

Integrate Riverbed SteelHead

EventTracker v8.x and above

Abstract

This guide provides instructions to configure a **Riverbed SteelHead** to send its syslog to EventTracker Enterprise

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version v8.x or above and Riverbed SteelHead CX series.

Audience

Administrators, who are assigned the task to monitor Riverbed SteelHead 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
Integration of Riverbed SteelHead with EventTracker manager	3
Configuring Log Delivery	3
EventTracker Knowledge Pack.....	4
Flex Reports	4
Alerts	8
Categories	8
Knowledge Objects.....	9
Import Riverbed SteelHead knowledge pack into EventTracker.....	9
Category	10
Alerts	11
Token Templates	12
Knowledge Objects.....	13
Flex Reports	14
Verify Riverbed SteelHead knowledge pack in EventTracker.....	16
Categories	16
Alerts	16
Token Template.....	17
Knowledge Objects.....	17
Flex Reports	18
Create Dashlets.....	19
Sample Flex Dashboards	22

Overview

The Riverbed SteelHead CX/GX solution accelerates the performance of all applications including on-premise, cloud, and software-as-a-service (SaaS) across the hybrid WAN for organizations.

EventTracker helps to monitor events from Riverbed SteelHead. It's knowledge object and flex reports will help you to analyze critical activities and to monitor login events.

Prerequisites

- EventTracker v8.x or above should be installed.
- Riverbed SteelHead CX should be configured for forwarding logs.
- Please add exception for port 514 in firewall if exists in between Riverbed SteelHead CX and EventTracker Manager.

Integration of Riverbed SteelHead with EventTracker manager

Configuring Log Delivery

To configure a Riverbed SteelHead to forward logs to a syslog server,

1. Log on to the Riverbed Steelhead Management Console.
2. From Web GUI choose **Administration**.
3. Select **System Settings** and **Logging** to display the Logging page.
4. Under the **Remote Log Servers** section.
5. Click **Add a New Log Server**.
6. For **Server IP**, type in the IP address of the **EventTracker Manager**.
7. For **Minimum Severity**, choose info.
8. Click **Add**.
9. Click **Save to Disk** to save your settings permanently.

Logging ⓘ

Logging Configuration

Minimum Severity: (applies only to system log)

Maximum Number of Log Files:

Lines Per Log Page:

Rotate Based On:

Time:

Disk Space: MBytes

Apply

Remote Log Servers:

Add a New Log Server Remove Selected

<input type="checkbox"/>	Remote Log Server	Minimum Severity
<input type="checkbox"/>	10.1.10.200	info

Log Actions

Rotate Logs

Per-Process Logging:

Add a New Process Logging Filter Remove Selected

<input type="checkbox"/>	Description	Process	Minimum Severity
<input type="checkbox"/>	QoS classification	qosd	info

Figure 1

EventTracker Knowledge Pack

Once logs are received by EventTracker manager, knowledge packs can be configured into EventTracker. The following Knowledge Packs are available in EventTracker Enterprise to support Riverbed SteelHead.

Flex Reports

- **Riverbed SteelHead - Login Activities** - This report gives information about user login activities.

LogTime	Computer	Username	Action	Client IP Address
02/13/2018 05:18:41 PM	RIVERBED	admin	launched	10.18.31.63
43144.72135	RIVERBED	admin	launched	10.18.31.65
02/13/2018 05:18:46 PM	RIVERBED	admin	launched	10.18.31.63

Figure 2

Sample logs:

2/13/2018 5:16:23 PM	3333	NTPLDTBLR38 / riverb...	N/A	N/A	syslog
Event Type: Information	Description: sep 13 01:19:21 il-cowsh cli[29557]: [cli.NOTICE]: user admin: CLI launched for user admin and rbm admin [web.NOTICE]: web: user admin logged in from 10.18.31.63, session count:2. [cli.NOTICE]: user admin: CLI exiting				
Log Type: Application					
Category Id: 0					

Figure 3

- **Riverbed SteelHead - Command Executed** - This report gives information about commands executed by

LogTime	Computer	Username	Executed Command
02/13/2018 05:18:41 PM	RIVERBED	admin	scp -f /config/db/lanai-fps
43144.72131	RIVERBED	admin	enable
02/13/2018 05:18:41 PM	RIVERBED	admin	loggig test
43144.72131	RIVERBED	admin	scp -f /config/db/lanai-fps
02/13/2018 05:18:41 PM	RIVERBED	admin	enable 15

users.

Figure 4

Sample logs:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
2/13/2018 5:16:23 PM	3333	NTPLDTBLR38 / riverb...	N/A	N/A	syslog
Event Type: Information	Description: cli[29557]: [cli.INFO]: user admin: Executing remote command: scp -f /config/db/lanai-fps				
Log Type: Application					
Category Id: 0					

Figure 5

- **Riverbed SteelHead - Suspicious IP Activity** - This report gives information about IP addresses which were added or removed from white list, gray list.

LogTime	Computer	Source IP Address	Action	List Type
03/14/2018 12:33:31 PM	RIVERBED_STEELHEAD	192.55.54.53	removing	white list
03/14/2018 12:33:31 PM	RIVERBED_STEELHEAD	192.55.54.53	removing	white list
03/14/2018 12:33:39 PM	RIVERBED_STEELHEAD	192.55.54.53	removing	white list
03/14/2018 12:33:39 PM	RIVERBED_STEELHEAD	192.55.54.53	removing	white list

Figure 6

Sample logs:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
2/13/2018 5:16:23 PM	3333	NTPLDTBLR38 / rherb...	N/A	N/A	syslog

Event Type: Information
 Log Type: Warning
 Category Id: 0

Description:
 Jan 24 12:13:39 198.1.1.1 Jan 24 12:13:39 drcrs mgmt[8016]: [mgmt.WARNING]: Peer 198.1.1.1 is currently trusted in the white list, but it is now using a new not-yet-trusted certificate. Consider removing its likely outdated white list entry.

Figure 7

- **Riverbed SteelHead - Blacklist IP Activity** - This report gives information about IP addresses which were added to Black List.

LogTime	Computer	Source IP Address	Source Port	Destination IP Address	Destination Port	Action	Reason
03/14/2018 12:33:31 PM	RIVERBED_STEELHEAD	192.168.27.10	50755	192.168.10.21	445	black list	Unable to decode authblob.
03/14/2018 12:33:31 PM	RIVERBED_STEELHEAD	192.168.10.21	57444	192.168.26.140	139	black list	Unknown reason. Status code: ERROR_SMBSIGNX_ACCESS_DENIED (0xc0000022)
03/14/2018 12:33:31 PM	RIVERBED_STEELHEAD	192.168.225.212	62844	192.168.190.5	445	black list	Generic user authentication error.
03/14/2018 12:33:31 PM	RIVERBED_STEELHEAD	192.168.25.9	55093	192.168.10.21	139	blacklisted	by SMB2 blade, shutting down the signing blade
03/14/2018 12:33:31 PM	RIVERBED_STEELHEAD	192.168.229.208	53688	192.168.27.16	445	black list	User in different domain.
03/14/2018 12:33:38 PM	RIVERBED_STEELHEAD	192.168.25.9	55093	192.168.10.21	139	blacklisted	by SMB2 blade, shutting down the signing blade

Figure 8

Sample logs:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
2/13/2018 5:16:23 PM	3333	NTPLDTBLR38 / rherb...	N/A	N/A	syslog

Event Type: Information
 Log Type: Application
 Category Id: 0

Description:
 Jan 24 01:10:49 198.1.1.1 Jan 24 01:10:49 drcrs sport[10173]: [smbmux_cfe.NOTICE] 89065360 {198.1.1.1:34742 198.1.1.1:445} SMB2 parser not being created: connection blacklisted for SMB2.

Figure 9

- **Riverbed SteelHead - Authentication Failure** - This report gives information about user's authentication failure.

LogTime	Computer	Client User Name	Source IP Address	Source Port	Destination IP Address	Destination Port	Error Code	Reason
03/14/2018 12:33:31 PM	RIVERBED_STEELHEAD	DOMRFWWSED2NWOSUBENS\$	192.168.229.208	64788	192.168.26.15	445	3221225572	No such user
03/14/2018 12:33:39 PM	RIVERBED_STEELHEAD	DOMRFWWSED2NWOSUBENS\$	192.168.229.208	64788	192.168.26.15	445	3221225572	No such user
03/14/2018 12:33:42 PM	RIVERBED_STEELHEAD	DOMRFWWSED2NWOSUBENS\$	192.168.229.208	64788	192.168.26.15	445	3221225572	No such user
03/14/2018 12:33:44 PM	RIVERBED_STEELHEAD	DOMRFWWSED2NWOSUBENS\$	192.168.229.208	64788	192.168.26.15	445	3221225572	No such user
03/14/2018 12:33:47 PM	RIVERBED_STEELHEAD	DOMRFWWSED2NWOSUBENS\$	192.168.229.208	64788	192.168.26.15	445	3221225572	No such user
03/14/2018 12:33:49 PM	RIVERBED_STEELHEAD	DOMRFWWSED2NWOSUBENS\$	192.168.229.208	64788	192.168.26.15	445	3221225572	No such user

Figure 10

Sample logs:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
2/13/2018 5:16:23 PM	3333	NTPLDTBLR38 / rherb...	N/A	N/A	syslog

Event Type: Information
 Log Type: Warning
 Category Id: 0

Description:
 Mar 02 11:48:34 rb-nor3070l Mar 2 11:48:34 RB-NORCX3070L sport[13508]: [authlibs/wb_comm/ntlmauth.WARN] 1350541 {192.168.229.208:64788 192.168.26.15:445} NTLM Auth Failed for user: DOMRFBW\WSED2NWOSUBEN\$ NT status string: NT_STATUS_NO_SUCH_USER
 Code: 3221225572 message: No such user

Figure 11

- **Riverbed SteelHead - Traffic Allow Details-** This report gives information about allowed traffic.

LogTime	Computer	Source IP Address	Destination IP Address
03/14/2018 12:33:31 PM	RIVERBED_STEELHEAD	192.55.54.53	192.55.54.53
03/14/2018 12:33:39 PM	RIVERBED_STEELHEAD	192.55.54.53	192.55.54.53
03/14/2018 12:33:42 PM	RIVERBED_STEELHEAD	192.55.54.53	192.55.54.53
03/14/2018 12:33:44 PM	RIVERBED_STEELHEAD	192.55.54.53	192.55.54.53
03/14/2018 12:33:46 PM	RIVERBED_STEELHEAD	192.55.54.53	192.55.54.53

Figure 12

Sample logs:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
2/13/2018 5:16:23 PM	3333	NTPLDTBLR38 / rherb...	N/A	N/A	syslog

Event Type: Information
 Log Type: Warning
 Category Id: 0

Description:
 Mar 02 11:08:12 rb-wccx5070 Mar 2 11:08:12 RB-WCCX5070 kernel: [intercept.WARN] it appears as though probes from 192.168.1.7 to 192.1.1.1 are being filtered. Passing through connections between these two hosts.

Figure 13

- **Riverbed SteelHead - Traffic Deny Details -** This report gives information about denied traffic.

LogTime	Computer	Source IP Address	Source Port	Destination IP Address	Destination Port	Reason
03/14/2018 12:33:31 PM	RIVERBED_STEELHEAD	192.168.229.208	61648	192.168.28.92	445	User possibly belongs to a different domain.
03/14/2018 12:33:31 PM	RIVERBED_STEELHEAD	192.168.229.208	64968	192.168.169.6	445	User possibly belongs to a different domain.
03/14/2018 12:33:42 PM	RIVERBED_STEELHEAD	192.168.229.208	61648	192.168.28.92	445	User possibly belongs to a different domain.
03/14/2018 12:33:42 PM	RIVERBED_STEELHEAD	192.168.229.208	64968	192.168.169.6	445	User possibly belongs to a different domain.
03/14/2018 12:33:39 PM	RIVERBED_STEELHEAD	192.168.229.208	61648	192.168.28.92	445	User possibly belongs to a different domain.
03/14/2018 12:33:39 PM	RIVERBED_STEELHEAD	192.168.229.208	64968	192.168.169.6	445	User possibly belongs to a different domain.

Figure 14

Sample logs:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
2/13/2018 5:16:23 PM	3333	NTPLDTBLR38 / riverb...	N/A	N/A	syslog
Event Type: Information		Description:			
Log Type: Warning		Mar 02 11:49:13 rb-dtxcx770h Mar 2 10:49:13 RB-DTXCX770H sport[8898]: [sskclient.NOTICE] 3044167 {192.12.1.169:63457 192.1.24.2:443}			
Category Id: 0		Dropping connection			

Figure 15

Alerts

- **Riverbed SteelHead: Blacklist IP Activity** - This alert will generate when an IP address is added to the blacklist.
- **Riverbed SteelHead: Login Activity Detected** - This alert will generate when a user logs on to the Riverbed SteelHead device through cli or web.
- **Riverbed SteelHead: CPU Load High** - This alert will generate when the CPU usage of a process is constantly high.
- **Riverbed SteelHead: Authentication Failure** - This alert will generate when the user request fails authentication.

Categories

- **Riverbed SteelHead: Suspicious IP Activity**- This category based report provides information related to IP addresses which were added or removed from white list, gray list.
- **Riverbed SteelHead: CPU Load Status** – This category based report provides information related to the CPU load status details.
- **Riverbed SteelHead: Command Executed**– This category based report provides information related to the commands executed by the users.
- **Riverbed SteelHead: User Login Activities**– This category based report provides information related to the user login activities.
- **Riverbed SteelHead: Authentication Failure**- This category based report provides information related to the user’s authentication failure.
- **Riverbed SteelHead: Blacklist IP Activity**- This category based report provides information related to the IP addresses which were added to Black List.
- **Riverbed SteelHead: Traffic Allow Details**- This category based report provides information related to the traffic allowed details.
- **Riverbed SteelHead: Traffic Deny Details**- This category based report provides information related to the traffic denied details.

Knowledge Objects

- **Riverbed SteelHead User Login Activities** – This knowledge object helps to analyze logs related to user logon details.
- **Riverbed SteelHead Command Executed** – This knowledge object helps to analyze logs related to commands executed by users.
- **Riverbed SteelHead CPU Load Status** – This knowledge object helps to analyze logs related to the CPU load status.
- **Riverbed SteelHead Suspicious IP Activity** – This knowledge object helps to analyze logs related to the IP addresses which were added or removed from white list, gray list.
- **Riverbed SteelHead Blacklist IP Activity** – This knowledge object helps to analyze logs related to IP addresses which were added to black list.
- **Riverbed SteelHead Authentication Failure** - This knowledge object helps to analyze logs related to user authentication failure.
- **Riverbed SteelHead Traffic Allow Details** - This knowledge object helps to analyze logs related to traffic allow details.
- **Riverbed SteelHead Traffic Deny Details** - This knowledge object helps to analyze logs related to traffic deny details.

Import Riverbed SteelHead knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
 - Alerts
 - Token templates
 - Knowledge Objects
 - Flex Reports
1. Launch **EventTracker Control Panel**.
 2. Double click **Export Import Utility**.

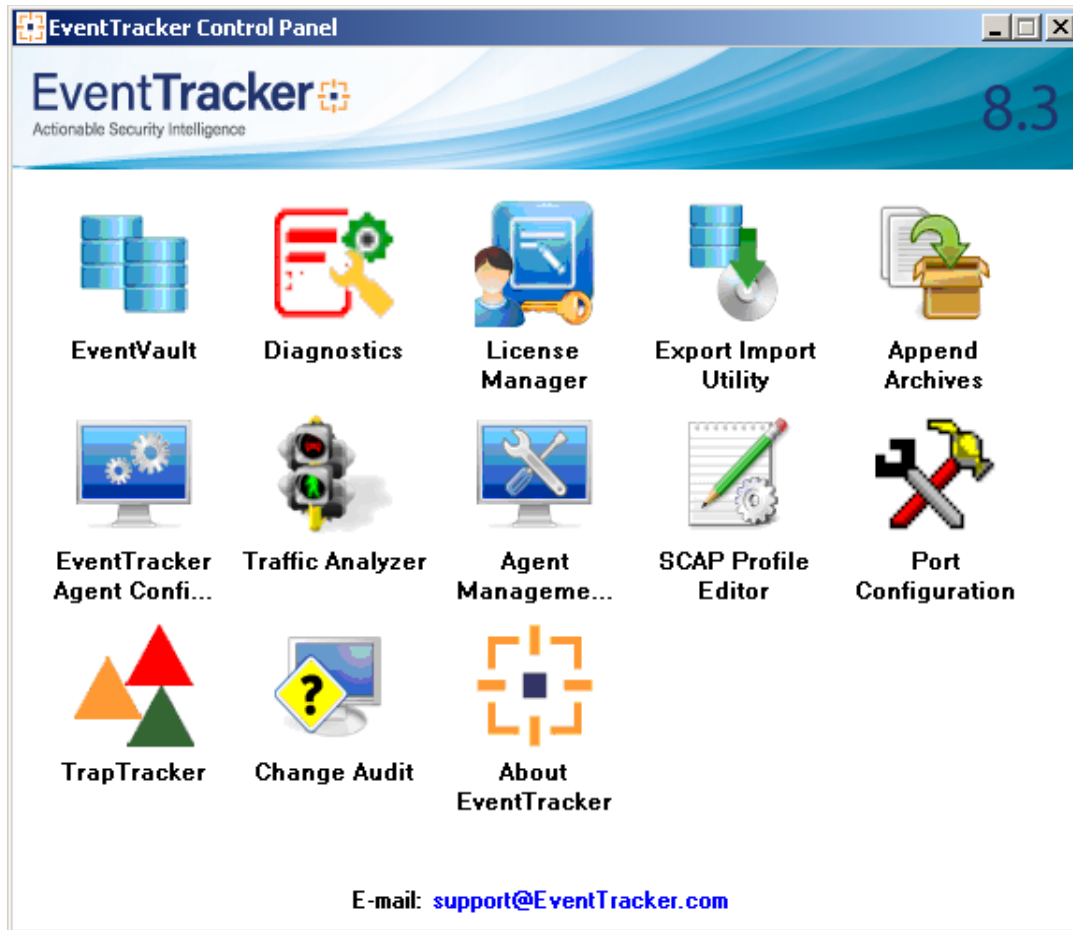



Figure 16

3. Click the **Import** tab.

Category

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

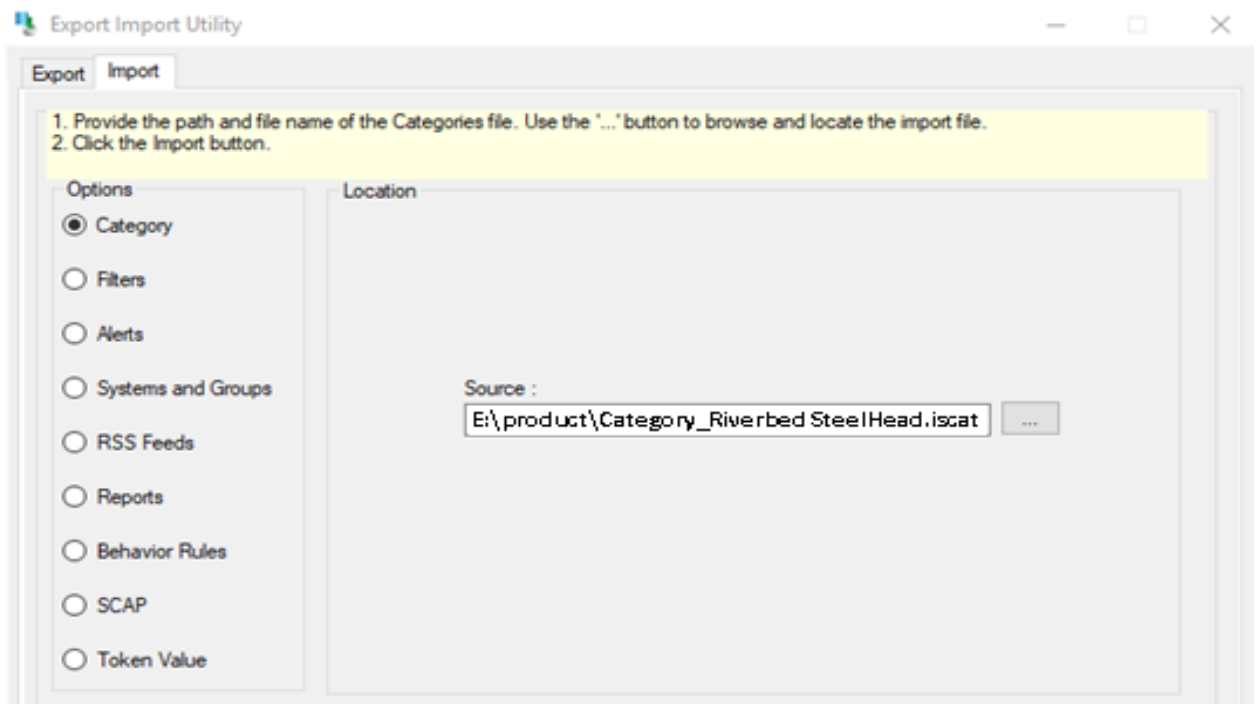


Figure 17

2. Locate .iscat file, and then click the **Open** button.
3. To import categories, click the **Import** button.

EventTracker displays success message.

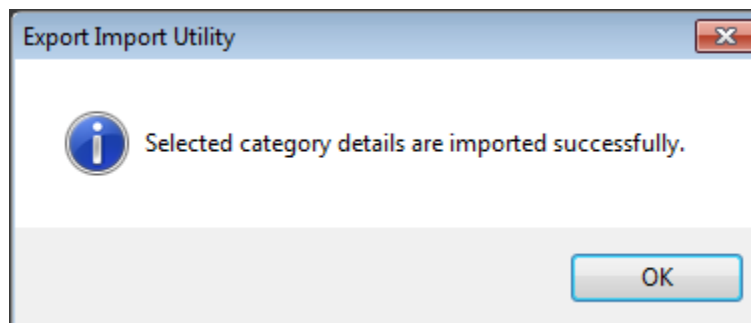



Figure 18

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

Alerts

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

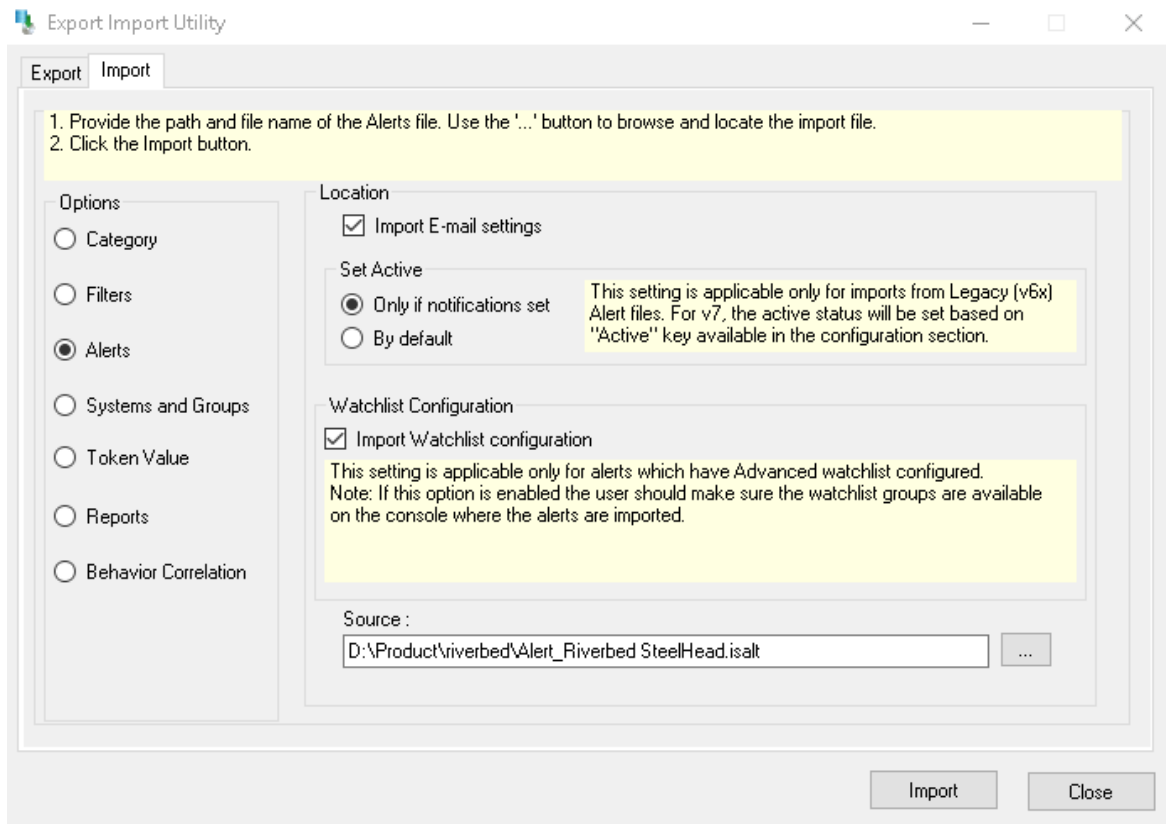




Figure 19

2. Locate **Alert_Riverbed SteelHead.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

Token Templates

1. Click **Parsing rules** under **Admin** option in the EventTracker manager page.
2. Move to **Template** and click on import configuration  icon on the top right corner.
3. In the popup window browse the file named **TokenTemplate_Riverbed SteelHead.ett**.
4. Now select all the check box and then click on  Import option.

SELECTED FILE IS: Token_Riverbed_SteelHead.ettd

<input type="checkbox"/>	TEMPLATE NAME	SEPARATOR	TEMPLATE DESCRIPTION	ADDED DATE	ADDED BY	GROUP NAME
<input type="checkbox"/>	Riverbed_SteelHead Command Executed	\n	cli[29557]: [cli\NFO]: user admin: Executing remote command: scp -f /config/db/1 ana1-fps	2/9/2018 12:55:25 PM	ETAdmin	Riverbed_SteelHead
<input type="checkbox"/>	Riverbed_SteelHead Login Activites	\n	[web.NOTICE]: web: user admin logged in from 10.18.31.63, session count:2.	2/8/2018 12:45:42 PM	ETAdmin	Riverbed_SteelHead
<input type="checkbox"/>	Riverbed_SteelHead Peer Trust List	\n	Jan 24 12:49:37 172.268.58 Jan 24 12:49:37 caers sport[13018]: [smb2cfe.WARN] 609 955148 [172.168.22.149/84 172.89.4.28/445] Adding blacklist entry for pair Client ip: 1 72.168.22.149 Server ip: 172.89.4.28. Reason: Client is performing secure protocol ne gotiation, SteelHead was unable to sign the connection	2/8/2018 4:51:38 PM	ETAdmin	Riverbed_SteelHead

Figure 20


Knowledge Objects

1. Click **Knowledge objects** under Admin option in the EventTracker manager page.
2. Locate the file named **KO_Riverbed SteelHead.etko**.

IMPORT

Select file KO_Riverbed SteelHead.etko

Figure 21

3. Now select all the check box and then click on  **'Import'** option.

<input checked="" type="checkbox"/>	OBJECT NAME	APPLIES TO	GROUP NAME
<input checked="" type="checkbox"/>	Riverbed SteelHead User Login Activities	Riverbed SteelHead CX series	Riverbed SteelHead
<input checked="" type="checkbox"/>	Riverbed SteelHead Command Executed	Riverbed SteelHead CX series	Riverbed SteelHead
<input checked="" type="checkbox"/>	Riverbed SteelHead CPU Load Status	Riverbed SteelHead CX series	Riverbed SteelHead
<input checked="" type="checkbox"/>	Riverbed SteelHead Peer Trust List	Riverbed SteelHead CX series	Riverbed SteelHead

Figure 22

4. Knowledge objects are now imported successfully.

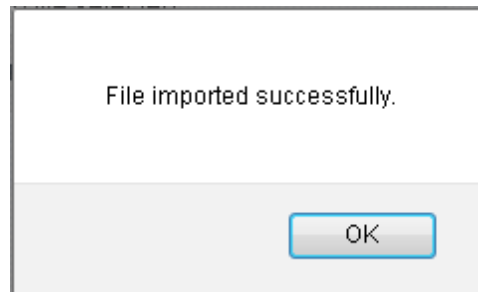


Figure 23

Flex Reports

On EventTracker Control Panel,

1. Click **Reports** option, and select new(etcrx) from the option.

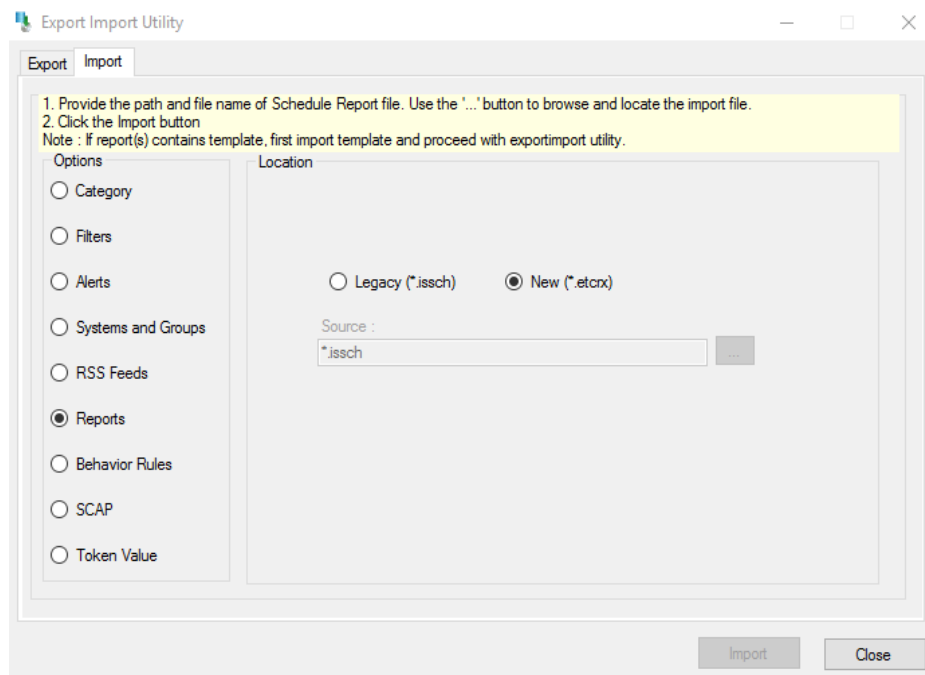


Figure 24

2. Locate the file named **FlexReports_ Riverbed SteelHead.etcrx**, and select all the check box.

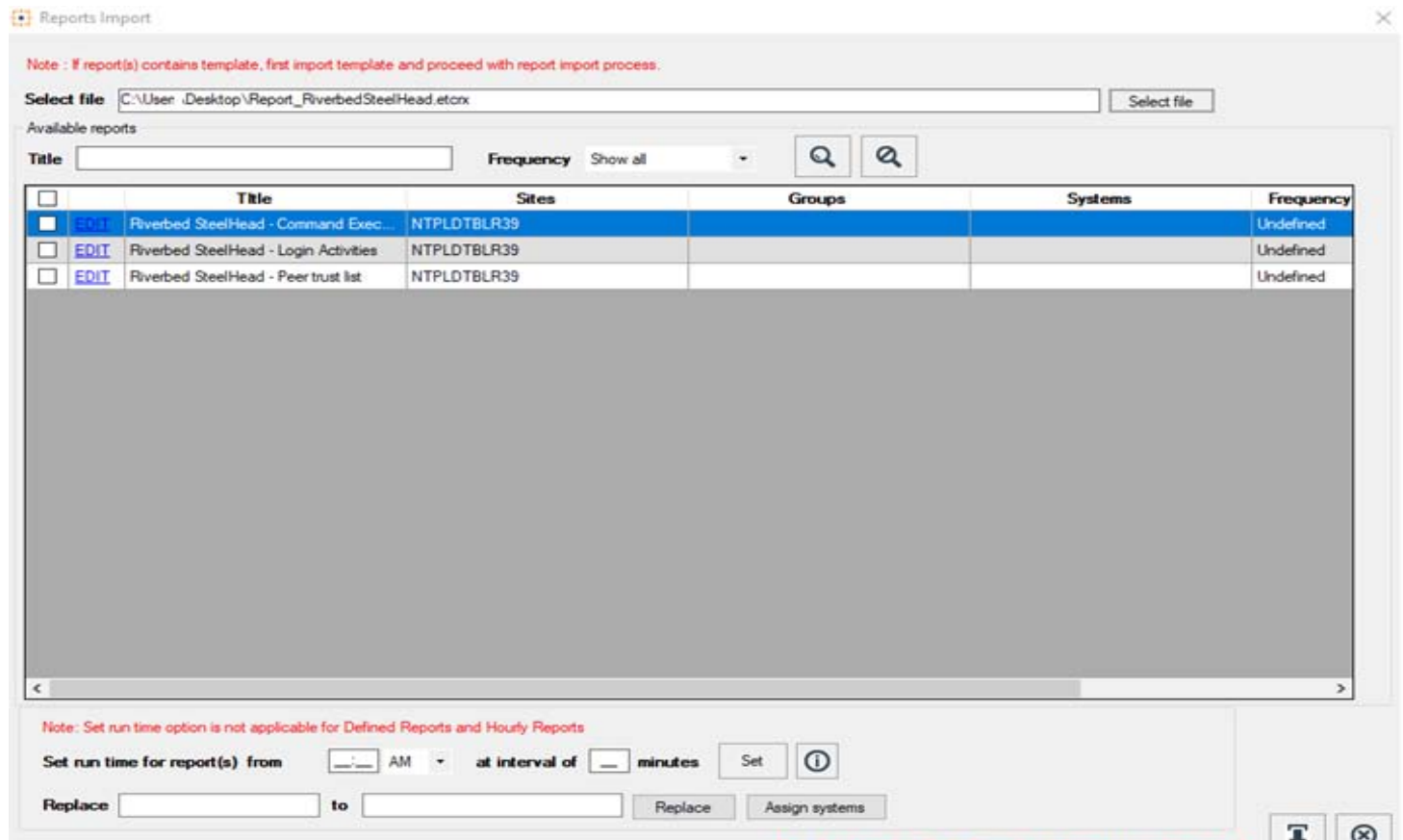


Figure 25

3. Click the **Import** button to import the reports. EventTracker displays success message.

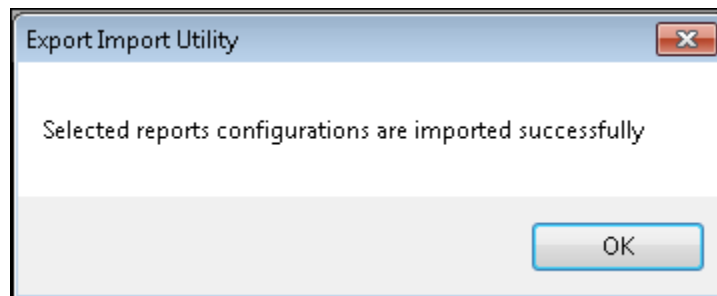


Figure 26

Verify Riverbed SteelHead knowledge pack in EventTracker

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 Riverbed SteelHead group folder to view the imported categories.

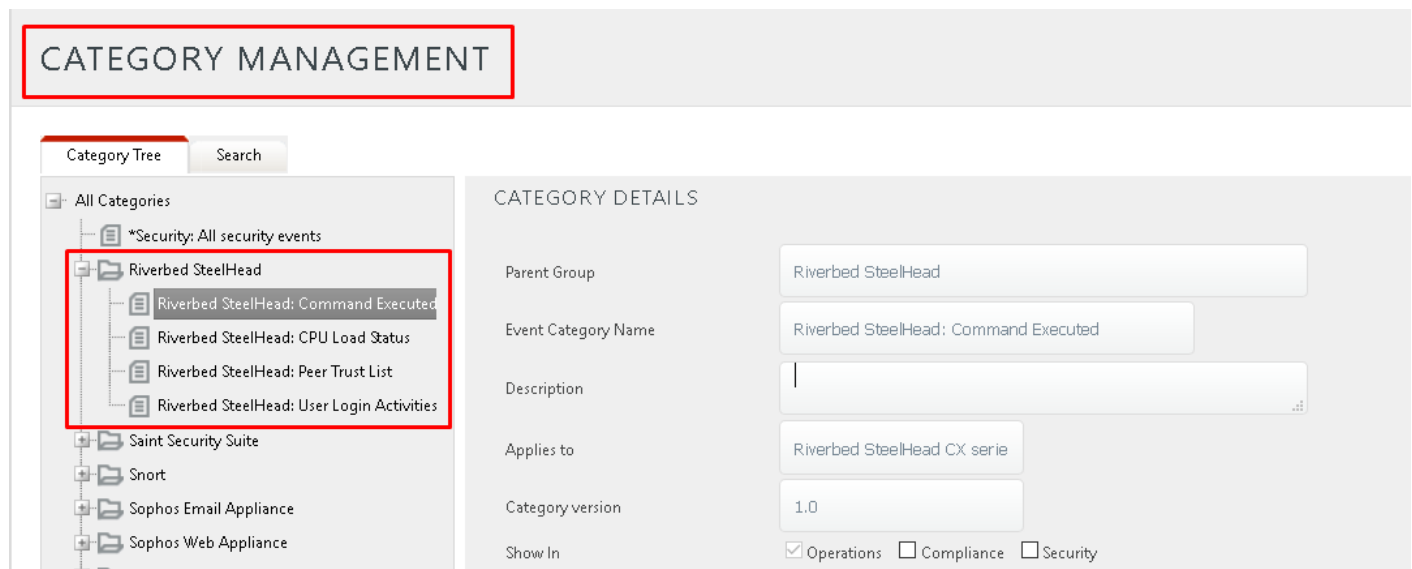


Figure 27

Alerts

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Alerts**.
2. In search box enter **Riverbed SteelHead** and then click the **Search** button.

EventTracker displays alert of **Riverbed SteelHead**.

ALERT MANAGEMENT

Show All Search by Alert name Riverbed SteelHead

ACTIVATE NOW Click 'Activate Now' after making all changes Total: 3 Page Size 25

<input type="checkbox"/>	ALERT NAME ^	THREAT	ACTIVE	E-MAIL	MESSAGE	RSS	FORWARD AS SNMP	FORWARD AS SYSLOG	REMEDIAL ACTION AT CONSOLE	REMEDIAL ACTION AT AGENT	APPLIES TO
<input type="checkbox"/>	Riverbed SteelHead: CPU Load High	Critical	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Riverbed SteelHea...
<input type="checkbox"/>	Riverbed SteelHead: Login Activity Dete...	Medium	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Riverbed SteelHea...
<input type="checkbox"/>	Riverbed SteelHead: Peer Blacklisted	Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Riverbed SteelHea...

DELETE

Figure 28

Token Template

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Parsing rules**.
2. On **Template** tab, click on the Riverbed SteelHead group folder to view the imported Templates.

PARSING RULE

Parsing Rule Template

Group : Riverbed SteelHead

Search...

TEMPLATE NAME	TEMPLATE DESCRIPTION	ADDED BY	ADDED DATE	ACTIVE	<input type="checkbox"/>	EDIT
Riverbed SteelHead Co...		jenish.r	2/12/2018 5:08:56 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Riverbed SteelHead Lo...		jenish.r	2/12/2018 5:08:56 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Riverbed SteelHead Pe...		jenish.r	2/12/2018 5:08:56 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Figure 29

Knowledge Objects

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Knowledge Objects**.

2. In the Knowledge Object tree, expand Riverbed SteelHead group folder to view the imported Knowledge objects.

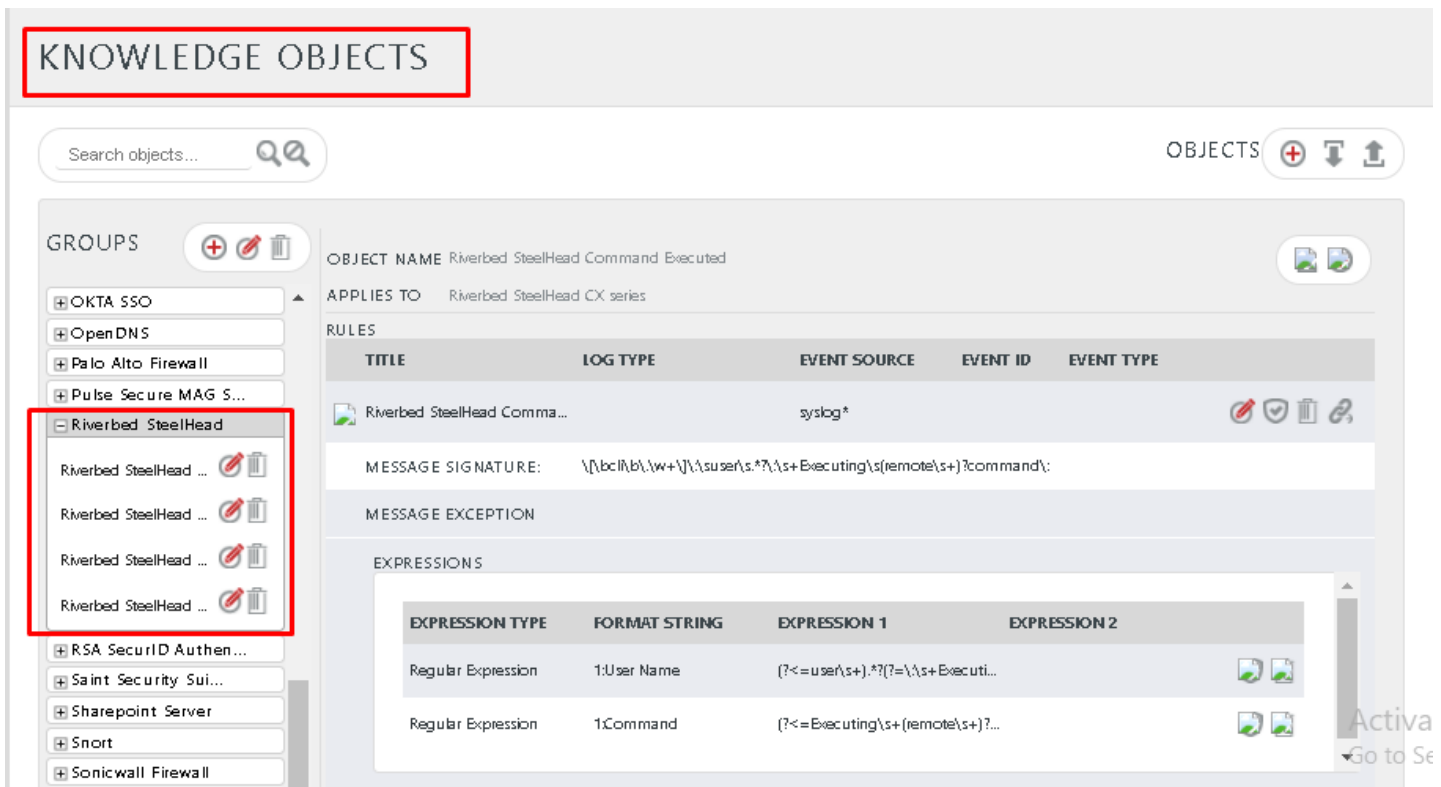


Figure 30

Flex Reports

1. In the **EventTracker Enterprise** web interface, click the **Reports** menu, and then select **Report Configuration**.

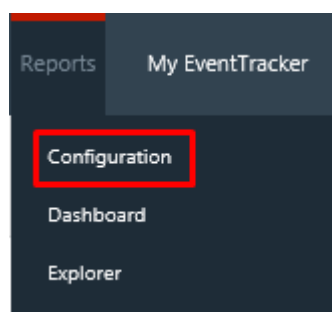


Figure 31

2. In **Reports Configuration** pane, select **Defined** option.
3. Click on the Riverbed SteelHead group folder to view the imported Riverbed SteelHead reports.

REPORTS CONFIGURATION

Scheduled Queued Defined

Search

REPORT GROUPS

- Pentaho
- Riverbed SteelHead**
- Saint Security Suite
- SMG
- Snort
- Sonicwall SMA

REPORTS CONFIGURATION : RIVERBED STEELHEAD

Total: 3

<input type="checkbox"/>	TITLE	CREATED ON	MODIFIED ON	<input type="button" value="i"/>	<input type="button" value="📅"/>	<input checkbox"="" type="button" value="+</input></th> </tr> </thead> <tbody> <tr> <td><input type="/> <td> <u>Riverbed SteelHead - Login Activities</u></td> <td>2/12/2018 5:10:53 PM</td> <td>1/1/1970 5:30:00 AM</td> <td><input type="button" value="i"/></td> <td><input type="button" value="📅"/></td> <td><input checkbox"="" type="button" value="+</input></td> </tr> <tr> <td><input type="/></td> <td> <u>Riverbed SteelHead - Peer trust list</u></td> <td>2/12/2018 5:10:53 PM</td> <td>1/1/1970 5:30:00 AM</td> <td><input type="button" value="i"/></td> <td><input type="button" value="📅"/></td> <td><input checkbox"="" type="button" value="+</input></td> </tr> <tr> <td><input type="/></td> <td> <u>Riverbed SteelHead - Command Executed</u></td> <td>2/12/2018 5:10:53 PM</td> <td>1/1/1970 5:30:00 AM</td> <td><input type="button" value="i"/></td> <td><input type="button" value="📅"/></td> <td><input 386="" 402"="" 467="" 537="" data-label="Caption" type="button" value="+</input></td> </tr> </tbody> </table> </div> <div data-bbox="/>Figure 32</td>	<u>Riverbed SteelHead - Login Activities</u>	2/12/2018 5:10:53 PM	1/1/1970 5:30:00 AM	<input type="button" value="i"/>	<input type="button" value="📅"/>	<input checkbox"="" type="button" value="+</input></td> </tr> <tr> <td><input type="/>	<u>Riverbed SteelHead - Peer trust list</u>	2/12/2018 5:10:53 PM	1/1/1970 5:30:00 AM	<input type="button" value="i"/>	<input type="button" value="📅"/>	<input checkbox"="" type="button" value="+</input></td> </tr> <tr> <td><input type="/>	<u>Riverbed SteelHead - Command Executed</u>	2/12/2018 5:10:53 PM	1/1/1970 5:30:00 AM	<input type="button" value="i"/>	<input type="button" value="📅"/>	<input 386="" 402"="" 467="" 537="" data-label="Caption" type="button" value="+</input></td> </tr> </tbody> </table> </div> <div data-bbox="/> Figure 32
--------------------------	-------	------------	-------------	----------------------------------	----------------------------------	---	--	----------------------	---------------------	----------------------------------	----------------------------------	---	---	----------------------	---------------------	----------------------------------	----------------------------------	---	--	----------------------	---------------------	----------------------------------	----------------------------------	---

Create Dashlets

1. Open **EventTracker Enterprise** in browser and logon.

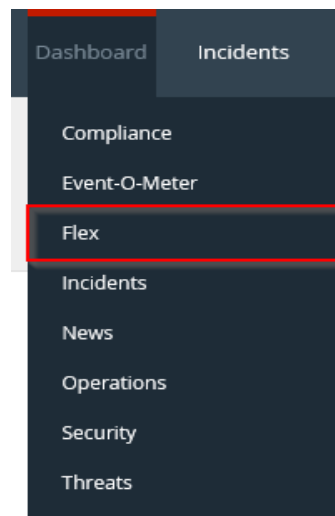


Figure 33

2. Navigate to **Dashboard>Flex**.
Flex Dashboard pane is shown.

Figure 34


3. Fill suitable title and description and click **Save** button.
4. Click  to configure a new flex dashlet. Widget configuration pane is shown.

Figure 35

5. Locate earlier scheduled report in **Data Source** dropdown.
6. Select **Chart Type** from dropdown.
7. Select extent of data to be displayed in **Duration** dropdown.
8. Select computation type in **Value Field Setting** dropdown.
9. Select evaluation duration in **As Of** dropdown.
10. Select comparable values in **X Axis** with suitable label.
11. Select numeric values in **Y Axis** with suitable label.
12. Select comparable sequence in **Legend**.
13. Click **Test** button to evaluate. Evaluated chart is shown.

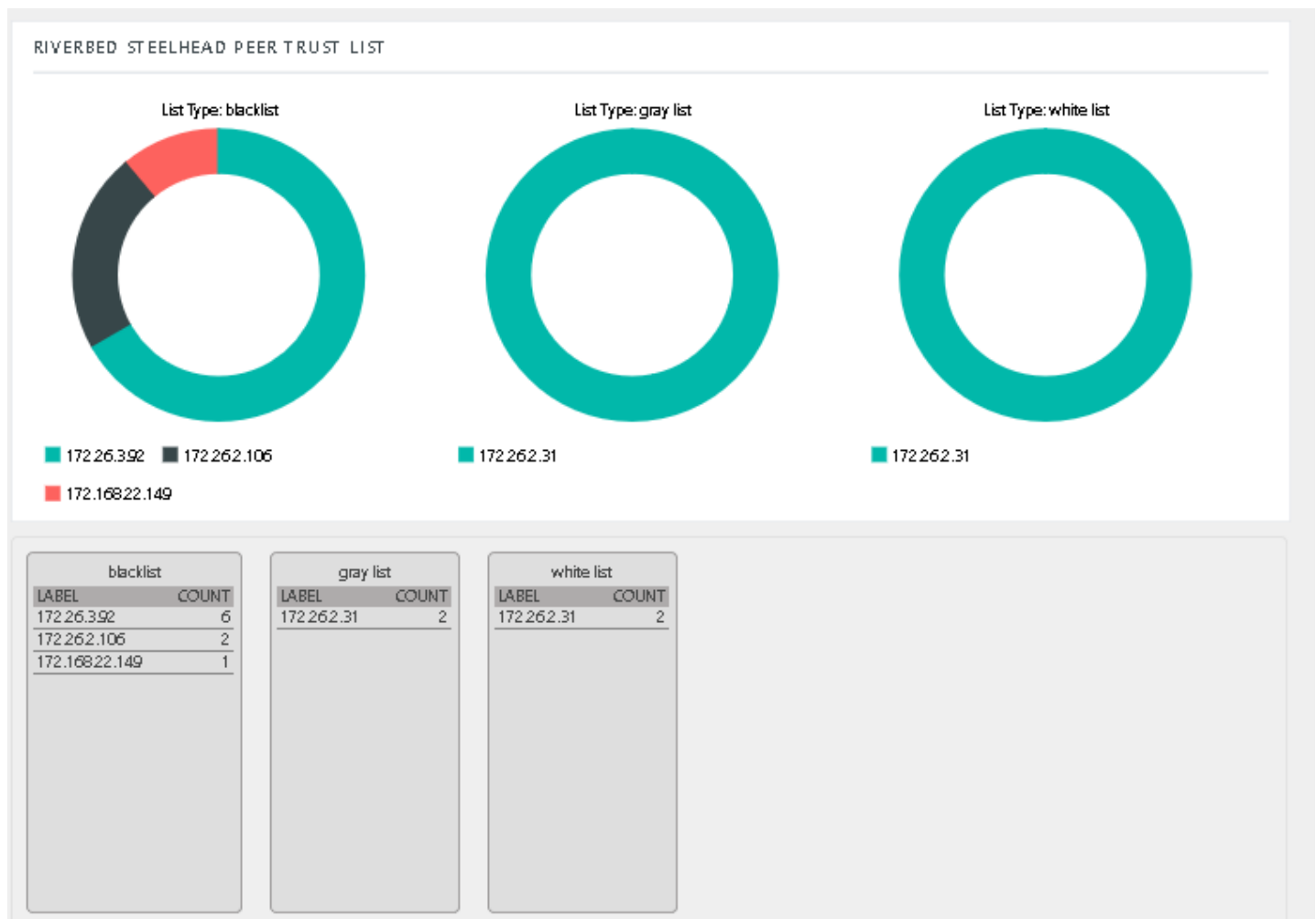


Figure 36

14. If satisfied, click **Configure** button.

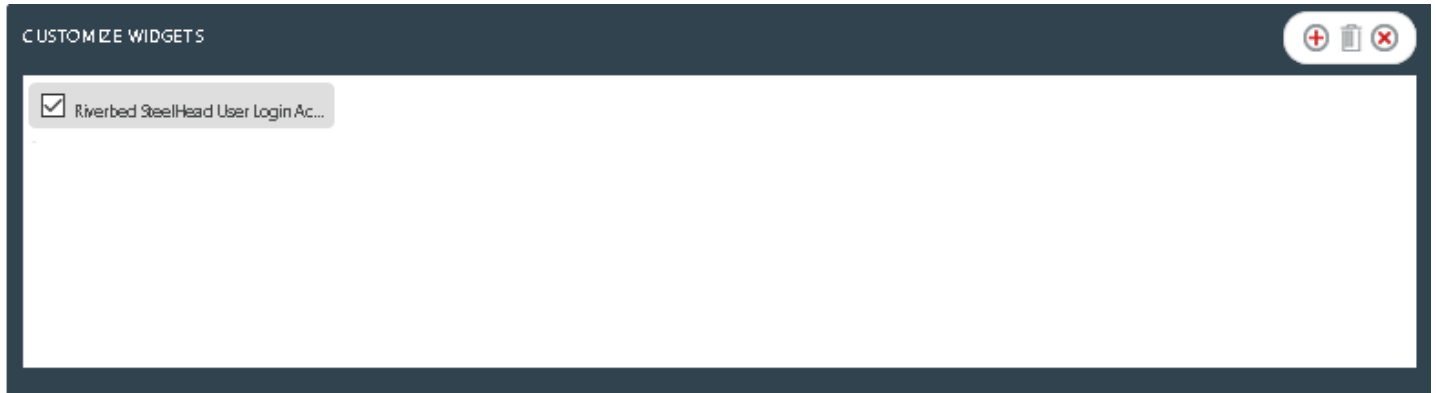




Figure 37

15. Click 'customize'  to locate and choose created dashlet.
16. Click  to add dashlet to earlier created dashboard.

Sample Flex Dashboards

For below dashboard:

WIDGET TITLE: Riverbed SteelHead Authentication Failure Details

DATA SOURCE: Riverbed SteelHead Authentication Failure Details

CHART TYPE: Donut

AXIS LABELS [X-AXIS]: Source IP Address

LEGEND[SERIES]: Listype

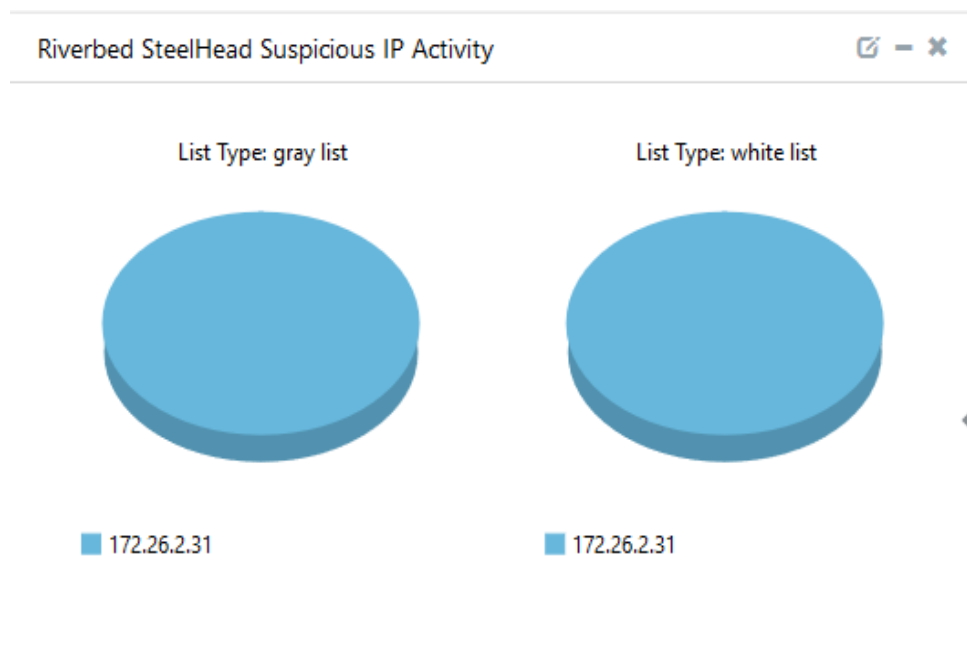


Figure 38

For below dashboard:

WIDGET TITLE: Riverbed SteelHead Suspicious IP Activity

DATA SOURCE: Riverbed SteelHead Suspicious IP Activity

CHART TYPE: Column

AXIS LABELS [X-AXIS]: Computer Name

LEGEND[SERIES]: Reason

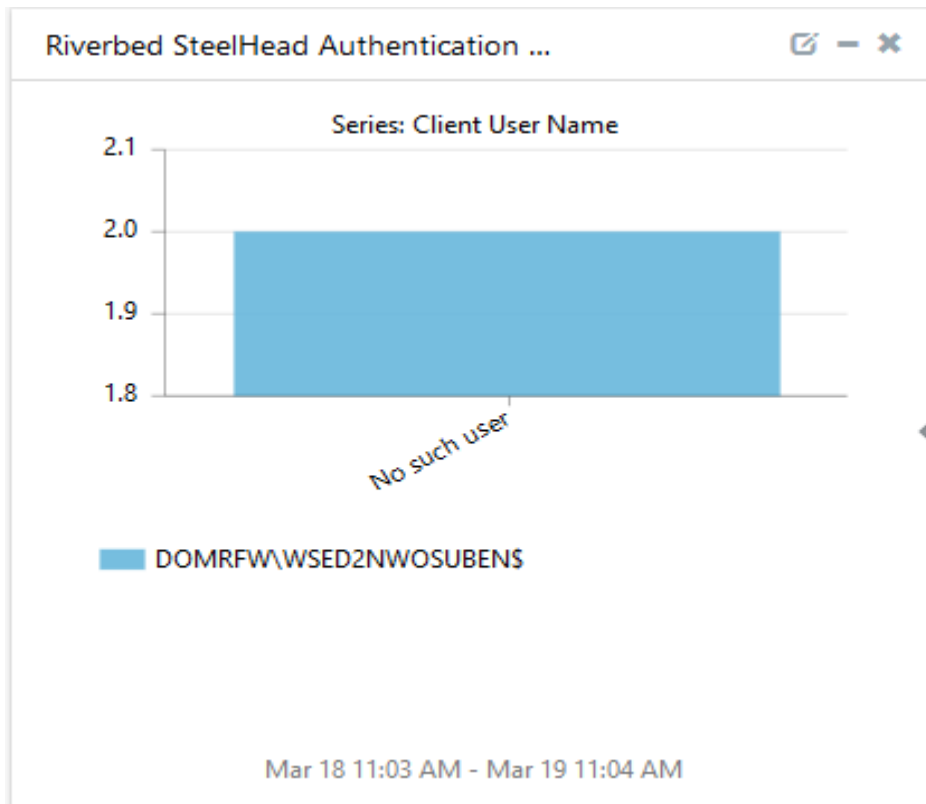


Figure 39