EventTracker
Secure. Comply. Succeed.

Integrate iboss Secure Web Gateway

EventTracker Enterprise

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

Publication Date: Sept. 26, 2016

Abstract

This guide provides instructions to configure **iboss Secure Web Gateway** 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 **iboss Secure Web Gateway 8.2.1.**

Audience

Administrators, who are responsible for monitoring **iboss Secure Web Gateway** 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.

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.

Table of Contents

Introduction

iboss Cybersecurity is a leading provider of innovative Web Security, Mobile Device Management and Threat Defense solutions. iboss delivers the industry's most effective web security, filtering, and reporting. The iboss is the most advanced, easy-to-use Web filter available on the market today.

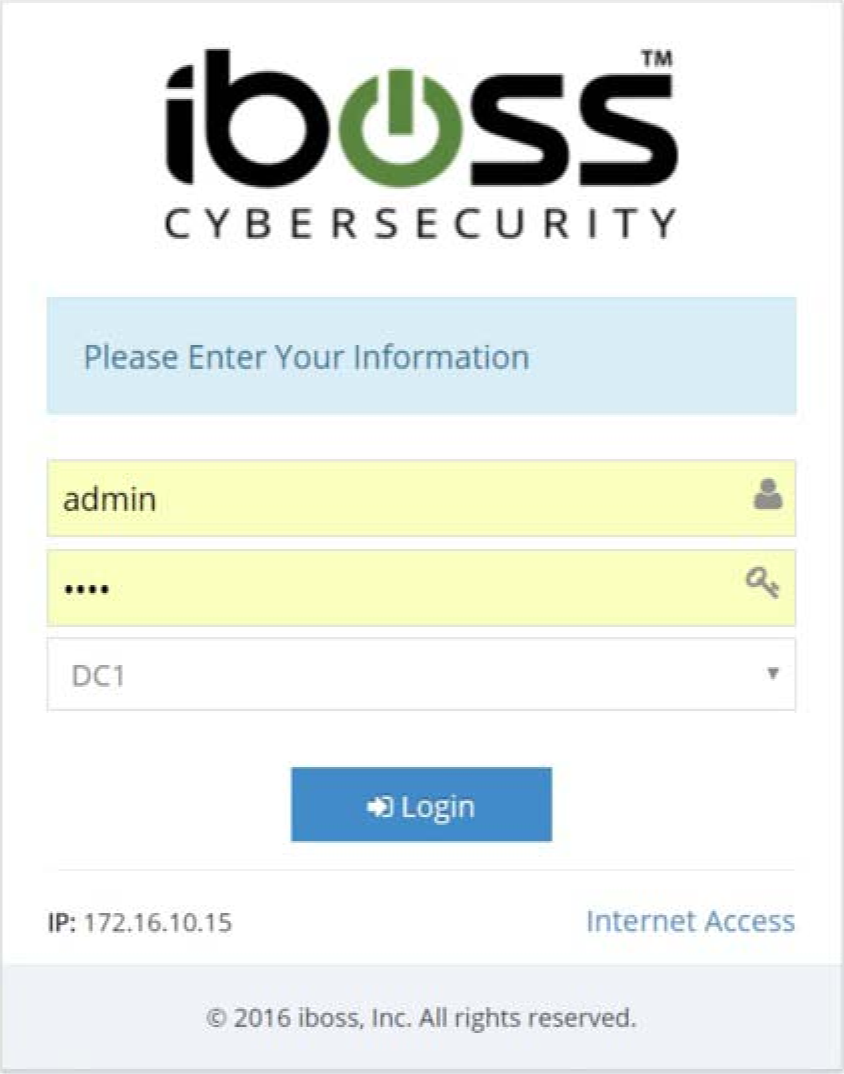
EventTracker collects the logs, helps administrator to analyze the events and generate the reports for the web traffic being allowed or blocked.

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.
- Iboss Secure Web Gateway version 8.2.1 must be installed and configured.

Integration Method for iboss Secure Web Gateway

1. Log into the iboss reporter web interface.



Please Enter Your Information

admin

••••

DC1

IP: 172.16.10.15

© 2016 iboss, Inc. All rights reserved.

Figure 1

2. Go to **Home→Settings→General**

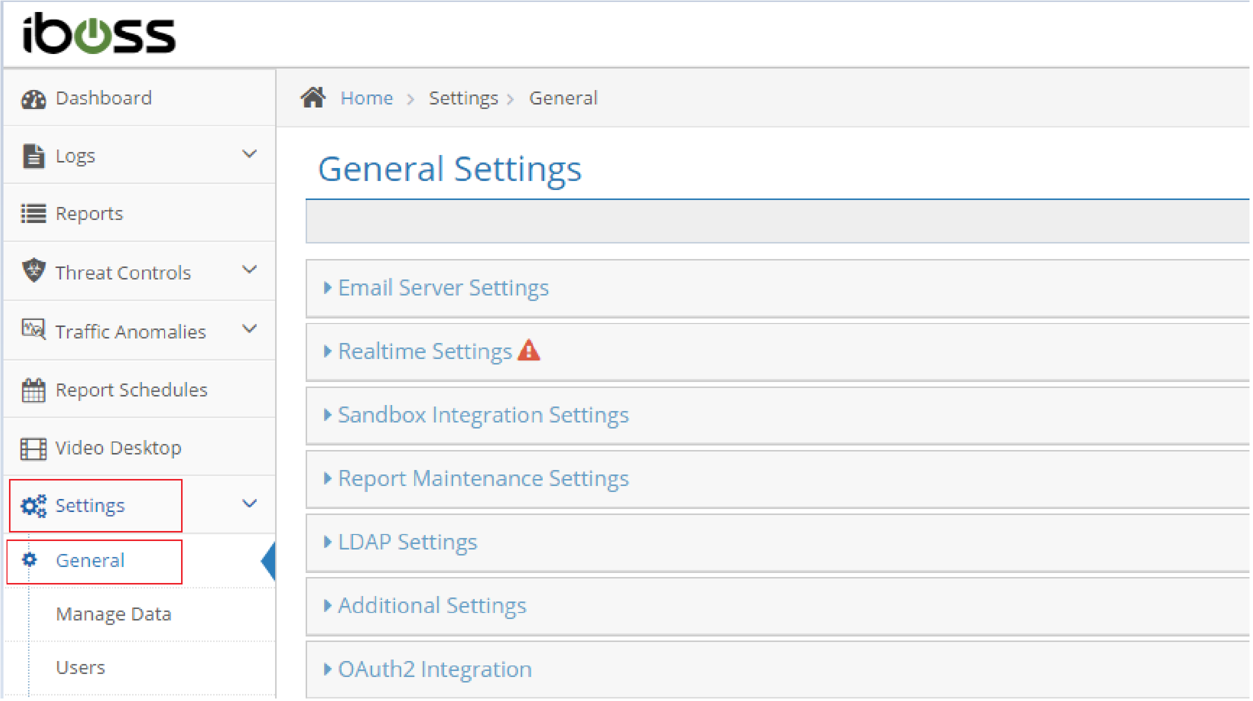


Figure 2

3. Click on **General→Syslog Logging** option is available.

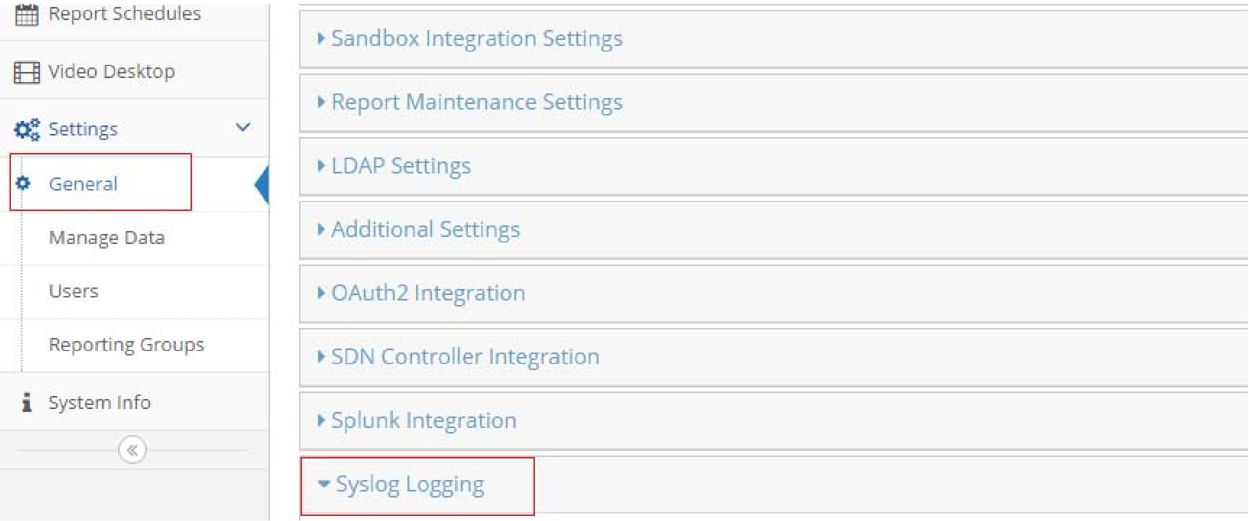
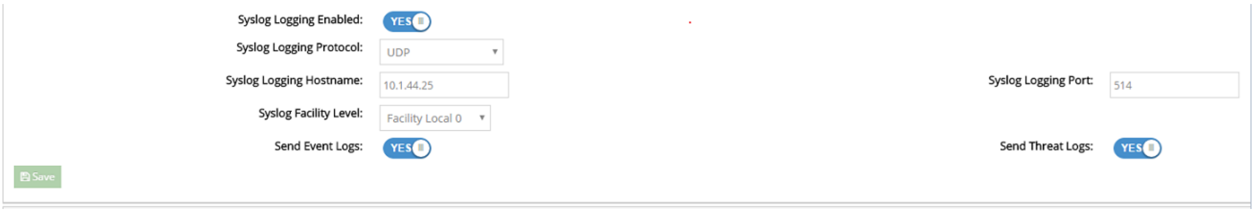


Figure 3

4. Configure **Syslog logging** as given below:



Syslog Logging Enabled: YES

Syslog Logging Protocol: UDP

Syslog Logging Hostname: 10.1.44.25

Syslog Logging Port: 514

Syslog Facility Level: Facility Local 0

Send Event Logs: YES

Send Threat Logs: YES

Figure 4

Syslog Logging to → YES

Send Event Logs → YES

Send Threat Logs → YES

Enter the following:

Syslog Logging Protocol: UDP

Syslog Logging Hostname: IP Address

Syslog Facility Level: Facility local0

Syslog Logging Port: 514

5. Click **Save**.

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 iboss.

Categories

- **iboss: Web traffic allowed**

  This category provides information related to specific website URLs allowed on the network.

- **iboss: Web traffic blocked**

  This category provides information related to specific website URLs blocked on the network.

Alerts

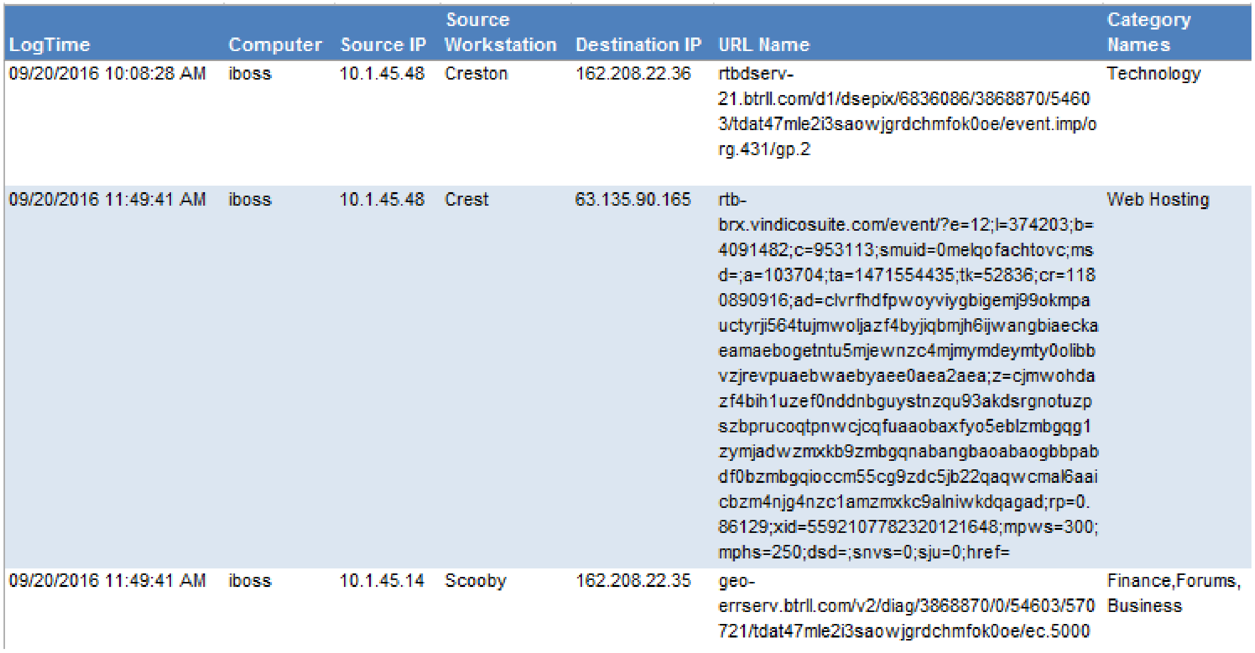
- **iboss: Web traffic blocked**

  This alert is generated when specific blocked Website URLs are accessed by the user.

Flex Reports

- **iboss-Web traffic allowed**

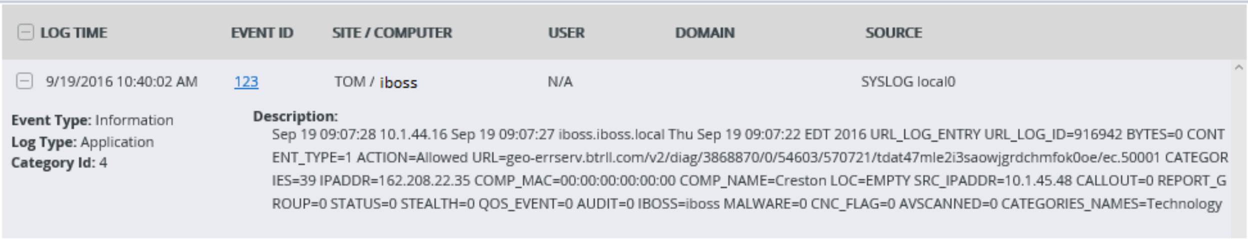
  This report provides the information related to URL and the respective category names being allowed by iboss.



LogTime	Computer	Source IP	Source Workstation	Destination IP	URL Name	Category Names
09/20/2016 10:08:28 AM	iboss	10.1.45.48	Creston	162.208.22.36	rtbdserv-21.btrll.com/d1/dsepix/6836086/3868870/54603/tdat47mle2i3saowjgrdchmfok0oe/event.imp/org.431/gp.2	Technology
09/20/2016 11:49:41 AM	iboss	10.1.45.48	Crest	63.135.90.165	rtb-brx.vindicosuite.com/event/?e=12;l=374203;b=4091482;c=953113;smuid=0melqofachtovc;msd=;a=103704;ta=1471554435;tk=52836;cr=1180890916;ad=clvrfhdfpwoyviygbigemj99okmpauctyrji564tujmwoljazf4byjiqbmjh6ijwangbiaeckaeamaebogetntu5mjewnzc4mjmymdeymty0olibbvzjrevpuaebwaebyaee0aea2aea;z=cjmwohdazf4bih1uzef0nddnbguystnzqu93akdsrgnotuzpszbprucoqtpnwcjcqfuaaobaxfyo5eblzmbgqg1zymjadwzmxkb9zmbgqnabangbaoabaogbbpabdf0bzmbgqioccm55cg9zdc5jb22qaqwcmal6aaicbzm4njg4nzc1amzmxkc9alniwkdqagad;rp=0.86129;xid=5592107782320121648;mpws=300;mphs=250;dsd=;snvs=0;sju=0;href=	Web Hosting
09/20/2016 11:49:41 AM	iboss	10.1.45.14	Scooby	162.208.22.35	geo-errserv.btrll.com/v2/diag/3868870/0/54603/570721/tdat47mle2i3saowjgrdchmfok0oe/ec.5000	Finance,Forums, Business

Figure 5

Logs Considered:



LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
9/19/2016 10:40:02 AM	123	TOM / iboss	N/A		SYSLOG local0

Event Type: Information
Log Type: Application
Category Id: 4

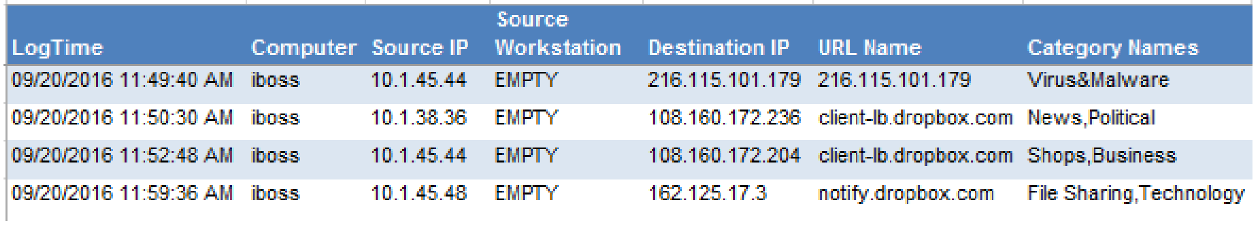
Description:

```
Sep 19 09:07:28 10.1.44.16 Sep 19 09:07:27 iboss.iboss.local Thu Sep 19 09:07:22 EDT 2016 URL_LOG_ENTRY URL_LOG_ID=916942 BYTES=0 CONT
ENT_TYPE=1 ACTION=Allowed URL=geo-errserv.btrll.com/v2/diag/3868870/0/54603/570721/tdat47mle2i3saowjgrdchmfok0oe/ec.50001 CATEGOR
IES=39 IPADDR=162.208.22.35 COMP_MAC=00:00:00:00:00:00 COMP_NAME=Creston LOC=EMPTY SRC_IPADDR=10.1.45.48 CALLOUT=0 REPORT_G
ROUP=0 STATUS=0 STEALTH=0 QOS_EVENT=0 AUDIT=0 IBOSS=iboss MALWARE=0 CNC_FLAG=0 AVSCANNED=0 CATEGORIES_NAMES=Technology
```

Figure 6

- **Iboss-Web traffic blocked**

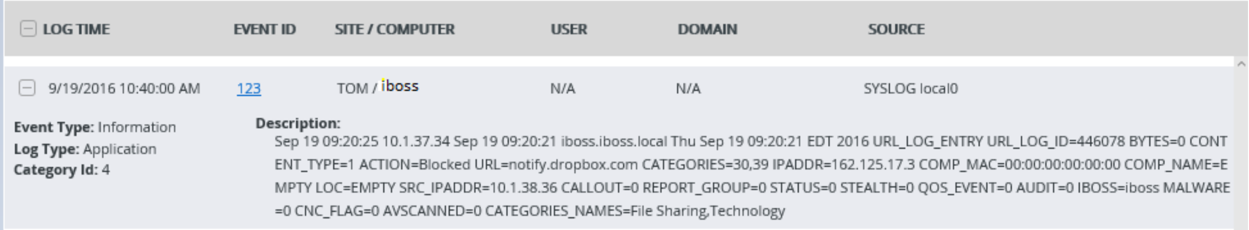
  This report provides the information related to URLs and the respective category names being blocked by iboss.



LogTime	Computer	Source IP	Source Workstation	Destination IP	URL Name	Category Names
09/20/2016 11:49:40 AM	iboss	10.1.45.44	EMPTY	216.115.101.179	216.115.101.179	Virus&Malware
09/20/2016 11:50:30 AM	iboss	10.1.38.36	EMPTY	108.160.172.236	client-lb.dropbox.com	News,Political
09/20/2016 11:52:48 AM	iboss	10.1.45.44	EMPTY	108.160.172.204	client-lb.dropbox.com	Shops,Business
09/20/2016 11:59:36 AM	iboss	10.1.45.48	EMPTY	162.125.17.3	notify.dropbox.com	File Sharing,Technology

Figure 7

Logs Considered:



LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
9/19/2016 10:40:00 AM	123	TOM / iboss	N/A	N/A	SYSLOG local0

Event Type: Information
Log Type: Application
Category Id: 4

Description:

```
Sep 19 09:20:25 10.1.37.34 Sep 19 09:20:21 iboss.iboss.local Thu Sep 19 09:20:21 EDT 2016 URL_LOG_ENTRY URL_LOG_ID=446078 BYTES=0 CONT
ENT_TYPE=1 ACTION=Blocked URL=notify.dropbox.com CATEGORIES=30,39 IPADDR=162.125.17.3 COMP_MAC=00:00:00:00:00:00 COMP_NAME=E
MPTY LOC=EMPTY SRC_IPADDR=10.1.38.36 CALLOUT=0 REPORT_GROUP=0 STATUS=0 STEALTH=0 QOS_EVENT=0 AUDIT=0 IBOSS=iboss MALWARE
=0 CNC_FLAG=0 AVSCANNED=0 CATEGORIES_NAMES=File Sharing,Technology
```

Figure 8

Import iboss Secure Web Gateway knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Parsing Rule
- Knowledge Objects
- Flex Reports

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

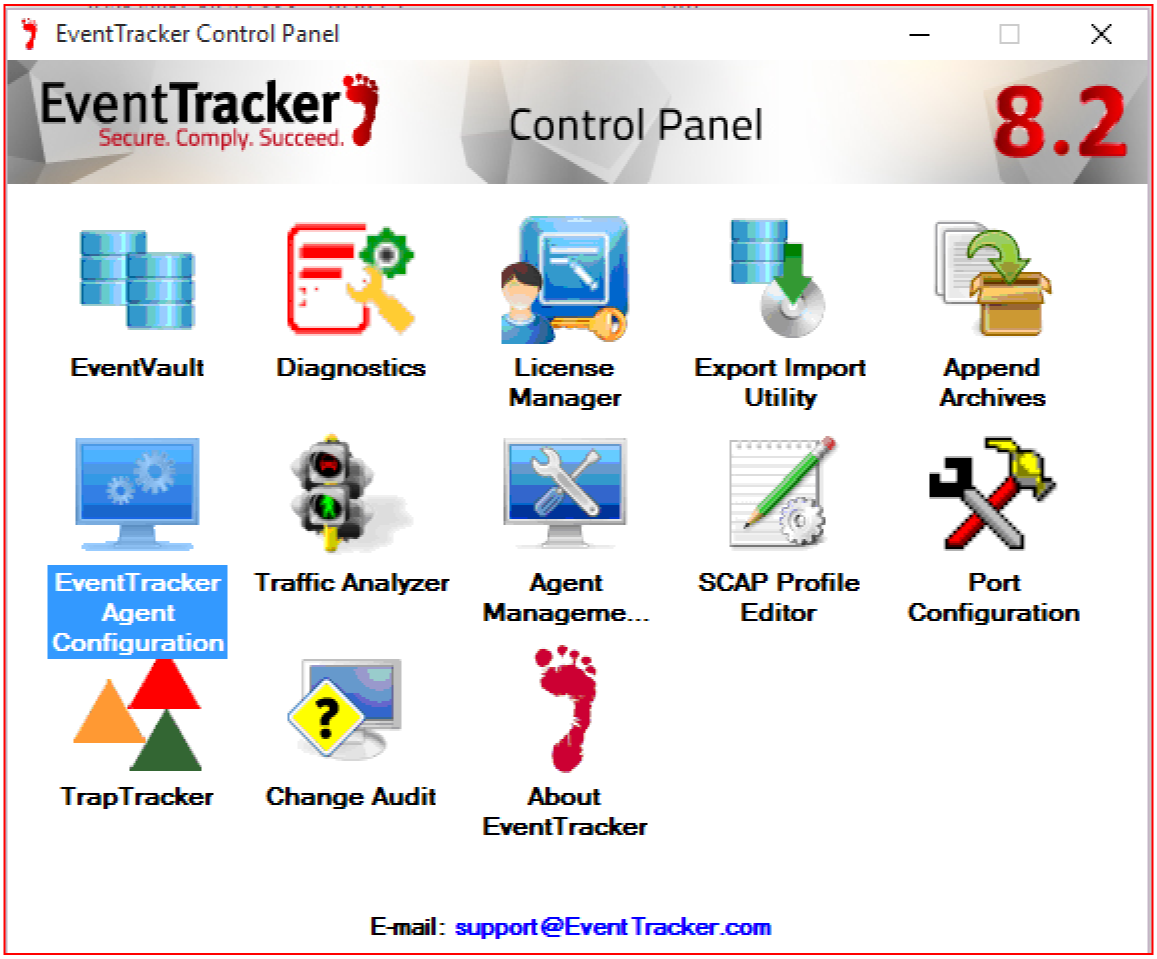


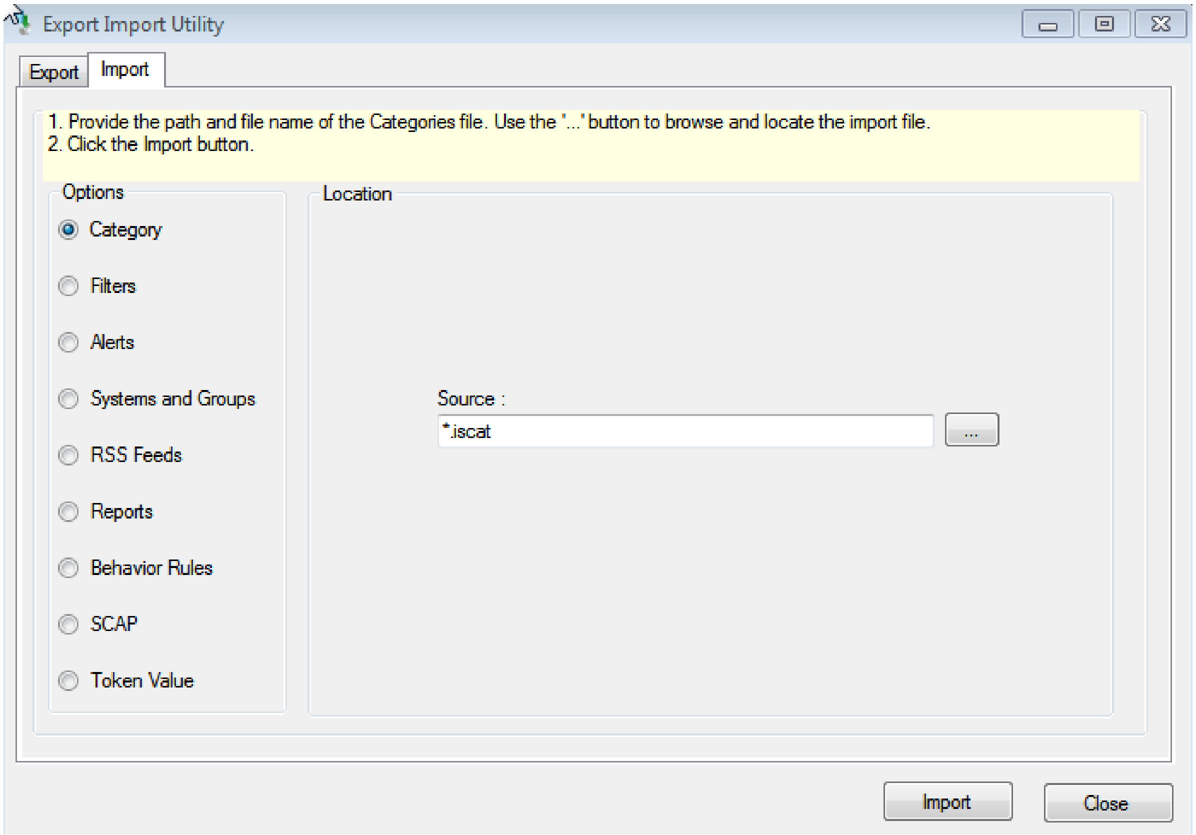
Figure 9

3. Click the **Import** tab.

Category

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

2. Locate the **All iboss group of categories.iscat** file, and then click **Open** button.



1. Provide the path and file name of the Categories file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

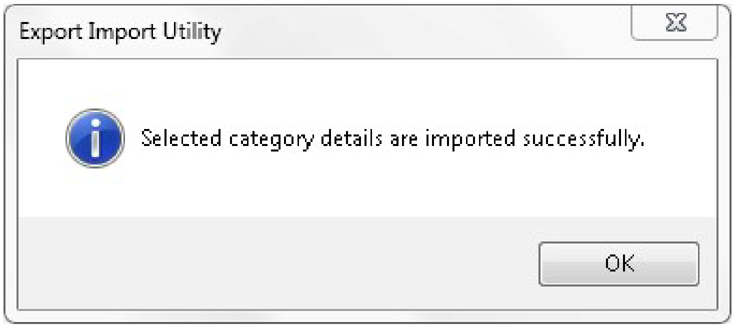
● Category
○ Filters
○ Alerts
○ Systems and Groups
○ RSS Feeds
○ Reports
○ Behavior Rules
○ SCAP
○ Token Value

Source : *.iscat

Figure 10

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

   EventTracker displays success message.



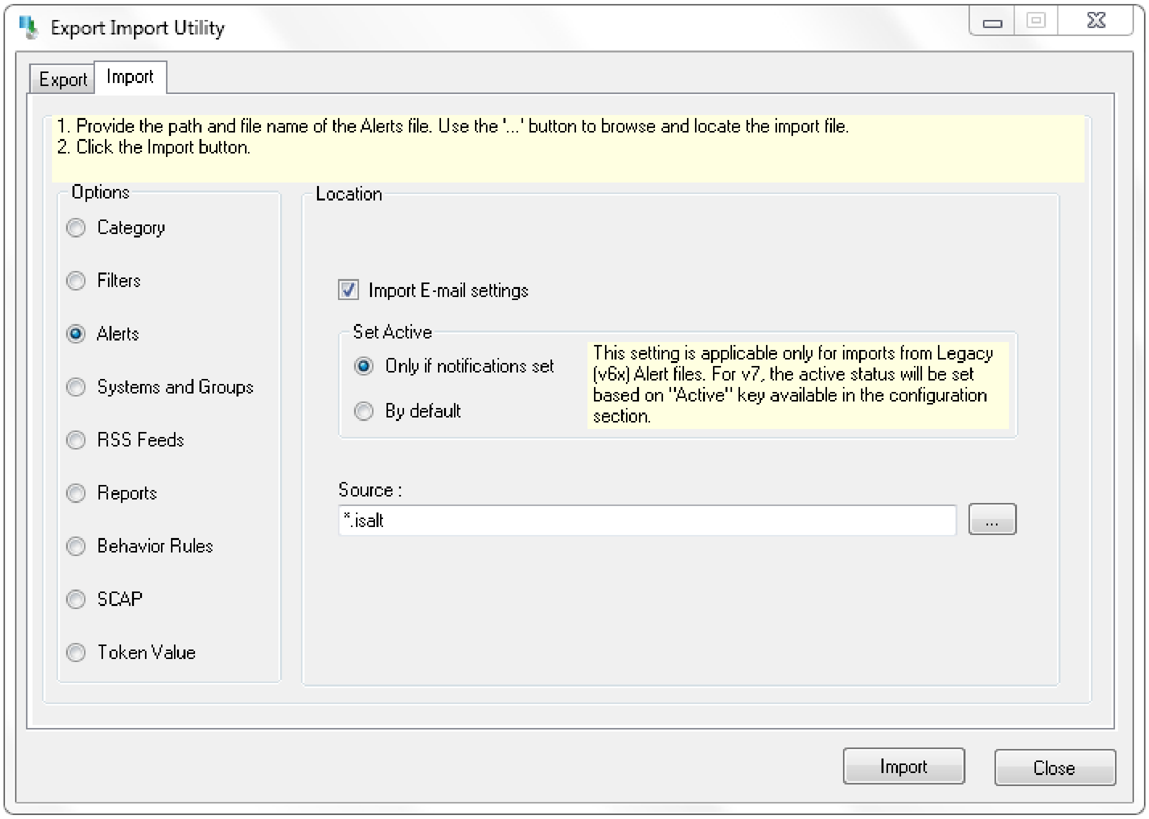
Selected category details are imported successfully.

Figure 11

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 iboss group of alerts.isalt** file, and then click the **Open** button.



1. Provide the path and file name of the Alerts file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Options

○ Category
○ Filters
● Alerts
○ Systems and Groups
○ RSS Feeds
○ Reports
○ Behavior Rules
○ SCAP
○ Token Value

Location

☑ Import E-mail settings

Set Active

● Only if notifications set
○ By default

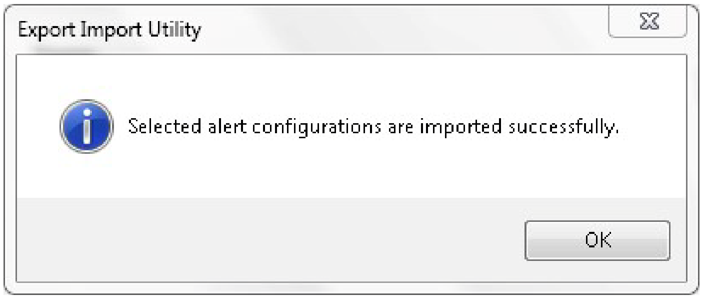
This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.

Source : *.isalt

Figure 12

2. To import alerts, click the **Import** button.

   EventTracker displays success message.



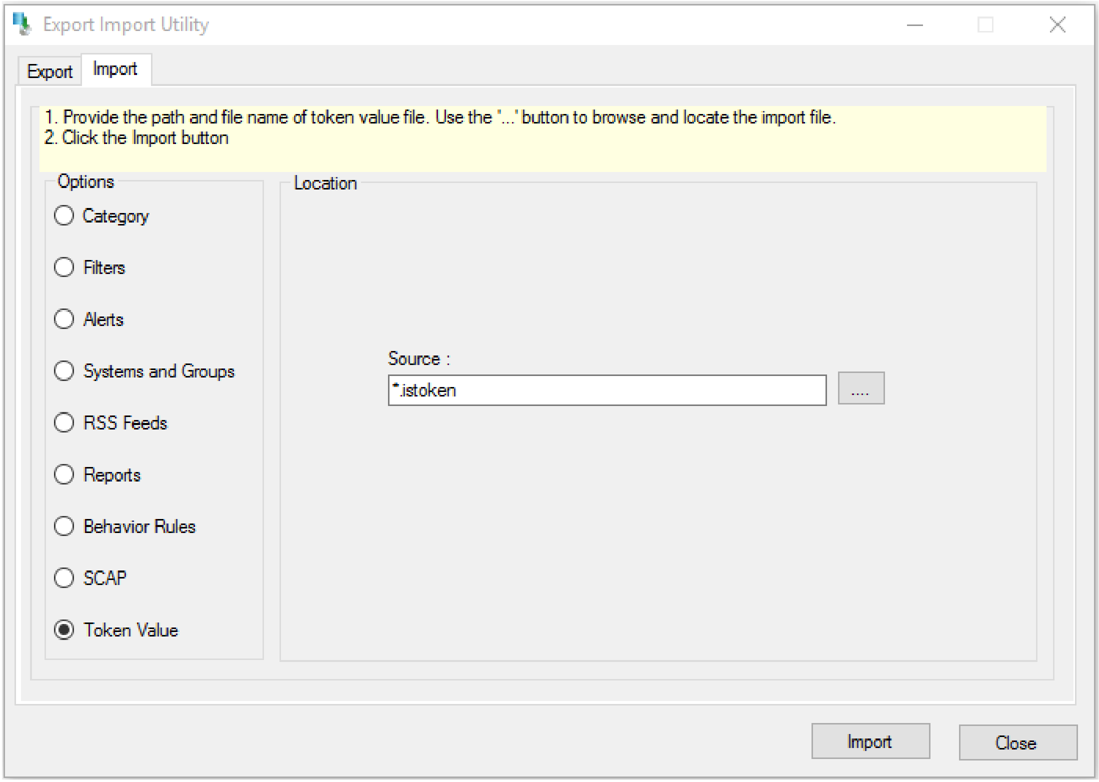
Selected alert configurations are imported successfully.

Figure 13

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

Parsing Rules

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



Export Import Utility

Export | Import

1. Provide the path and file name of token value file. Use the '...' button to browse and locate the import file.
2. Click the Import button

Options

○ Category
○ Filters
○ Alerts
○ Systems and Groups
○ RSS Feeds
○ Reports
○ Behavior Rules
○ SCAP
● Token Value

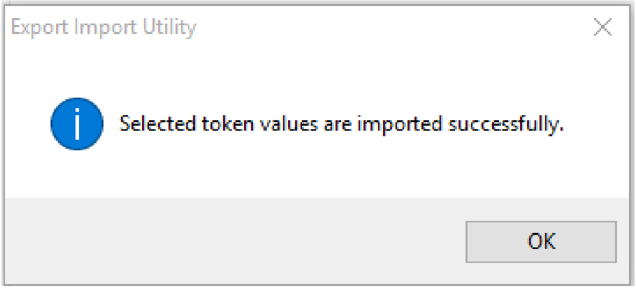
Location

Source : *.istoken

Figure 14

2. Locate the **All iboss group of parsing rules.istoken** file, and then click the **Open** button.

3. To import tokens, click the **Import** button.
   EventTracker displays success message.



Export Import Utility

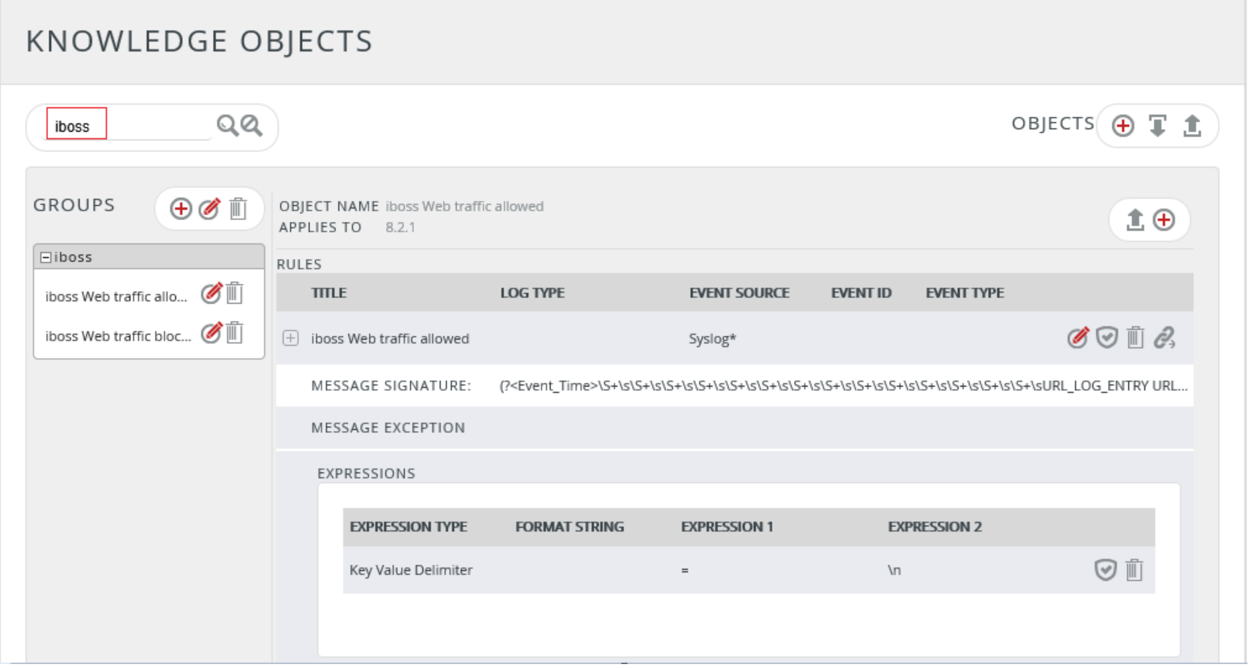
Selected token values are imported successfully.

Figure 15

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

Knowledge Object

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



KNOWLEDGE OBJECTS

iboss

OBJECTS

GROUPS

⊟iboss
- iboss Web traffic allo...
- iboss Web traffic bloc...

OBJECT NAME iboss Web traffic allowed
APPLIES TO 8.2.1

RULES

TITLE	LOG TYPE	EVENT SOURCE	EVENT ID	EVENT TYPE
iboss Web traffic allowed		Syslog*		

MESSAGE SIGNATURE: (?<Event_Time>\S+\s\S+\s\S+\s\S+\s\S+\s\S+\s\S+\s\S+\s\S+\s\S+\s\S+\s\S+\s\S+\s\S+\sURL_LOG_ENTRY URL...

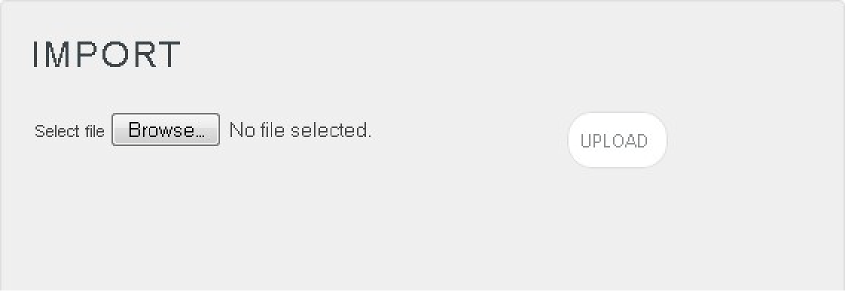
MESSAGE EXCEPTION

EXPRESSIONS

EXPRESSION TYPE	FORMAT STRING	EXPRESSION 1	EXPRESSION 2
Key Value Delimiter		=	\n

Figure 16

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



IMPORT

Select file Browse... No file selected.

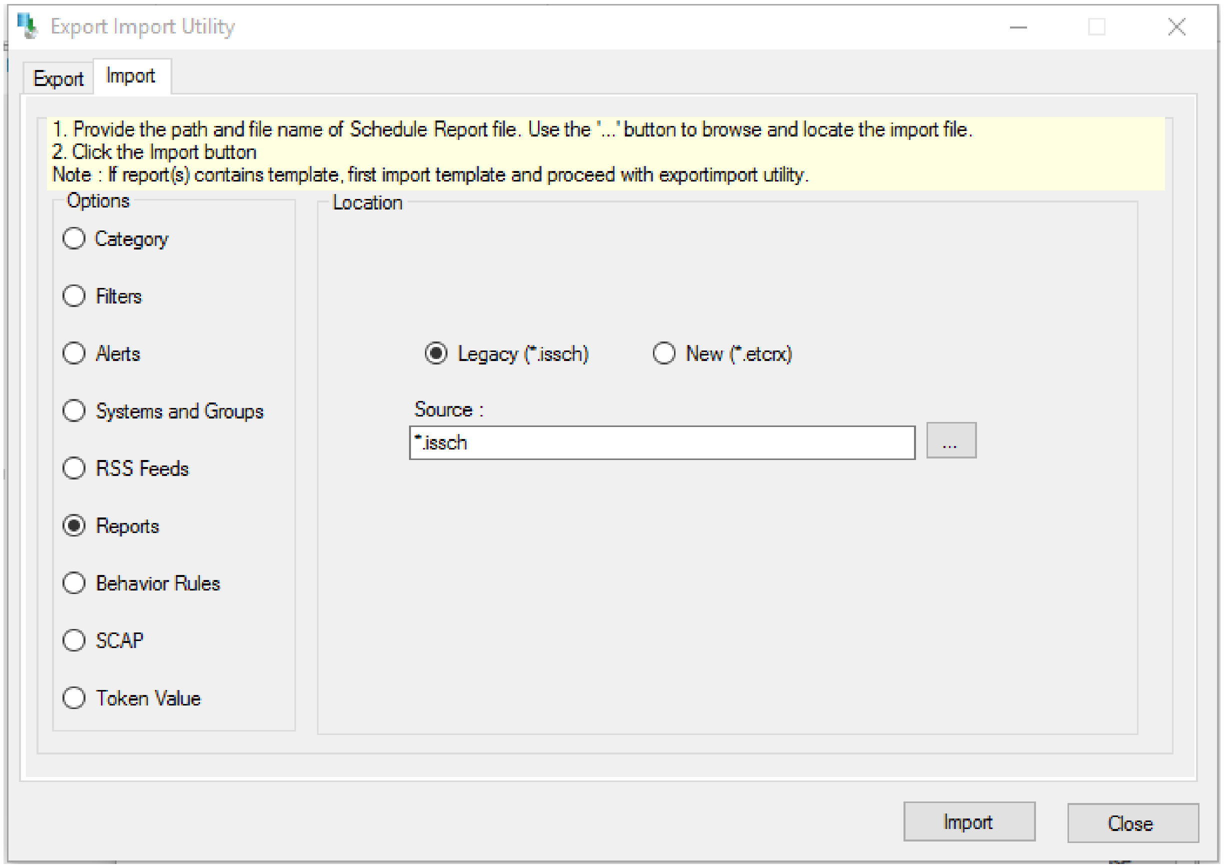
Figure 17

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

Flex Reports

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

2. Locate the **All iboss group of flex reports.issch** file, and then click the **Open** button.

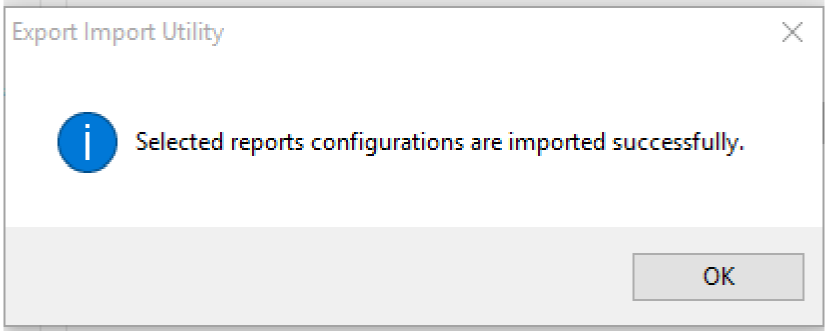


1. Provide the path and file name of Schedule Report file. Use the '...' button to browse and locate the import file.
2. Click the Import button
Note : If report(s) contains template, first import template and proceed with exportimport utility.

Source : *.issch

Figure 18

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



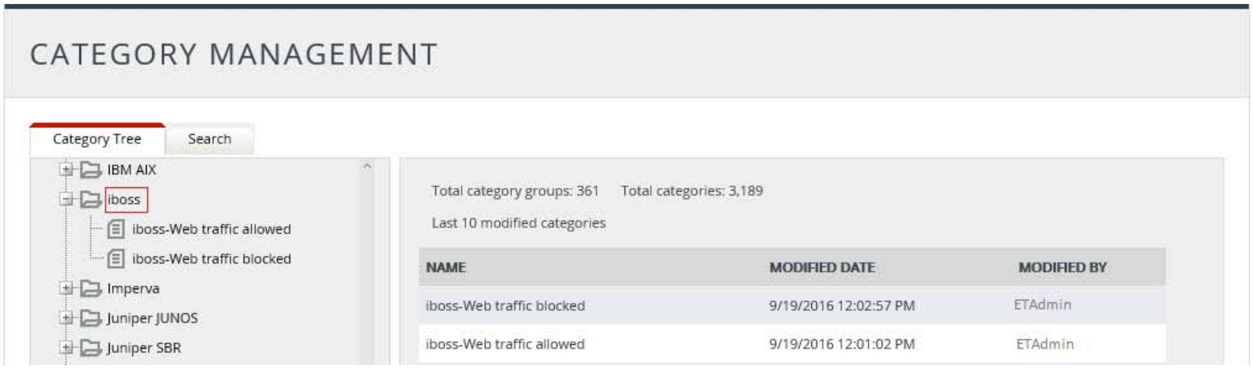
Selected reports configurations are imported successfully.

Figure 19

Verify iboss Secure Web Gateway knowledge pack in EventTracker

Category

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Categories**.
2. In the **Category Tree**, expand **iboss** group folder to see the imported categories.



CATEGORY MANAGEMENT

Total category groups: 361   Total categories: 3,189

Last 10 modified categories

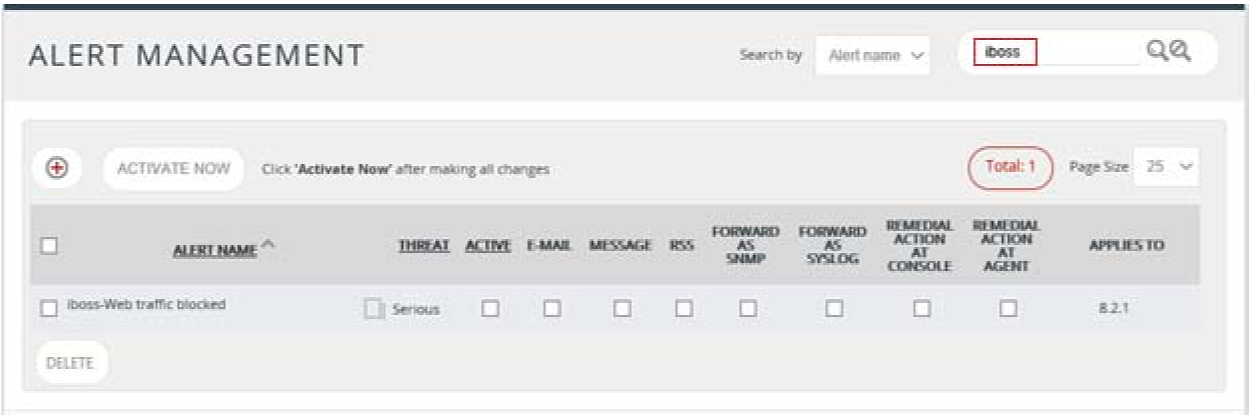
NAME	MODIFIED DATE	MODIFIED BY
iboss-Web traffic blocked	9/19/2016 12:02:57 PM	ETAdmin
iboss-Web traffic allowed	9/19/2016 12:01:02 PM	ETAdmin

Figure 20

Alerts

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

   Alert Management page will display the imported **iboss** alert.



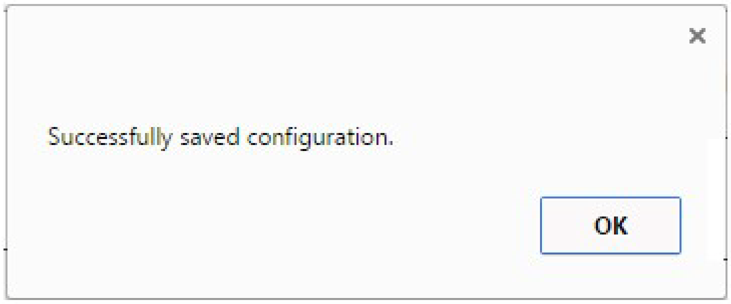
ALERT MANAGEMENT

Click '**Activate Now**' after making all changes

□	ALERT NAME	THREAT	ACTIVE	E-MAIL	MESSAGE	RSS	FORWARD AS SNMP	FORWARD AS SYSLOG	REMEDIAL ACTION AT CONSOLE	REMEDIAL ACTION AT AGENT	APPLIES TO
□	iboss-Web traffic blocked	Serious	□	□	□	□	□	□	□	□	8.2.1

Figure 21

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



Successfully saved configuration.

Figure 22

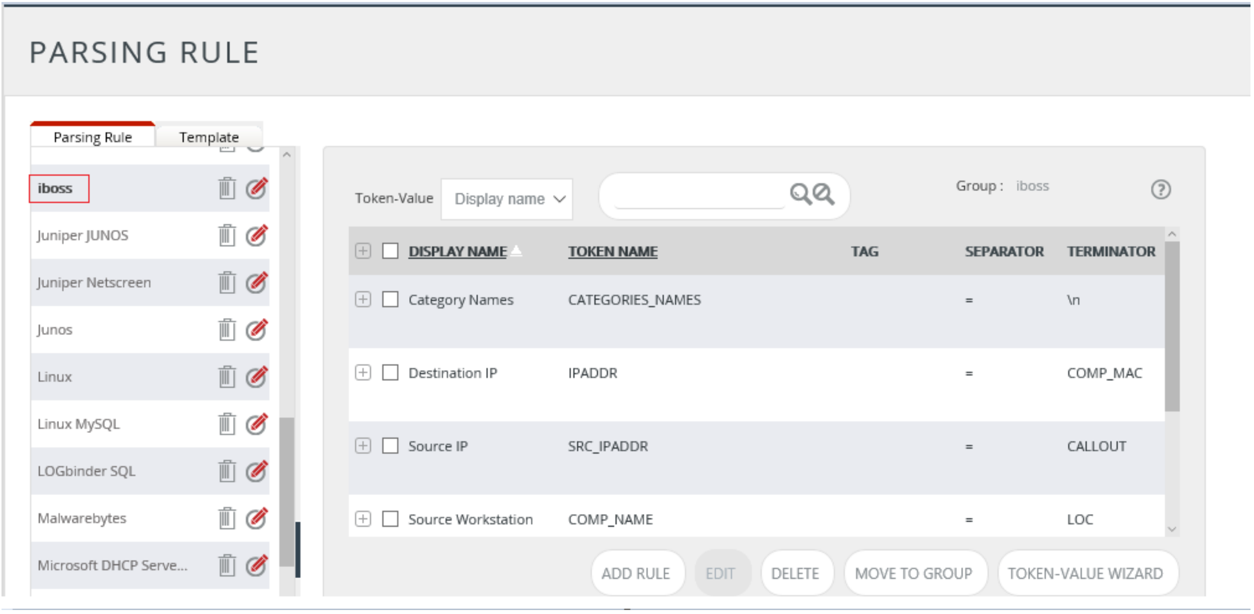
4. Click the **OK** button, and then click the **Activate now** button.

   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.

Parsing Rules

1. In the **EventTracker Enterprise** web interface, click the **Admin** menu, and then click **Parsing Rules**.



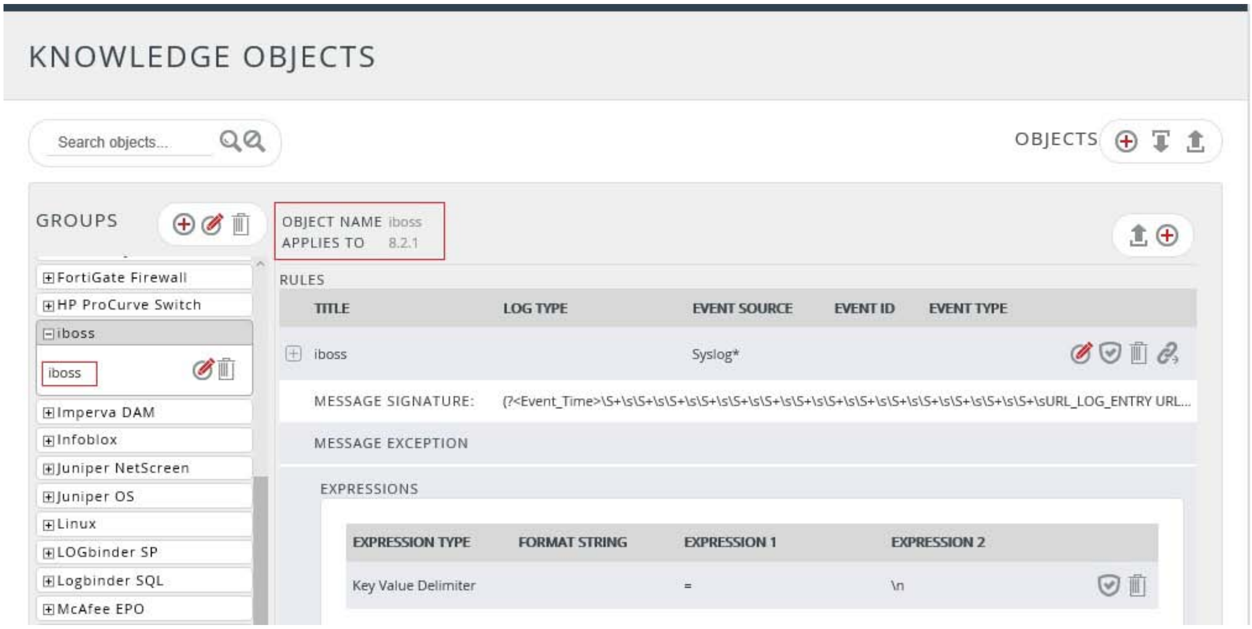
DISPLAY NAME	TOKEN NAME	TAG	SEPARATOR	TERMINATOR
Category Names	CATEGORIES_NAMES		=	\n
Destination IP	IPADDR		=	COMP_MAC
Source IP	SRC_IPADDR		=	CALLOUT
Source Workstation	COMP_NAME		=	LOC

Figure 23

Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**.

2. Scroll down and select **iboss** in **Objects** pane. Imported **iboss** object details are shown.



KNOWLEDGE OBJECTS

Search objects...

OBJECTS

GROUPS

OBJECT NAME iboss
APPLIES TO 8.2.1

- FortiGate Firewall
- HP ProCurve Switch
- iboss
  - iboss
- Imperva DAM
- Infoblox
- Juniper NetScreen
- Juniper OS
- Linux
- LOGbinder SP
- Logbinder SQL
- McAfee EPO

RULES

TITLE	LOG TYPE	EVENT SOURCE	EVENT ID	EVENT TYPE
iboss		Syslog*		

MESSAGE SIGNATURE: (?<Event_Time>\S+\s\S+\s\S+\s\S+\s\S+\s\S+\s\S+\s\S+\s\S+\s\S+\s\S+\s\S+\s\S+\s\S+\sURL_LOG_ENTRY URL...

MESSAGE EXCEPTION

EXPRESSIONS

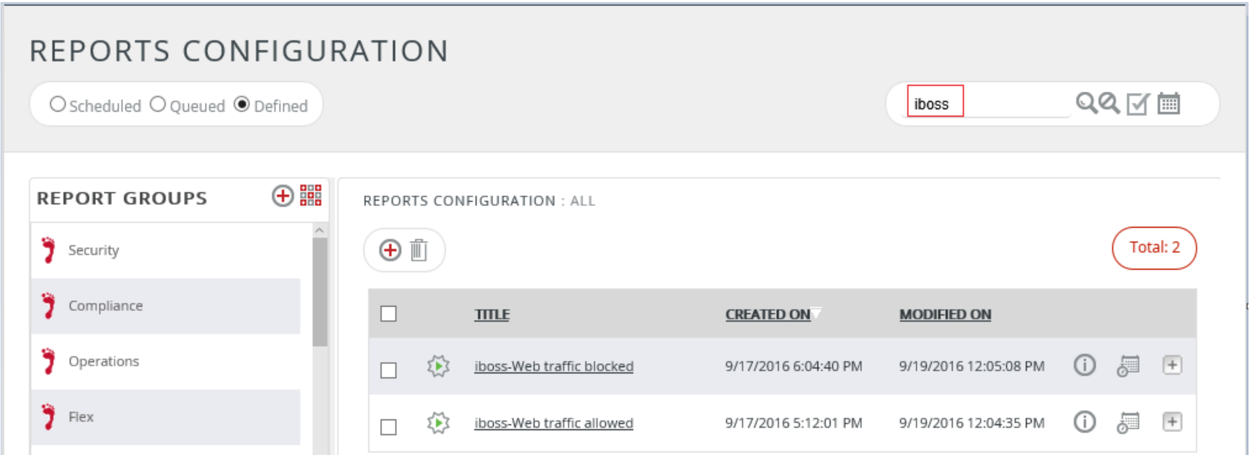
EXPRESSION TYPE	FORMAT STRING	EXPRESSION 1	EXPRESSION 2
Key Value Delimiter		=	\n

Figure 24

Flex Reports

1. In the **EventTracker Enterprise** web interface, click the **Reports** menu, and then select **Configuration**.
2. In **Reports Configuration** pane, select **Defined** option.
3. In search box enter '**iboss'**, and then click the **Search** button.

EventTracker displays Flex reports of **iboss.**


REPORTS CONFIGURATION

○ Scheduled ○ Queued ● Defined

iboss

REPORT GROUPS

- Security
- Compliance
- Operations
- Flex

REPORTS CONFIGURATION : ALL

Total: 2

□		TITLE	CREATED ON	MODIFIED ON
□		iboss-Web traffic blocked	9/17/2016 6:04:40 PM	9/19/2016 12:05:08 PM
□		iboss-Web traffic allowed	9/17/2016 5:12:01 PM	9/19/2016 12:04:35 PM

Figure 25

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.

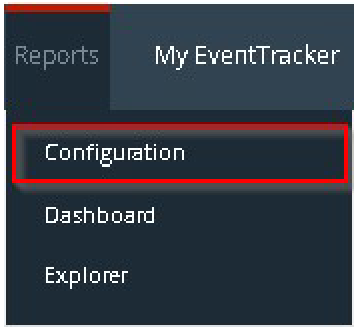
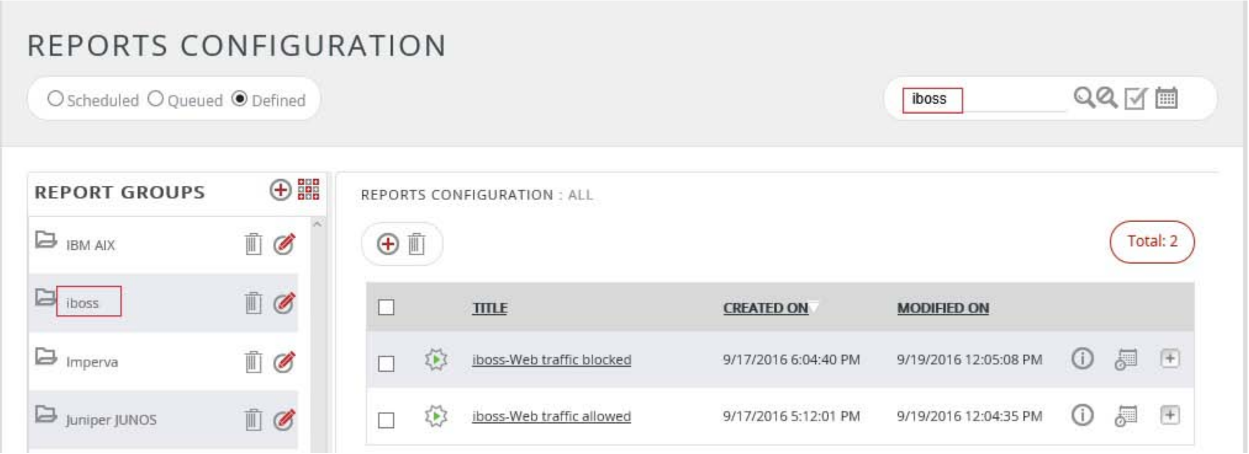


Figure 26

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



REPORTS CONFIGURATION

○ Scheduled ○ Queued ● Defined

iboss

REPORT GROUPS

- IBM AIX
- iboss
- Imperva
- Juniper JUNOS

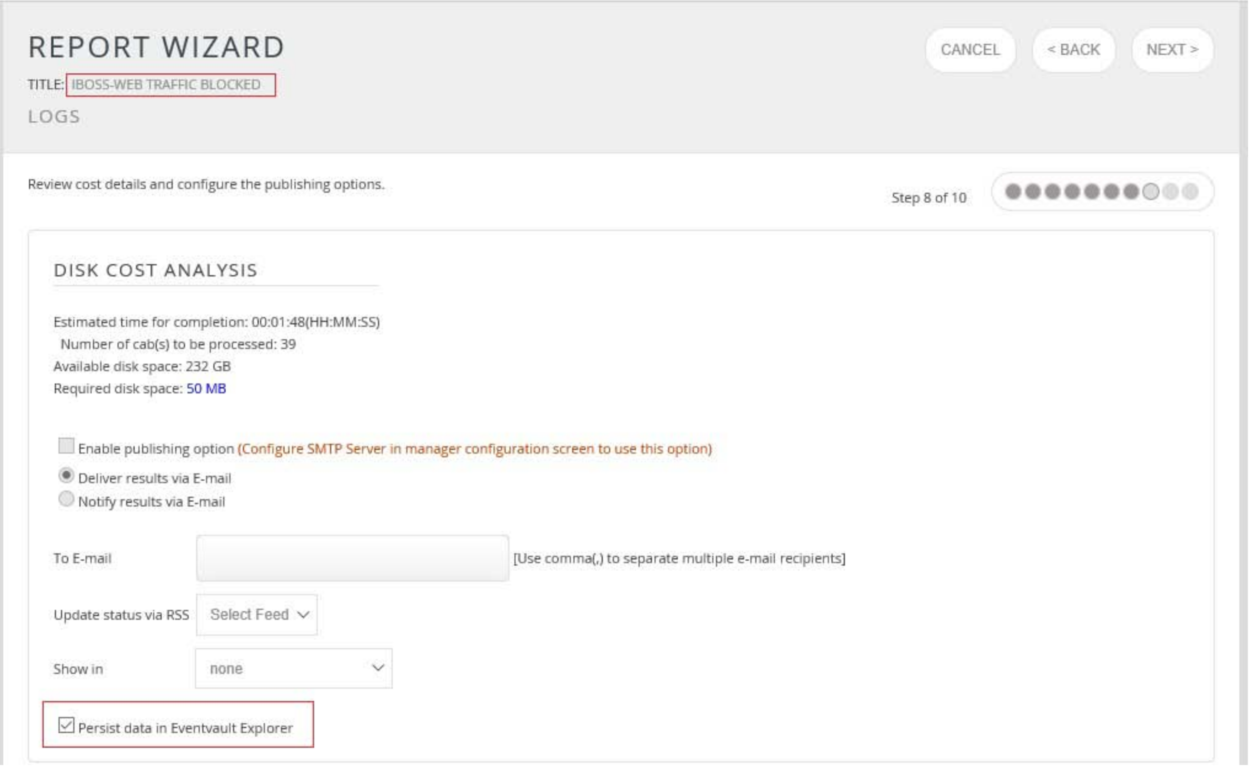
REPORTS CONFIGURATION : ALL

Total: 2

□		TITLE	CREATED ON	MODIFIED ON
□		iboss-Web traffic blocked	9/17/2016 6:04:40 PM	9/19/2016 12:05:08 PM
□		iboss-Web traffic allowed	9/17/2016 5:12:01 PM	9/19/2016 12:04:35 PM

Figure 27

4. Click on ‘**schedule**’ to plan a report for later execution.
5. Click **Next** button to proceed.
6. In review page, check **Persist data in Eventvault Explorer** option.



REPORT WIZARD

CANCEL < BACK NEXT >

TITLE: IBOSS-WEB TRAFFIC BLOCKED

LOGS

Review cost details and configure the publishing options.

Step 8 of 10

DISK COST ANALYSIS

Estimated time for completion: 00:01:48(HH:MM:SS)
Number of cab(s) to be processed: 39
Available disk space: 232 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]

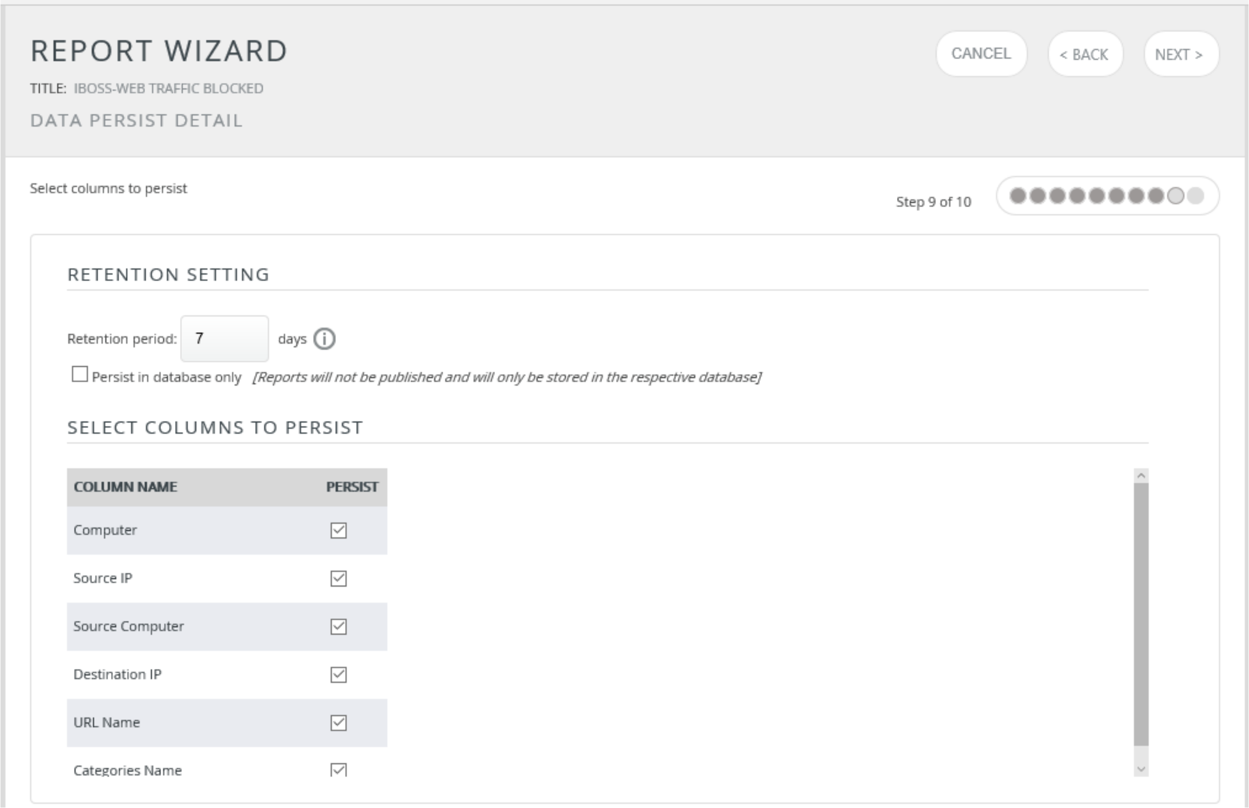
Update status via RSS: Select Feed

Show in: none

☑ Persist data in Eventvault Explorer

Figure 28

7. In next page, check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.



TITLE: IBOSS-WEB TRAFFIC BLOCKED

Select columns to persist

RETENTION SETTING

Retention period: 7 days

☐ Persist in database only *[Reports will not be published and will only be stored in the respective database]*

SELECT COLUMNS TO PERSIST

COLUMN NAME	PERSIST
Computer	☑
Source IP	☑
Source Computer	☑
Destination IP	☑
URL Name	☑
Categories Name	☑

Figure 29

8. Proceed to next step and click **Schedule** button.
9. Wait till the reports get generated.

Create Dashlets

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

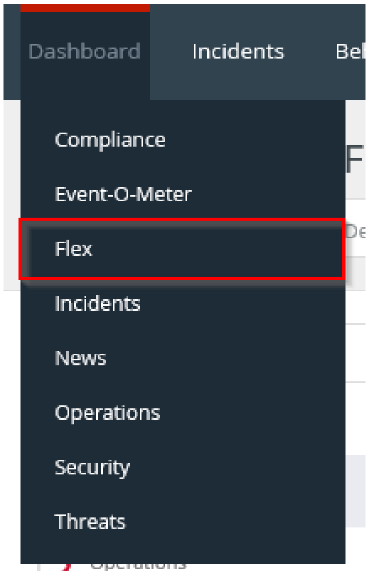
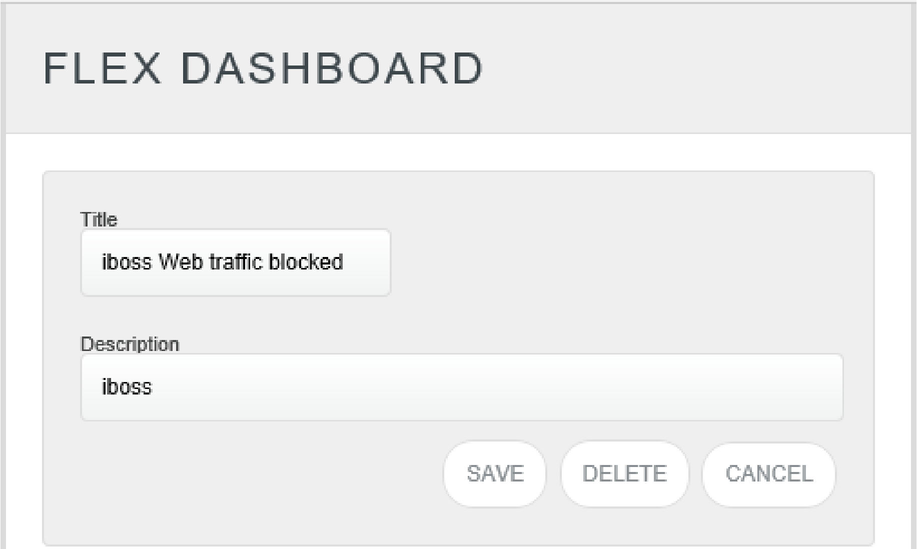


Figure 30

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

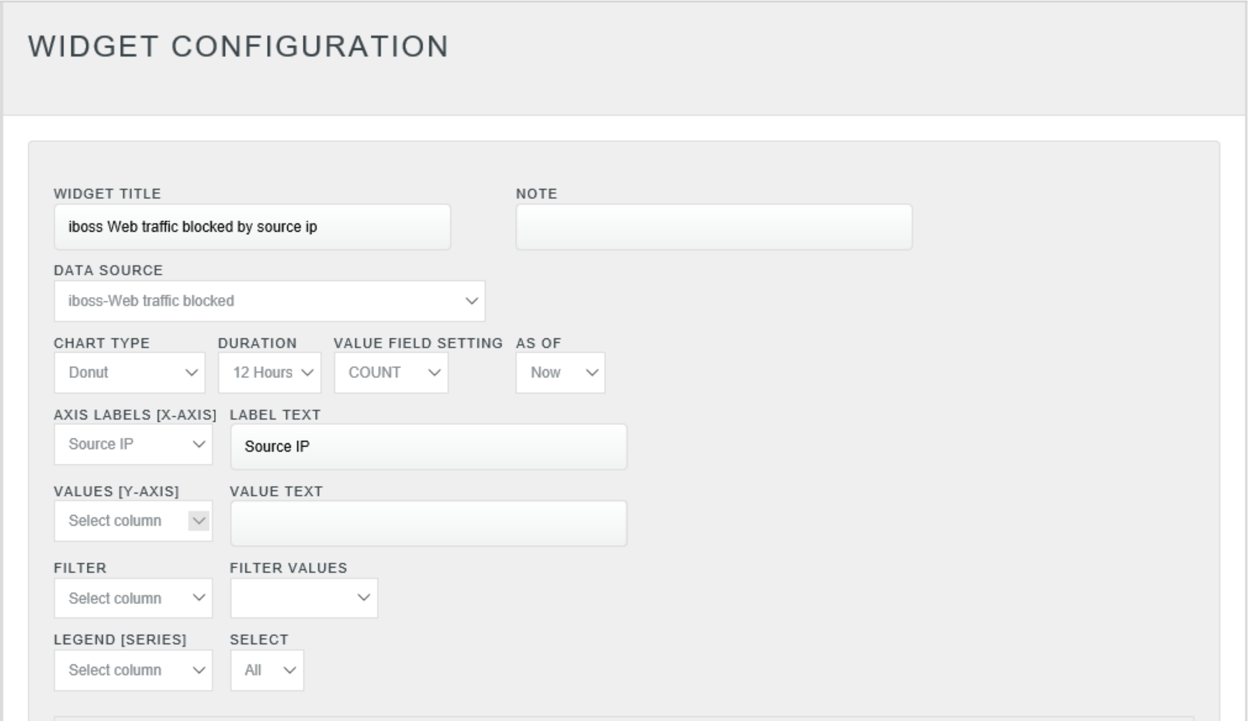

FLEX DASHBOARD

Title: iboss Web traffic blocked

Description: iboss

Figure 31

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



WIDGET CONFIGURATION

WIDGET TITLE: iboss Web traffic blocked by source ip

NOTE:

DATA SOURCE: iboss-Web traffic blocked

CHART TYPE: Donut

DURATION: 12 Hours

VALUE FIELD SETTING: COUNT

AS OF: Now

AXIS LABELS [X-AXIS]: Source IP

LABEL TEXT: Source IP

VALUES [Y-AXIS]: Select column

VALUE TEXT:

FILTER: Select column

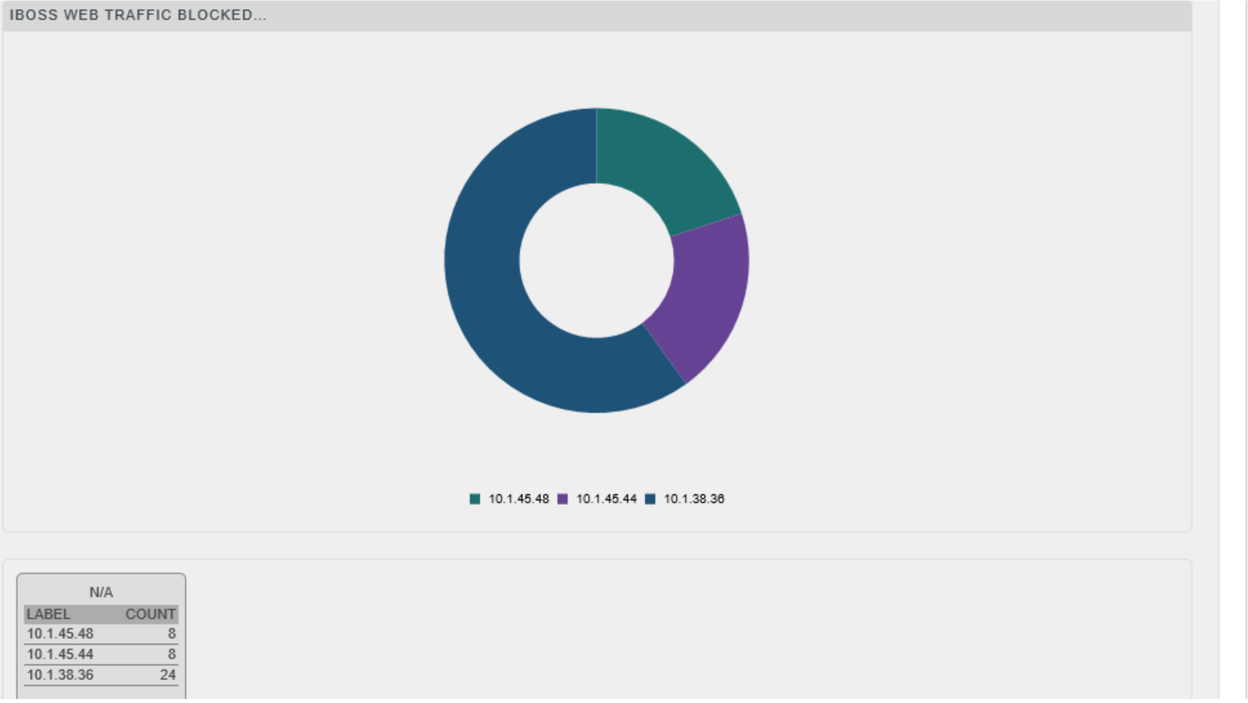
FILTER VALUES:

LEGEND [SERIES]: Select column

SELECT: All

Figure 32

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

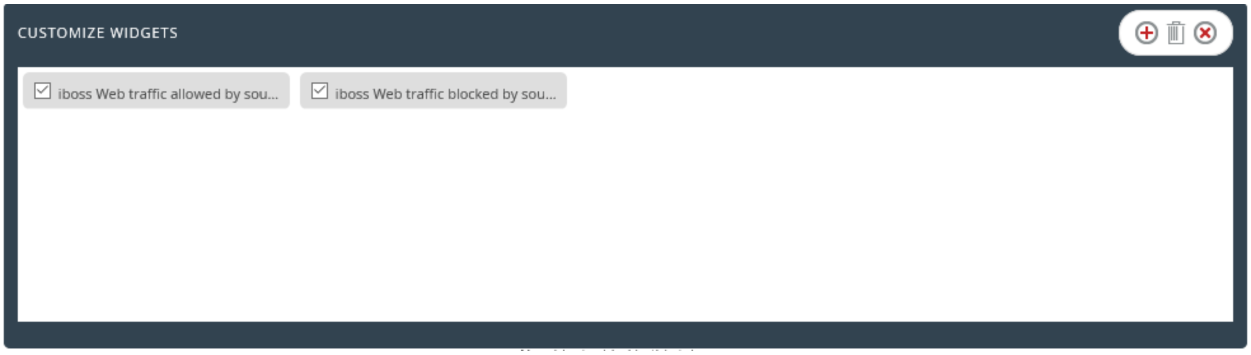


N/A

LABEL	COUNT
10.1.45.48	8
10.1.45.44	8
10.1.38.36	24

Figure 33

15. If satisfied, Click **Configure** button.


CUSTOMIZE WIDGETS

☑ iboss Web traffic allowed by sou... ☑ iboss Web traffic blocked by sou...

Figure 34

16. Click 'customize' ⚙ to locate and choose created dashlet.
17. Click ⊕ to add dashlet to earlier created dashboard.

Sample Flex Dashboards

For below dashboard **DATA SOURCE: iboss: Web traffic blocked**

1. **iboss: Web traffic blocked by source IP**

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

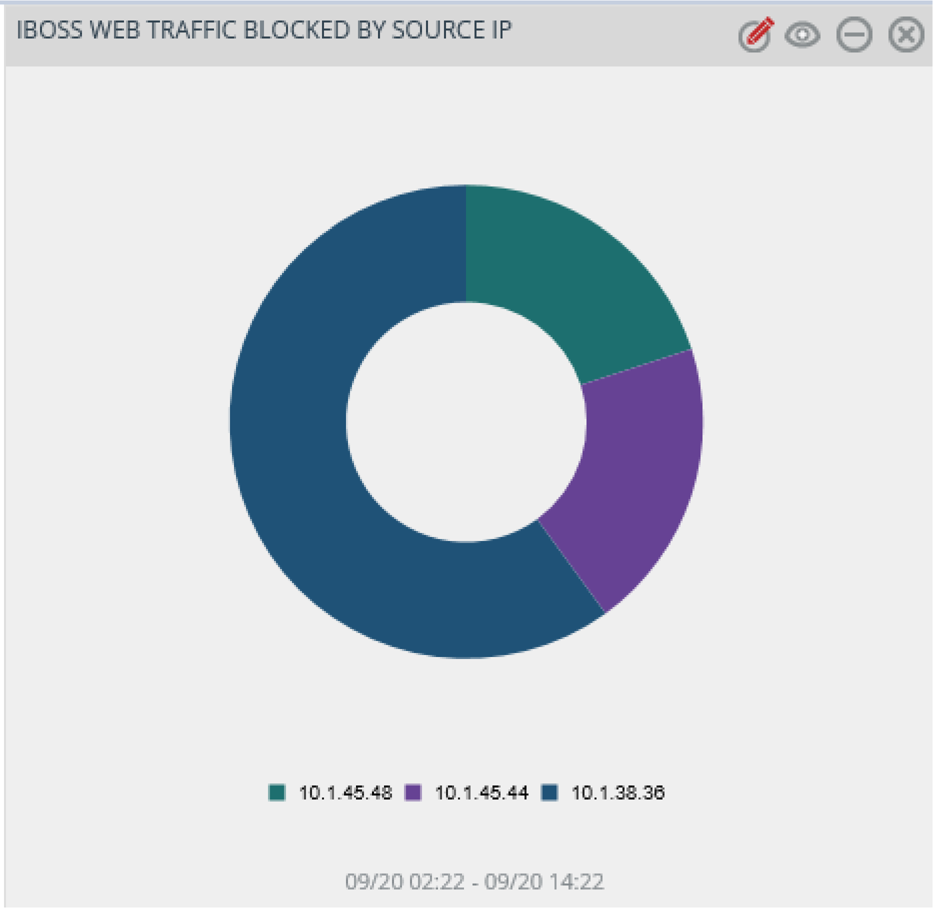


Figure 35

For below dashboard **DATA SOURCE: iboss: Web traffic allowed**

2. **iboss: Web traffic allowed by source IP**

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

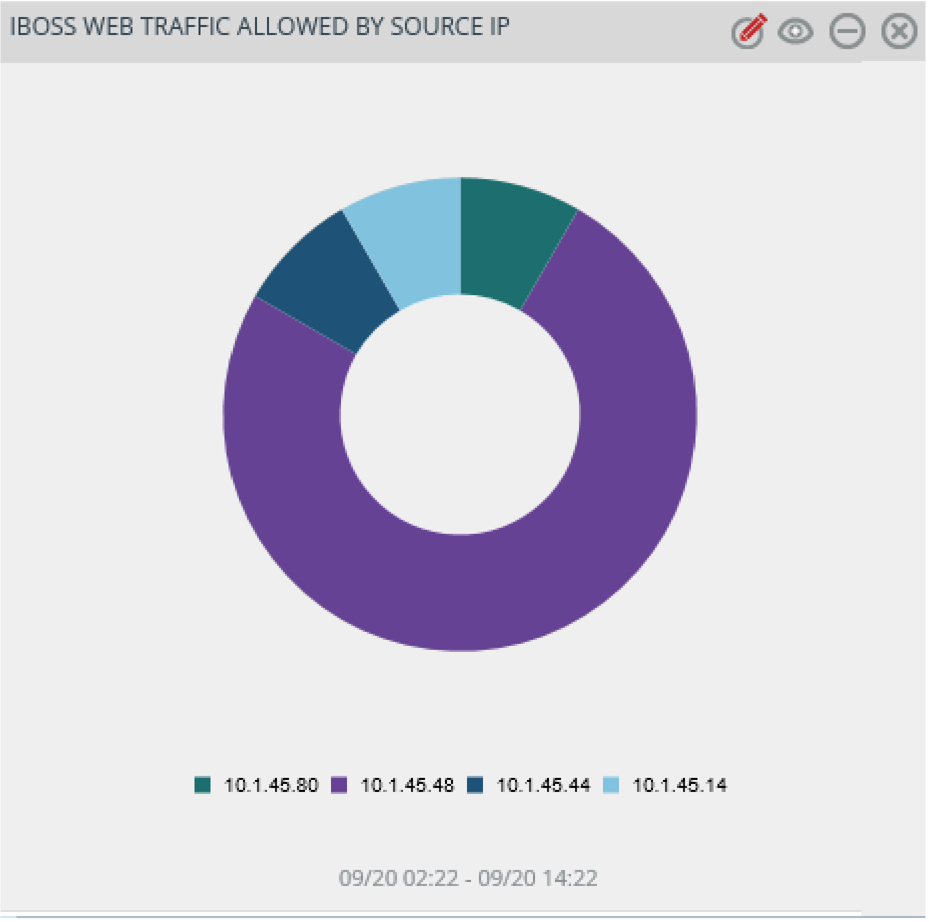


Figure 36

For below dashboard **DATA SOURCE: iboss: Web traffic blocked**

3. **iboss: Web traffic blocked by category**

- **WIDGET TITLE:** Web traffic blocked by category
  CHART TYPE: Donut
  AXIS LABELS [X-AXIS]: Categories Name
  Label Text: Category Name

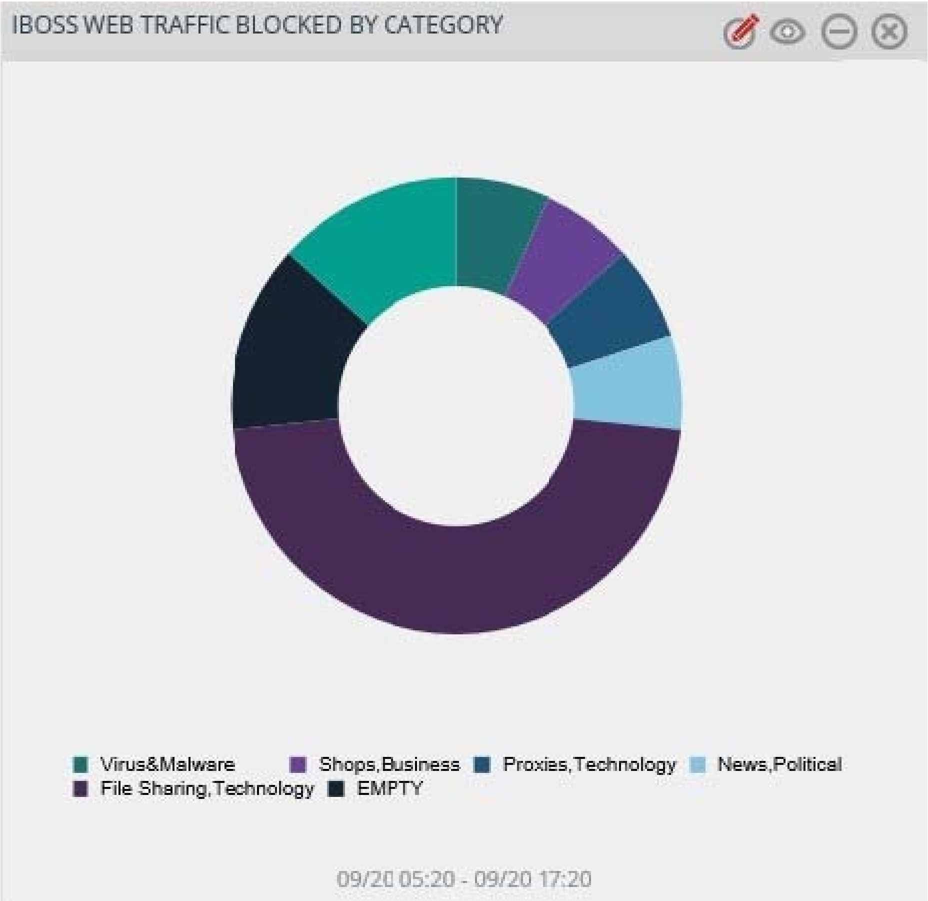


Figure 37

For below dashboard **DATA SOURCE: iboss: Web traffic allowed**

4. **iboss: Web traffic allowed by category**

- **WIDGET TITLE:** Web traffic allowed by Interface
  CHART TYPE: Donut
  AXIS LABELS [X-AXIS]: Categories Name
  Label Text: Category Name

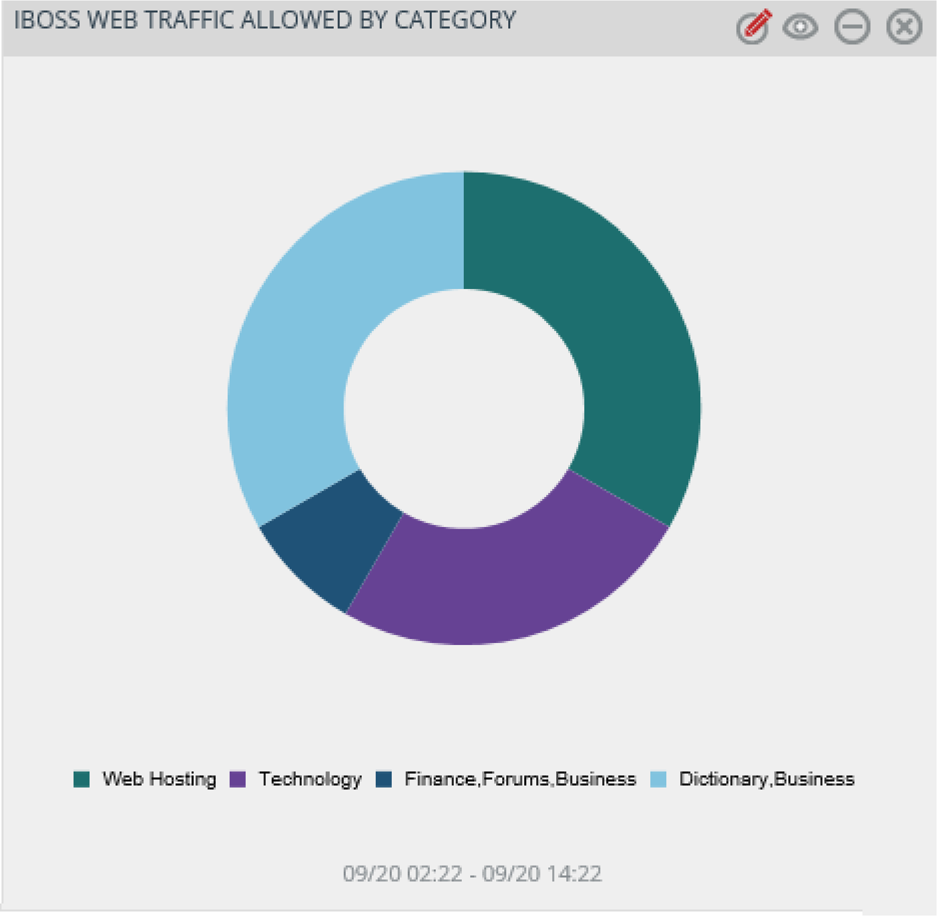


Figure 38