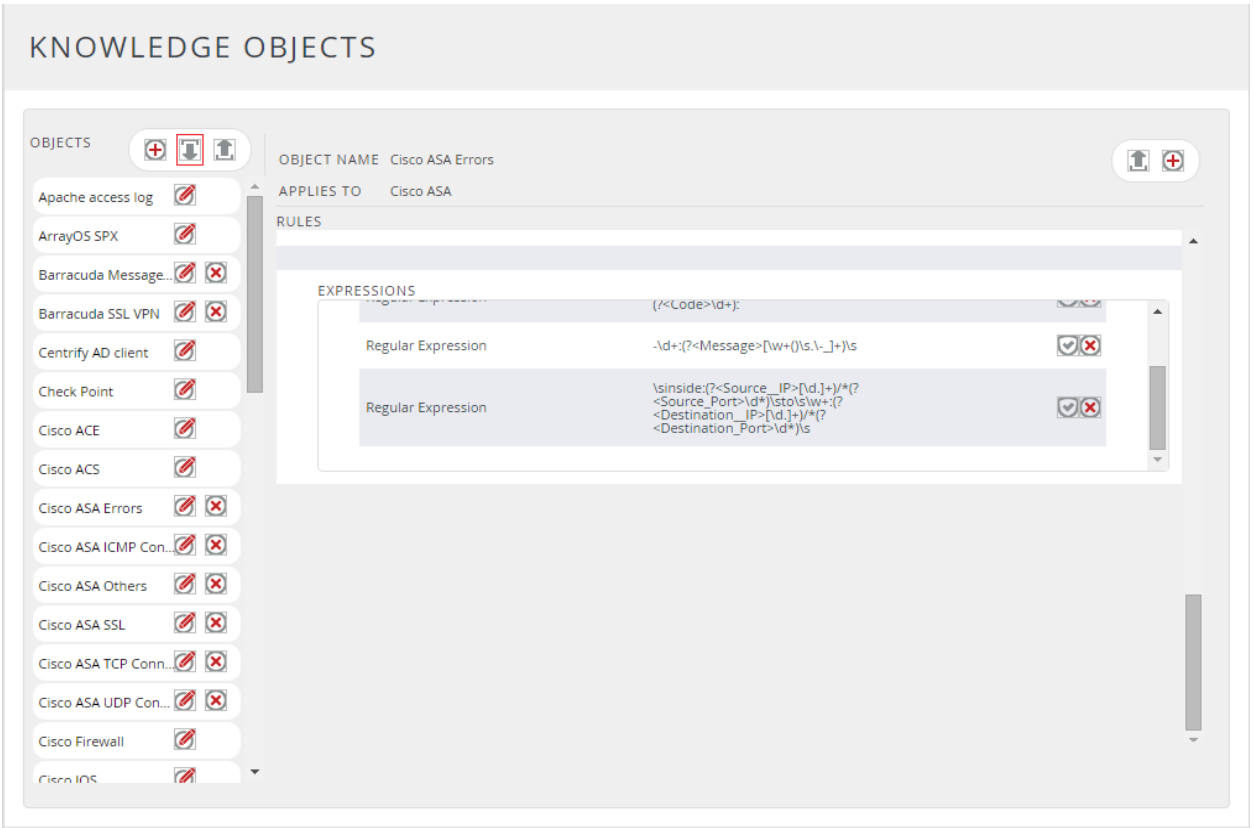

Figure 15

4. Choose the Knowledge object template (**All Cyberoam UTM group of knowledge object.EKTO**) files and click on **UPLOAD** button.

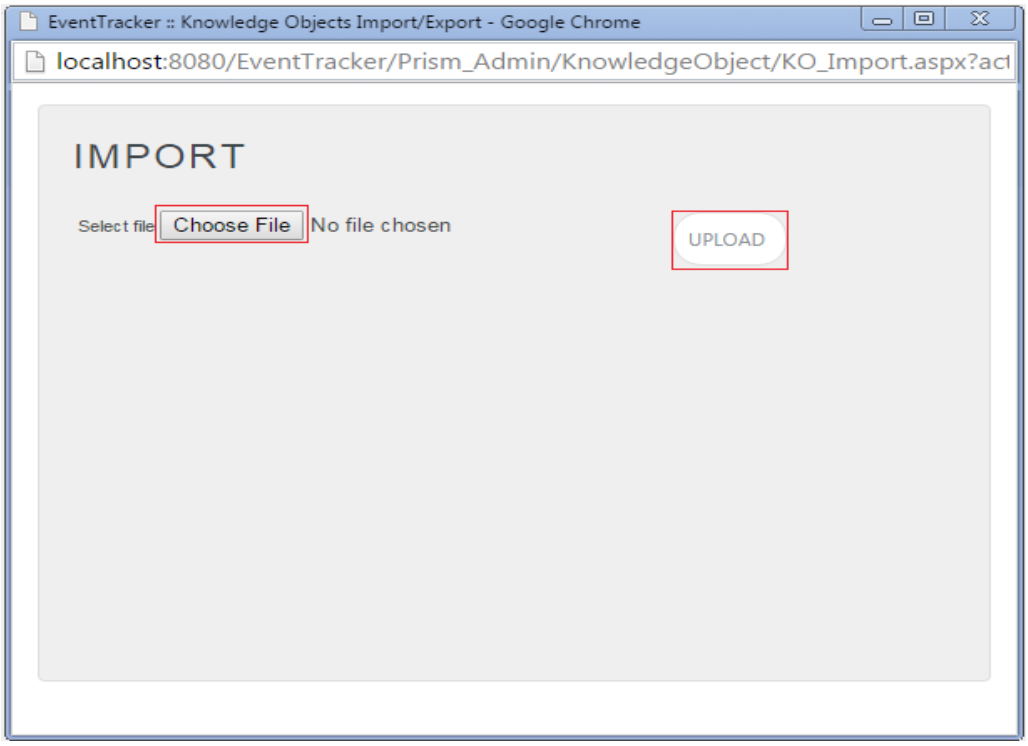

Figure 16

5. Select Knowledge Object and click on **Overwrite or Merge** button.

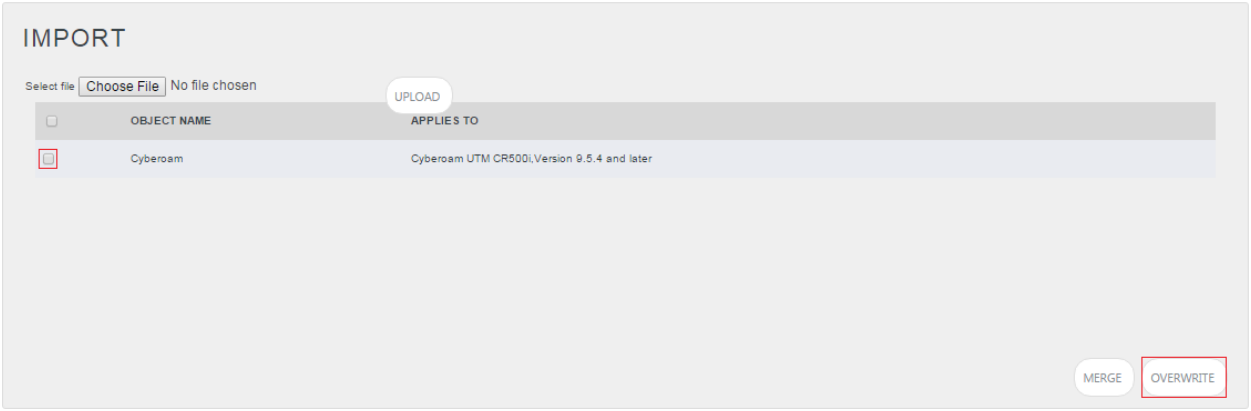

Figure 17

EventTracker displays success message.

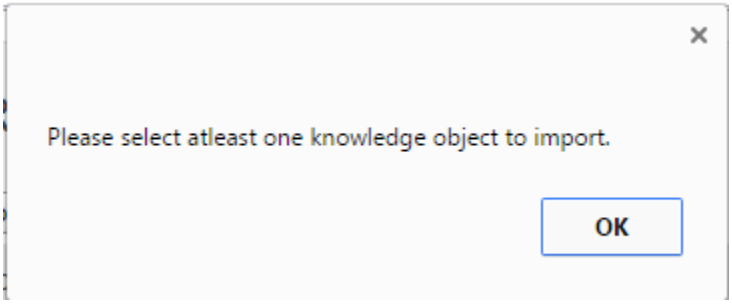

Figure 18

6. Click **OK** it will automatically close the window.

Configure Flex Dashboard

1. Scheduled flex reports after importing them.
2. During scheduling, please check **Persist data in EventVault Explorer** and select all the columns to persist.

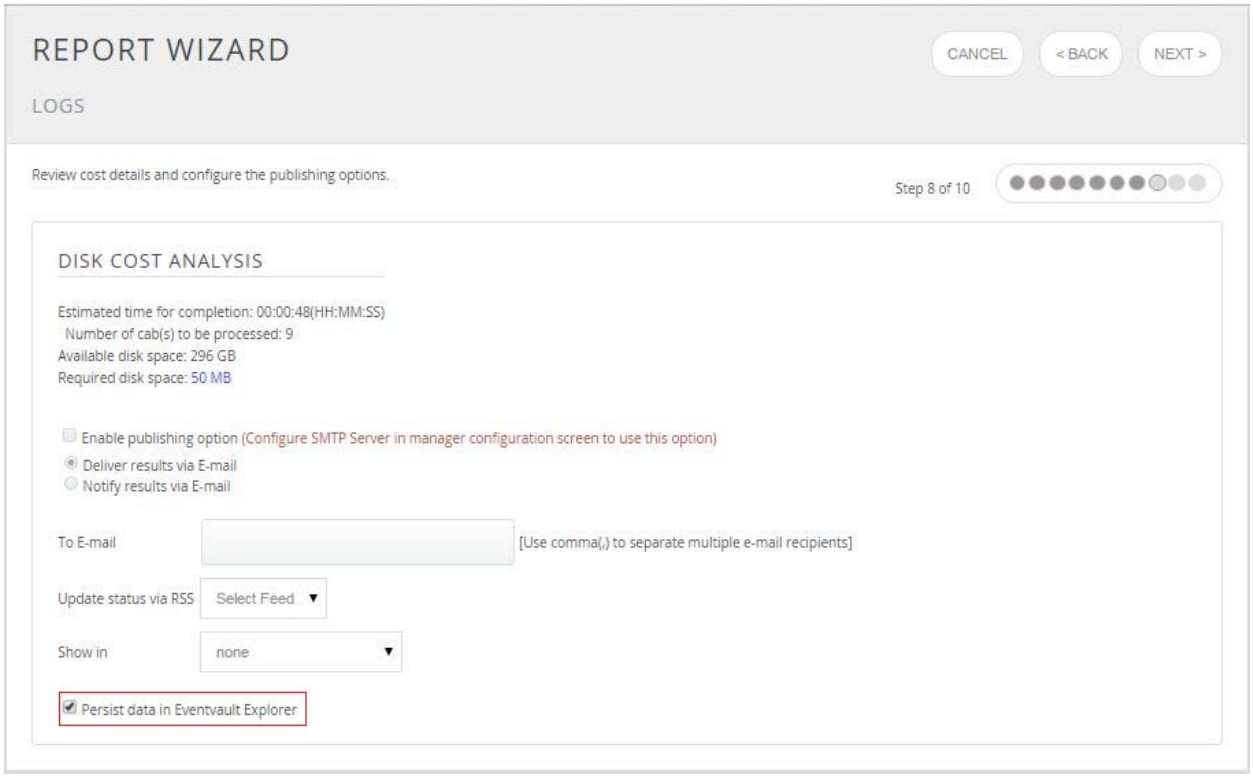

Figure 19

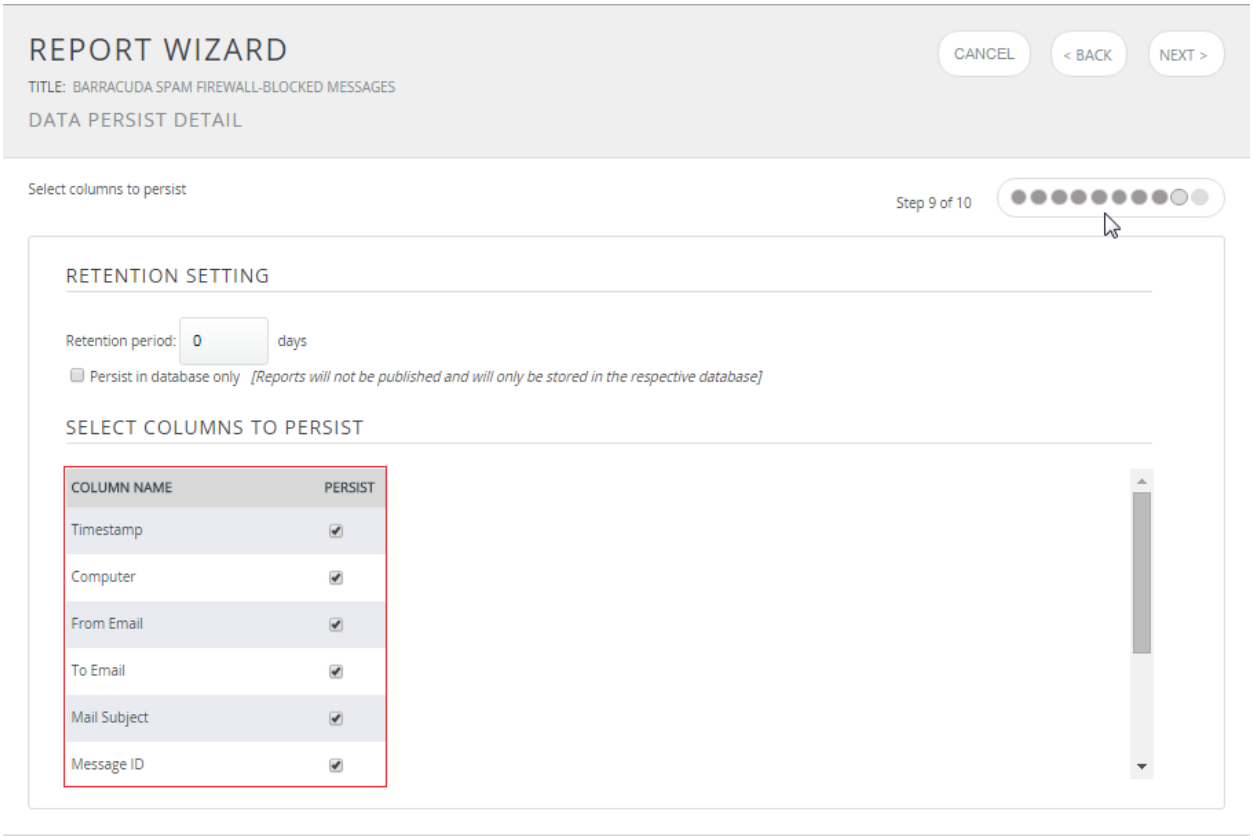

Figure 20

3. Now, wait for the report to run as per scheduled time.
4. After generating report, click on **Dashboard > Flex.**
5. Click on **Add Dashboard** icon and fill **Title** and **Description** box and save it.

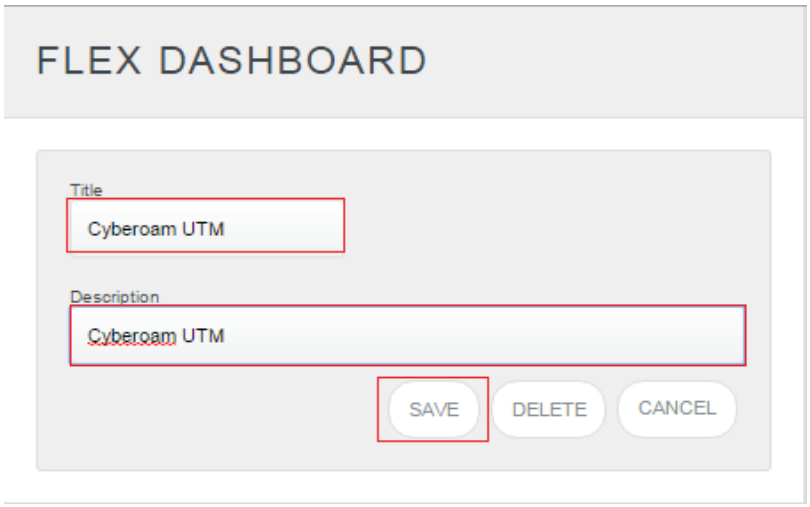

Figure 21

6. Now, create dashlet for Cyberoam UTM by clicking on **Configure flex dashlet** .

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

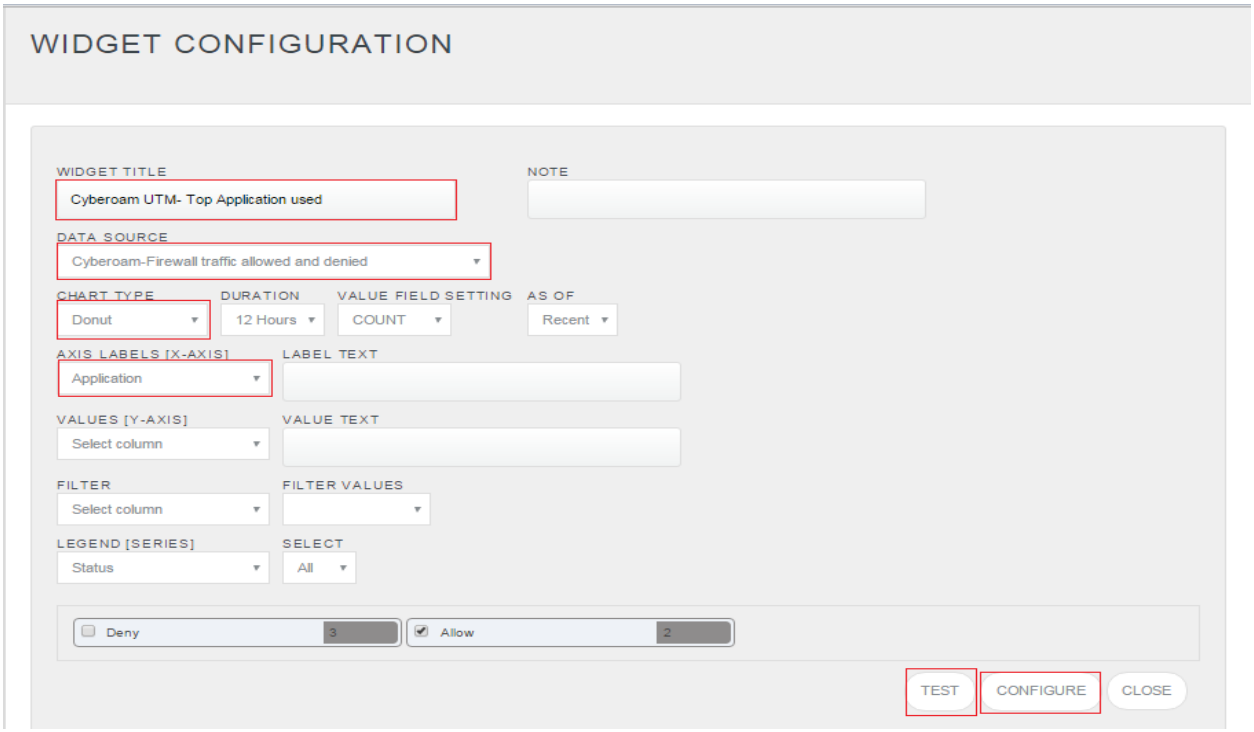

Figure 22

8. After selecting and filling all the options, click on the **TEST** button to check the Dashlet. If data are coming properly, then click on **CONFIGURE** button.

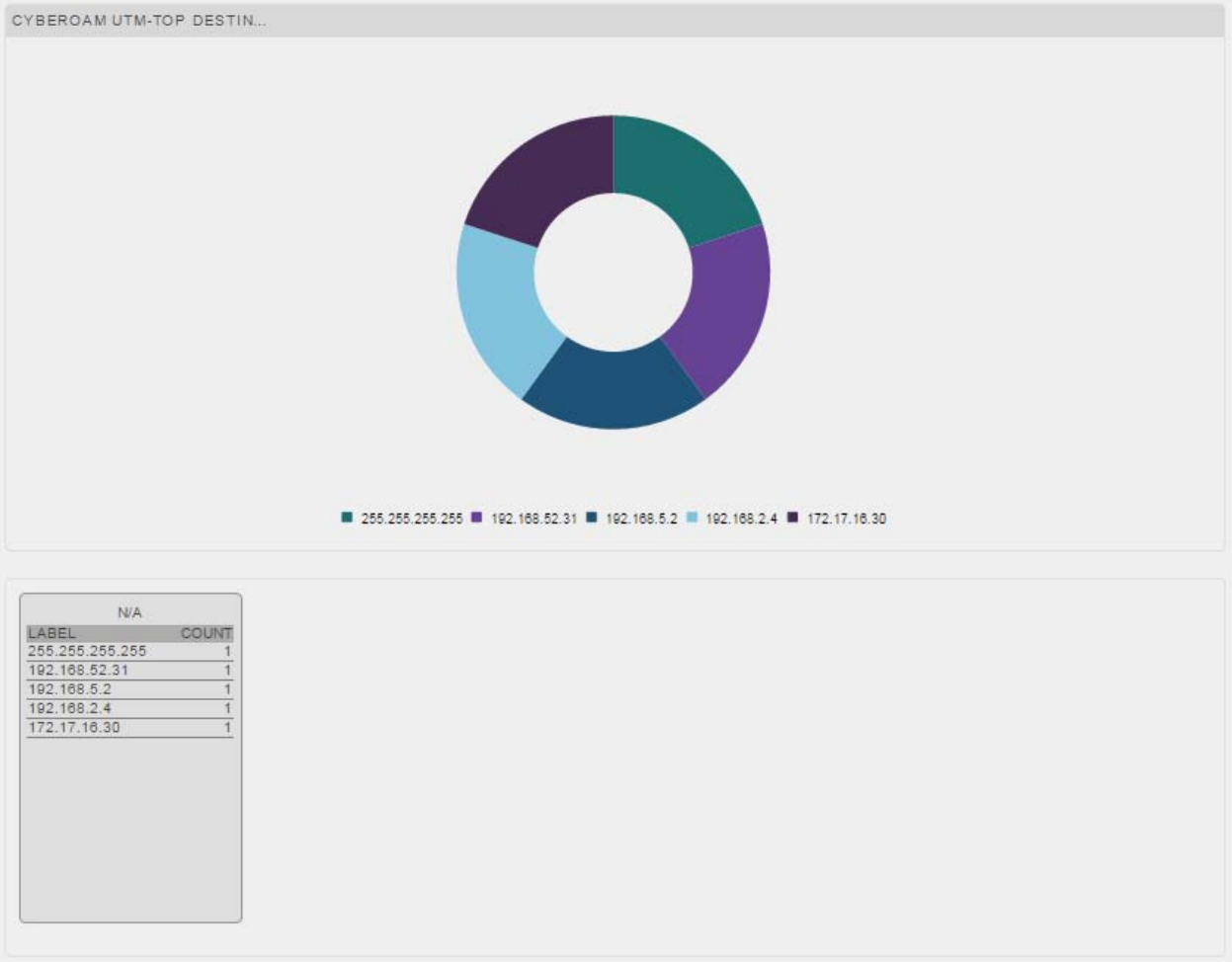

Figure 23

9. After creation of dashlet for Cyberoam UTM, click on **Customize flex dashlet** .
10. Select Cyberoam UTM-Top destination usage dashlet and click on **ADD** button .

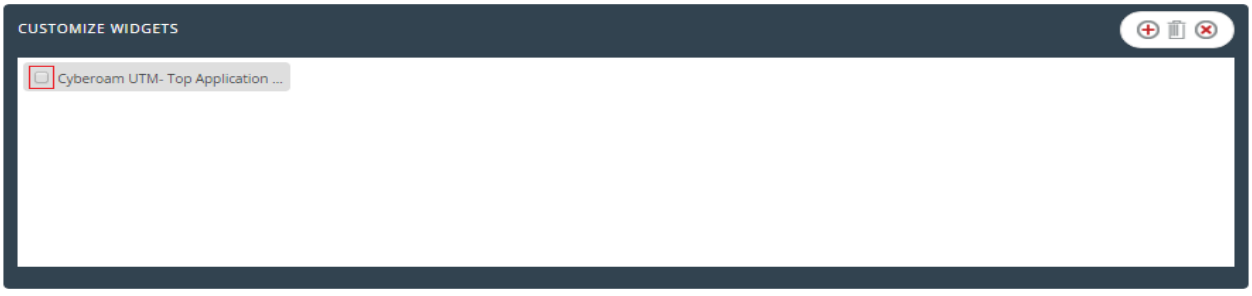

Figure 24

11. Now, you can see the Dashlet on Dashboard.

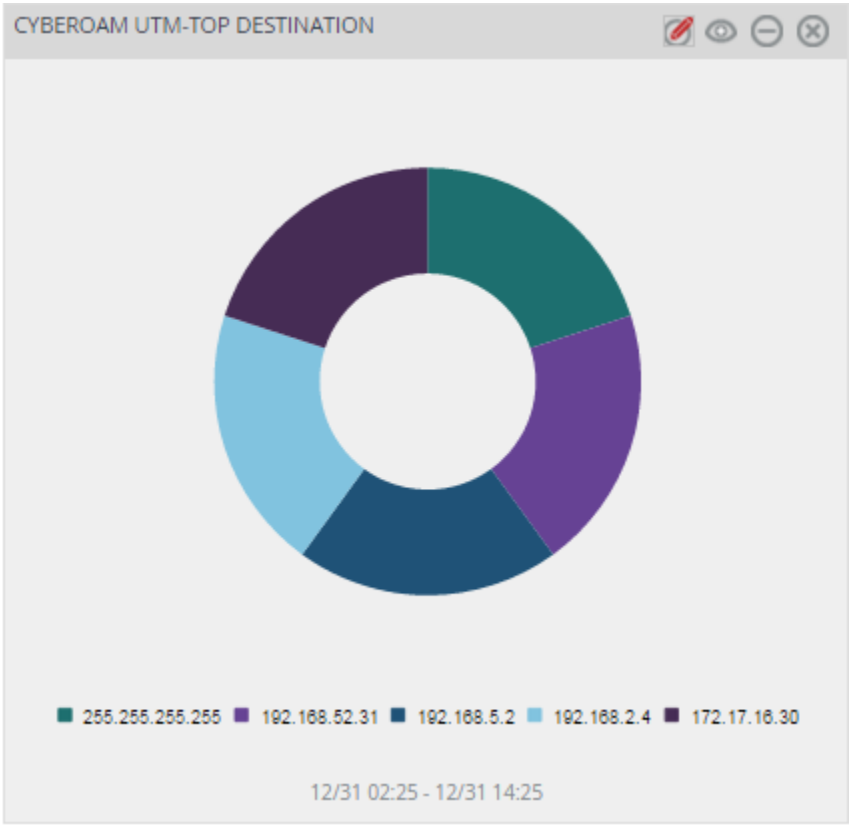

Figure 25

Verify Cyberoam UTM knowledge pack in EventTracker

Verify 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 **Cyberoam UTM** group folder to view the imported categories.

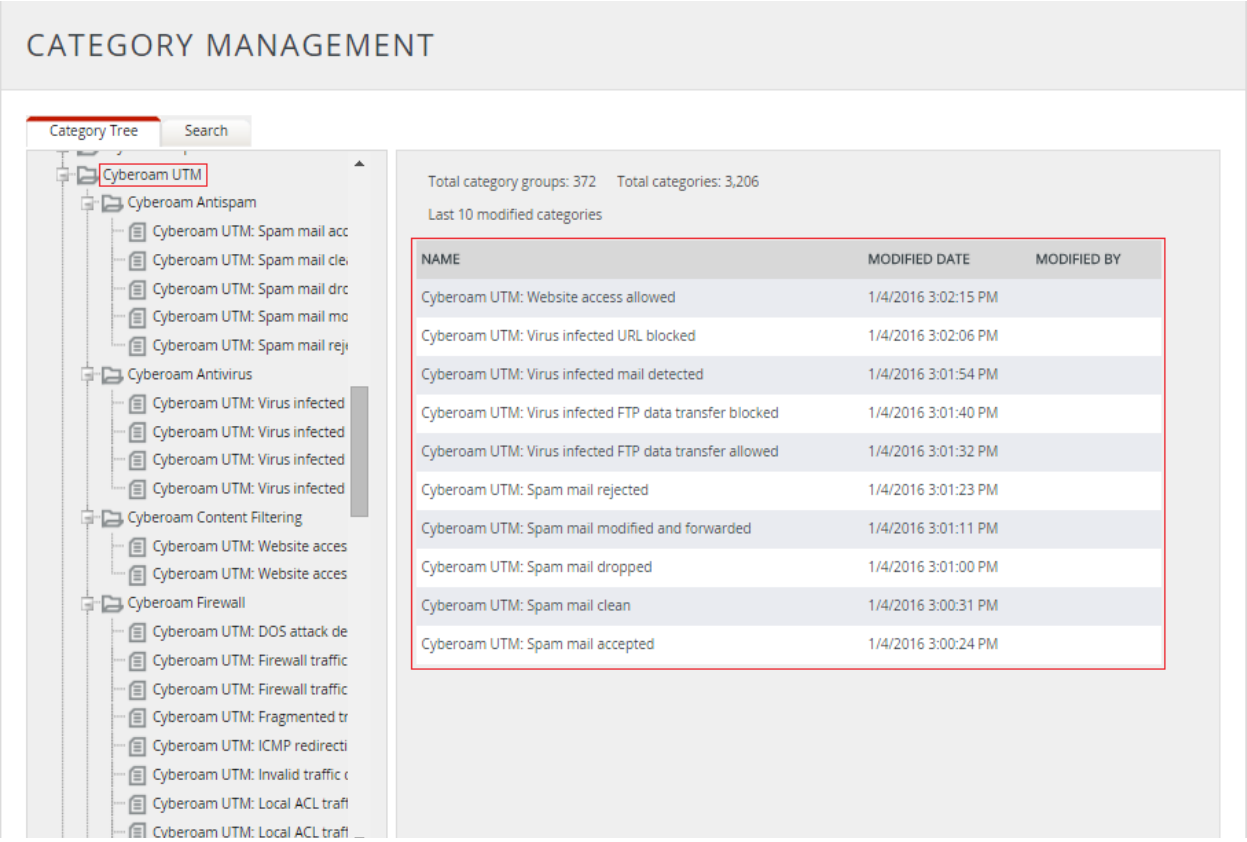

Figure 26

Verify Alerts

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

   Alert Management page will display all the imported Cyberoam UTM alerts.

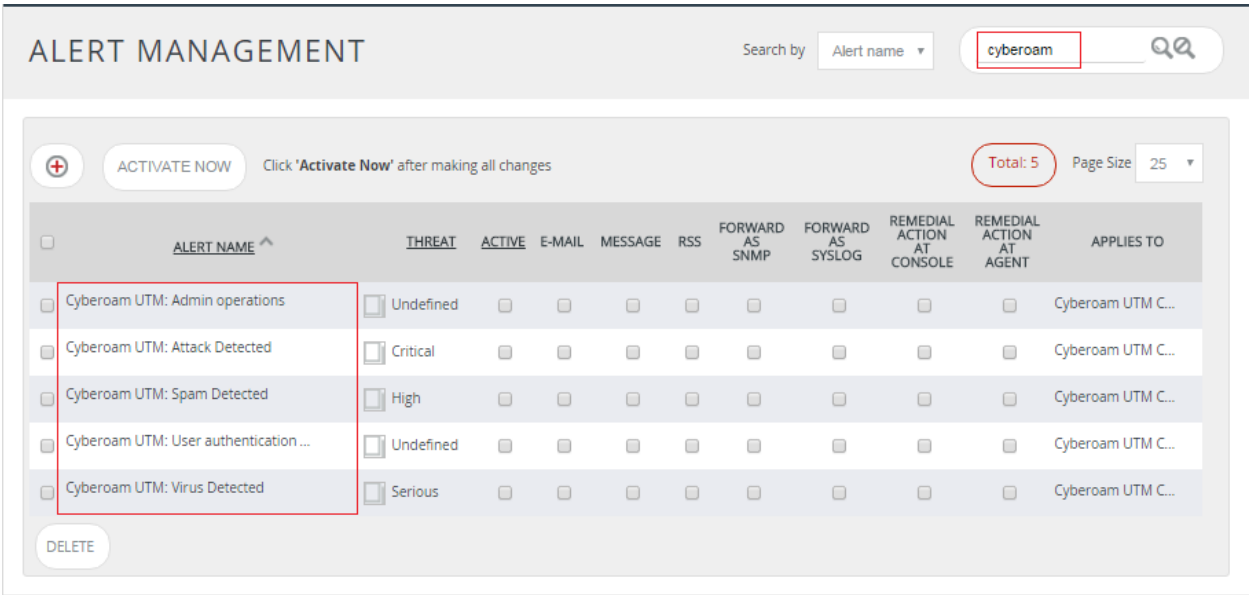

Figure 27

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

   EventTracker displays message box.

Figure 28

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.

Verifying Flex Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports**.
3. Select the **Configuration**.

   In the **Reports Configuration**, select **Defined** from radio button. **EventTracker** displays **Defined** page.
4. Click the **Cyberoam** report group.

   EventTracker displays Flex reports of Cyberoam UTM.

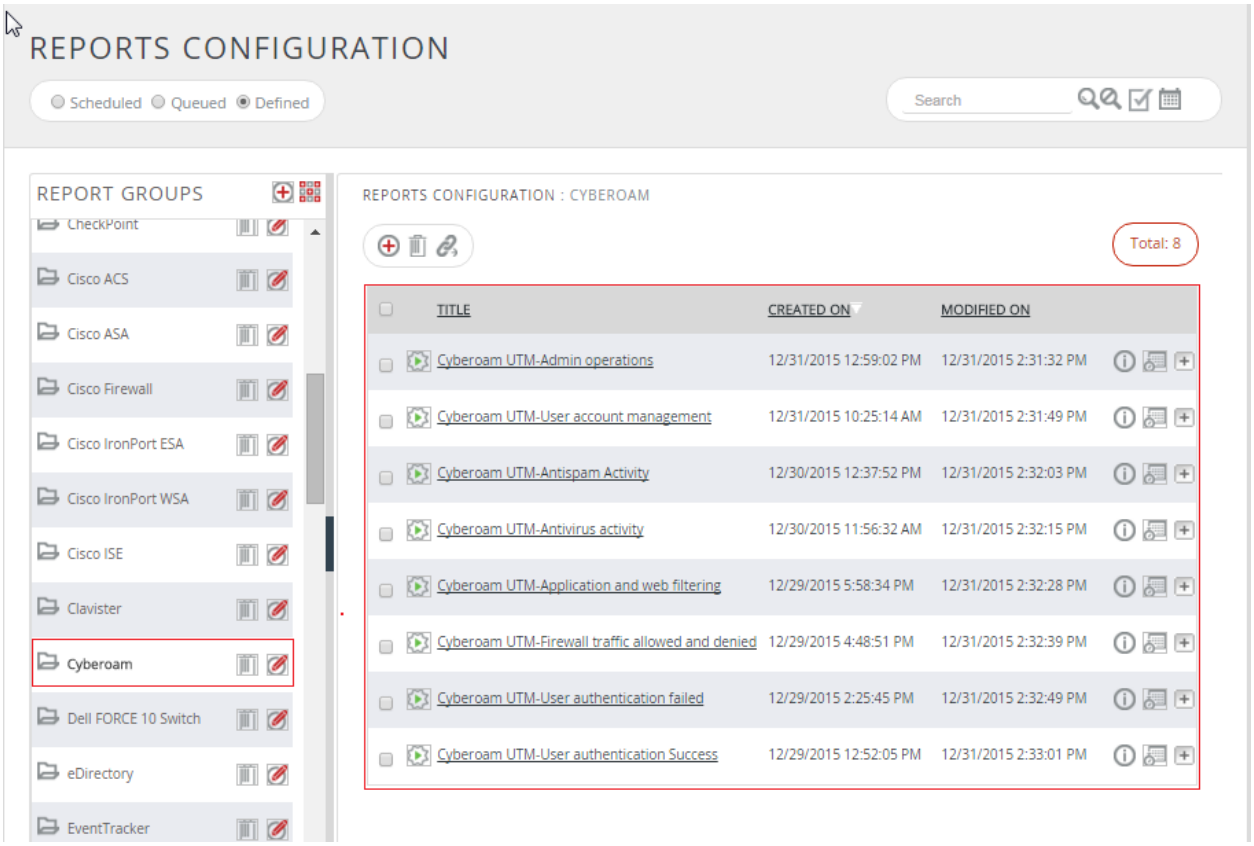

Figure 29

Verify Tokens

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

3. Imported Cyberoam UTM tokens added in Token-Value Groups list at left side of **Parsing rule** tab of EventTracker Enterprise (as shown in below figure).

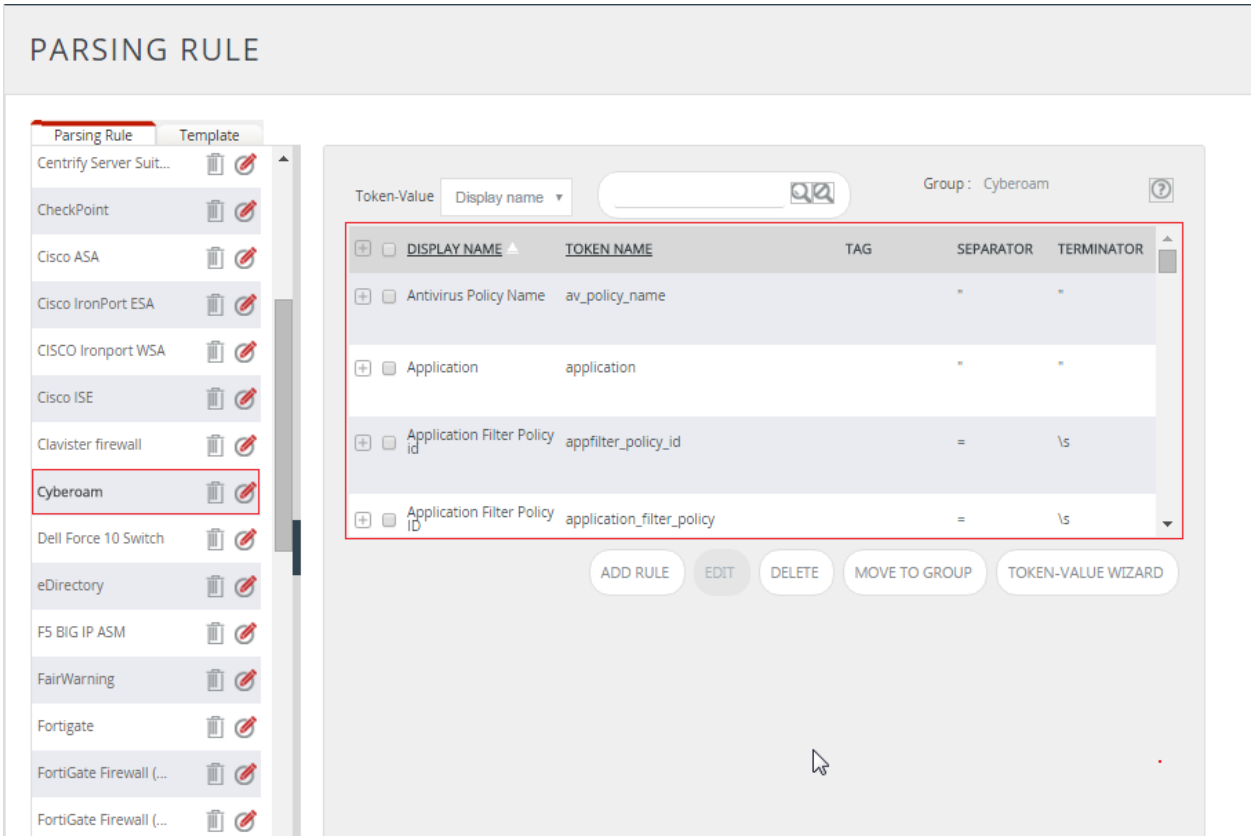

Figure 30

Verifying Template

1. Logon to **EventTracker Enterprise**, Go to **Parsing rule**.
2. Click on **Template** tab.
3. Check the template you had uploaded.

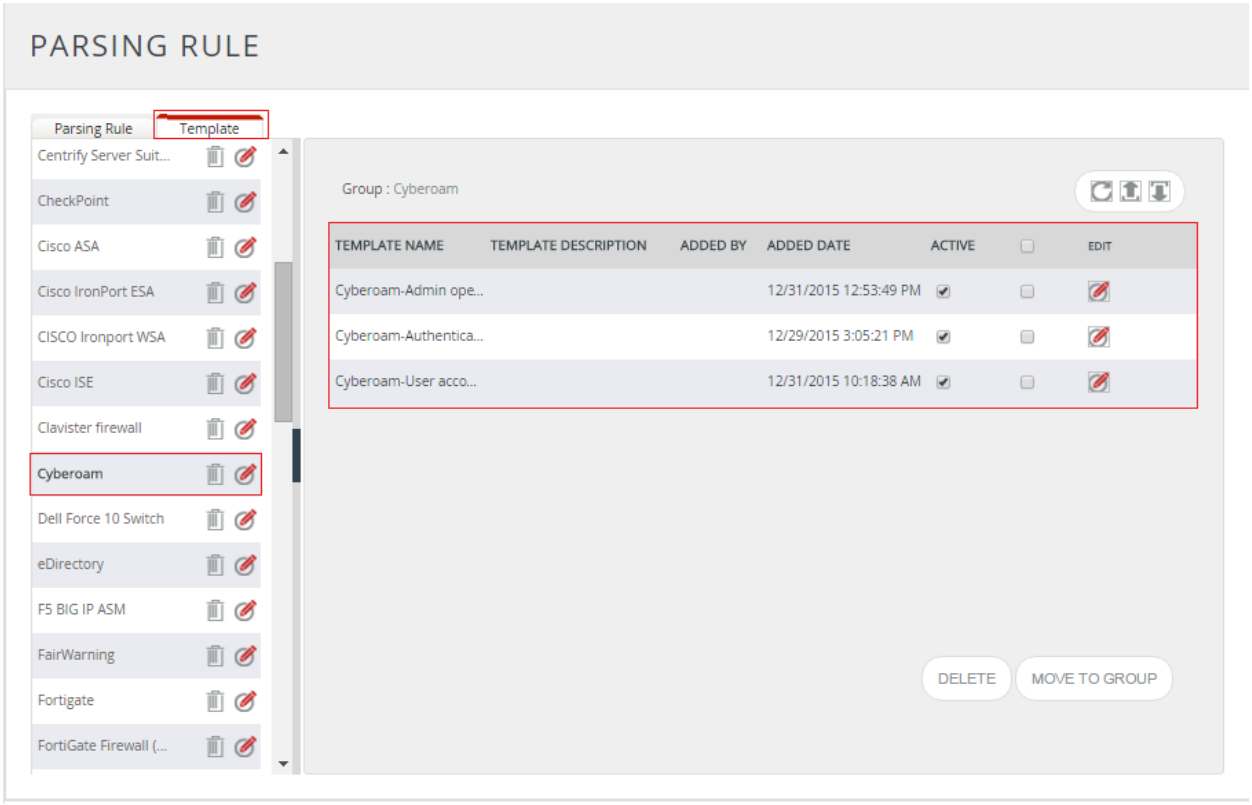

Figure 31

Verifying Knowledge Objects

1. Logon to **EventTracker Enterprise**.
2. Click on **Knowledge Object** option.

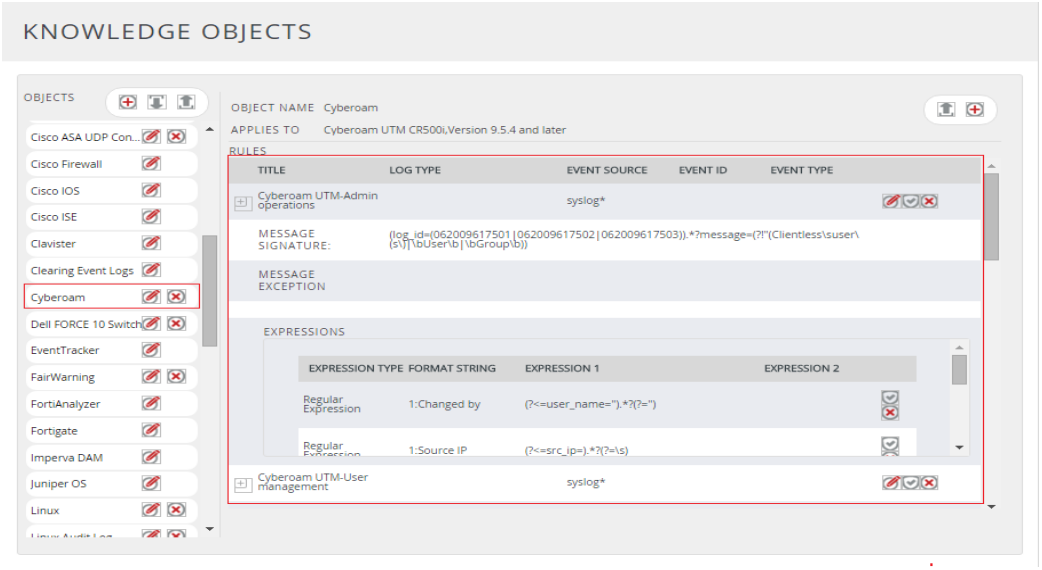

Figure 32

3. Check the Knowledge Object you had uploaded.

Sample Report

1) Cyberoam UTM-Authentication success.

Cyberoam UTM-User authentication Success

LogTime	User Name	User Group	Activity	Status	Method Used	Authentication Client	Authentication Mechanism	Reason	Source IP
12/29/2015 12:36:13 PM	john.smith	Project Leaders_grp	logged in	Successful	Firewall	SSO	LDAP		10.10.1.23
12/29/2015 12:36:13 PM	john.smith	Cyberoam General Department_grp	logged out	Successful			N/A		10.10.1.5
12/29/2015 12:38:15 PM	john.smith	Project Leaders_grp	logged in	Successful	Firewall	SSO	LDAP		10.10.1.23
12/29/2015 12:38:16 PM	john.smith	Cyberoam General Department_grp	logged out	Successful			N/A		10.10.1.5

Figure 33

2) Cyberoam UTM-Admin operations

Cyberoam-Admin operations

LogTime	Parameter	Changed By	Source IP	Status	Using
12/31/2015 10:39:38 AM	Web Filter Policy 'porn_block'	David	10.10.1.23	Successful	GUI
12/31/2015 10:39:38 AM	Log Settings	David	10.10.1.45	Successful	GUI
12/31/2015 10:39:38 AM	Firewall Rule(s)	David	10.10.1.5	Successful	GUI

Figure 34

3) Cyberoam UTM-User management

Cyberoam-User account management

LogTime	User or group	operation on	Operation	Changed By	Source IP	using	Status
12/31/2015 10:25:30 AM	Clientless user(s)		changed	David	10.10.1.45	GUI	Successful
12/31/2015 10:25:30 AM	User	john	changed	David	10.10.1.45	GUI	Successful
12/31/2015 10:25:30 AM	User	sam	deleted	David	10.10.1.5	GUI	Successful
12/31/2015 10:25:30 AM	Group	HR GROUP	added	David	10.10.1.23	GUI	Successful

Figure 35

Sample Dashboard

1) Cyberoam UTM-Top source

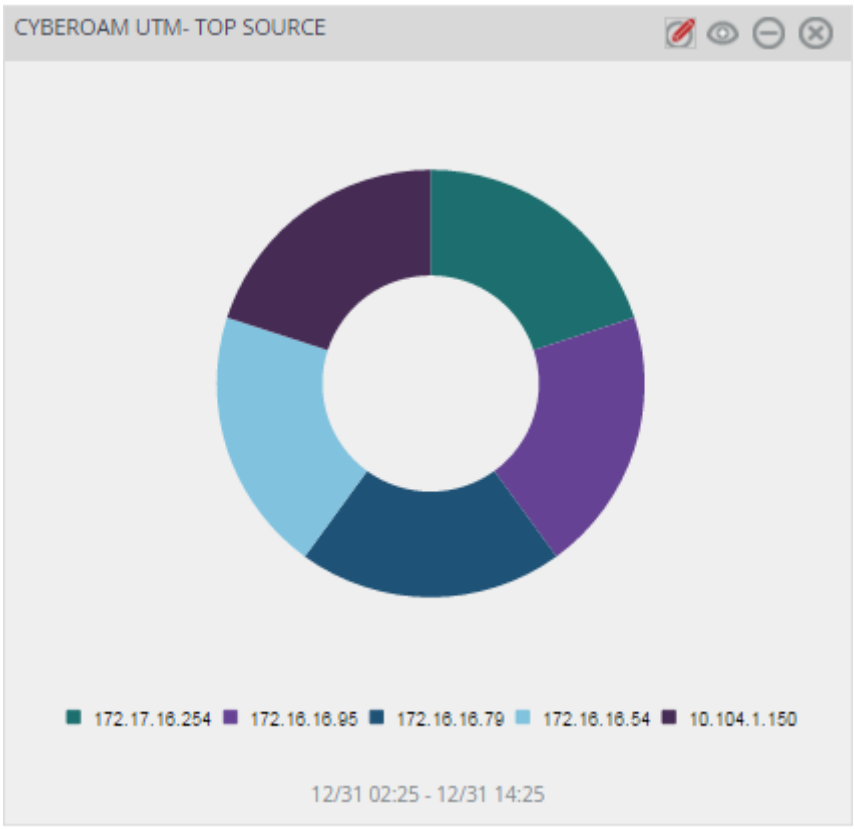

Figure 36

2) Cyberoam UTM-Top destination

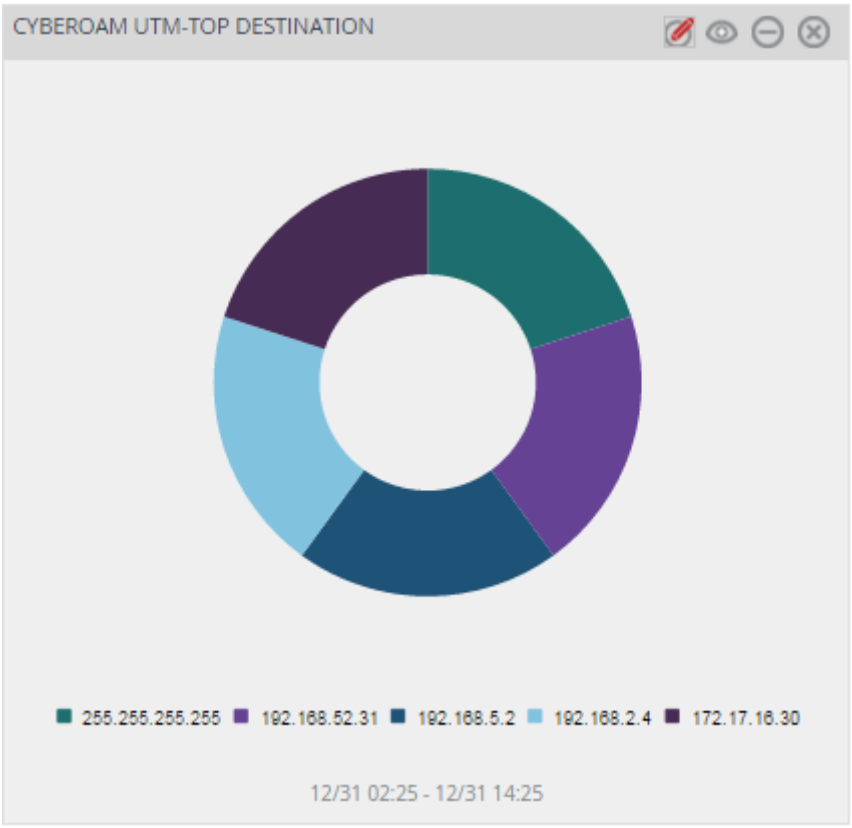

Figure 37