

# Integrating Cyberoam UTM EventTracker Enterprise

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

Publication Date: Jan 6, 2016

## 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.** 

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

Abstract	1
Intended audience	1
Scope	1
Cyberoam UTM Appliance	3
Overview	3
Pre-requisite	3
Configure Cyberoam UTM to forward all logs to EventTracker	3
Configure Syslog logging	3
EventTracker Knowledge Pack	6
Categories	6
Alerts	7
Reports	8
Dashboards	9
Import Cyberoam UTM knowledge pack into EventTracker	10
Import Category	10
Import Alerts	11
Import Flex Reports	13
Import Tokens	14
Import Template	15
Import Knowledge Object	17
Configure Flex Dashboard	19
Verify Cyberoam UTM knowledge pack in EventTracker	23
Verify Categories	23
Verify Alerts	24
Verifying Flex Reports	26
Verify Tokens	26
Verifying Template	27
Verifying Knowledge Objects	28
Sample Report	29
Sample Dashboard	30



# 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.







- 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.



Name*	Syslog
IP Address*	172.16.1.10
Port*	514
Facility*	DAEMON 👻
Severity Level*	Debug 👻
Format*	CyberoamStandardFormat -

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.

Options	Location
<ul> <li>Filters</li> </ul>	
Alerts	
Systems and Groups	Source :
RSS Feeds	-iscat
Reports	
Behavior Rules	
SCAP	
🗇 Token Value	



- 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.

Export Import Utility	×
Selected category details are imported successfully.	
ок	
Figure 4	

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

#### Import Alerts

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



Click the Import button.		
Category	Location	
) Filters	Import E-mail settings	
Alerts	Set Active	This setting is applicable only for imports from Legacy
Systems and Groups	<ul> <li>Only if notifications set</li> <li>By default</li> </ul>	(v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section
RSS Feeds		
Reports	Source :	
Behavior Rules	Jsart	
SCAP		
) Token Value		

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.

Export Import Utility	23
Selected alert configurations are imported successfully	<i>(</i> .
Ок	:
Figure 6	

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



#### Import Flex Reports

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

ort Import		
Provide the path and file name of Click the Import button	Schedule Report file. Use the '' button to browse and locate the import	ort file.
Options	ocation	
Category		
Filters		
Alerts	Legacy (*issch)      New (*.etcrx)	
Systems and Groups	Source :	
RSS Feeds	*issch	
Reports		
Behavior Rules		
SCAP		
Token Value		
	ſ	

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.





0

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

#### Import Tokens

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

🖖 Export Import Utility		
Export Import		
Export       Import         1. Provide the path and file name of t         2. Click the Import button         Options       Loc         Options       Loc         Octategory       Filters         Alerts       Systems and Groups         RSS Feeds       Reports         Behavior Rules       SCAP	oken value file. Use the '' button to browse and locate the import file.	
Token Value		
	Import	
	import	Close

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)

PARSING F	ULE								
Parsing Rule Te Barracuda Message Ar Barracuda Spam Firew	emplate	•	Group : Cyberoam						CEE
centrify	1		TEMPLATE NAME	TEMPLATE DESCRIPTION	ADDED BY	ADDED DATE	ACTIVE		EDIT
Centrify Server Suit	Ŵ Ø		Cyberoam-Admin ope			12/31/2015 12:53:49 PM	۲		0
CheckPoint	1		Cyberoam-Authentica			12/29/2015 3:05:21 PM	۲		<b>Ø</b>
Cisco ASA	Ü 🧭		Cyberoam-User acco			12/31/2015 10:18:38 AM			<b>Ø</b>
Cisco IronPort ESA	1	11							
CISCO Ironport WSA	Ê 🏉	1.							
Cisco ISE	1								
Clavister firewall	Ü 🧭								
Cyberoam	Ê Ø								
Dell Force 10 Switch	Ê 🏉						_	(C	
eDirectory	11 🧭						DELETE	MOVE	TO GROUP
F5 BIG IP ASM	Ē Ø	-							





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

C Token Template - Google Chrome	23
localhost:8080/EventTracker/Analysis/TokenTemplateImportExport.aspx?Type=Import	
SELECT FILE Choose File No file chosen	
Note: Please select file of type *.ettd (eventtracker template dashlets).	
No data found	

Figure 12

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

•	TEMPLATE NAME	SEPARATOR	TEMPLATE DESCRIPTION	ADDED DATE	ADDED BY	GROUP NAME
•	Cyberoam-Admin operations	\n	date=2013-08-07 time=13:29:20 timezone="IST" device_name="CR500ia" devic e_id= C070123456-ABCDE log_id=062009617502 log_type="Event" log_compo nent="GUI" log_subtype="Admin" status="Successful" priority=Information us er_name="David" usergroupname="open_grp" reason="" src_ip=10.10.1.45 m essage="Log Settings were changed by 'david' from '10.10.1.45' using 'GUI"	12/31/2015 12:53:49 PM		
•	Cyberoam-Authentication	١n	date=2013-08-07 time=13:37:22 timezone="IST" device_name="CR500ia" devic e_id= C070123456-ABCDE log_id=062910617701 log_type="Event" log_compo nent="Firewall Authentication" log_subtype="Authentication" status="Successf ul" priority=Information user_name="john.smith" usergroupname="Project Le aders_grp" auth_client="SSO" auth_mechanism="LDAP" reason="" src_ip=10.1 0.1.23 message="User john.smith of group Project Leaders_grp logged in succ essfully to Firewall through LDAP authentication mechanism from 10.10.1.23"	12/29/2015 3:05:21 PM		
•	Cyberoam-User account management	\n	date=2013-08-07 time=13:26:51 timezone="IST" device_name="CR500ia" devic e_id= C070123456-ABCDE log_id=062009617503 log_type="Event" log_compo nent="GUI" log_subtype="Admin" priority=Information user_name="David" us ergroupname="open_grp" status="Successful" reason="" src_ip=10.10.1.5 mes	12/31/2015 10:18:38 AM		

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.)

e		OBJECT NA	AME Cisco ASA Errors		1
Apache access log	Ø	APPLIES T	O Cisco ASA		
ArrayOS SPX	0	RULES			
Barracuda Messag	e 🧭 💌	EVDD	ESSIONS		
Barracuda SSL VPN		LAP R		(/ <code>\d+):</code>	
Centrify AD client	0		Regular Expression	-\d+:(? <message>[\w+()\s.\]+)\s</message>	$\checkmark$
Check Point	0		Regular Expression	\sinside:(? <source_ip>[\d.]+)/*(? <source_port>\d*)\sto\s\w+:(? <destination_ip>\d+)\f2</destination_ip></source_port></source_ip>	
Cisco ACE	Ø			<destination_port>\d*)\s</destination_port>	
Cisco ACS	Ø				Ŧ
Cisco ASA Errors	<b>Ø</b> 🗵				
Cisco ASA ICMP Co	n🧭 🗵				
Cisco ASA Others	<b>Ø</b> 🗵				
Cisco ASA SSL	Ø 🗵				
Cisco ASA TCP Con	n🧭 🗵				
Cisco ASA UDP Cor	n 🧭 💌				
Cisco Firewall	0				
		-			





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.

IMPORT	
Select file Choose File No file chosen	UPLOAD
OBJECT NAME	APPLIES TO
Cyberoam	Cyberoam UTM CR500i, Version 9.5.4 and later
	MERGE OVERWRITE
	Figure 17

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.

REPORT WI	ZARD		CANC	EL < BACK NEXT >
LOGS				
Review cost details and conf	igure the publishing options.		Step 8 of 10	•••••••
DISK COST ANA	LYSIS			
Estimated time for comp Number of cab(s) to be Available disk space: 29( Required disk space: 50 Enable publishing op Deliver results via E- Notify results via E-	oletion: 00:00:48(HH:MM:SS) processed: 9 5 GB MB otion (Configure SMTP Server in manage mail nail	er configuration screen to use this option)		
To E-mail		[Use comma(,) to separate multiple e-mail recipients]		
Update status via RSS	Select Feed V			
Show in	none 🔻			
Persist data in Event	vault Explorer			

Figure 19



BARRACUDA SPAM FIREWAI	L-BLOCKED MESSAGES	CANCEL	BACK
A PERSIST DETAIL			
columns to persist		Step 9 of 10	•••••
RETENTION SETTIN	G		
Retention period: 0	days		
Persist in database only SELECT COLUMNS COLUMN NAME	(Reports will not be published and will TO PERSIST PERSIST	<i>ily be stored in the respective database]</i>	*
Persist in database only SELECT COLUMNS COLUMN NAME Timestamp	(Reports will not be published and will TO PERSIST PERSIST	<i>ily be stored in the respective database]</i>	-
Persist in database only SELECT COLUMNS COLUMN NAME Timestamp Computer	Reports will not be published and will TO PERSIST PERSIST ©	<i>ily be stored in the respective database]</i>	Ĺ
Persist in database only SELECT COLUMNS COLUMN NAME Timestamp Computer From Email	Reports will not be published and will TO PERSIST PERSIST C C C C	<i>ily be stored in the respective database]</i>	Í
Persist in database only SELECT COLUMNS COLUMN NAME Timestamp Computer From Email To Email	Reports will not be published and will TO PERSIST PERSIST C C C C C C	<i>ily be stored in the respective database]</i>	Î
Persist in database only SELECT COLUMNS COLUMN NAME Timestamp Computer From Email To Email Mail Subject	Reports will not be published and will         TO PERSIST         Image: Comparison of the published and will         Image: Comparison of the	<i>ily be stored in the respective database]</i>	Î

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.

FLEX DASHBOARD
Title Cyberoam UTM Description
SAVE DELETE CANCEL





- 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].

IDGET CONFIGURATION	
WIDGET TITLE	NOTE
Cyberoam UTM- Top Application used	
DATA SOURCE	
Cyberoam-Firewall traffic allowed and denied	
CHART TYPE DURATION VALUE FIELD SETTING	AS OF Recent *
AXIS LABELS [X-AXIS] LABEL TEXT	
VALUES [Y-AXIS] VALUE TEXT	
FILTER FILTER VALUES	
LEGEND [SERIES] SELECT Status Y All Y	
Deny 3	2
	TEST CONFIGURE CLOSE



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  $^{igodold p}$  .

CUSTOMIZE WIDGETS	(† 11) 😣
Cyberoam UTM- Top Application	

#### 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.



IEGORY MANAGEME			
gory Tree Search			
Cyberoam UTM Cyberoam Antispam Cyberoam Antispam Cyberoam UTM: Spam mail acc	Total category groups: 372 Total categories: 3,206 Last 10 modified categories		
Cyberoam UTM: Spam mail clea	NAME	MODIFIED DATE	MODIFIED BY
🖳 🗐 Cyberoam UTM: Spam mail dro	Cyberoam UTM: Website access allowed	1/4/2016 3:02:15 PM	
Cyberoam UTM: Spam mail mo	Cyberoam UTM: Virus infected URL blocked	1/4/2016 3:02:06 PM	
Cyberoam OTM: Spam mail reje	Cyberoam UTM: Virus infected mail detected	1/4/2016 3:01:54 PM	
Cyberoam UTM: Virus infected	Cyberoam UTM: Virus infected FTP data transfer blocked	1/4/2016 3:01:40 PM	
Cyberoam UTM: Virus infected     Cyberoam UTM: Virus infected	Cyberoam UTM: Virus infected FTP data transfer allowed	1/4/2016 3:01:32 PM	
Gyberoam UTM: Virus infected	Cyberoam UTM: Spam mail rejected	1/4/2016 3:01:23 PM	
Cyberoam Content Filtering	Cyberoam UTM: Spam mail modified and forwarded	1/4/2016 3:01:11 PM	
Cyberoam UTM: Website acces	Cyberoam UTM: Spam mail dropped	1/4/2016 3:01:00 PM	
Cyberoam Firewall	Cyberoam UTM: Spam mail clean	1/4/2016 3:00:31 PM	
Cyberoam UTM: DOS attack de	Cyberoam UTM: Spam mail accepted	1/4/2016 3:00:24 PM	
Cyberoam UTM: Firewall traffic     Cyberoam UTM: Firewall traffic			
- 🗐 Cyberoam UTM: Fragmented tr			
🗐 Cyberoam UTM: ICMP redirecti			
- 🗐 Cyberoam UTM: Invalid traffic (			
Cyberoam UTM: Local ACI traff			

#### 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.



LERT MANAGEMENT						Search I	by Alert na	ame 🔻	cyberoar	nQQ
ACTIVATE NOW     Click 'Activate	Now' after makin	g all chanį	ges						(Total: 5	Page Size 25 🔻
ALERT NAME	THREAT	<u>ACTIVE</u>	E-MAIL	MESSAGE	RSS	FORWARD AS SNMP	FORWARD AS SYSLOG	REMEDIAL ACTION AT CONSOLE	REMEDIAL ACTION AT AGENT	APPLIES TO
Cyberoam UTM: Admin operations	Undefined									Cyberoam UTM C
Cyberoam UTM: Attack Detected	Critical									Cyberoam UTM C
Cyberoam UTM: Spam Detected	High									Cyberoam UTM C
Cyberoam UTM: User authentication	Undefined									Cyberoam UTM C
Cyberoam UTM: Virus Detected	Serious									Cyberoam UTM C
DELETE										



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

EventTracker displays message box.

	×
Successfully stund configuration	
Successfully saved configuration.	
	ОК
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.

REPORTS CO	ONFIGU	RATI	101	N			
O Scheduled O Queue	ed					Search	QQ 🛛 🗎
REPORT GROUPS	+	REPO	ORTS	CONFIGURATION : CYBEROAM			
CheckPoint		Œ	ÐÎÎ	<i>a</i>			Total: 8
Cisco ACS	1			111E			
Cisco ASA	1			<u>IIILE</u>	CREATED ON	MODIFIED ON	
Cisco Firewall				Cyberoam UTM-Admin operations	12/31/2015 12:59:02 P	M 12/31/2015 2:31:32 P	M () 🎘 🕈
			1	Cyberoam UTM-User account management	12/31/2015 10:25:14 A	M 12/31/2015 2:31:49 P	M () 🗐 Ŧ
CISCO IFONPORT ESA			1	Cyberoam UTM-Antispam Activity	12/30/2015 12:37:52 P	M 12/31/2015 2:32:03 P	M () 🗐 Ŧ
Cisco IronPort WSA	1		255	Cubaranae UTM Antiview activity	12/20/2015 11:56:22 4	M 12/21/2015 2:22:15 D	
Cisco ISE	1			<u>Cyberoam OTM-Antivirus activity</u>	12/30/2015 11:56:32 A	MI 12/31/2015 2:52:15 PI	
Clavister	III 🖉			Cyberoam UTM-Application and web filtering	12/29/2015 5:58:34 PN	/ 12/31/2015 2:32:28 P	M () 🗐 Ŧ
<b>P</b>			1	Cyberoam UTM-Firewall traffic allowed and denied	12/29/2015 4:48:51 PM	/ 12/31/2015 2:32:39 P	M () 🖉 Ŧ
Cyberoam				Cyberoam LITM-User authentication failed	12/29/2015 2·25·45 PM	/ 12/31/2015 2·32·49 P	
Dell FORCE 10 Switch	1		652	Gyber ean of the open addren dealern dilled	12.20720102.20.40 FW		
eDirectory				Cyberoam UTM-User authentication Success	12/29/2015 12:52:05 P	M 12/31/2015 2:33:01 P	M () 🖉 Ŧ
EventTracker							



## 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).

PARSING	RULE							
Parsing Rule T Centrify Server Suit	emplate	•	Token-Value Display name	v (	20	Group : Cyberoan	n 🖸	?)
Cisco ASA	i ø			TOKEN NAME	TAG	SEPARATOR	TERMINATOR	Â
Cisco IronPort ESA	Ü 🧭	i l	\pm 📄 Antivirus Policy Name	av_policy_name		-	1	
CISCO Ironport WSA	Ū Ø		+ Application	application			•	
Cisco ISE	Ü 🧭							
Clavister firewall	Ê 🏈		+ Application Filter Policy	appfilter_policy_id		=	\s	
Cyberoam	1 🧭	U	Application Filter Policy	application filter policy		=	\s	
Dell Force 10 Switch	10 🧭	11		-++				
eDirectory	1 🧭	11		ADD RULE EDIT	DELETE MOVE TO	GROUP	N-VALUE WIZARD	J
F5 BIG IP ASM	Ū 🏉							
FairWarning	Ū 🏉							
Fortigate	1							
FortiGate Firewall (	Ū 🏉				$\square$			
FortiGate Firewall (	1							



## Verifying Template

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



PARSING	RULE								
Parsing Rule	emplate								
Centrify Server Suit CheckPoint	U Ø		Group : Cyberoam						Cii
Cisco ASA	Ē Ø		TEMPLATE NAME	TEMPLATE DESCRIPTION	ADDED BY	ADDED DATE	ACTIVE		EDIT
Cisco IronPort ESA	Ü 🧭		Cyberoam-Admin ope			12/31/2015 12:53:49 PM			0
CISCO Ironport WSA	Ū Ø		Cyberoam-Authentica			12/29/2015 3:05:21 PM			<b>Ø</b>
Cisco ISE	1		Cyberoam-User acco			12/31/2015 10:18:38 AM			0
Clavister firewall	Ū Ø	Ъ.							
Cyberoam	Ü 🏉								
Dell Force 10 Switch	Ŵ								
eDirectory	1 🧭								
F5 BIG IP ASM	Ŵ								
FairWarning	1 🧭						DELETE	MOVE	TO CROUP
Fortigate	Ŵ Ø						DELETE	MOVE	TO GROUP
FortiGate Firewall (	Ē 🏈								

Figure 31

#### Verifying Knowledge Objects

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

KNOWL	EDGE	OBJECT	<sup>S</sup>						
DBJECTS	• • •	OBJECT N	AME Cyberoam					C	L 🛨
Cisco ASA UDP Co	on 🧭 💌	APPLIES T	O Cyberoam	UTM CR500i,Version 9.5.	4 and later				
Cisco Firewall	0	TITLE		LOG TYPE	EVENT SOURCE	EVENT ID	EVENT TYPE		-
Cisco IOS	0	Cyber	oam UTM-Admin		syslog*				
Lisco ISE	0	D opera	tions		-70				
Clavister	0	MESS SIGN	MESSAGE (log_id=(062009617501 062009617502 062009617503)).*?message=(?!"(Clientless\suser\ SIGNATURE: (s\) \bUser\b \bGroup\b))						
Elearing Event Lo	gs 🧭	MESS	AGE						
yberoam	<b>Ø</b> 🗵	EXCE	PTION						
Dell FORCE 10 Sw	vitch 🧭 💌	EXP	RESSIONS						
eventTracker	Ø	-							-
airWarning	<b>Ø</b> 🗵		EXPRESSION	TYPE FORMAT STRING	EXPRESSION 1		EXPRESSION 2		
ortiAnalyzer	0		Regular Expression	1:Changed by	(?<=user_name=").*?(?=")			<b>×</b>	
Fortigate	0		Regular						-
mperva DAM	0		Everession	1:Source IP	(?<=src_ip=).*?(?=\s)			10	-
uniper OS	Ø	± Cyber mana	oam UTM-User gement		syslog*			<b>8</b> .	
.inux	<b>Ø</b> 🗵								
Linux Audit Los	<b>7</b>	-							

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_gr	p 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_gr	p 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

