EventTracker

Actionable Security Intelligence

Integrate Blue Coat ProxySG

Publication Date: December 15, 2016

Abstract

This guide provides instructions to configure Blue Coat ProxySG to send the syslog events to EventTracker.

Scope

The configurations detailed in this guide are consistent with **EventTracker** version 7.X and later, and Blue Coat ProxySG Appliance SGOS 5.3 and later.

Audience

Blue Coat ProxySG users, who wish to forward syslog messages to EventTracker manager.

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.

Table of Contents

Overview

The Blue Coat ProxySG device is designed to integrate protection and control functions for Internet and intranet traffic without sacrificing performance and employee productivity. The device assists you in managing internet abuse by increasing security, limiting liability, and managing bandwidth usage. The Blue Coat Syslog range of appliances provides points of control that accelerate and secure business applications for users across the distributed organization.

The EventTracker Enterprise enables you to capture log data and report on critical points of your Blue Coat ProxySG internet access control solution including web cache usage. EventTracker Enterprise provides an additional level of support by enabling you to generate reports and run searches on data to improve your ability to manage your Blue Coat ProxySG activity.

Prerequisites

Prior to configuring the Blue Coat ProxySG and EventTracker, ensure that you meet the following prerequisites:

- EventTracker 7.0 and later should be installed.
- Administrator access on the EventTracker.
- Blue Coat Syslog SGOS version 5.4 should be installed.

Configuration

Blue Coat ProxySG generates two types of event logs

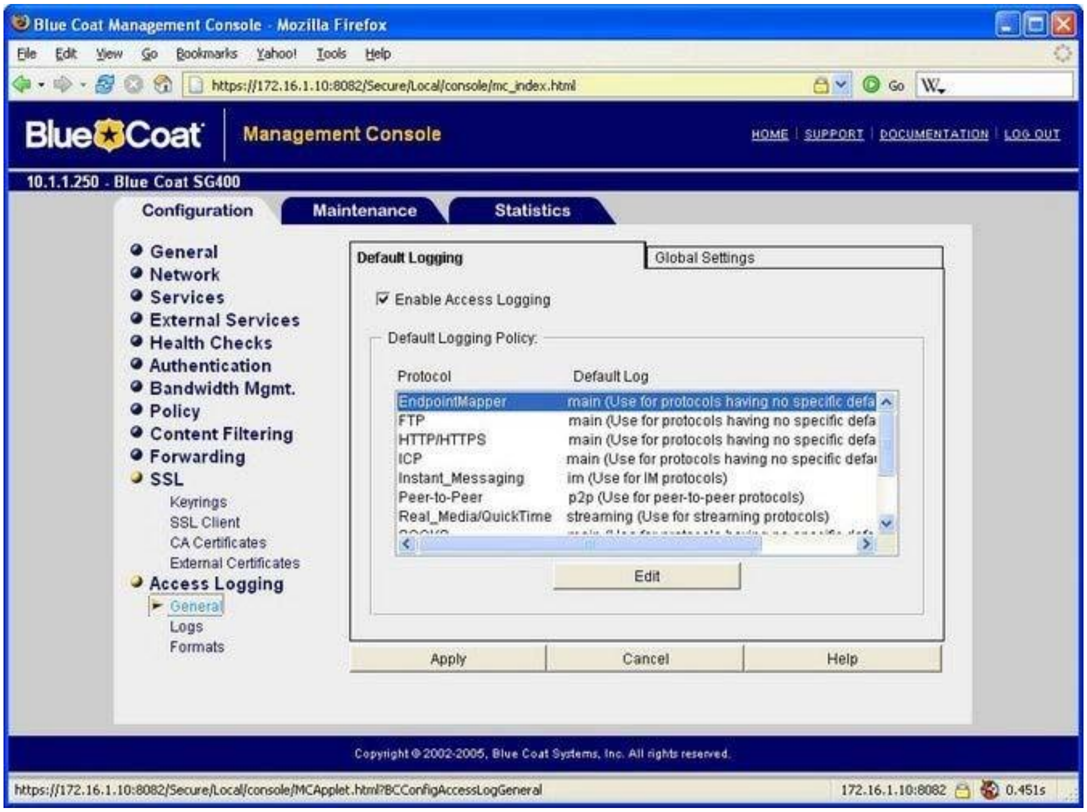
1. Access activity event log
2. System(Operation) event log

A. Enable Access Logging

Access logging enables you to monitor web traffic for your environment. The Blue Coat ProxySG device can be set up to generate real-time or schedule logs and reports. Once you set up the Blue Coat ProxySG device for access logging, you must enable it to send the logs to the EventTracker Enterprise. You must enable access logging on your Blue Coat SG device.

1. In the **Blue Coat Management Console** navigation menu, Select Configuration > Access Logging > General

The **Default Logging** tab appears. This window might appear differently depending on the version of Blue Coat ProxySG you are running.


Blue Coat Management Console - Mozilla Firefox
File Edit View Go Bookmarks Yahoo! Tools Help
https://172.16.1.10:8082/Secure/Local/console/mc_index.html
Go
Blue Coat
Management Console
HOME | SUPPORT | DOCUMENTATION | LOG OUT
10.1.1.250 - Blue Coat SG400
Configuration
Maintenance
Statistics
General
Network
Services
External Services
Health Checks
Authentication
Bandwidth Mgmt.
Policy
Content Filtering
Forwarding
SSL
Keyrings
SSL Client
CA Certificates
External Certificates
Access Logging
General
Logs
Formats
Default Logging
Global Settings
Edit
Apply
Cancel
Help
Copyright © 2002-2005, Blue Coat Systems, Inc. All rights reserved.
https://172.16.1.10:8082/Secure/Local/console/MCApplet.html?BCConfigAccessLogGeneral
172.16.1.10:8082
0.451s

☑ Enable Access Logging

Default Logging Policy:

Protocol	Default Log
EndpointMapper	main (Use for protocols having no specific defa
FTP	main (Use for protocols having no specific defa
HTTP/HTTPS	main (Use for protocols having no specific defa
ICP	main (Use for protocols having no specific defau
Instant_Messaging	im (Use for IM protocols)
Peer-to-Peer	p2p (Use for peer-to-peer protocols)
Real_Media/QuickTime	streaming (Use for streaming protocols)

Figure 1

2. Select the Enable Access Logging check box.

   If the Enable Access Logging check box is not selected, logging is disabled globally for all the formats listed.

3. For each of the following protocols, click **Edit**, edit the entry as noted, and then click on **OK**.

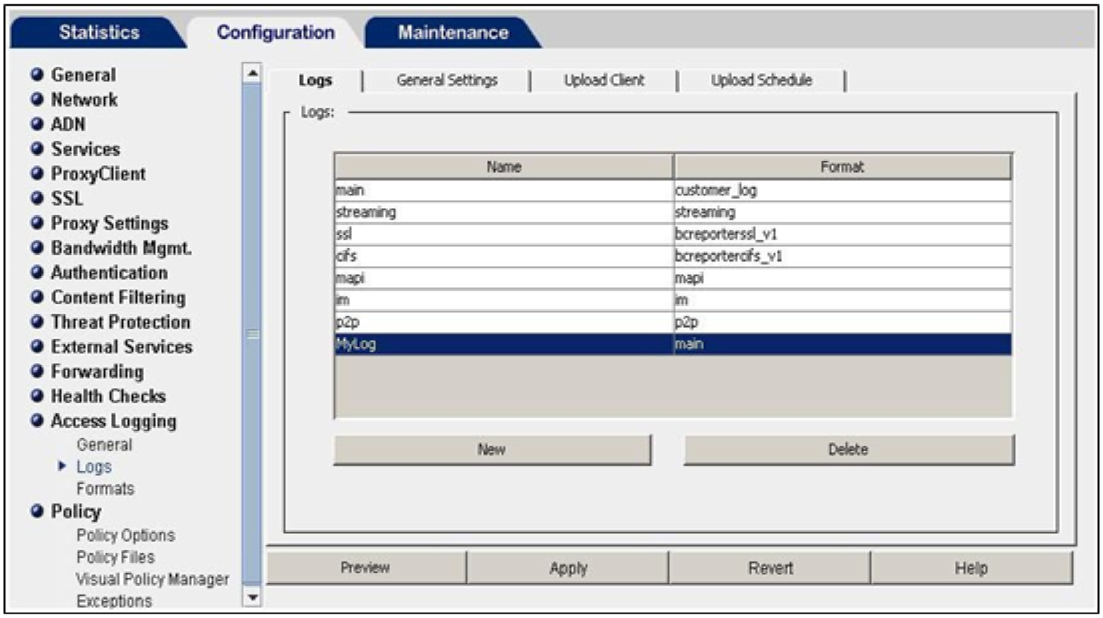
   - **FTP** - main
   - **HTTP/HTTPS** - main
   - **SOCKS** - main
   - **TCP-Tunnel** - main
   - **ICP** - main
   - **Instant Messaging** - IM
   - **Windows Media** – streaming
   - **Real Media/QuickTime**—streaming

4. Click **Apply**.

   After you enable access logging on Blue Coat ProxySG, forward the access log to EventTracker Enterprise.

   Caution - Note that this will only work if the SYSLOG server supports receiving events via TCP (UDP will not work).

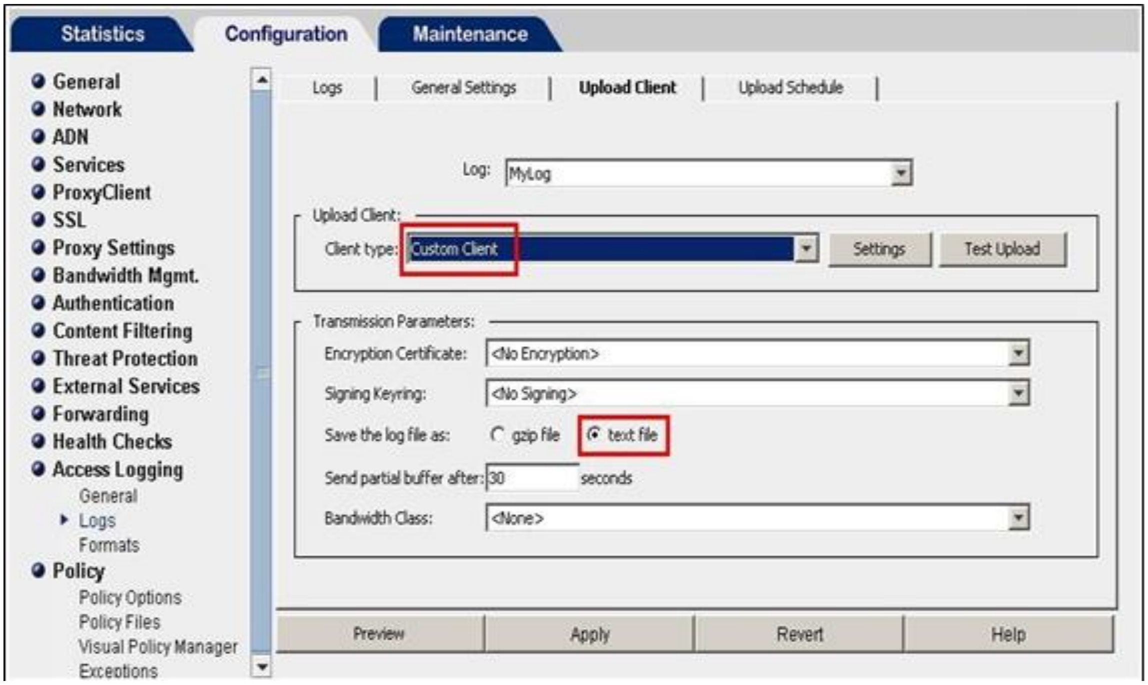
5. Define an Access Log file configured to your requirements (called 'MyLog' here).



Name	Format
main	customer_log
streaming	streaming
ssl	bcreporterssl_v1
cifs	bcreportercifs_v1
mapi	mapi
im	im
p2p	p2p
MyLog	main

Figure 2

6. For this Access Log, configure the Upload Client as type "Custom Client" and 'Save the log file as:' a 'text file'.



Log: MyLog

Upload Client:

Client type: Custom Client

Transmission Parameters:

Encryption Certificate: <No Encryption>

Signing Keyring: <No Signing>

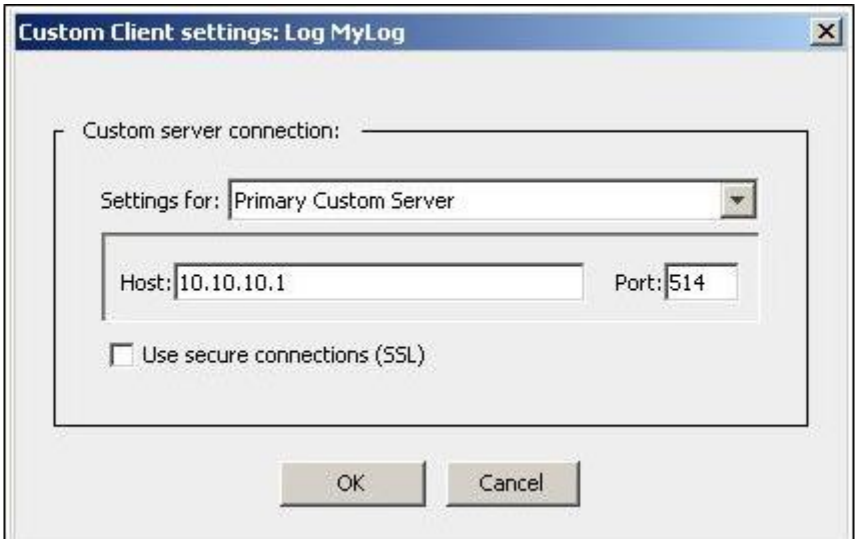
Save the log file as: ○ gzip file ● text file

Send partial buffer after: 30 seconds

Bandwidth Class: <None>

Figure 3

7. (Optional) To reduce the transmission time for log uploads, in the 'Send partial buffer after' field, enter a value as low as 5.
8. Point the Custom Client to your SYSLOG server EventTracker Enterprise, specifying its appropriate TCP port number.



Custom Client settings: Log MyLog

Custom server connection:

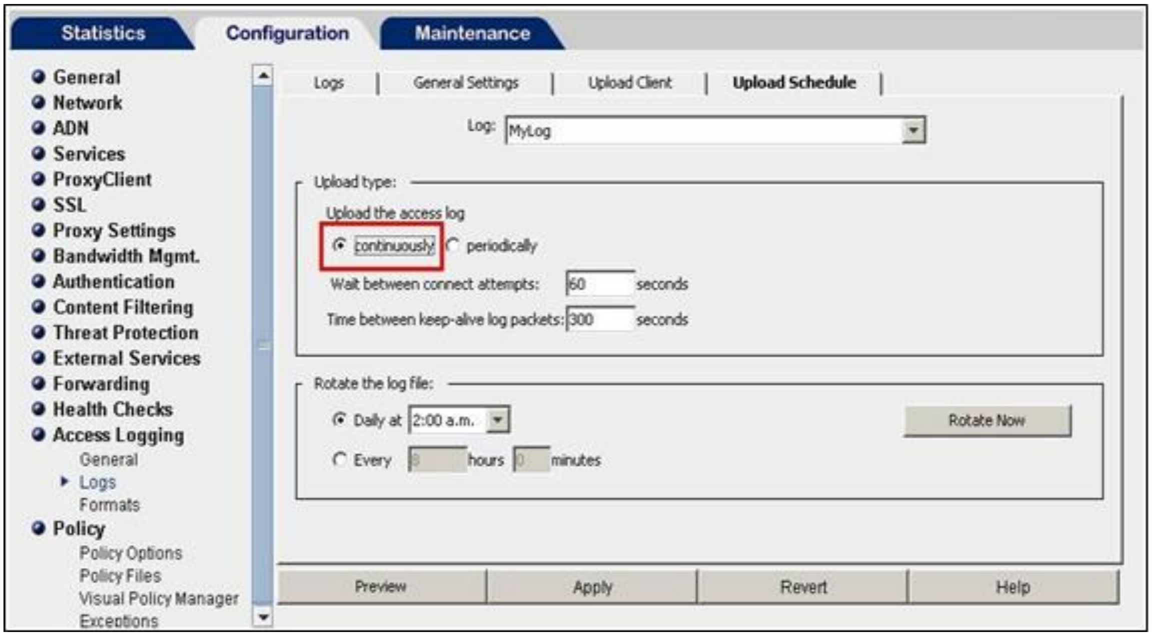
Settings for: Primary Custom Server

Host: 10.10.10.1 Port: 514

□ Use secure connections (SSL)

Figure 4

9. For the log’s upload schedule, specify to upload continuously.



Log: MyLog

Upload type:

Upload the access log

● continuously ○ periodically

Wait between connect attempts: 60 seconds

Time between keep-alive log packets: 300 seconds

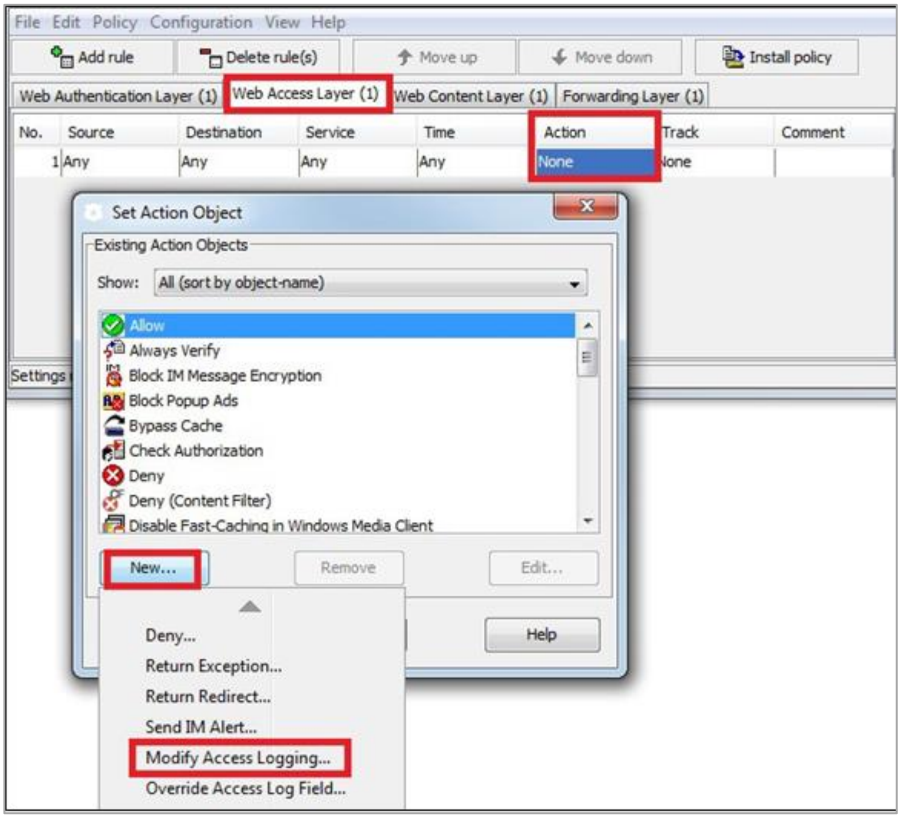
Rotate the log file:

● Daily at 2:00 a.m.

○ Every 0 hours 0 minutes

Figure 5

10. Next, load Visual Policy Manager. In a Web Access Layer, set the Action to 'Modify Access Logging'.

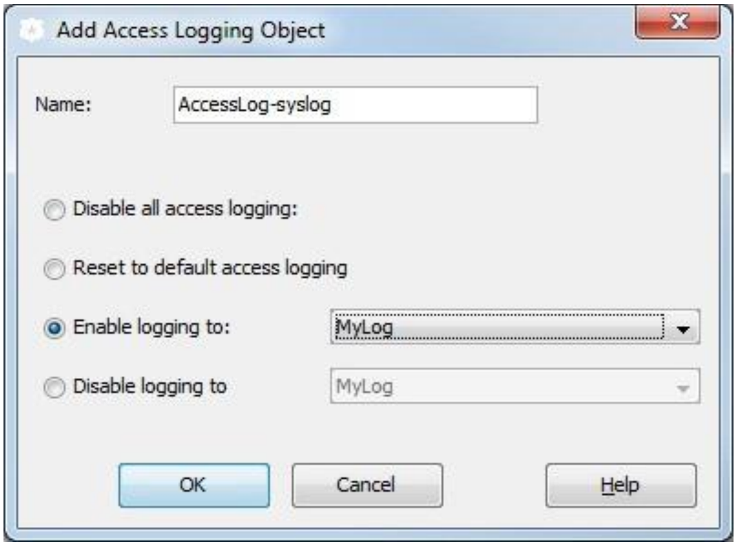


No.	Source	Destination	Service	Time	Action	Track	Comment
1	Any	Any	Any	Any	None	None	

Show: All (sort by object-name)

Figure 6

11. In the Access Logging object, enable logging to your new access log.


Add Access Logging Object

Name: AccessLog-syslog

○ Disable all access logging:

○ Reset to default access logging

● Enable logging to: MyLog

○ Disable logging to MyLog

Figure 7

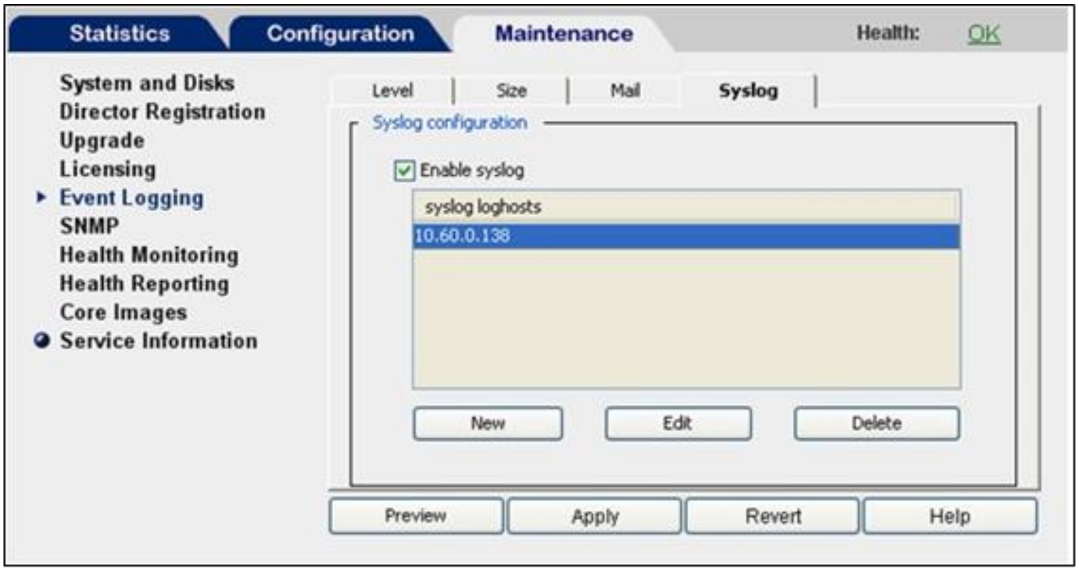
B. System Event Log

Event logs are operational logs and do not contain information about proxy access. By configuring syslog, it forwards the system event log to EventTracker Enterprise.

Syslog Configuration

To enable syslog monitoring, perform the following steps:

1. Select **Maintenance > Event Logging > Syslog**.



☑ Enable syslog

syslog loghosts: 10.60.0.138

Figure 8

2. In the **Loghost** field, enter the IP address of EventTracker Enterprise.

3. Select **Enable Syslog**.

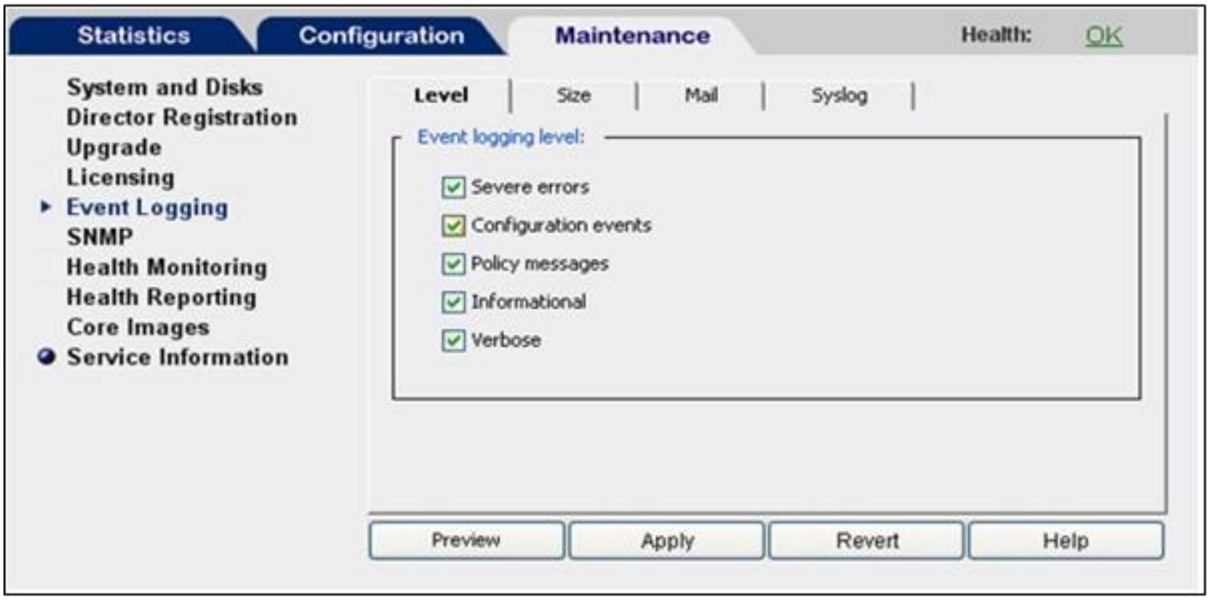
4. Click **Apply**.

Configuring Events to Log

The event level options are listed from the most to least important events. Because each event requires some disk space, setting the event logging to log all events fills the event log more quickly.

To set the event logging level

1. Select **Maintenance > Event Logging > Level**



Event logging level:

☑ Severe errors
☑ Configuration events
☑ Policy messages
☑ Informational
☑ Verbose

Figure 9

2. Select the events you want to log.

   When you select an event level, all levels above the selection are included. For example, if you select **Verbose**, all event levels are included.

3. 3. Click **Apply**.

Event Logging Level Options

Event Logging Level	Description
Severe errors	Writes only severe error messages to the event log.
Configuration events	Writes severe and configuration change error messages to the event log.
Policy messages	Writes severe, configuration change, and policy event error messages to the event log.
Informational	Writes severe, configuration change, policy event, and information error messages to the event log.
Verbose	Writes all error messages to the event log.

Table 1

Setting Event Log Size

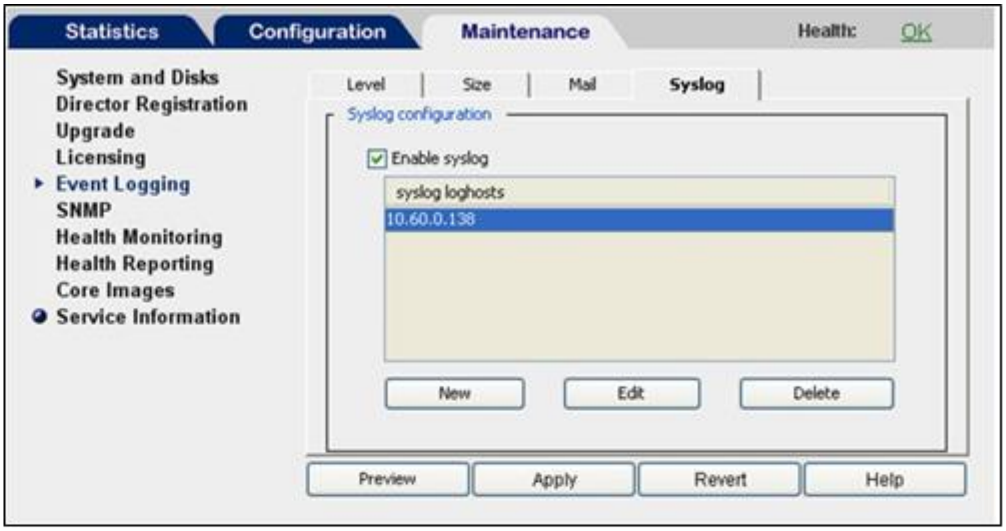
You can limit the size of the appliance's event log and specify what the appliance should do if the log size limit is reached.

To set event log size

1. Select **Maintenance > Event Logging > Size**.
2. In the **Event log size** field, enter the maximum size of the event log in megabytes.
3. Select either **Overwrite earlier events** or **Stop logging new events** to specify the desired behavior when the event log reaches maximum size.
4. Click **Apply**.

To enable syslog monitoring

5. Select **Maintenance > Event Logging > Syslog**.



☑ Enable syslog

syslog loghosts
10.60.0.138

Figure 10

6. In the **Loghost** field, enter the IP address of EventTracker Enterprise.
7. Select **Enable Syslog**.
8. Click **Apply**.

Verifying Blue Coat ProxySG access activity and system syslog messages in EventTracker Enterprise

Log Search Steps

1. Click the **Search** tab.
   The **EventTracker LogSearch** page appears.

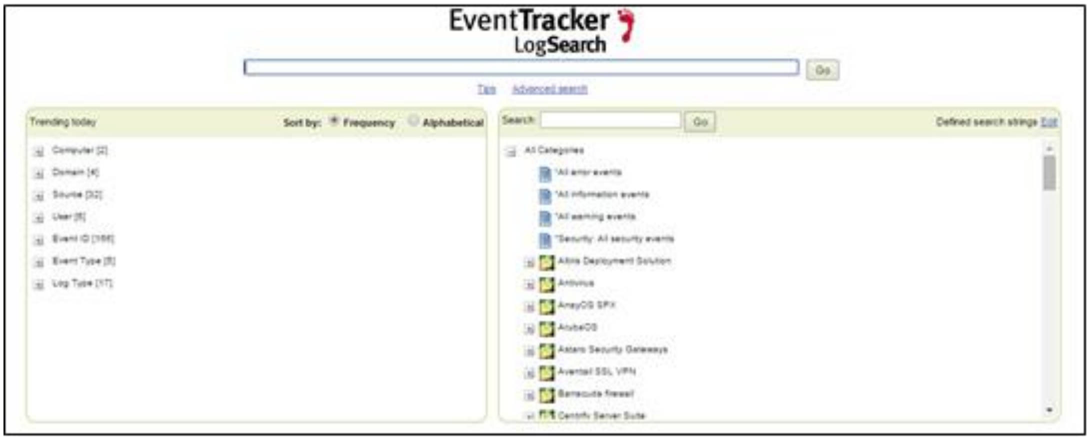
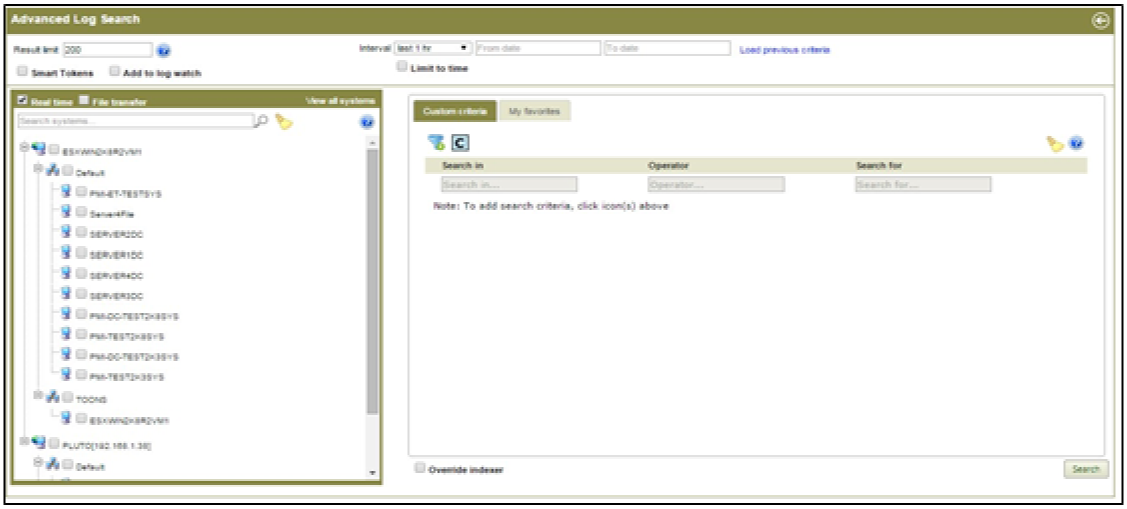


Figure 11

2. Click **Advanced search**.
   The **Advanced Log Search** page appears.



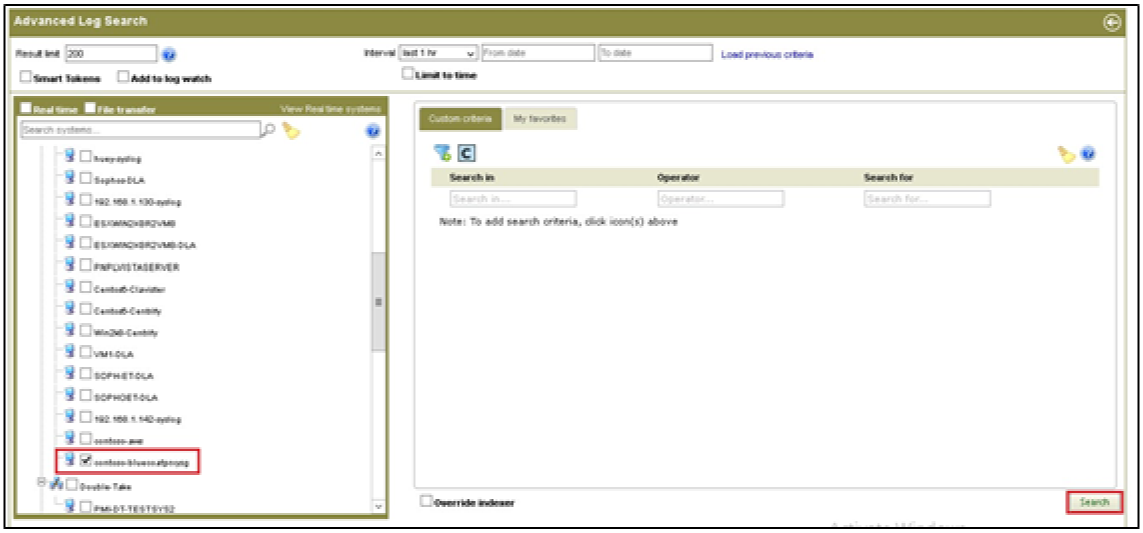
Result limit 200

Interval last 1 hr

Note: To add search criteria, click icon(s) above

Figure 12

3. Select the system and then click **Search**.



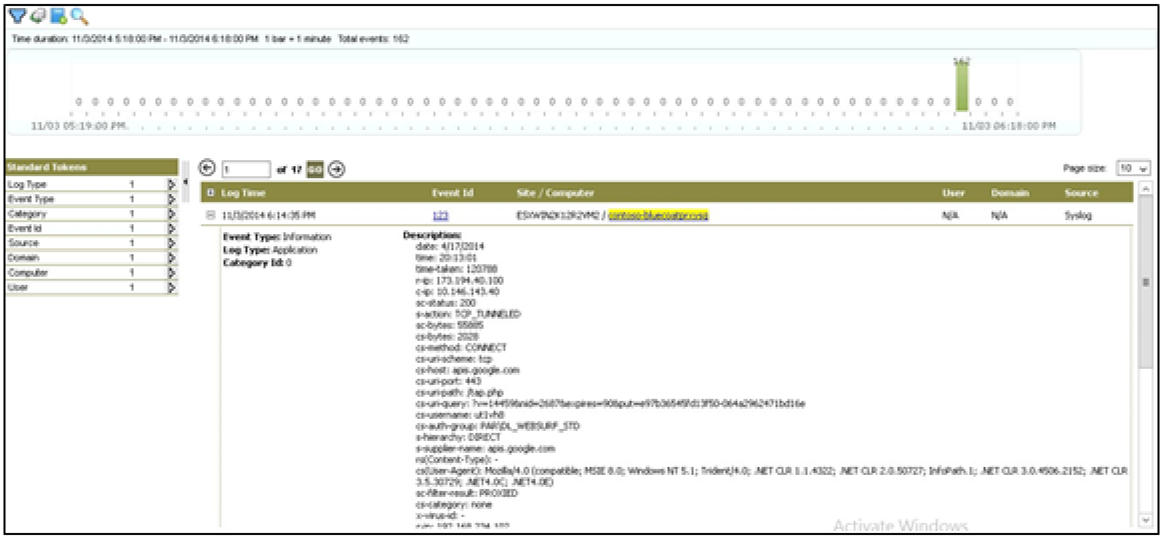
Result limit 200

Interval last 1 hr

Note: To add search criteria, click icon(s) above

Figure 13

The **Advanced Log Search** result is displayed.



Time duration: 11/3/2014 5:18:00 PM - 11/3/2014 6:18:00 PM 1 bar = 1 minute Total events: 162

Standard Tokens	
Log Type	1
Event Type	1
Category	1
Event Id	1
Source	1
Domain	1
Computer	1
User	1

1 of 17 GO   Page size: 10

Log Time	Event Id	Site / Computer	User	Domain	Source
11/3/2014 6:14:35 PM	123	ESXWIN2K12R2VM2 / contoso-bluecoatpr.com	N/A	N/A	Syslog

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

Description:
   date: 4/17/2014
   time: 20:13:01
   time-taken: 120788
   r-ip: 173.194.40.100
   c-ip: 10.146.143.40
   sc-status: 200
   s-action: TCP_TUNNELED
   sc-bytes: 55885
   cs-bytes: 2028
   cs-method: CONNECT
   cs-uri-scheme: tcp
   cs-host: apis.google.com
   cs-uri-port: 443
   cs-uri-path: /tap.php
   cs-uri-query: ?v=14459&nid=2687&expires=90&put=e97b3654f9d13f50-064a2962471bd16e
   cs-username: ut1vh8
   cs-auth-group: PAR\DL_WEBSURF_STD
   s-hierarchy: DIRECT
   s-supplier-name: apis.google.com
   rs(Content-Type): -
   cs(User-Agent): Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; InfoPath.1; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET4.0C; .NET4.0E)
   sc-filter-result: PROXIED
   cs-category: none
   x-virus-id: -
   s-ip: 192.168.234.102
```

Figure 14

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 to support Blue Coat ProxySG monitoring.

Categories

Blue Coat PorxySG: Web access allowed - This category based report provides information related to web access allowed.

Blue Coat PorxySG: Web access denied - This category based report provides information related to web access denied.

Alerts

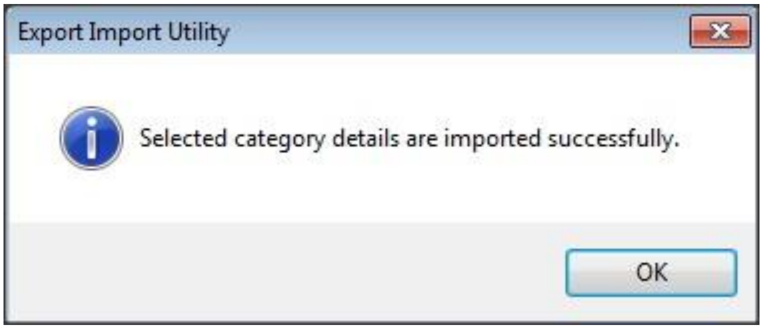
Blue Coat PorxySG: Web access denied - This alert is generated when web access denied.

Import Blue Coat ProxySG knowledge pack into EventTracker

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.
3. Click the **Import** tab.
4. **Import Category/ Alert/ Tokens/Reports** as given below.

To import Category

1. Click **Category** option, and then click the browse ... button.
2. Locate the **All Blue Coat ProxySG group of categories.iscat** file, and then click the **Open** button.
3. Click the **Import** button to import the categories.
   EventTracker displays success message.



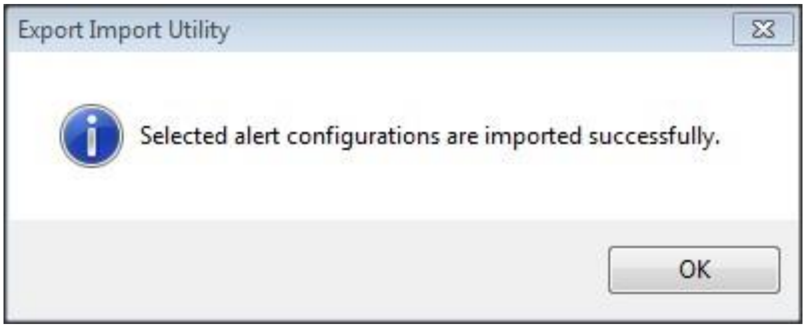
Selected category details are imported successfully.

Figure 15

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

To import Alerts

1. Click **Alert** option, and then click the browse ... button.
2. Locate the **All Blue Coat ProxySG group of alerts.isalt** file, and then click the **Open** button.
3. Click the **Import** button to import the alerts.
   EventTracker displays success message.



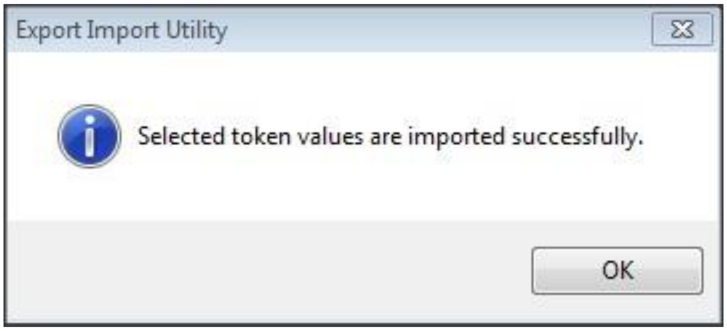
Selected alert configurations are imported successfully.

Figure 16

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

To import Tokens

1. Click **Token value** option, and then click the browse … button.
2. Locate the **All Blue Coat ProxySG group of tokens.istoken** file, and then click the **Open** button.
3. Click the **Import** button to import the tokens.
   EventTracker displays success message.



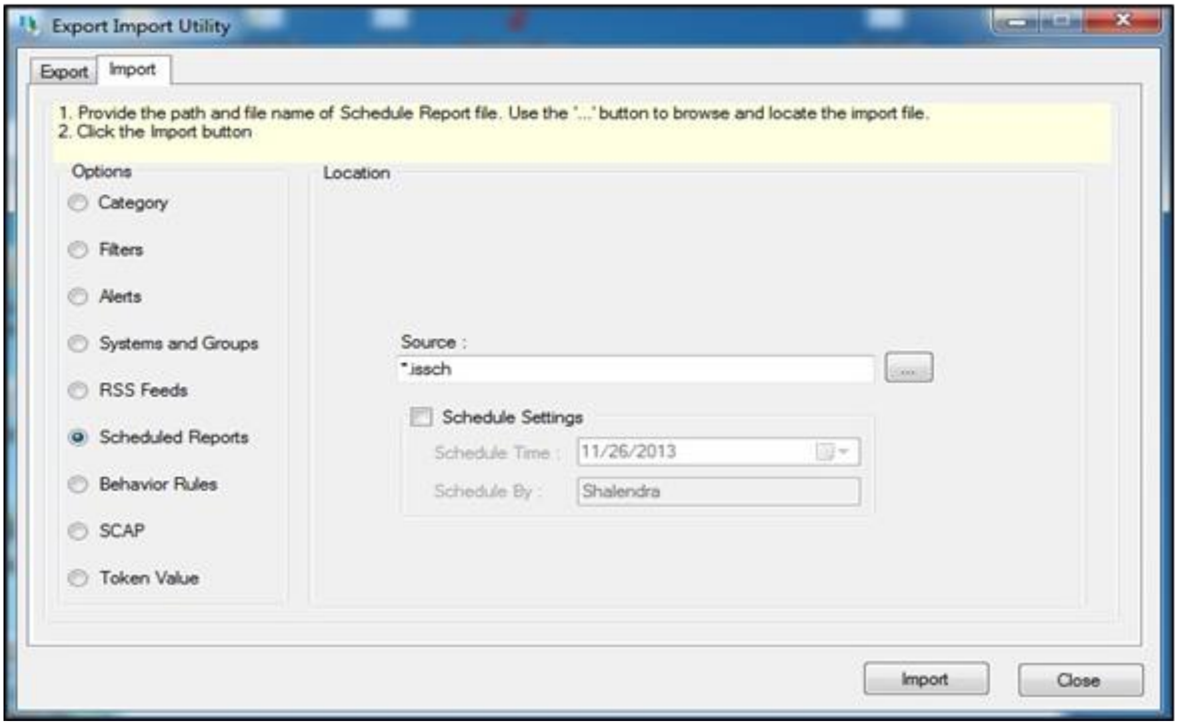
Selected token values are imported successfully.

Figure 17

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

To import Flex Reports

1. Click **Scheduled Report** option, and then click the browse [...] 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

Source : *.issch

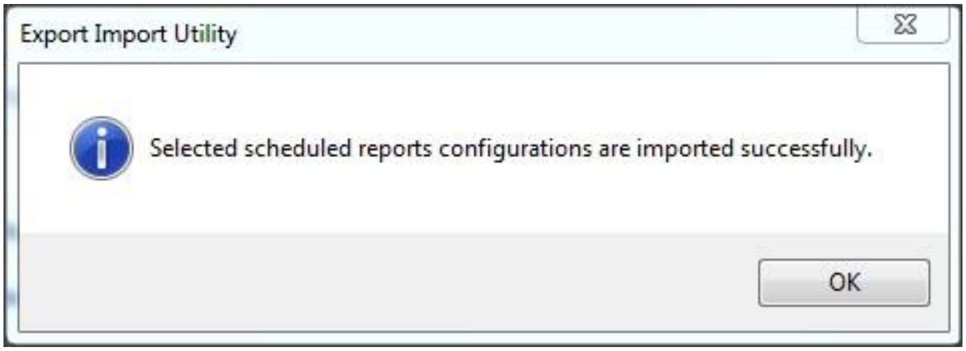
□ Schedule Settings

Schedule Time : 11/26/2013

Schedule By : Shalendra

Figure 18

2. Locate the **All Blue Coat ProxySG group of Flex Report.issch** file, and then click the **Open** button.
3. Click the **Import** button to import the scheduled reports.
   EventTracker displays success message.



Selected scheduled reports configurations are imported successfully.

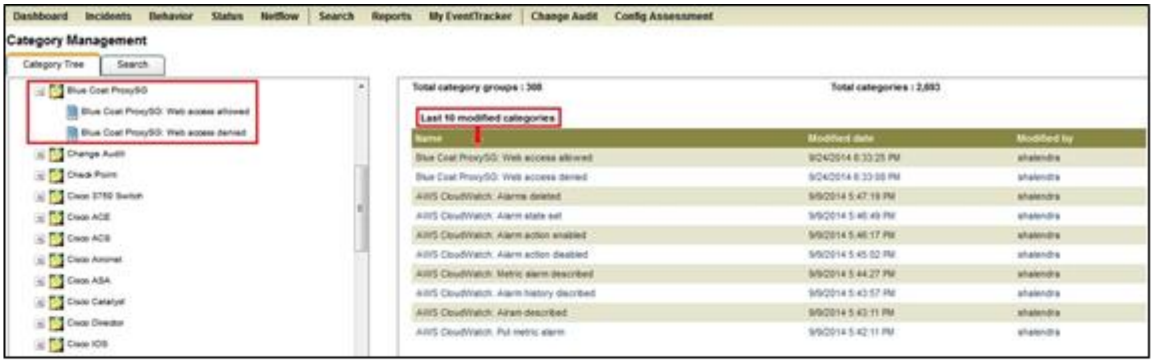
Figure 19

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

Verify Blue Coat ProxySG knowledge pack in EventTracker

Verify Blue Coat ProxySG categories

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and then click **Categories**.
3. In the **Category Tree**, expand **Blue Coat ProxySG** group folder to see the imported categories.



Total category groups : 308

Total categories : 2,693

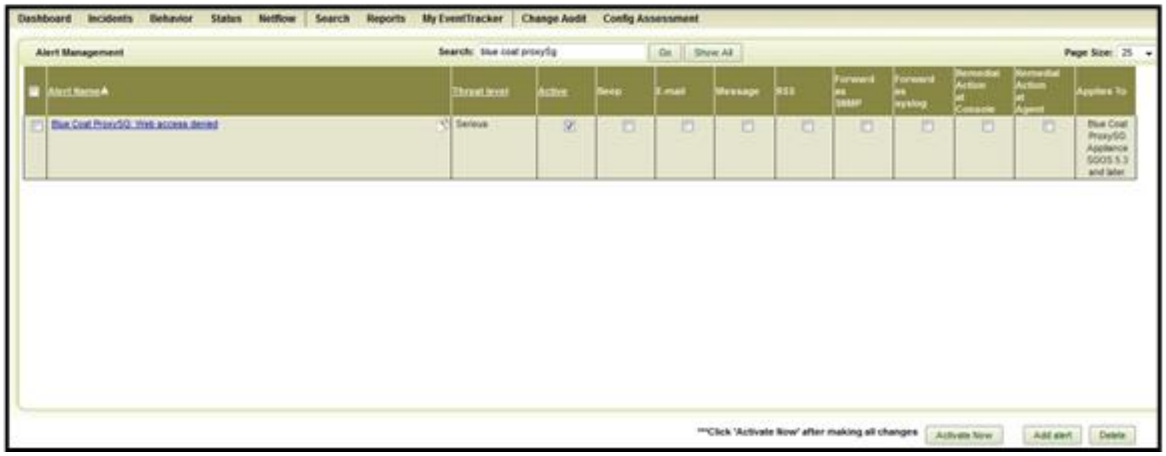
Last 10 modified categories

Name	Modified date	Modified by
Blue Coat ProxySG: Web access allowed	9/24/2014 6:33:25 PM	shalendra
Blue Coat ProxySG: Web access denied	9/24/2014 6:33:08 PM	shalendra
AWS CloudWatch: Alarms deleted	9/9/2014 5:47:19 PM	shalendra
AWS CloudWatch: Alarm state set	9/9/2014 5:46:49 PM	shalendra
AWS CloudWatch: Alarm action enabled	9/9/2014 5:46:17 PM	shalendra
AWS CloudWatch: Alarm action disabled	9/9/2014 5:45:02 PM	shalendra
AWS CloudWatch: Metric alarm described	9/9/2014 5:44:27 PM	shalendra
AWS CloudWatch: Alarm history described	9/9/2014 5:43:57 PM	shalendra
AWS CloudWatch: Airam described	9/9/2014 5:43:11 PM	shalendra
AWS CloudWatch: Put metric alarm	9/9/2014 5:42:11 PM	shalendra

Figure 20

Verify Blue Coat ProxySG alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and then click **Alerts**.
3. In the **Search** field, type ‘Blue Coat ProxySG ', and then click the **Go** button.
   Alert Management page will display all the imported Blue Coat ProxySG alerts.



Search: blue coat proxySg

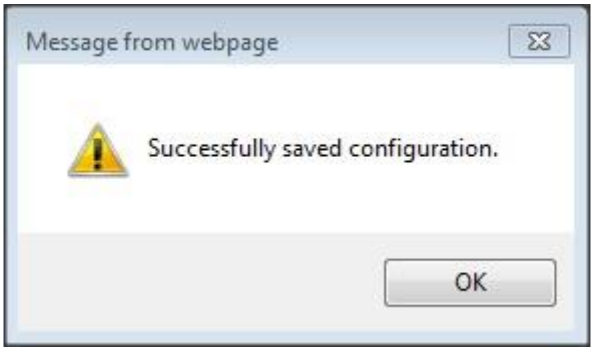
Page Size: 25

□	Alert Name▲	Threat level	Active	Beep	E-mail	Message	RSS	Forward as SNMP	Forward as syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
□	Blue Coat ProxySG: Web access denied	Serious	☑	□	□	□	□	□	□	□	□	Blue Coat ProxySG Appliance SGOS 5.3 and later

**Click 'Activate Now' after making all changes

Figure 21

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



Successfully saved configuration.

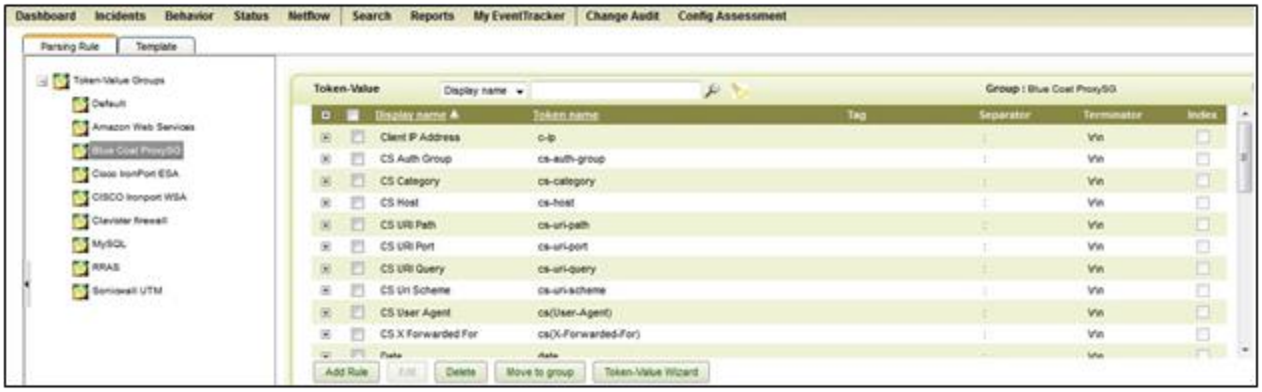
Figure 22

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 Blue Coat ProxySG tokens

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and then click **Parsing rule**.
3. Imported Blue Coat ProxySG tokens added in Token-Value Groups list.



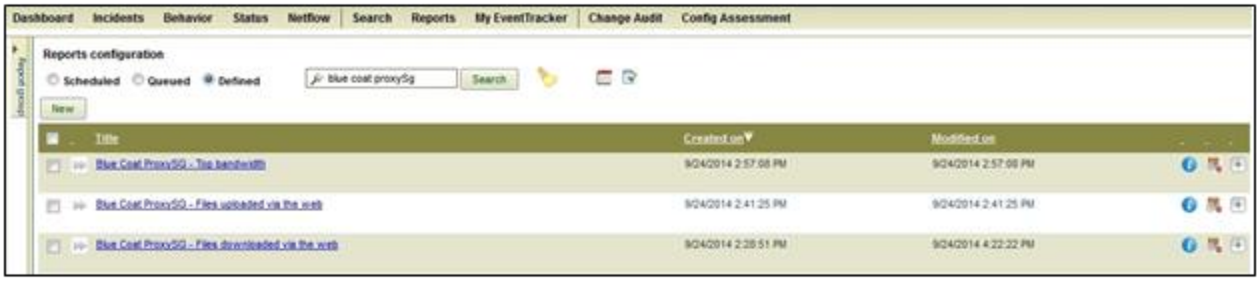
Group : Blue Coat ProxySG

Display name	Token name	Tag	Separator	Terminator	Index
Client IP Address	c-ip		:	\n	□
CS Auth Group	cs-auth-group		:	\n	□
CS Category	cs-category		:	\n	□
CS Host	cs-host		:	\n	□
CS URI Path	cs-uri-path		:	\n	□
CS URI Port	cs-uri-port		:	\n	□
CS URI Query	cs-uri-query		:	\n	□
CS Uri Scheme	cs-uri-scheme		:	\n	□
CS User Agent	cs(User-Agent)		:	\n	□
CS X Forwarded For	cs(X-Forwarded-For)		:	\n	□
Date	date		-	\n	□

Figure 23

Verify Blue Coat ProxySG Flex Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports**.
3. Select the **Configuration**.
   In the **Reports Configuration**, select **Defined** from radio button. EventTracker displays **Defined** page.
4. In search box enter '**Blue Coat ProxySG**', EventTracker displays Flex reports of Blue Coat ProxySG.



Reports configuration

○ Scheduled ○ Queued ● Defined

blue coat proxySg

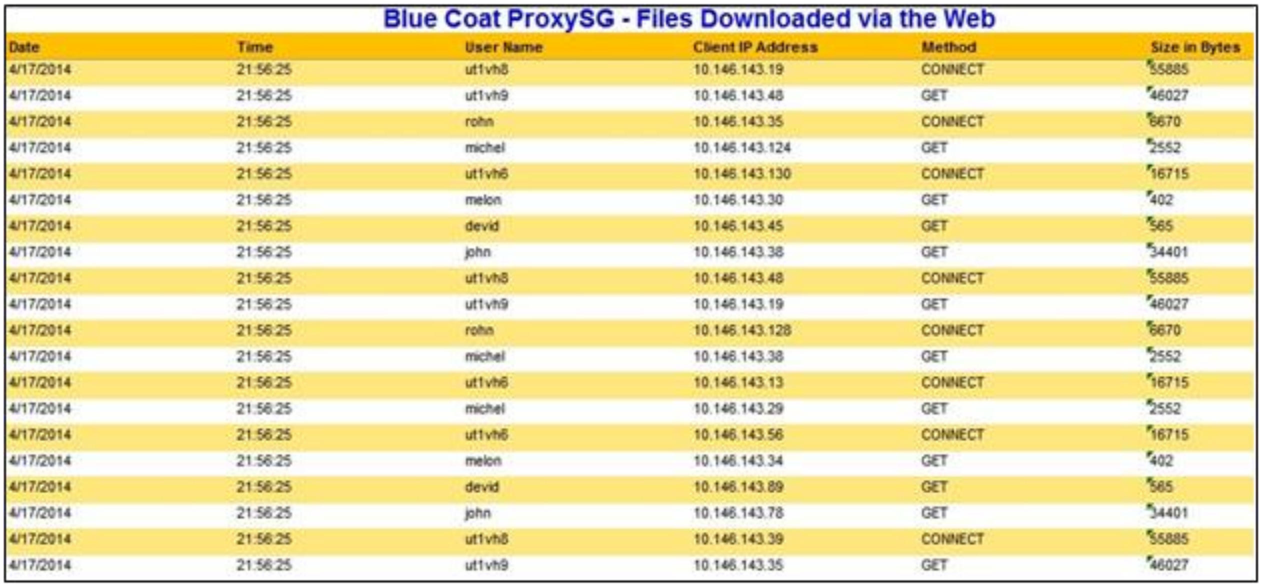
	Title	Created on	Modified on
□	Blue Coat ProxySG - Top bandwidth	9/24/2014 2:57:08 PM	9/24/2014 2:57:08 PM
□	Blue Coat ProxySG - Files uploaded via the web	9/24/2014 2:41:25 PM	9/24/2014 2:41:25 PM
□	Blue Coat ProxySG - Files downloaded via the web	9/24/2014 2:28:51 PM	9/24/2014 4:22:22 PM

Figure 24

Here you can find imported defined reports such as ‘Blue Coat ProxySG – Top bandwidth, Files uploaded via the web, Files downloaded via the web & etc.’ report.

Sample Report

Files downloaded via the Web



Blue Coat ProxySG - Files Downloaded via the Web

Date	Time	User Name	Client IP Address	Method	Size in Bytes
4/17/2014	21:56:25	ut1vh8	10.146.143.19	CONNECT	55885
4/17/2014	21:56:25	ut1vh9	10.146.143.48	GET	46027
4/17/2014	21:56:25	rohn	10.146.143.35	CONNECT	6670
4/17/2014	21:56:25	michel	10.146.143.124	GET	2552
4/17/2014	21:56:25	ut1vh6	10.146.143.130	CONNECT	16715
4/17/2014	21:56:25	melon	10.146.143.30	GET	402
4/17/2014	21:56:25	devid	10.146.143.45	GET	565
4/17/2014	21:56:25	john	10.146.143.38	GET	34401
4/17/2014	21:56:25	ut1vh8	10.146.143.48	CONNECT	55885
4/17/2014	21:56:25	ut1vh9	10.146.143.19	GET	46027
4/17/2014	21:56:25	rohn	10.146.143.128	CONNECT	6670
4/17/2014	21:56:25	michel	10.146.143.38	GET	2552
4/17/2014	21:56:25	ut1vh6	10.146.143.13	CONNECT	16715
4/17/2014	21:56:25	michel	10.146.143.29	GET	2552
4/17/2014	21:56:25	ut1vh6	10.146.143.56	CONNECT	16715
4/17/2014	21:56:25	melon	10.146.143.34	GET	402
4/17/2014	21:56:25	devid	10.146.143.89	GET	565
4/17/2014	21:56:25	john	10.146.143.78	GET	34401
4/17/2014	21:56:25	ut1vh8	10.146.143.39	CONNECT	55885
4/17/2014	21:56:25	ut1vh9	10.146.143.35	GET	46027

Figure 25