EventTracker
Secure. Comply. Succeed.

Integrate Websense Web Security Gateway (WSG)

EventTracker Enterprise

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

Publication Date: Jan. 19, 2017

Abstract

This guide provides instructions to configure Websense Web Security Gateway (WSG) 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 Websense Web Security Gateway (WSG) v7.7 and later.

Audience

Websense Web Security Gateway users, who wish to forward events to EventTracker Manager.

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.

Table of Contents

Abstract..1

Scope..1

Audience..1

Prerequisites..3

Integrate EventTracker with Websense WSG..3

Deploy Websense Multiplexer..3

Enable and configure SIEM integration..6

EventTracker Knowledge Pack (KP)..6

Import Websense WSG Knowledge Pack into EventTracker..8

Import Category..9

Import Alerts..10

Import Tokens..11

Import Flex Reports..12

Verify Websense WSG knowledge pack in EventTracker..13

Verify Websense WSG Categories..13

Verify Websense WSG Alerts..13

Verify Websense WSG Tokens..14

Verify Websense WSG Flex Reports..15

Create Flex Dashboards in EventTracker..16

Schedule Reports..16

Create Dashlets..19

Sample Flex Dashboards..22

Prerequisites

- EventTracker should be installed
- Websense Web Security Gateway v7.7 and later should be installed and configured

Integrate EventTracker with Websense WSG

Websense Web Security solutions can be configured to pass Internet activity (log) data to EventTracker product.

To enable this configuration:

1. Install an instance of **Websense Multiplexer** for each Websense Policy Server in your network.

   In appliance-based deployments Policy Server runs on the full policy source appliance and all users directory and filtering appliances.

2. In **Websense-Web Security Gateway**, to activate the integration and configure Multiplexer to send log data to EventTracker in the format required, select **Settings**, select **General** and then select **SIEM Integration**.

Deploy Websense Multiplexer

Websense Multiplexer can run on supported Windows/Linux platforms/Websense V-Series appliances.

- ❖ To install Multiplexer on Windows, use the TRITON Unified Installer (**WebsenseTRITON77Setup.exe**), available from the Downloads page of https://www.websense.com/. (Enter your product and version, and then select the Windows installer.)

  Perform a custom installation.

- ❖ To install Multiplexer on Linux, use the Web Security Linux Installer (**WebsenseWeb77Setup_Lnx.tar.gz**), available from the Downloads page of https://www.websense.com/. (Enter your product and version, and then select the Linux installer.)

Perform a custom installation.

- To add Multiplexer to an existing software installation, launch the installer for your platform and select the **Modify** option.

  1. On Windows, if you chose to keep installation files after the initial installation, select **Start, select All Programs, and then select Websense.**
  2. To start the installer without having to re-extract files, select **Websense TRITON Setup.**

- To enable Multiplexer on a full policy source or user directory and filtering appliance:

  1. In **Appliance Manager**, select **Administration,** select **Toolbox**, and then select **Command Line Utility** page
  2. Select the **Web Security** module.
  3. Select **multiplexer**, then use the **enable** command.

     Install only one Multiplexer instance for each Policy Server instance.

- If more than one Multiplexer is installed for a Policy Server, only the last installed instance of Multiplexer is used.

- Configuration for each Multiplexer instance is stored by its Policy Server. This means that you can configure different settings for each Multiplexer instance, if, for example, you use a different SIEM product in different regions.

  The following diagram shows a possible configuration for SIEM integration:

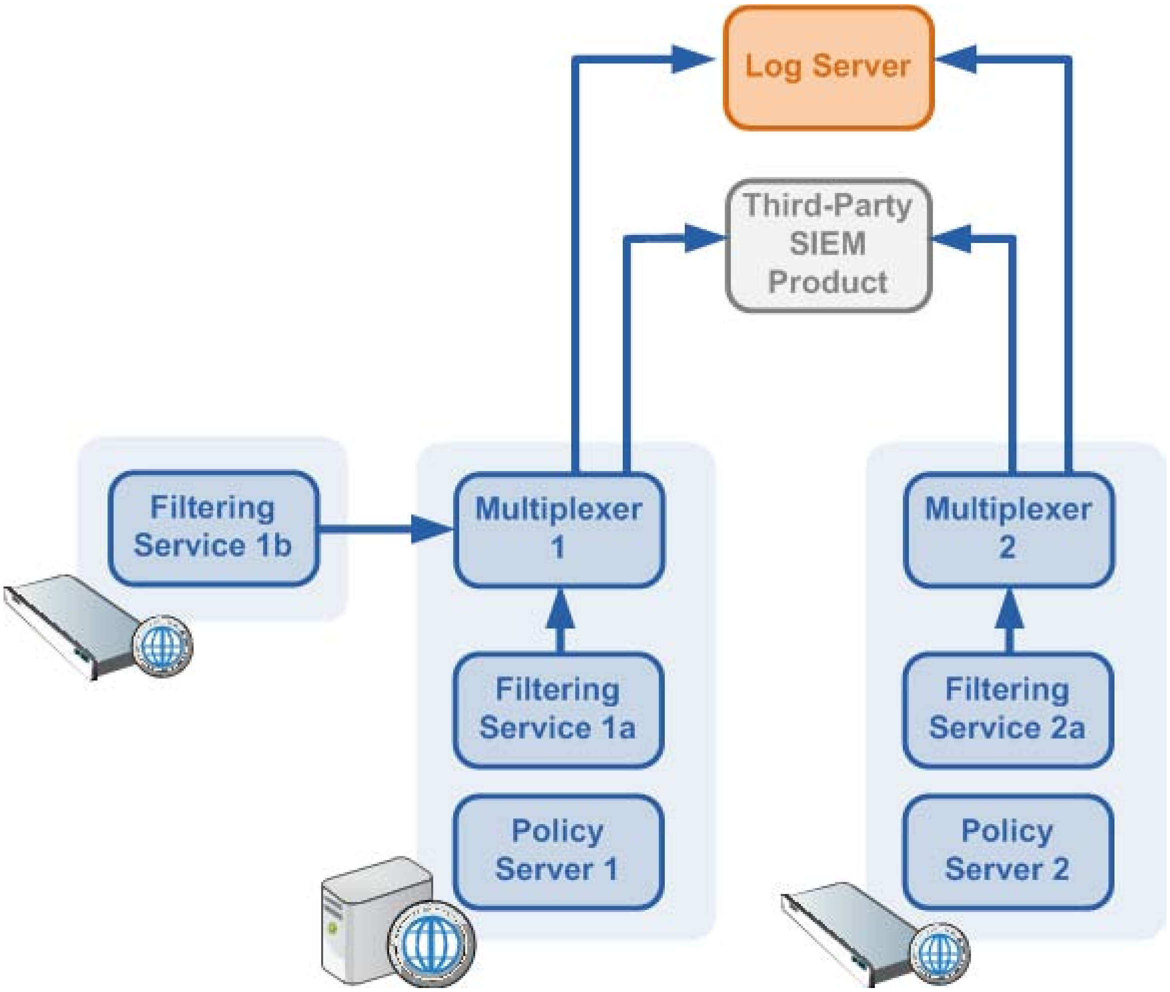


Figure 1

This deployment includes 2 Policy Server instances, each with its own Multiplexer instance.

- There are two Filtering Service instances associated with Policy Server 1; both pass Internet activity data to Multiplexer 1.
- Each Multiplexer instance passes the data that it receives from its associated Filtering Service instances to both Websense Log Server and a third-party SIEM product.

The illustration shows two V-Series appliances and an additional server; all Websense components shown in the diagram could be deployed on supported Windows/Linux server/V-Series appliance.

Enable and configure SIEM integration

Log on to Web Security Gateway to activate and configure SIEM integration.

1. Select Settings, select General, and then select SIEM Integration.
2. Select Enable SIEM integration for the Policy Server.
3. Provide the IP address or hostname of the EventTracker machine. Then, provide 514 as the Communication Port.
4. Specify the UDP to use when sending data to the EventTracker machine.
5. Select the syslog/key-value pairs (Splunk and others) from the SIEM format drop down.
6. Click OK to save the changes done.
7. Click Save and Deploy to implement the changes done.

After the changes have been saved, it forwards the logs to EventTracker.

EventTracker Knowledge Pack (KP)

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

The following Knowledge Packs are available in EventTracker v7.x to support Websense WSG monitoring:

Categories:-

- **Websense WSG: Bandwidth web category access blocked -** This category based report provides information related to blocked bandwidth web category access.

- **Websense WSG: Bandwidth web category access permitted -** This category based report provides information related to permitted bandwidth web category access.

- **Websense WSG: Baseline web category access blocked -** This category based report provides information related to blocked baseline web category access.

- **Websense WSG: Baseline web category access permitted -** This category based report provides information related to permitted baseline web category access.

- **Websense WSG: Productivity web category access blocked -** This category based report provides information related to blocked productivity web category access.

- **Websense WSG: Productivity web category access permitted -** This category based report provides information related to permitted productivity web category access.

- **Websense WSG: Security web category access blocked -** This category based report provides information related to blocked security web category access.
- **Websense WSG: Security web category access permitted -** This category based report provides information related to permitted security web category access.
- **Websense WSG: Social networking web category access blocked -** This category based report provides information related to blocked social networking web category access.
- **Websense WSG: Social networking web category access permitted -** This category based report provides information related to permitted social networking web category access.

Alerts:-

- **Websense WSG: Bandwidth web category access blocked -** This alert is generated when any Bandwidth web category access blocked from Websense WSG.
- **Websense WSG: Baseline web category access blocked -** This alert is generated when any Baseline web category access blocked from Websense WSG.
- **Websense WSG: Productivity web category access blocked -** This alert is generated when any productivity web category access blocked from Websense WSG.
- **Websense WSG: Security web category access blocked -** This alert is generated when any Security web category access blocked from Websense WSG**.**
- **Websense WSG: Social networking web category access blocked -** This alert is generated when any Social networking web category access permitted from Websense WSG.

Import Websense WSG Knowledge Pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Parsing Rule
- Flex Reports

1. Launch **EventTracker Control Panel**.

2. Double click **Export Import Utility**, and then click the **Import** tab.

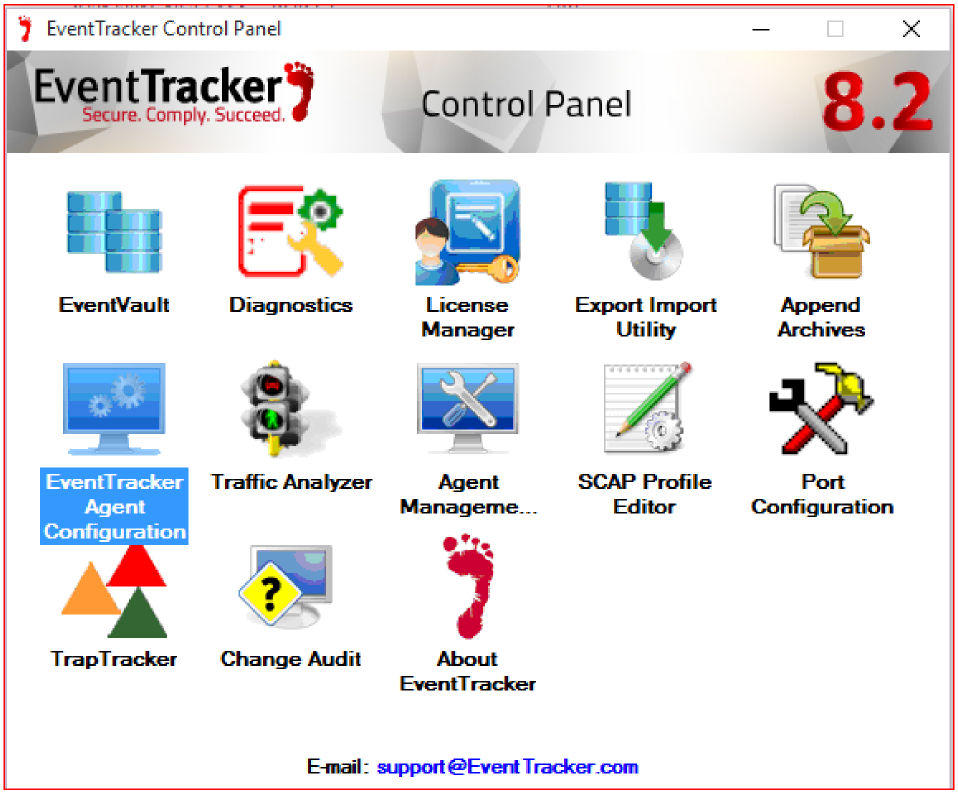


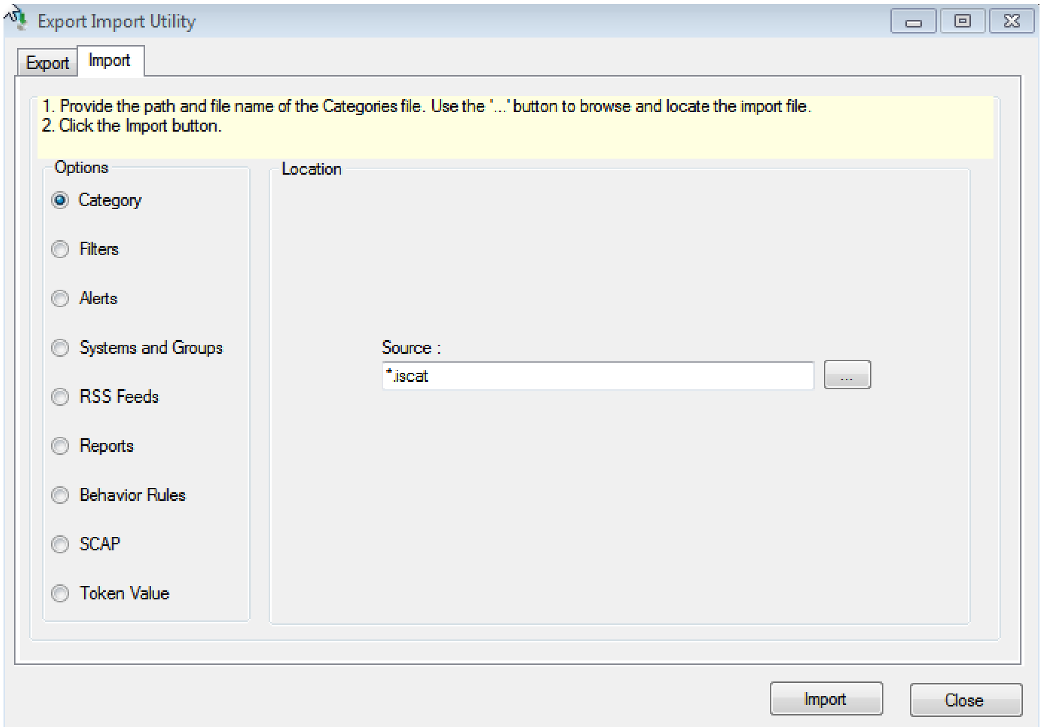
Figure 2

3. Click the **Import** tab.

Import Category

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

2. Locate the **All Websense WSG 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.

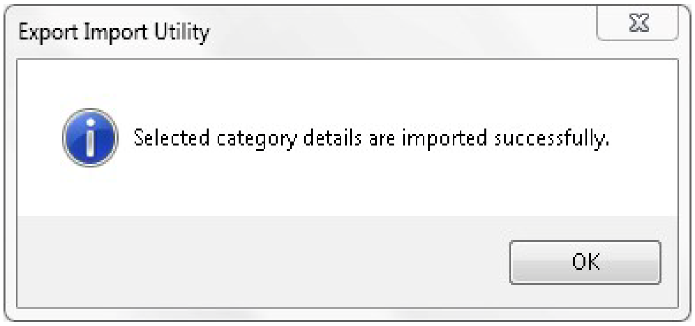
● Category
○ Filters
○ Alerts
○ Systems and Groups
○ RSS Feeds
○ Reports
○ Behavior Rules
○ SCAP
○ Token Value

Source : *.iscat

Figure 3

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

   EventTracker displays success message.



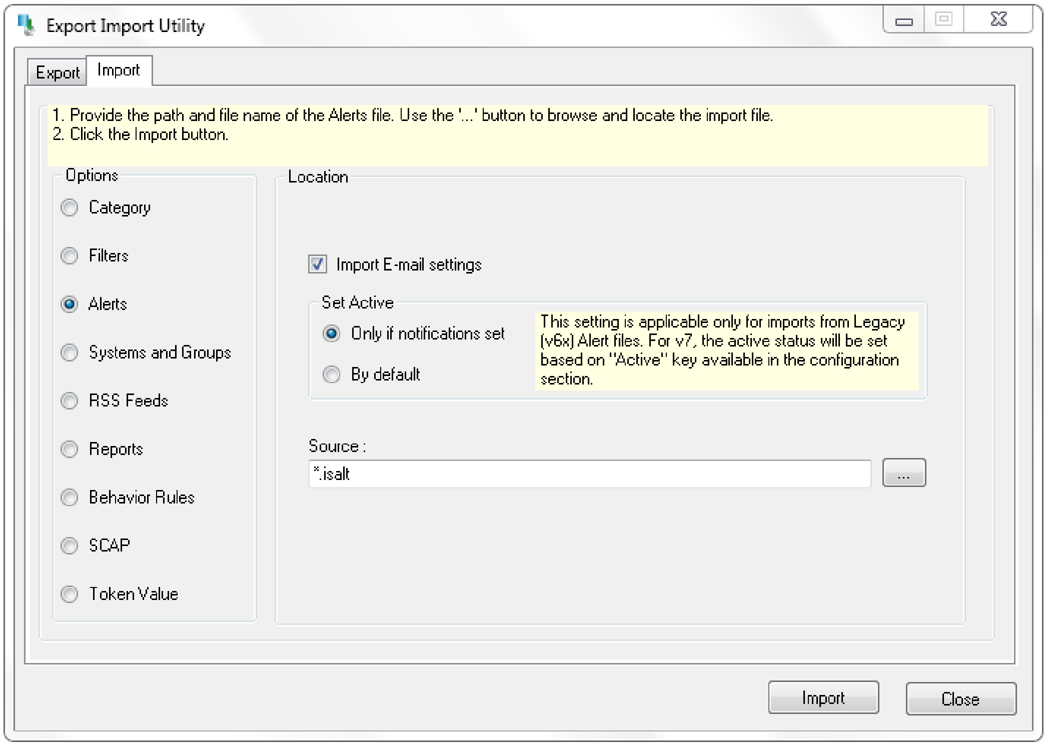
Selected category details are imported successfully.

Figure 4

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

Import Alerts

1. Click **Alerts** option, and then click the browse ... button.
2. Locate the **All Websense WSG 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

☑ Import E-mail settings

Set Active
● Only if notifications set
○ By default

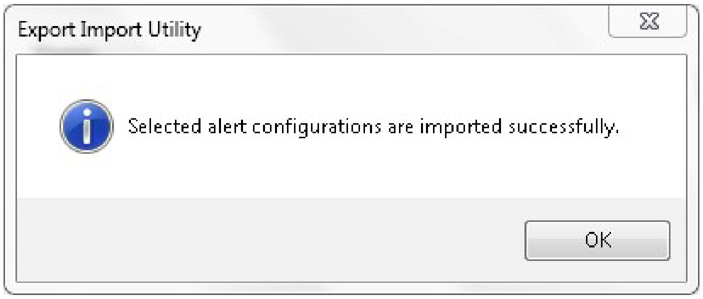
This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.

Source : *.isalt ...

Figure 5

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

EventTracker displays success message.



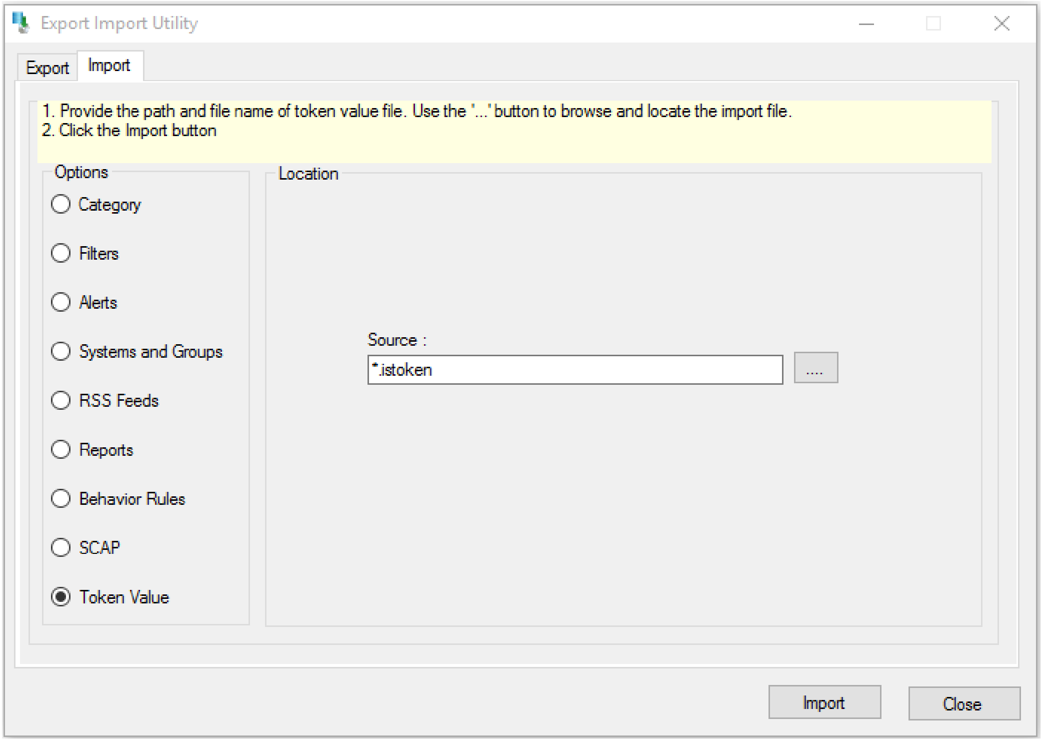
Selected alert configurations are imported successfully.

Figure 6

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

Import Tokens

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



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

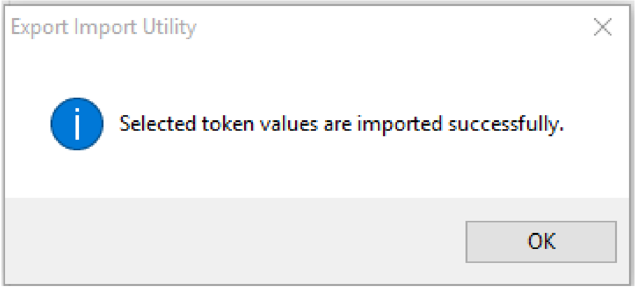
Location

Source : *.istoken

Figure 7

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

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



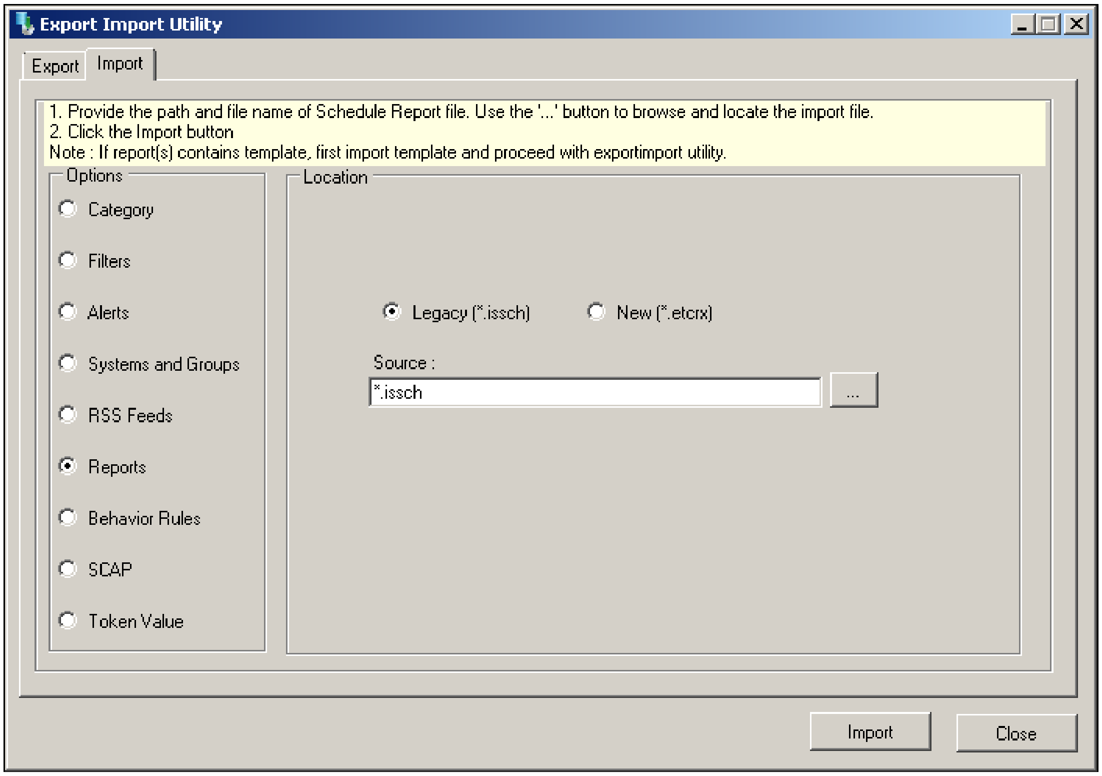
Selected token values are imported successfully.

Figure 8

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

Import Flex Reports

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



Export Import Utility

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.

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

Location: ● Legacy (*.issch) ○ New (*.etcrx)

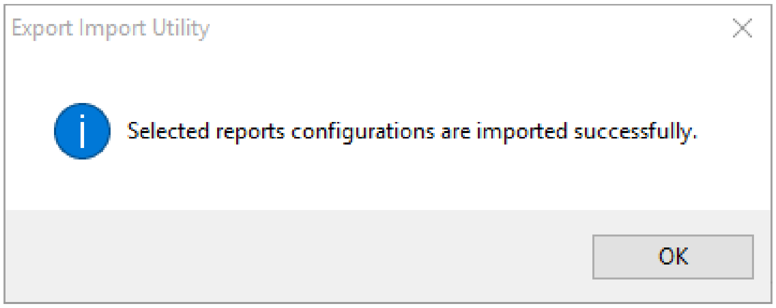
Source : *.issch

Figure 9

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

3. To import scheduled reports, click the **Import** button.

   EventTracker displays success message.



Export Import Utility

Selected reports configurations are imported successfully.

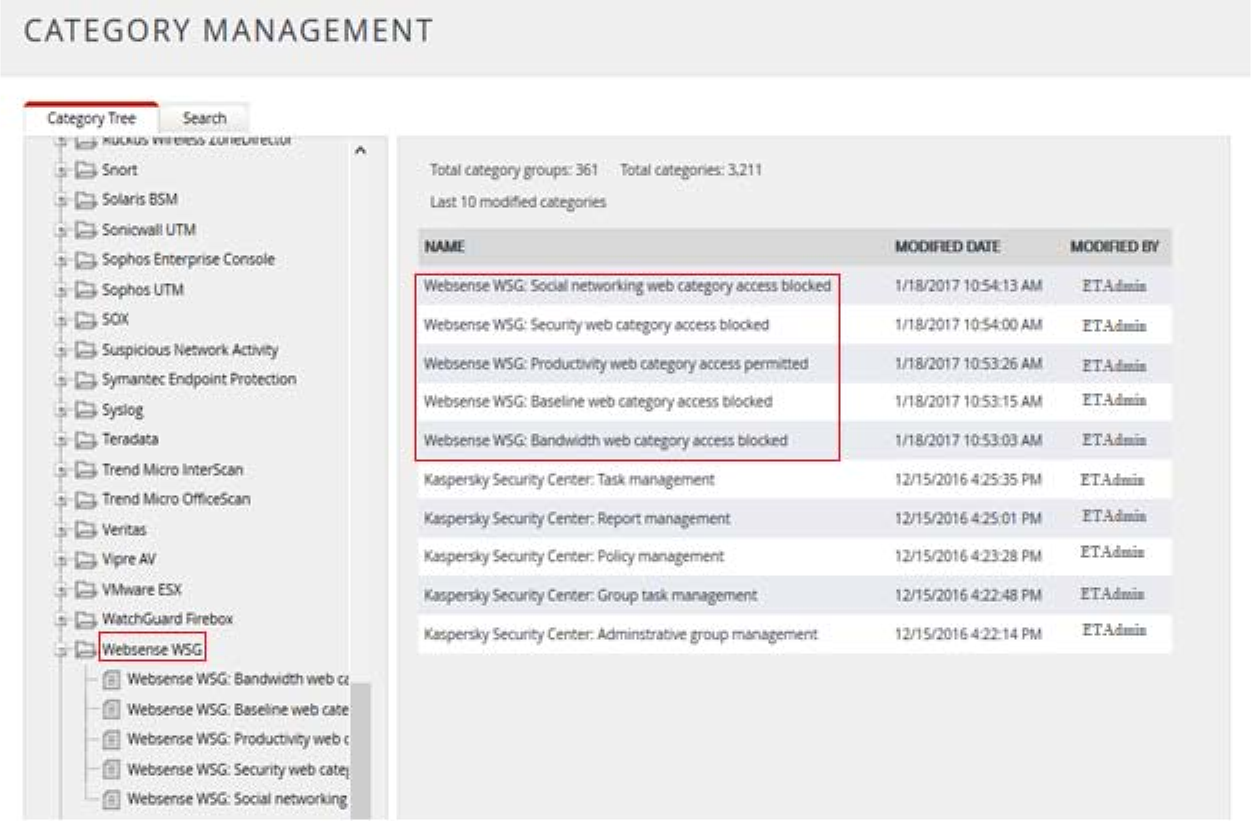
Figure 10

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

Verify Websense WSG knowledge pack in EventTracker

Verify Websense WSG Categories

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Categories**.
3. In the **Category Tree**, expand **Websense WSG** group folder to view the imported categories.


CATEGORY MANAGEMENT
Category Tree
Search
Ruckus Wireless ZoneDirector
Snort
Solaris BSM
Sonicwall UTM
Sophos Enterprise Console
Sophos UTM
SOX
Suspicious Network Activity
Symantec Endpoint Protection
Syslog
Teradata
Trend Micro InterScan
Trend Micro OfficeScan
Veritas
Vipre AV
VMware ESX
WatchGuard Firebox
Websense WSG
Websense WSG: Bandwidth web ca
Websense WSG: Baseline web cate
Websense WSG: Productivity web c
Websense WSG: Security web cate
Websense WSG: Social networking

Total category groups: 361 Total categories: 3,211

Last 10 modified categories

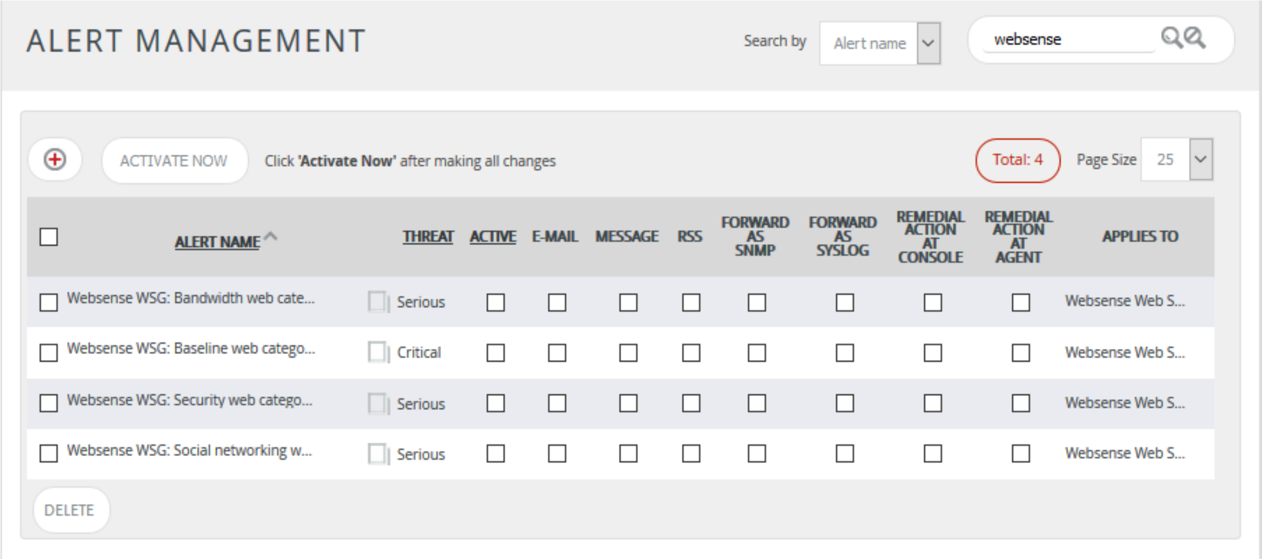
NAME	MODIFIED DATE	MODIFIED BY
Websense WSG: Social networking web category access blocked	1/18/2017 10:54:13 AM	ETAdmin
Websense WSG: Security web category access blocked	1/18/2017 10:54:00 AM	ETAdmin
Websense WSG: Productivity web category access permitted	1/18/2017 10:53:26 AM	ETAdmin
Websense WSG: Baseline web category access blocked	1/18/2017 10:53:15 AM	ETAdmin
Websense WSG: Bandwidth web category access blocked	1/18/2017 10:53:03 AM	ETAdmin
Kaspersky Security Center: Task management	12/15/2016 4:25:35 PM	ETAdmin
Kaspersky Security Center: Report management	12/15/2016 4:25:01 PM	ETAdmin
Kaspersky Security Center: Policy management	12/15/2016 4:23:28 PM	ETAdmin
Kaspersky Security Center: Group task management	12/15/2016 4:22:48 PM	ETAdmin
Kaspersky Security Center: Adminstrative group management	12/15/2016 4:22:14 PM	ETAdmin

Figure 11

Verify Websense WSG Alerts

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

   Alert Management page will display all the imported Websense WSG alerts.

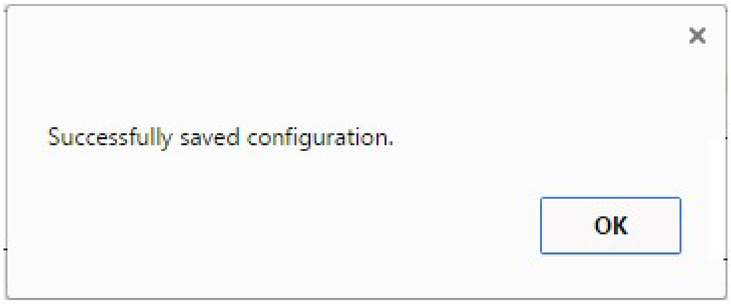


□	ALERT NAME	THREAT	ACTIVE	E-MAIL	MESSAGE	RSS	FORWARD AS SNMP	FORWARD AS SYSLOG	REMEDIAL ACTION AT CONSOLE	REMEDIAL ACTION AT AGENT	APPLIES TO
□	Websense WSG: Bandwidth web cate...	□ Serious	□	□	□	□	□	□	□	□	Websense Web S...
□	Websense WSG: Baseline web catego...	□ Critical	□	□	□	□	□	□	□	□	Websense Web S...
□	Websense WSG: Security web catego...	□ Serious	□	□	□	□	□	□	□	□	Websense Web S...
□	Websense WSG: Social networking w...	□ Serious	□	□	□	□	□	□	□	□	Websense Web S...

Figure 12

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

   EventTracker displays message box.



Successfully saved configuration.

Figure 13

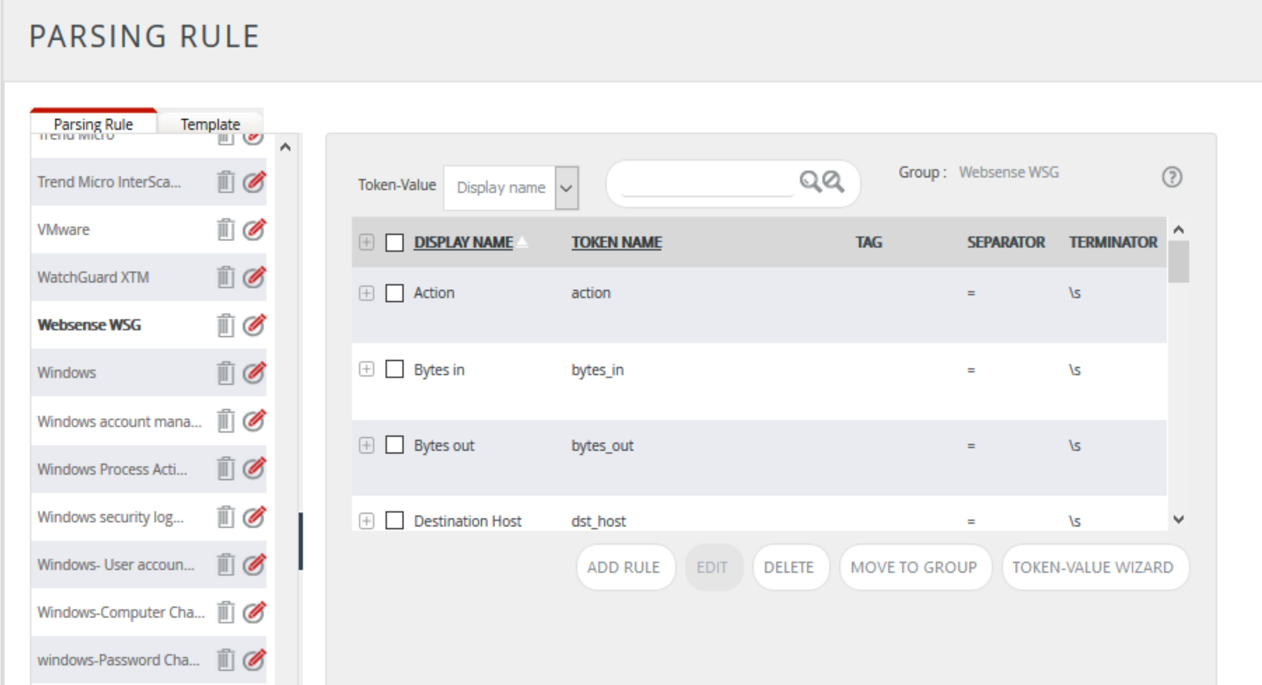
5. Click the **OK** button, and then click the **Activate now** button.

   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.

Verify Websense WSG Tokens

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

The imported Websense WSG tokens are added in Token-Value Groups list. Please refer Figure 12.



Trend Micro
Trend Micro InterSca...
VMware
WatchGuard XTM
Websense WSG
Windows
Windows account mana...
Windows Process Acti...
Windows security log...
Windows- User accoun...
Windows-Computer Cha...
windows-Password Cha...

Token-Value: Display name

Group : Websense WSG

DISPLAY NAME	TOKEN NAME	TAG	SEPARATOR	TERMINATOR
Action	action		=	\s
Bytes in	bytes_in		=	\s
Bytes out	bytes_out		=	\s
Destination Host	dst_host		=	\s

Figure 14

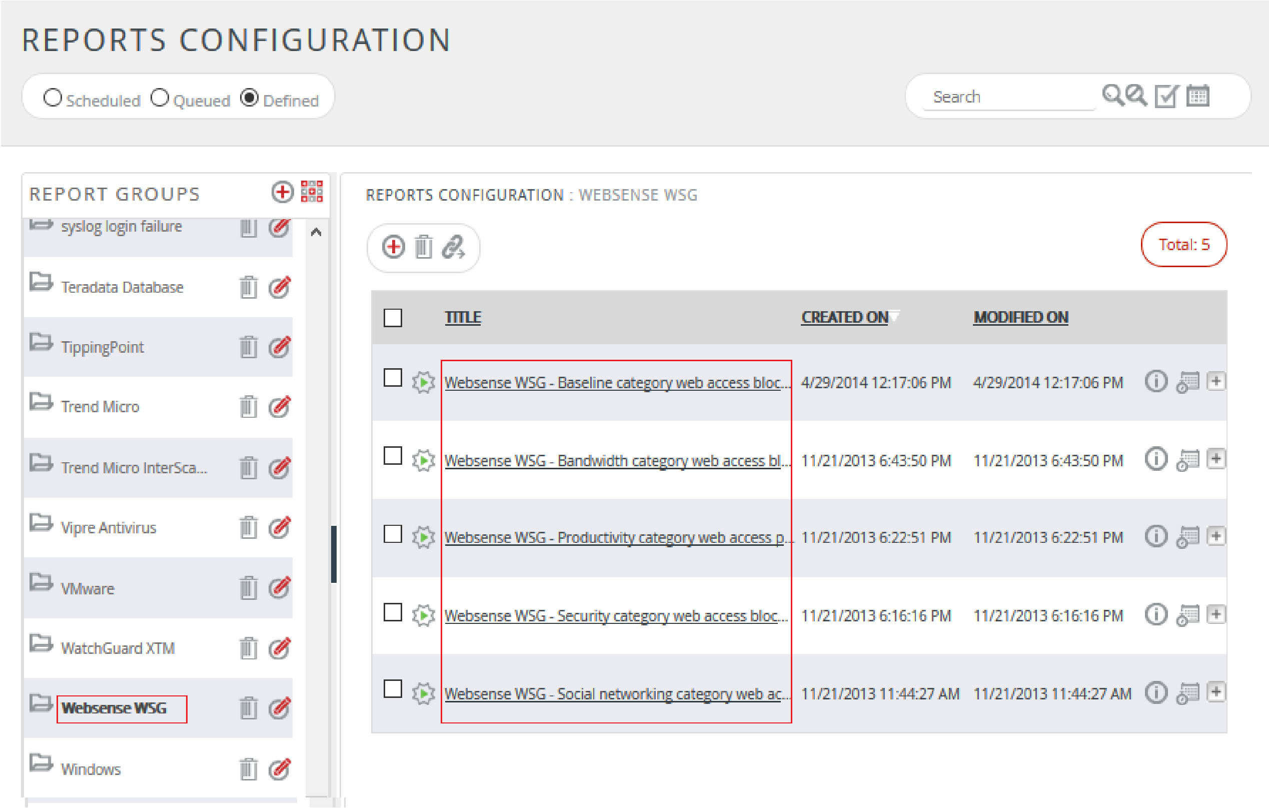
Verify Websense WSG Flex Reports

1. Logon to **EventTracker Enterprise**.
2. Select the **Reports** menu, and then select **Configuration**.
3. In **Reports Configuration**, select **Defined** option.

   EventTracker displays **Defined** page.

4. In search box enter '**Websense WSG**'.

   EventTracker displays Flex reports of Websense WSG.



REPORTS CONFIGURATION

○ Scheduled ○ Queued ● Defined

Search

REPORT GROUPS

- syslog login failure
- Teradata Database
- TippingPoint
- Trend Micro
- Trend Micro InterSca...
- Vipre Antivirus
- VMware
- WatchGuard XTM
- Websense WSG
- Windows

REPORTS CONFIGURATION : WEBSENSE WSG

Total: 5

□	TITLE	CREATED ON	MODIFIED ON
□	Websense WSG - Baseline category web access bloc...	4/29/2014 12:17:06 PM	4/29/2014 12:17:06 PM
□	Websense WSG - Bandwidth category web access bl...	11/21/2013 6:43:50 PM	11/21/2013 6:43:50 PM
□	Websense WSG - Productivity category web access p...	11/21/2013 6:22:51 PM	11/21/2013 6:22:51 PM
□	Websense WSG - Security category web access bloc...	11/21/2013 6:16:16 PM	11/21/2013 6:16:16 PM
□	Websense WSG - Social networking category web ac...	11/21/2013 11:44:27 AM	11/21/2013 11:44:27 AM

Figure 15

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.

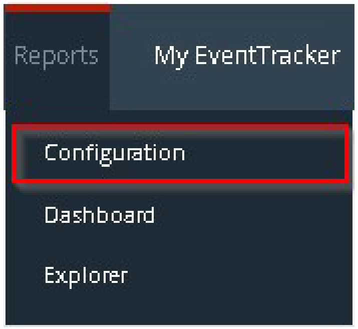
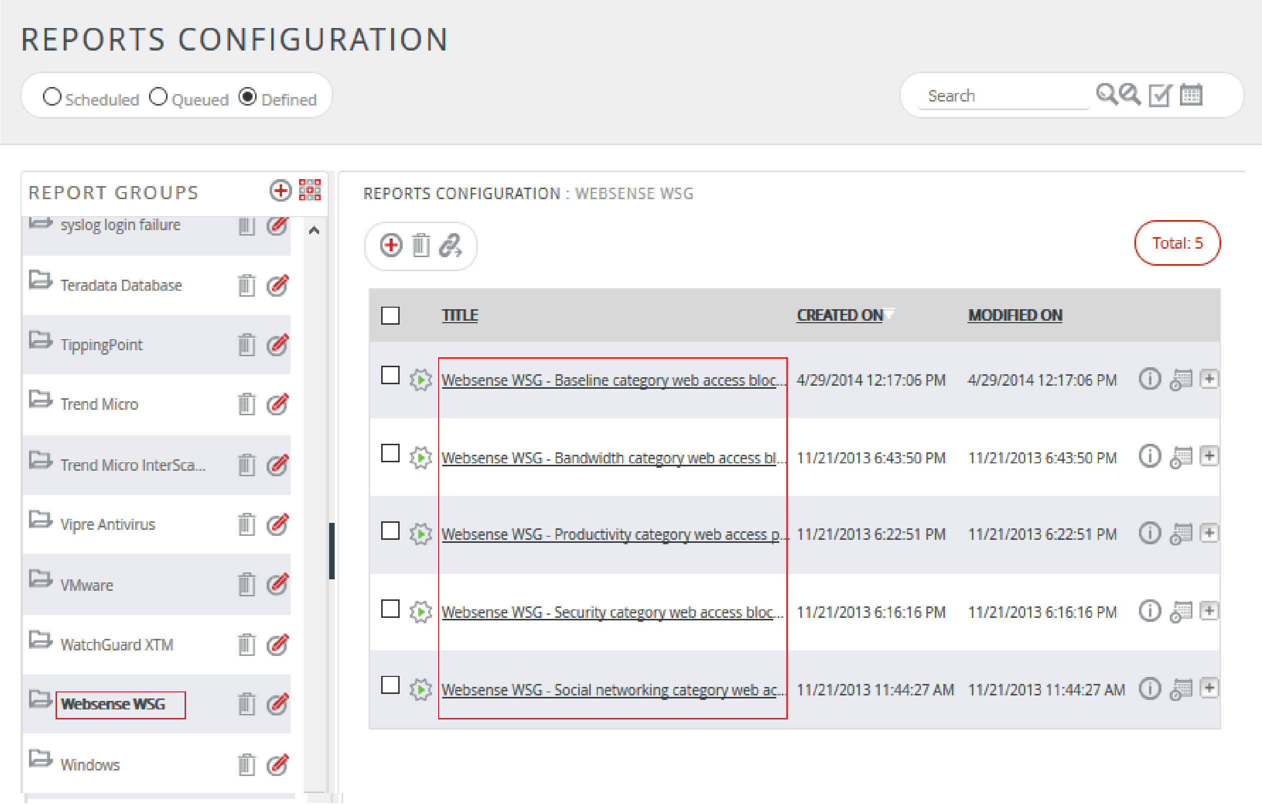


Figure 16

2. Navigate to **Reports>Configuration**.

3. Select **Websense security gateway** in report groups. Check **Defined** dialog box.



REPORTS CONFIGURATION

○ Scheduled ○ Queued ● Defined

Search

REPORT GROUPS

- syslog login failure
- Teradata Database
- TippingPoint
- Trend Micro
- Trend Micro InterSca...
- Vipre Antivirus
- VMware
- WatchGuard XTM
- Websense WSG
- Windows

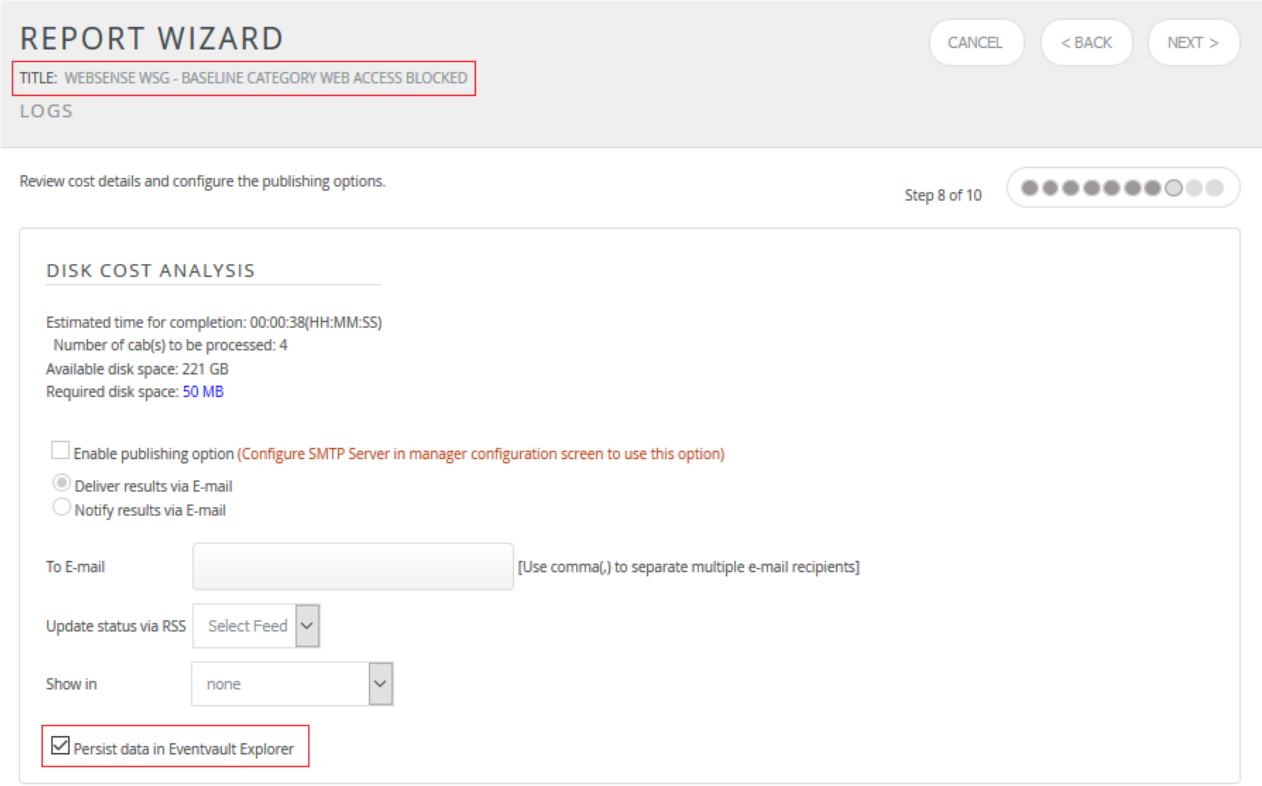
REPORTS CONFIGURATION : WEBSENSE WSG

Total: 5

□	TITLE	CREATED ON	MODIFIED ON
□	Websense WSG - Baseline category web access bloc...	4/29/2014 12:17:06 PM	4/29/2014 12:17:06 PM
□	Websense WSG - Bandwidth category web access bl...	11/21/2013 6:43:50 PM	11/21/2013 6:43:50 PM
□	Websense WSG - Productivity category web access p...	11/21/2013 6:22:51 PM	11/21/2013 6:22:51 PM
□	Websense WSG - Security category web access bloc...	11/21/2013 6:16:16 PM	11/21/2013 6:16:16 PM
□	Websense WSG - Social networking category web ac...	11/21/2013 11:44:27 AM	11/21/2013 11:44:27 AM

Figure 17

1. Click on '**schedule**' to plan a report for later execution.
2. Click **Next** button to proceed.
3. In review page, check **Persist data in EventVault Explorer** option.



TITLE: WEBSENSE WSG - BASELINE CATEGORY WEB ACCESS BLOCKED

LOGS

Review cost details and configure the publishing options.

Step 8 of 10

DISK COST ANALYSIS

Estimated time for completion: 00:00:38(HH:MM:SS)
Number of cab(s) to be processed: 4
Available disk space: 221 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]

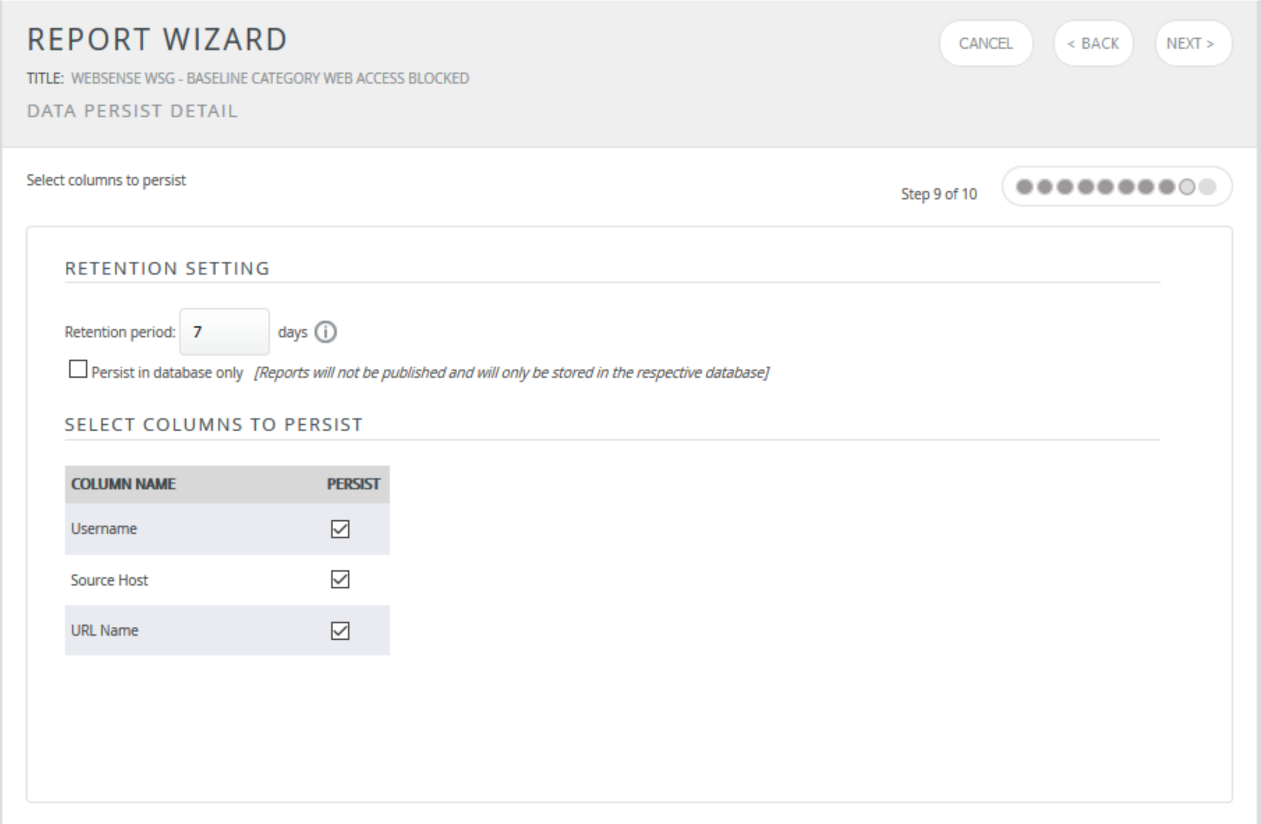
Update status via RSS: Select Feed

Show in: none

☑ Persist data in Eventvault Explorer

Figure 18

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



REPORT WIZARD

TITLE: WEBSENSE WSG - BASELINE CATEGORY WEB ACCESS BLOCKED

DATA PERSIST DETAIL

Select columns to persist

Step 9 of 10

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
Username	☑
Source Host	☑
URL Name	☑

Figure 19

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

Create Dashlets

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

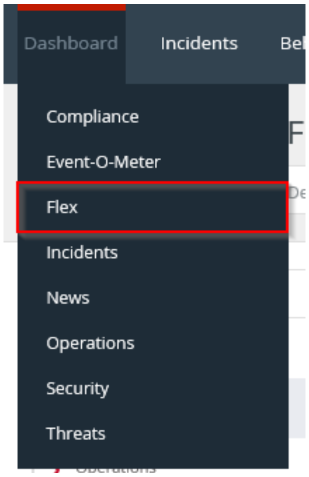
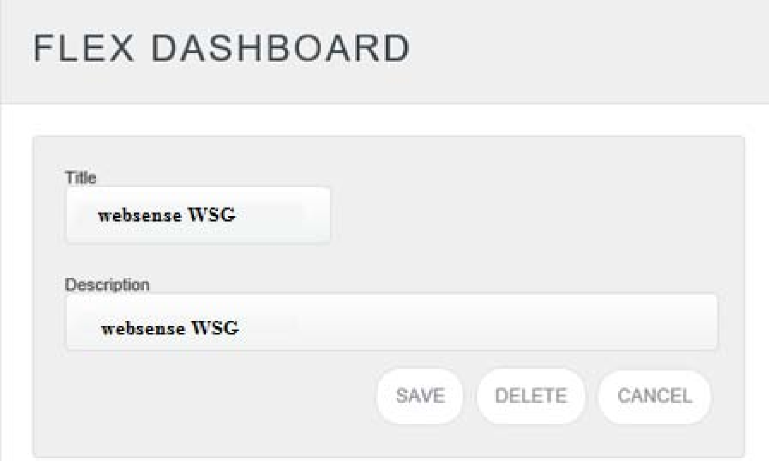


Figure 20

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



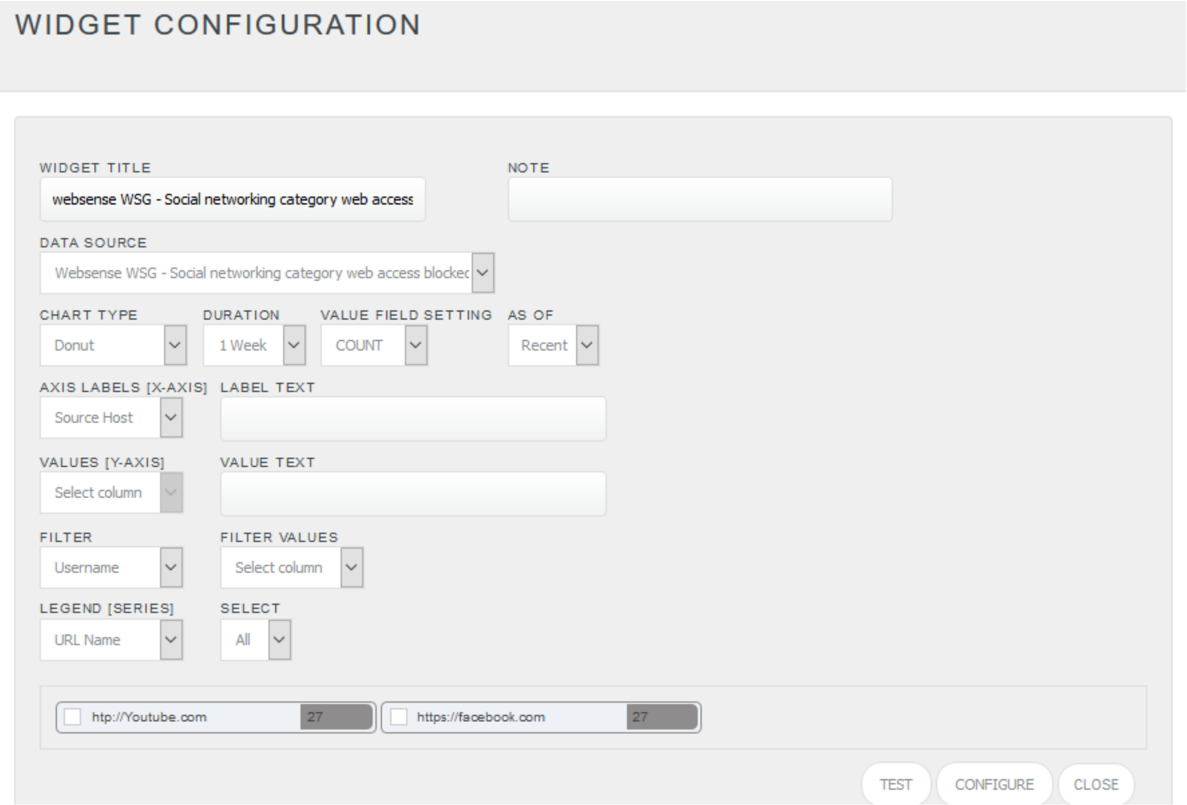
FLEX DASHBOARD

Title: websense WSG

Description: websense WSG

Figure 21

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: websense WSG - Social networking category web access

NOTE:

DATA SOURCE: Websense WSG - Social networking category web access blockec

CHART TYPE: Donut

DURATION: 1 Week

VALUE FIELD SETTING: COUNT

AS OF: Recent

AXIS LABELS [X-AXIS]: Source Host

LABEL TEXT:

VALUES [Y-AXIS]: Select column

VALUE TEXT:

FILTER: Username

FILTER VALUES: Select column

LEGEND [SERIES]: URL Name

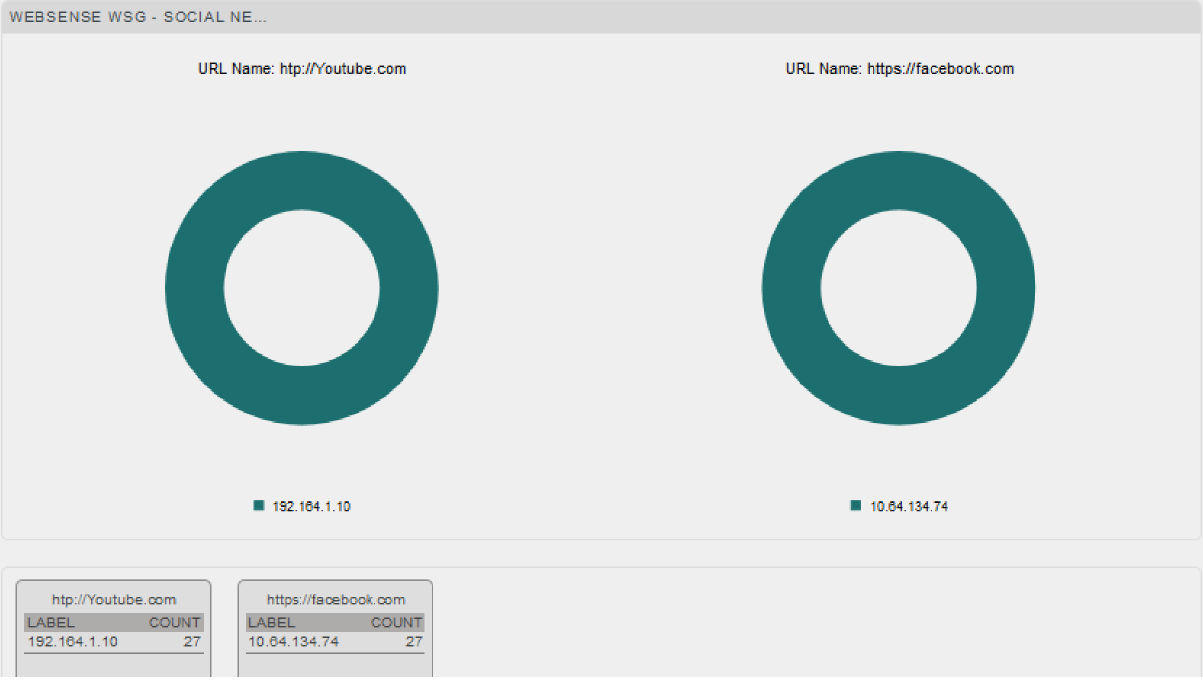
SELECT: All

□ http://Youtube.com 27

□ https://facebook.com 27

Figure 22

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.


WEBSENSE WSG - SOCIAL NE...
URL Name: htp://Youtube.com
URL Name: https://facebook.com
■ 192.164.1.10
■ 10.64.134.74

http://Youtube.com

LABEL	COUNT
192.164.1.10	27

https://facebook.com

LABEL	COUNT
10.64.134.74	27

Figure 23

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

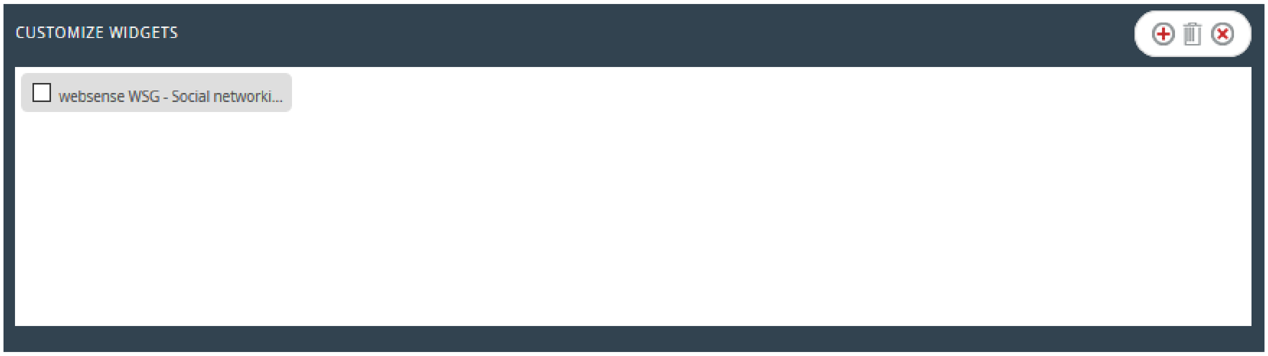


Figure 24

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: Websense WSG - Social networking category web access blocked

Websense WSG - Social networking category web access blocked
WIDGET TITLE: Websense WSG - Social networking category web access blocked
CHART TYPE: Donut
AXIS LABELS [X-AXIS]: Source IP
FILTER: User Name
LEGEND (SERIES): URL Name

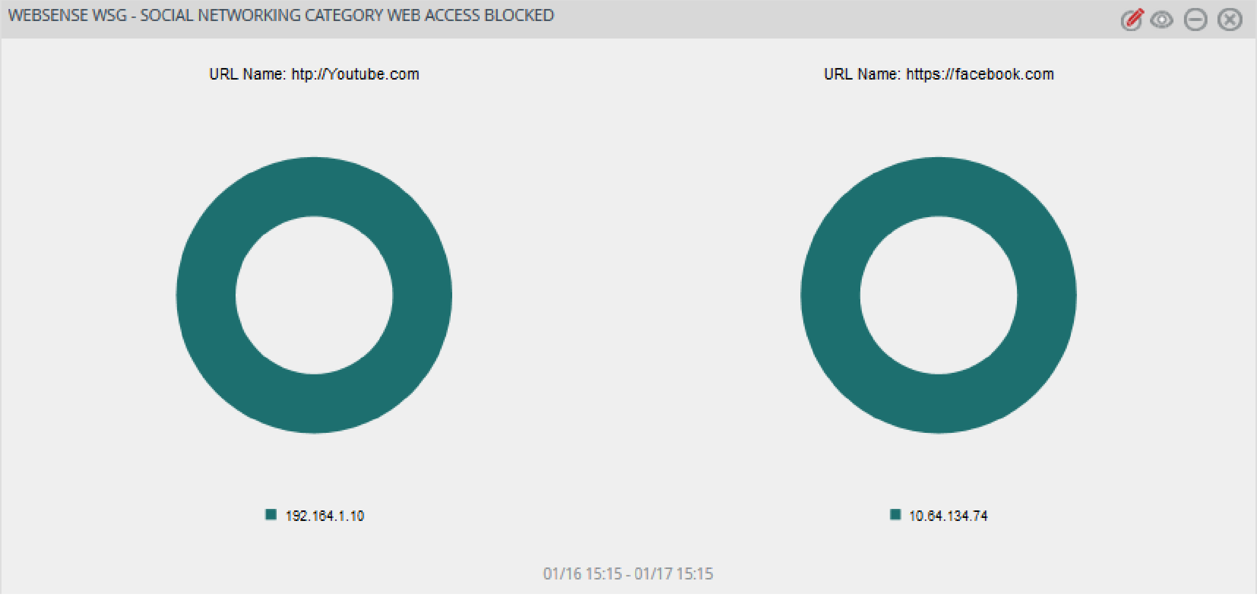

WEBSENSE WSG - SOCIAL NETWORKING CATEGORY WEB ACCESS BLOCKED
URL Name: htp://Youtube.com
URL Name: https://facebook.com
■ 192.164.1.10
■ 10.64.134.74
01/16 15:15 - 01/17 15:15

Figure 25