

Integrate TippingPoint *EventTracker Enterprise*

Abstract

This guide provides instructions to configure **TippingPoint** to send the syslog events to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 7.x and later, and **TippingPoint for the S-Series (330) IPS device, TOS version 3.6.4 and 3.6.5**.

Audience

Administrators, who are responsible for monitoring **TippingPoint** using EventTracker Enterprise.

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
 - Scope..... 1
 - Audience..... 1
- Introduction 3
- Pre-requisites..... 3
- Integration Method for TippingPoint 3
- EventTracker Knowledge Pack (KP)..... 5
 - Categories 5
 - Alerts..... 5
 - Flex Reports..... 5
- Import TippingPoint knowledge pack into EventTracker..... 6
 - Category 7
 - Alerts..... 9
 - Templates 10
 - Knowledge Object..... 11
 - Flex Reports..... 13
- Verify TippingPoint knowledge pack in EventTracker..... 14
 - Category 14
 - Alerts..... 14
 - Templates 15
 - Knowledge Object..... 16
 - Flex Reports..... 16
- Create Flex Dashboards in EventTracker 17
 - Schedule Reports..... 17
 - Create Dashlets..... 19
- Sample Flex Dashboards..... 22

Introduction

The TippingPoint Next-Generation Intrusion Prevention System (IPS) offers comprehensive threat protection against advanced and evasive targeted attacks with high accuracy. Using a combination of technologies such as deep packet inspection, threat reputation and advanced malware analysis, it provides enterprises with a proactive approach to security.

EventTracker collects the logs, helps administrator to analyze the events and generate the reports for the TippingPoint IPS traffic being allowed or blocked.

Pre-requisites

- EventTracker v7.x or later should be installed.
- An exception should be added into windows firewall on EventTracker machine for syslog port 514.
- TippingPoint 330 IPS module must be configured.

Integration Method for TippingPoint

1. Log into IPS Local Security Manager (LMS) with valid credentials.



Figure 1

2. On IPS LMS Expand **System** then select **Syslog Servers**.
3. Enable **System Log**, **Audit Log** and **Quarantine log**.
4. Enter the IP address of **EventTracker Manager Machine**.
5. Click on **APPLY** to save.

SYSTEM »

- ⊕ IPS
- ⊕ Events
- ⊖ System
 - ⊕ Update
 - Management Port
 - Management Routing
 - SMS/NMS
 - High Availability
 - Compact Flash
 - Thresholds
 - Email Server
 - Syslog Servers
 - Named Networks
 - License
 - Tech Support Report
- ⊕ Network
- ⊕ Authentication
- Back To Top

Syslog Servers

Format

- Enable RFC format for remote syslog messages
- Enable additional event information for remote syslog messages
- Enable additional event information for SNMP traps

System Log

- Enable syslog offload for System Log
IP Address:

Audit Log

- Enable syslog offload for Audit Log
IP Address:

Quarantine Log

- Enable syslog offload for Quarantine Log
IP Address:

Apply

Figure 2

NOTE: Once Syslog Server destination is configured, events must be sent via the **Action Sets Contact(s)** to forward to Remote system (Syslog) and Management Console. Both steps must be configured before logs are sent.

IPS »

- ⊖ IPS
 - Security Profiles
 - Traffic Management Profiles
 - Reputation Groups
 - Action Sets
 - Notification Contacts
 - Services
 - Preferences
- ⊖ Events
- ⊖ System
 - ⊕ Update
 - Management Port
 - Management Routing
 - SMS/NMS
 - High Availability
 - Compact Flash
 - Thresholds
 - Email Server
 - Syslog Servers
 - Named Networks

Action Sets

25 Records per page

Action Set	Action(s)	TCP Reset	Packet Trace	Contact(s)	Function(s)
Recommended	Category Dependent				
Block	Block				Edit
Block + Console	Block			Management Console	Edit Delete
Block + Notify	Block			Management Console - Remote System Log	Edit
Block + Notify + Trace	Block		Enabled	Management Console - Remote System Log	Edit
Permit	Permit			Management Console	Edit
Permit + Notify	Permit			Management Console	Edit
Permit + Notify + Trace	Permit		Enabled	Management Console - Remote System Log	Edit
Quarantine	Block + Quarantine			Management Console - Remote System Log	Edit Delete
Rate Limit	Rate Limit 10 Mbps			Management Console	Edit Delete
Trust	Trust			Management Console	Edit

Figure 3

EventTracker Knowledge Pack (KP)

Once logs are received in to EventTracker, Alerts and reports can be configured into EventTracker.

The following Knowledge Packs are applicable in EventTracker v7.x and later to support TippingPoint.

Categories

- **TippingPoint: IPS traffic allowed**

This category provides information related to IP traffic allowed on the network.

- **TippingPoint: IPS traffic blocked**

This category provides information related to IP traffic blocked on the network.

Alerts

- **TippingPoint: IPS traffic blocked**

This alert is generated if the IP traffic is blocked when an attack is detected by the TippingPoint IPS.

Flex Reports

- **TippingPoint-IPS traffic allowed**

This report provides the information related to IP traffic being allowed based on the rules configured on TippingPoint IPS.

Event Time	Device Name	Alert Severity	Alert Message	Source IP	Source Port	Destination IP	Destination Port	Protocol	Action	Security Zone
Oct 10 08:11:54	IPS01	Minor	ICMP: Redirect Undefined Code	90.138.157.173	0	90.138.157.175	0	icmp	Permit + Notify	ANY-ANY

Figure 4

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
10/18/2016 12:22:43 PM	2042	TOM / TIPPINGPOINT		BUILTIN	Syslog auth

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

Description:
 Oct 10 08:11:54 10.4.254.252 Oct 10 08:11:54 IPS01 ALT v5 20081024T213932+0360 irobot/192.168.65.22,265155 1 Permit Minor 00000002-0002-0002-00000000161 "0161: ICMP: Redirect Undefined Code" "0161: ICMP: Redirect Undefined Code" icmp " " 90.138.157.173 0 90.138.157.17 5 0 20081024T213932+0360 1 " " 0 ANY-ANY 3ab8eea0-4331-11d6-b47a-00a0c995f27f Permit + Notify

Figure 5

- TippingPoint-IPS traffic blocked

This report provides the information related to IP traffic being blocked when an attack is detected based on the rules configured on TippingPoint IPS.

Event Time	Device Name	Alert Severity	Alert Message	Source IP	Source Port	Destination IP	Destination Port	Protocol	Action	Security Zone
Oct 17 08:11:54	IPS01	Major	HTTP: SQL Injection (SELECT)	12.52.13.49	65483	76.13.28.196	20480	http	Block + Notify	ANY-ANY
Oct 17 12:31:44	IPS01	Low	HTTP: PUT Method Execution over HTTP/WebDAV	52.78.12.48	52189	172.226.91.19	20480	http	Block + Notify	ANY-ANY
Oct 18 11:39:31	IPS01	Critical	HTTP: PNG File Format Anomaly	52.84.0.84	20480	172.226.91.28	2000	tcp	Block + Notify	ANY-ANY

Figure 6

Logs Considered

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
10/18/2016 11:50:08 AM	2042	TOM / TIPPINGPOINT		BUILTIN	Syslog auth

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

Description:
 Oct 17 08:11:54 10.4.254.252 Oct 17 08:11:54 IPS01 BLK v7 20161010T081154-0600 IPS01/10.4.254.252 864670 2 Block Major 2723862f-e101-11de-9da2-000799a25643 "5670: HTTP: SQL Injection (SELECT)" "5670: HTTP: SQL Injection (SELECT)" http " " 192.168.190.49 65483 76.13.28.196 20480 20161010T081154-0600 1 " " 0 ANY-ANY 3ab8eea0-4331-11d6-b47a-00a0c995f27f Block + Notify 0

Figure 7

Import TippingPoint knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence

- Categories
- Alerts
- Templates

- Flex Reports
- Knowledge Objects


1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.



Figure 8

3. Click the **Import** tab.

Category

1. Click **Category** option, and then click the browse  button.
2. Locate the **All TippingPoint group of categories.iscat** file, and then click **Open** button.

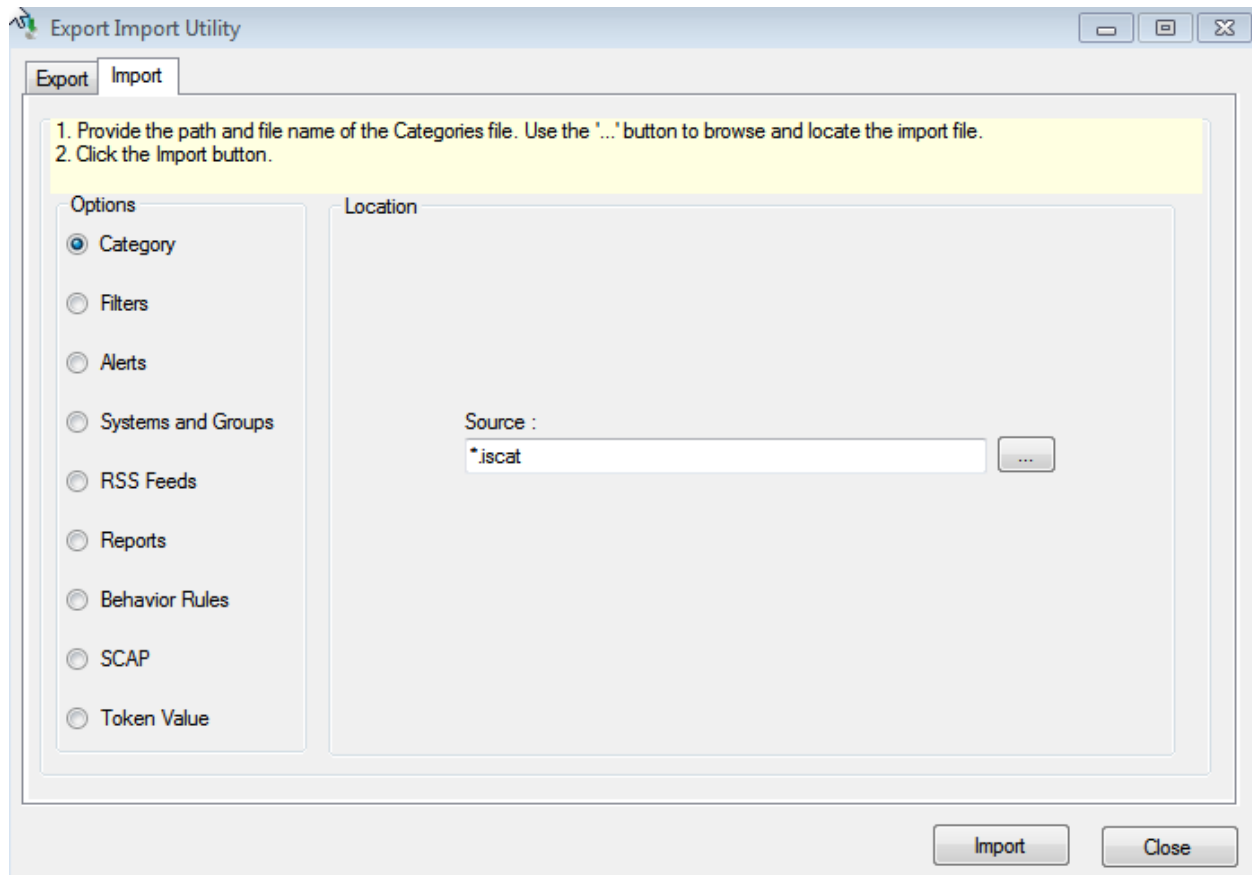


Figure 9

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

EventTracker displays success message.

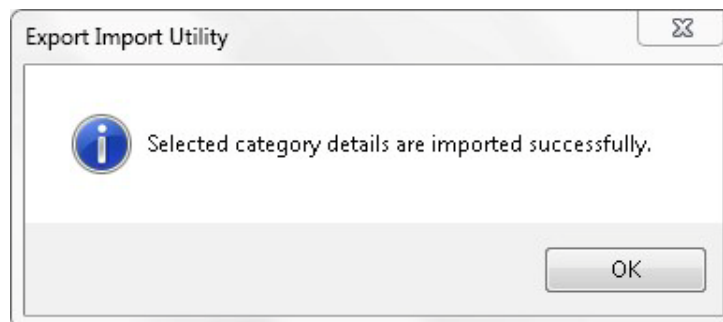



Figure 10

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

Alerts

1. Click **Alerts** option, and then click the browse  button.
2. Locate the **All TippingPoint group of alerts.isalt** file, and then click the **Open** button.

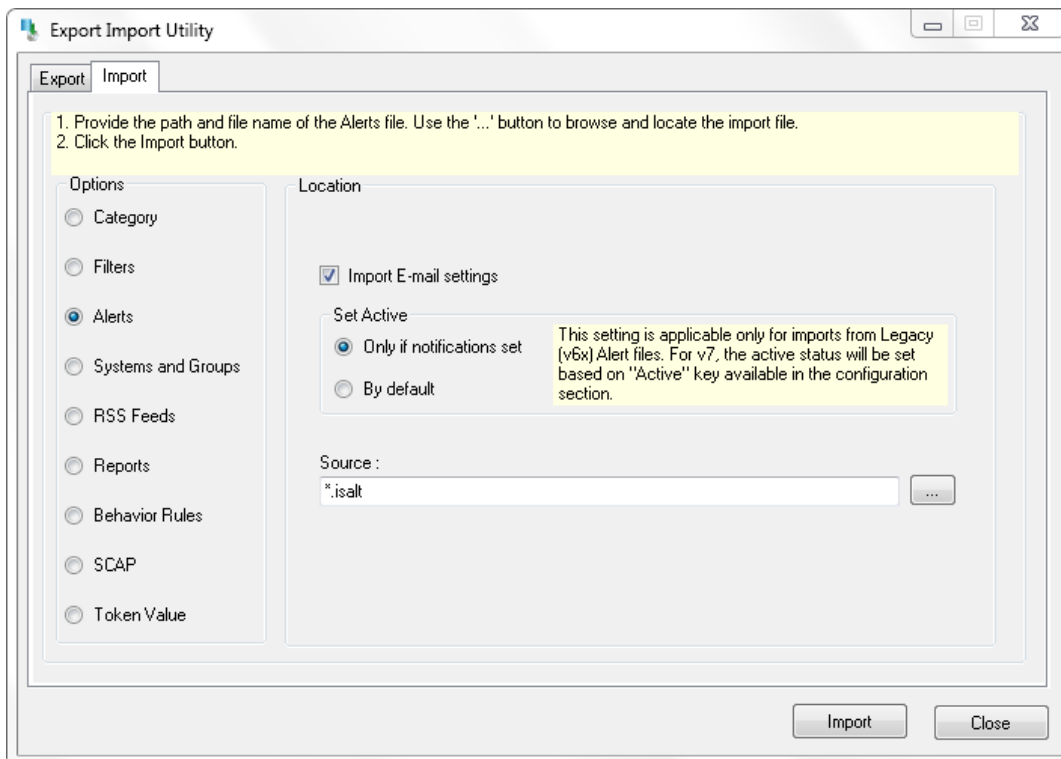


Figure 11

2. To import alerts, click the **Import** button.
EventTracker displays success message.

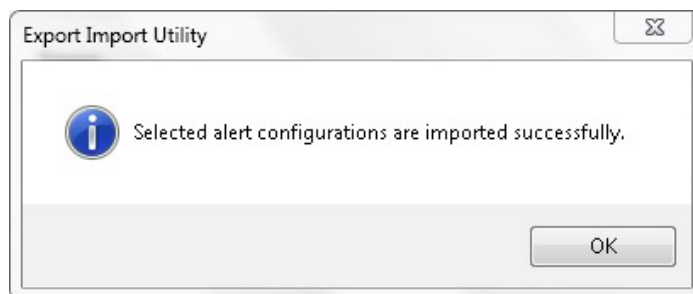



Figure 12

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

Templates

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab, and then click on  'Import' option.

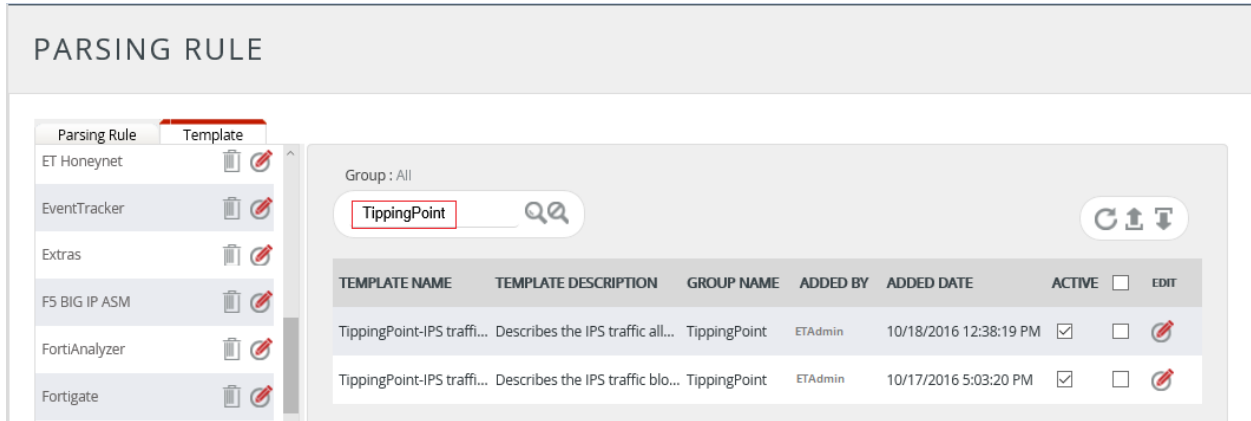


Figure 13

3. Click on **Browse** button.

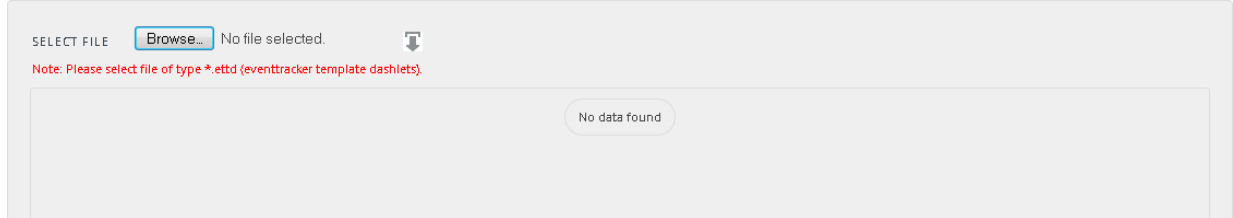



Figure 14

4. Locate **All TippingPoint** group of **templates.ettd** file, and then click the **Open** button

SELECTED FILE IS: All TippingPoint group of templates.ett

<input checked="" type="checkbox"/>	TEMPLATE NAME	SEPARATOR	TEMPLATE DESCRIPTION	ADDED DATE	ADDED BY	GROUP NAME
<input checked="" type="checkbox"/>	TippingPoint-IPS traffic allowed	\n	Oct 10 08:11:54 10.4.254.252 Oct 10 08:11:54 IPS01 ALT v5 20081024T213932 +0360 irobot/192.168.65.22,265155 1 Permit Minor 00000002-0002-0002-0002-0000000000161 "0161: ICMP: Redirect Undefined Code" "0161: ICMP: Redirect Undefined Code" icmp " " 90.138.157.173 0 90.138.157.175 0 20081024T213932+0360 1 " " 0 ANY-ANY 3ab8eea0-4331-11d6-b47a-00a0c995f27f Permit + Notify	10/18/2016 12:38:19 PM	ETAdmin	TippingPoint
<input checked="" type="checkbox"/>	TippingPoint-IPS traffic blocked	\n	Oct 14 11:39:31 10.4.254.252 Oct 14 11:39:31 IPS01 BLK v7 20161014T113931-0600 IPS01/10.4.254.252 864676 2 Block Critical 00000002-0002-0002-0002-00000003547 "3547: HTTP: PNG File Format Anomaly" "3547: HTTP: PNG File Format Anomaly" tcp " " 52.84.0.84 20480 192.168.190.56 2000 20161014T113931-0600 1 " " 0 ANY-ANY 3ab8eea0-4331-11d6-b47a-00a0c995f27f Block + Notify 0 52.84.0.84 N/A	10/17/2016 5:03:20 PM	ETAdmin	TippingPoint

Figure 15

- Now select the check box and then click on  'Import' option. EventTracker displays success message.

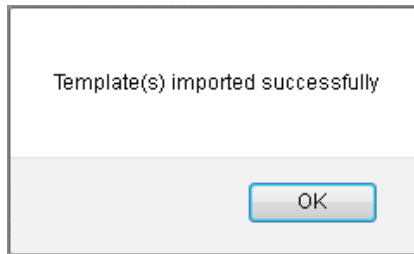



Figure 16

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

Knowledge Object

- Click the **Admin** menu, and then click **Knowledge Objects**.
- Click on  'Import' option.

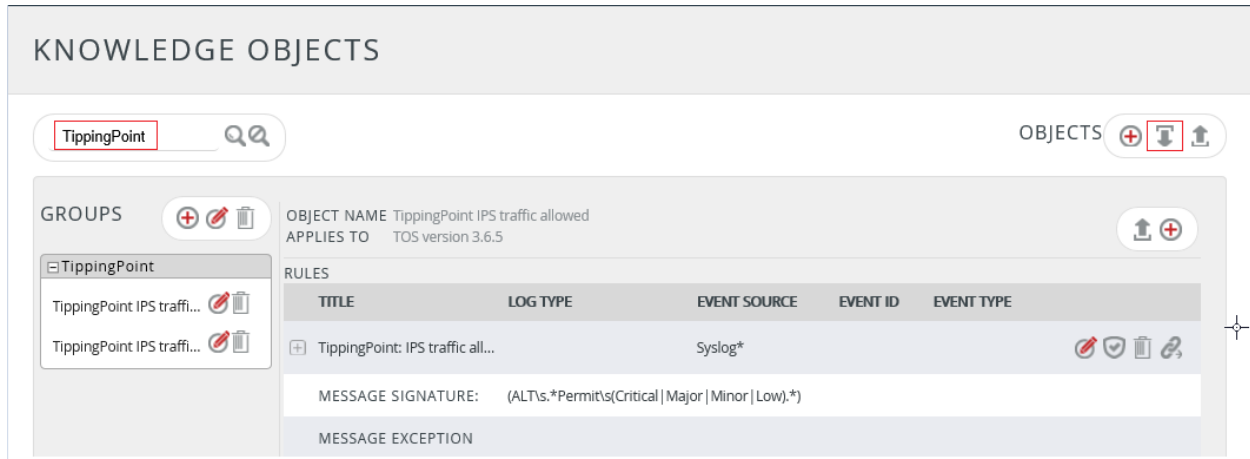


Figure 17

3. In **IMPORT** pane click on **Browse** button.

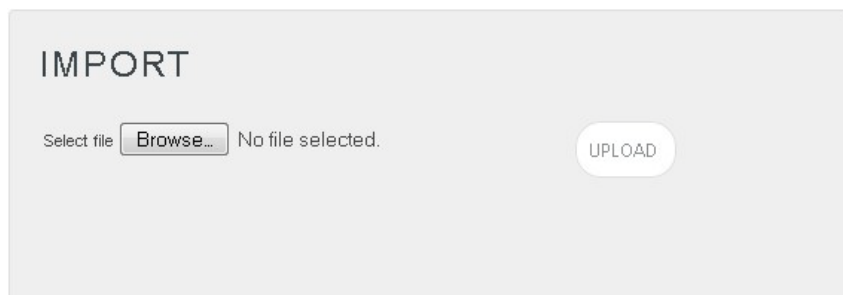


Figure 18

4. Locate **All TippingPoint group of knowledge object.etko** file, and then click the **UPLOAD** button then **OVERWRITE**.

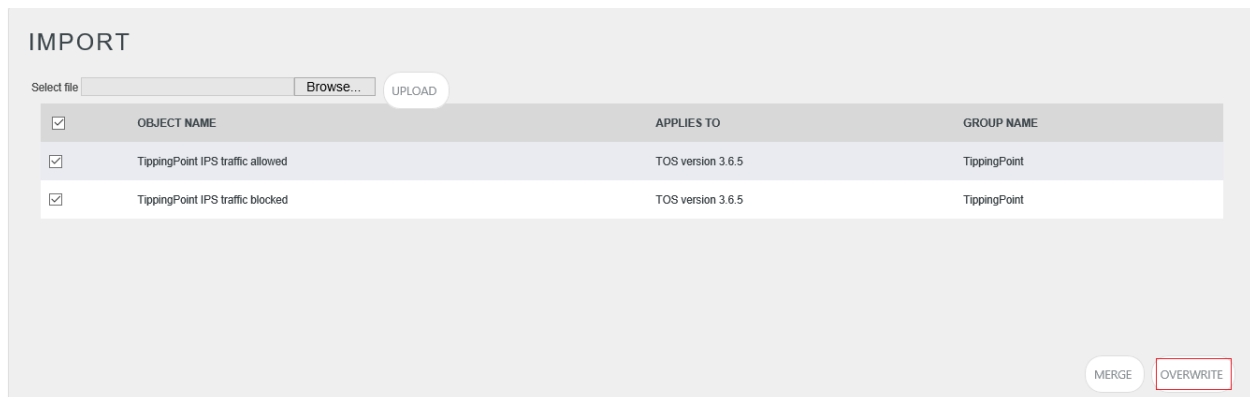



Figure 19

Flex Reports

1. Click **Reports** option, and then click the browse  button.
2. Locate the **All TippingPoint group of flex reports.issch** file, and then click the **Open** button.

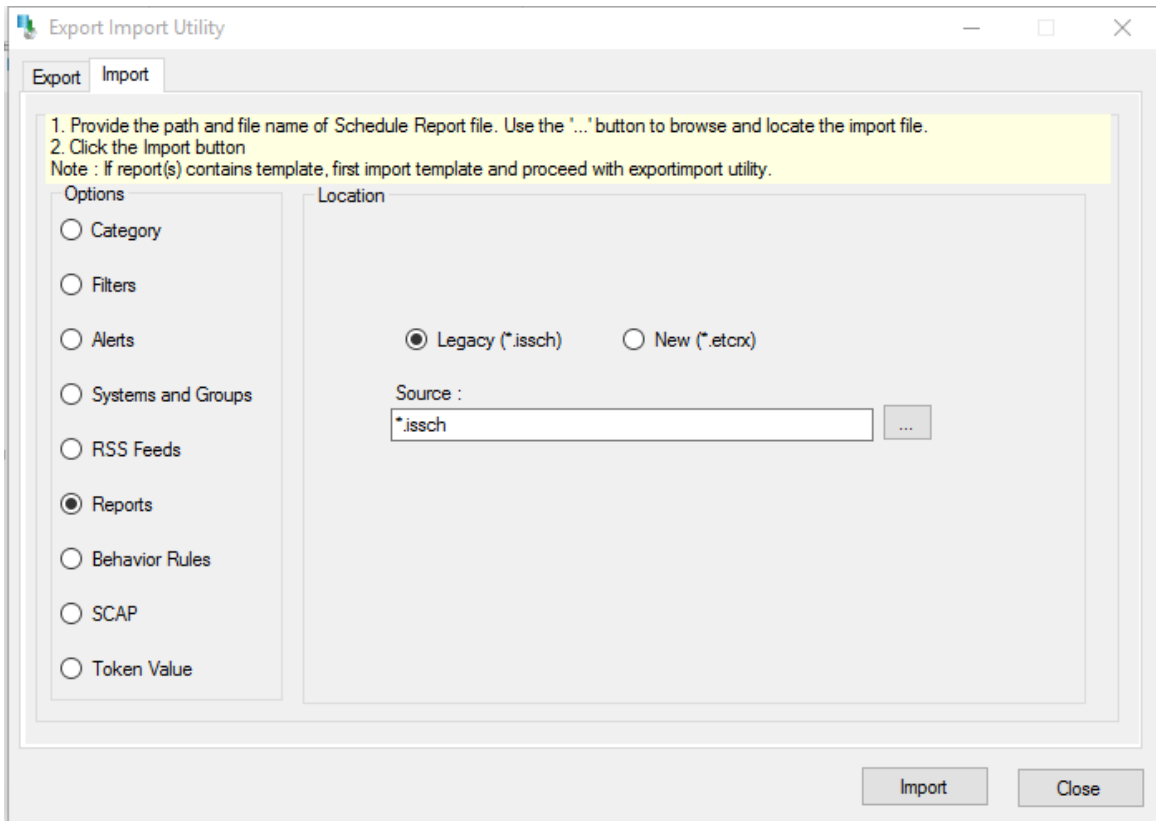


Figure 20

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

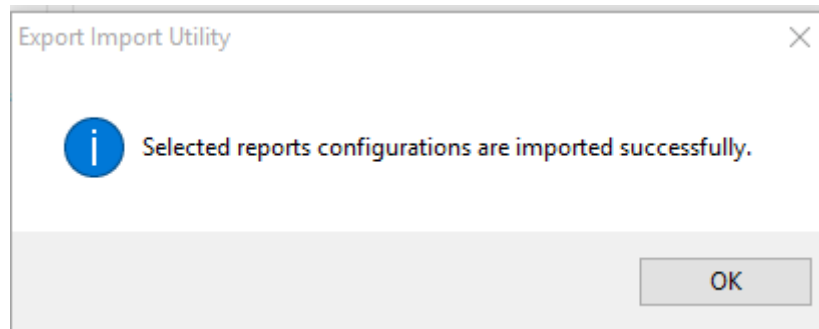


Figure 21

Verify TippingPoint knowledge pack in EventTracker

Category

1. In the **EventTracker Enterprise** web interface.
2. Click the **Admin** dropdown, and then click **Categories**.
3. In the **Category Tree**, search **TippingPoint** to see the imported categories.

The screenshot shows the 'CATEGORY MANAGEMENT' interface. On the left, there is a 'Category Tree' and a 'Search' field containing 'TippingPoint'. Below the search field, two categories are listed: 'TippingPoint: IPS traffic allowed' and 'TippingPoint: IPS traffic blocked'. On the right, a summary shows 'Total category groups: 362' and 'Total categories: 3,191'. Below this, a table displays the 'Last 10 modified categories'.

NAME	MODIFIED DATE	MODIFIED BY
TippingPoint: IPS traffic allowed	10/17/2016 2:51:28 PM	ETAdmin
TippingPoint: IPS traffic blocked	10/17/2016 2:48:52 PM	ETAdmin

Figure 22

Alerts

1. In the **EventTracker Enterprise**, web interface, click the **Admin** dropdown, and then click **Alerts**.
2. In the **Search** field, type '**TippingPoint**', and then click **Go** button.

Alert Management page will display all the imported **TippingPoint** alert

The screenshot shows the 'ALERT MANAGEMENT' interface. At the top right, there is a search field with 'TippingPoint' entered. Below the search field, there is an 'ACTIVATE NOW' button and a note: 'Click 'Activate Now' after making all changes'. A 'Total: 1' indicator is shown next to a 'Page Size' dropdown set to '25'. Below this, a table displays the alert details.

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"/> TippingPoint: IPS traffic blocked	<input type="checkbox"/> High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TOS version 3.6.5

At the bottom left, there is a 'DELETE' button.

Figure 23

- To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.



Figure 24

- Click the **OK** button, 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.

Templates

- Click the **Admin** menu, and then click **Parsing rule**.
- Select **Template** tab, and then click on **Import** option.

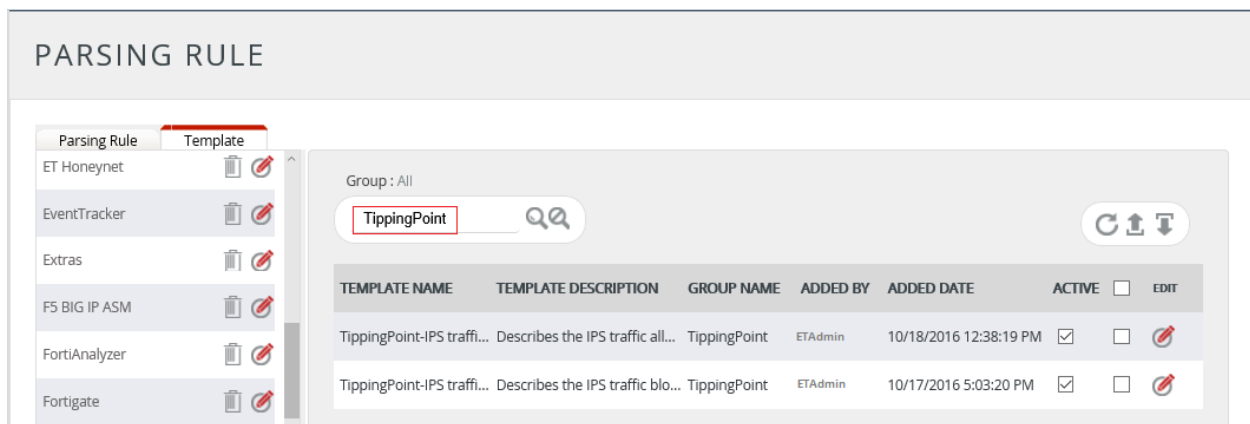


Figure 25

Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**.
2. Scroll down and select **TippingPoint** in **Objects** pane. Imported **TippingPoint** object details are shown.

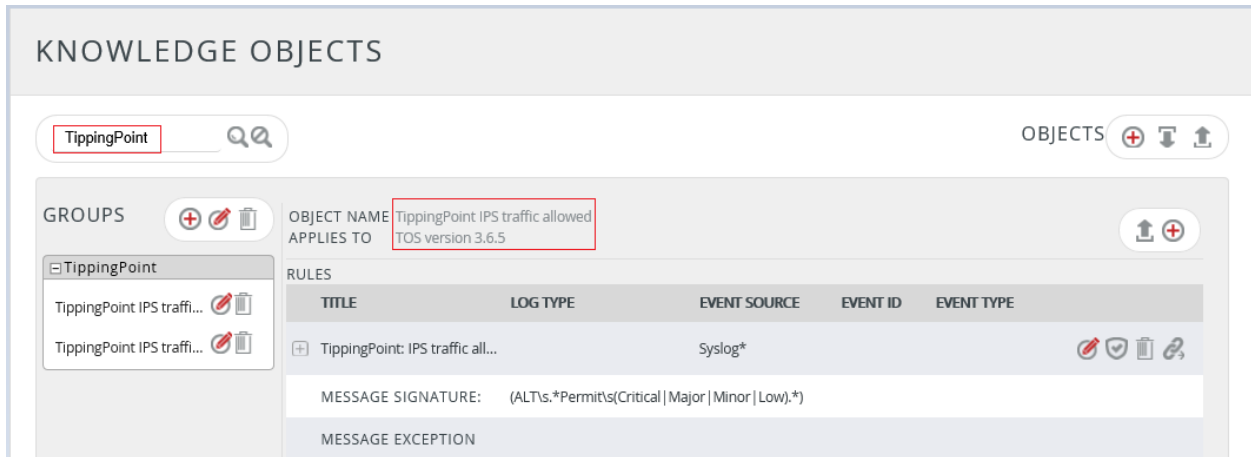


Figure 26

Flex Reports

1. In the **EventTracker Enterprise**, web interface.
2. Click the **Reports** menu, and then select **Configuration**.
3. In **Reports Configuration** pane, select **Defined** option.
4. In search box enter '**TippingPoint**', and then click the **Search** button. EventTracker displays Flex reports of **TippingPoint**

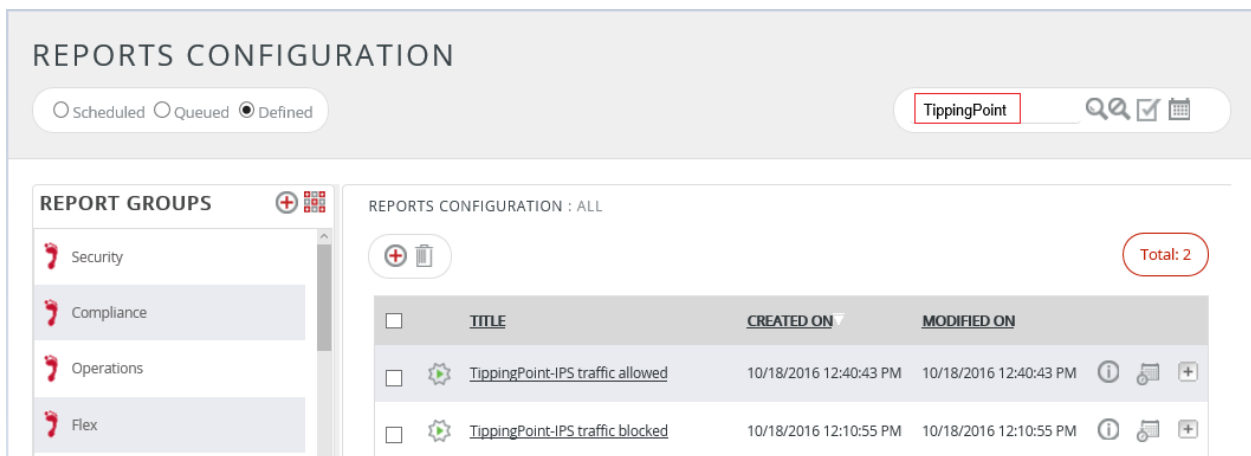


Figure 27

Create Flex Dashboards in EventTracker

NOTE: To configure the flex dashboards, schedule and generate the reports. Flex dashboard feature is available from EventTracker Enterprise v8.0.

Schedule Reports

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

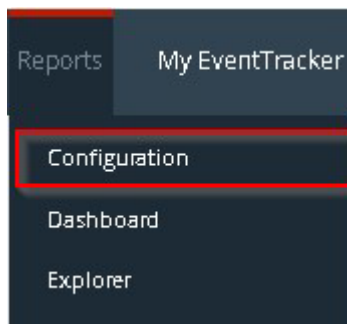
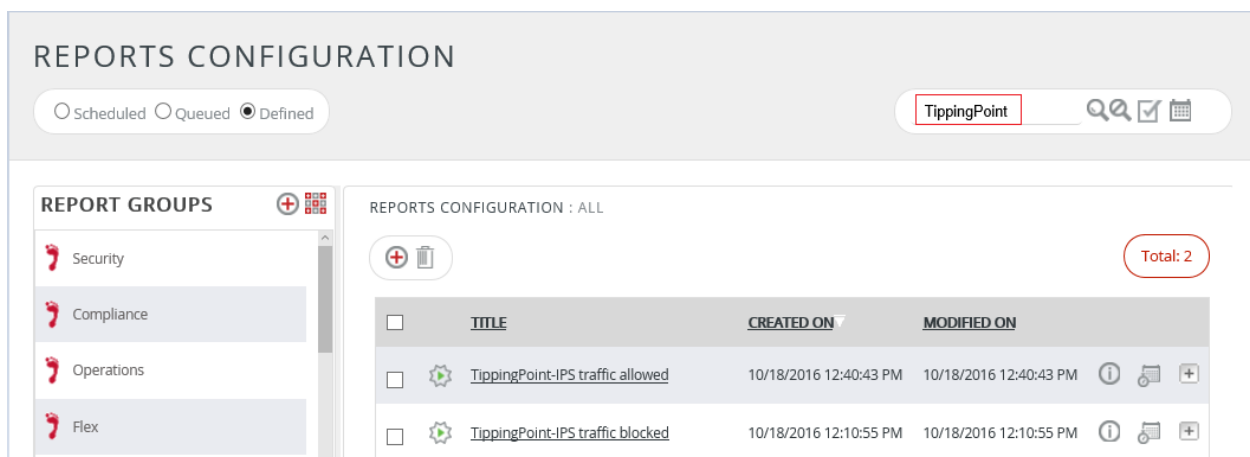


Figure 28

2. Navigate to **Reports>Configuration**.
3. Select **TippingPoint** in report groups. Check **Defined** dialog box.



REPORTS CONFIGURATION

Scheduled Queued Defined

TippingPoint

REPORT GROUPS


- Security
- Compliance
- Operations
- Flex

REPORTS CONFIGURATION : ALL

Total: 2

<input type="checkbox"/>	TITLE	CREATED ON	MODIFIED ON	
<input type="checkbox"/>	TippingPoint-IPS traffic allowed	10/18/2016 12:40:43 PM	10/18/2016 12:40:43 PM	ⓘ ⚙ +
<input type="checkbox"/>	TippingPoint-IPS traffic blocked	10/18/2016 12:10:55 PM	10/18/2016 12:10:55 PM	ⓘ ⚙ +

Figure 29

5. Click on **'schedule'**  to plan a report for later execution.

REPORT WIZARD

TITLE: TIPPINGPOINT-IPS TRAFFIC ALLOWED

LOGS

Review cost details and configure the publishing options. Step 8 of 10

DISK COST ANALYSIS

Estimated time for completion: 00:01:38(HH:MM:SS)
Number of cab(s) to be processed: 34
Available disk space: 194 GB
Required disk space: 50 MB

Enable publishing option (Configure SMTP Server in manager configuration screen to use this option)
 Deliver results via E-mail
 Notify results via E-mail

To E-mail: [Use comma(,) to separate multiple e-mail recipients]

Update status via RSS:

Show in:

Persist data in Eventvault Explorer

Figure 30

REPORT WIZARD

TITLE: TIPPINGPOINT-IPS TRAFFIC ALLOWED

DATA PERSIST DETAIL

Select columns to persist Step 9 of 10

RETENTION SETTING

Retention period: 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
Event Time	<input checked="" type="checkbox"/>
Device Name	<input checked="" type="checkbox"/>
Alert Severity	<input checked="" type="checkbox"/>
Alert Message	<input checked="" type="checkbox"/>
Source IP	<input checked="" type="checkbox"/>

Figure 31

6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.
7. Proceed to next step and click **Schedule** button.
8. Wait till the reports get generated.

Create Dashlets

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

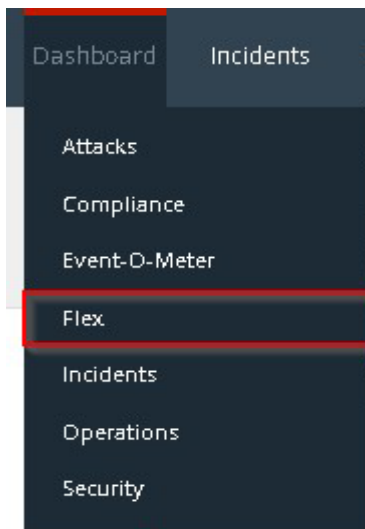


Figure 32

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

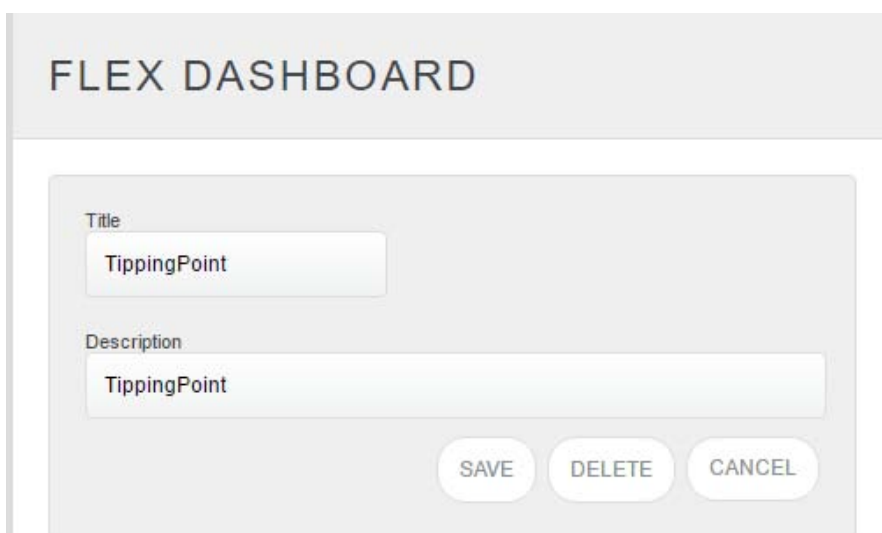

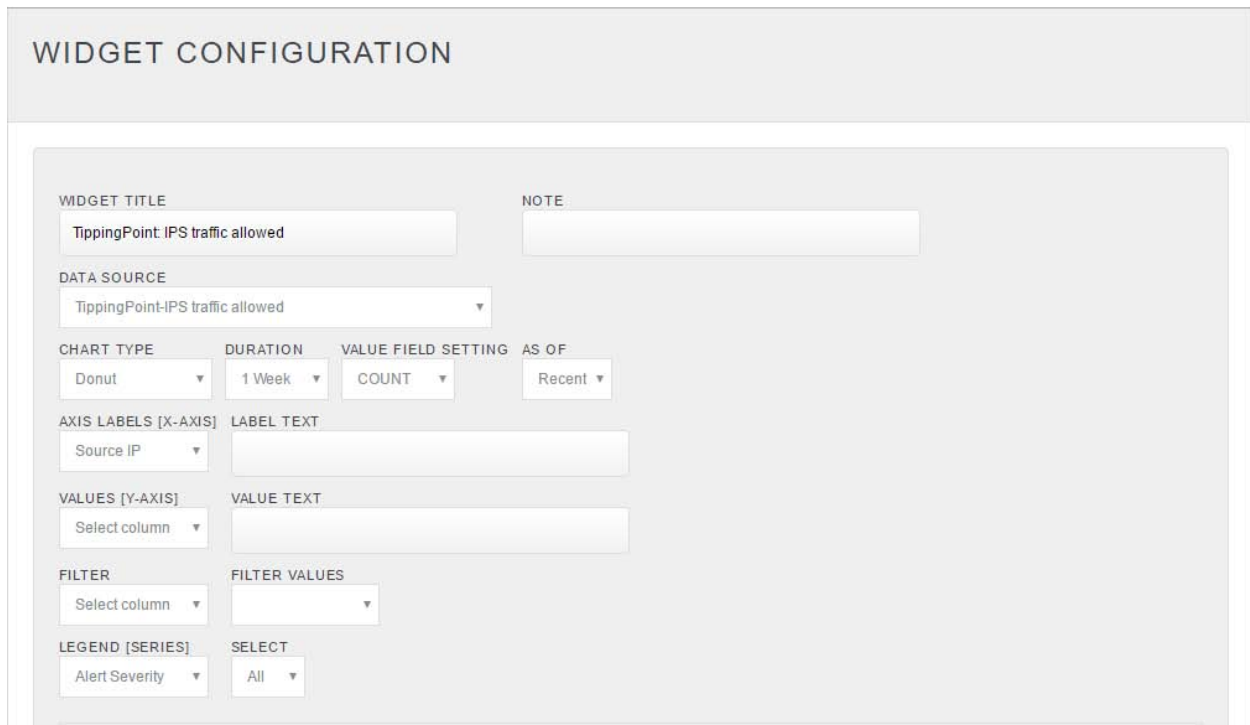


Figure 33

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



WIDGET CONFIGURATION

WIDGET TITLE: TippingPoint: IPS traffic allowed

NOTE:

DATA SOURCE: TippingPoint-IPS traffic allowed

CHART TYPE: Donut

DURATION: 1 Week

VALUE FIELD SETTING: COUNT

AS OF: Recent

AXIS LABELS [X-AXIS]: Source IP

VALUES [Y-AXIS]: Select column

FILTER: Select column

LEGEND [SERIES]: Alert Severity

SELECT: All

Figure 34

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.

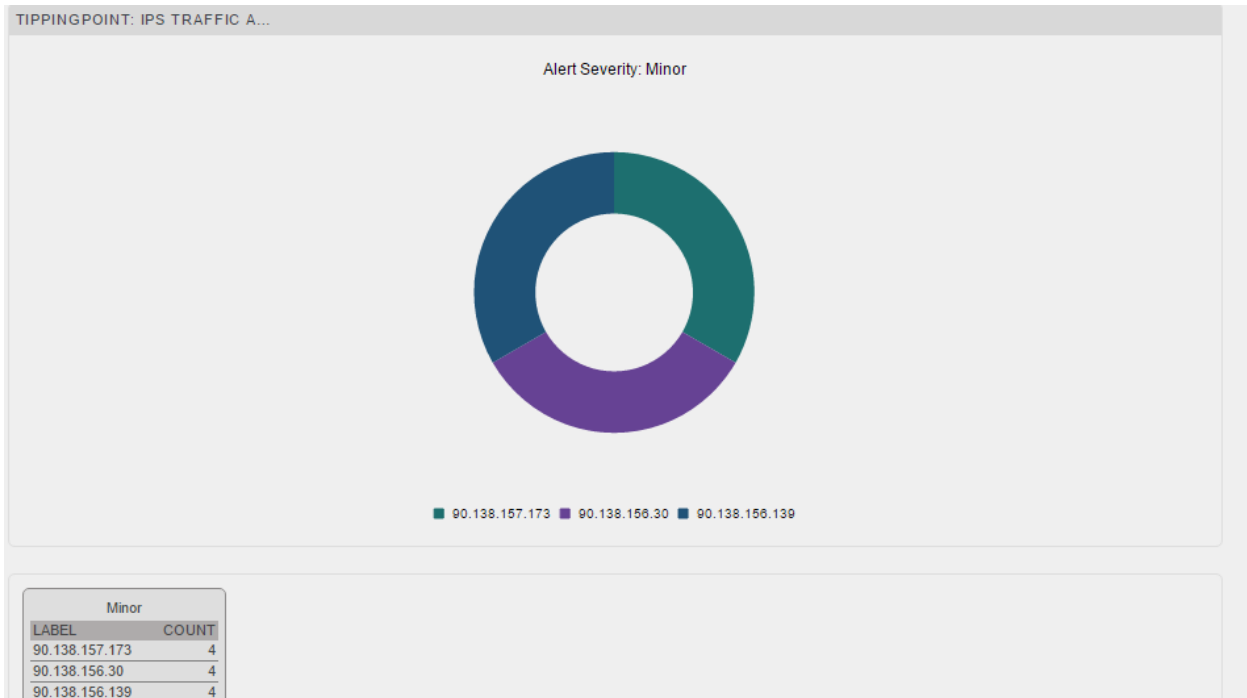




Figure 35

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



Figure 36

15. Click 'customize'  to locate and choose created dashlet.

16. Click  to add dashlet to earlier created dashboard.

Sample Flex Dashboards

For below dashboard **DATA SOURCE: TippingPoint: IPS traffic allowed**

1. TippingPoint: IPS traffic allowed

- **WIDGET TITLE:** IPS traffic allowed by Source IP
CHART TYPE: Donut
AXIS LABELS [X-AXIS]: Source IP
Label Text: Source IP

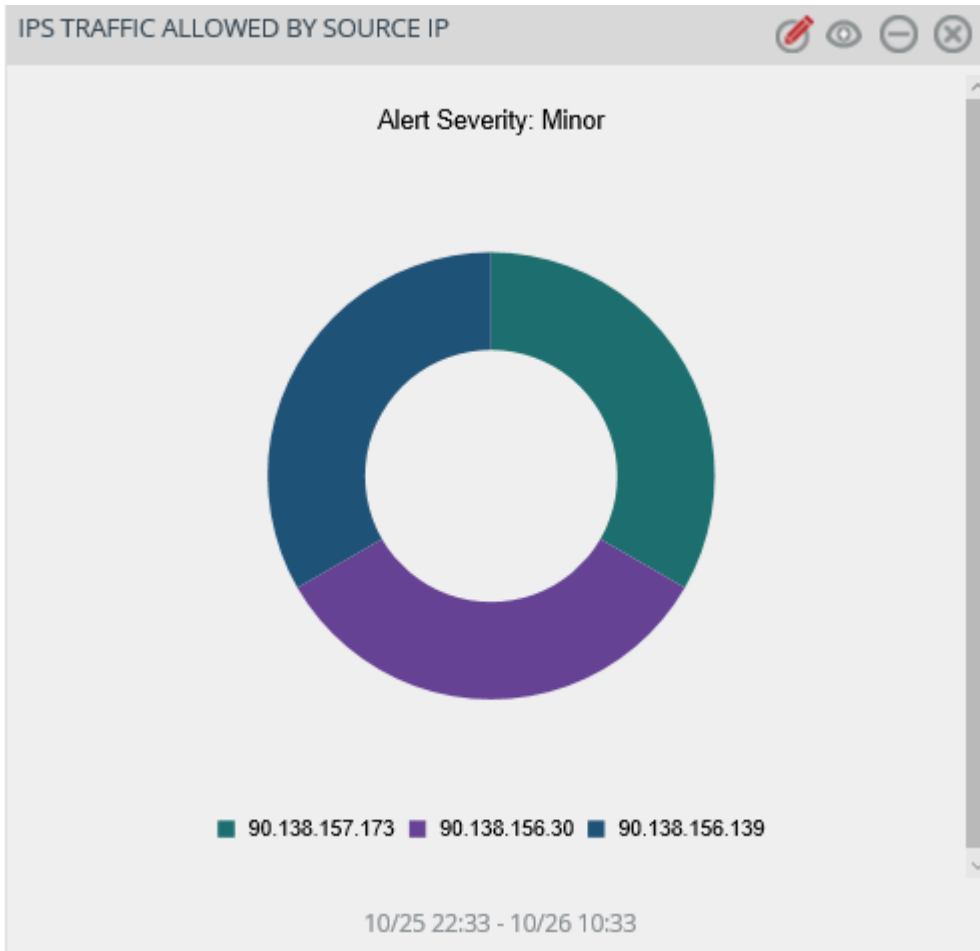


Figure 37

For below dashboard **DATA SOURCE: TippingPoint: IPS traffic blocked**

2. **TippingPoint: IPS traffic blocked by source IP**

- **WIDGET TITLE:** IPS traffic blocked by source IP
CHART TYPE: Stacked column
AXIS LABELS [X-AXIS]: Source IP
Label Text: Source IP

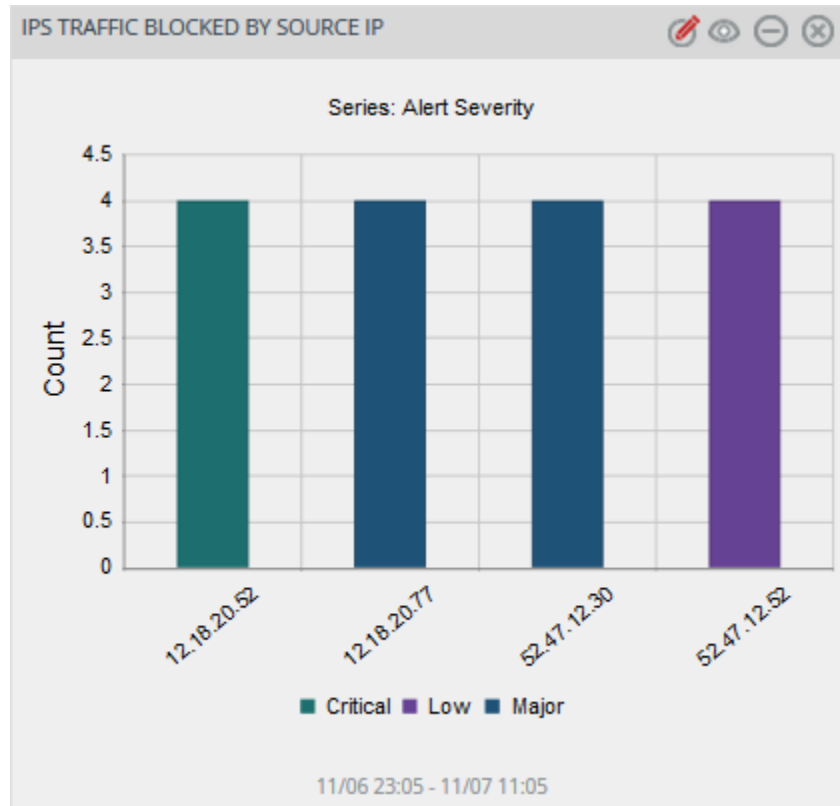


Figure 38