Integrate Blue Coat ProxySG
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.

© 2017 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
Table of Contents

Abstract ........................................................................................................................................... 1
Overview .......................................................................................................................................... 3
Prerequisites ................................................................................................................................... 3
Configuration .................................................................................................................................. 3
   A. Enable Access Logging ........................................................................................................ 3
   B. System Event Log ................................................................................................................ 8
      Syslog Configuration .............................................................................................................. 8
      Configuring Events to Log .................................................................................................. 9
   Verifying Blue Coat ProxySG access activity and system syslog messages in EventTracker Enterprise ........ 11
EventTracker Knowledge Pack (KP) .............................................................................................. 13
   Categories .................................................................................................................................. 13
   Alerts .......................................................................................................................................... 13
Import Blue Coat ProxySG knowledge pack into EventTracker ......................................................... 14
   To import Category .................................................................................................................. 14
   To import Alerts ...................................................................................................................... 14
   To import Tokens .................................................................................................................... 15
   To import Flex Reports .......................................................................................................... 16
Verify Blue Coat ProxySG knowledge pack in EventTracker ............................................................ 17
   Verify Blue Coat ProxySG categories ..................................................................................... 17
   Verify Blue Coat ProxySG alerts ............................................................................................ 17
   Verify Blue Coat ProxySG tokens ............................................................................................ 18
   Verify Blue Coat ProxySG Flex Reports .................................................................................. 18
Sample Report ............................................................................................................................... 19
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.

![Figure 1](image_url)

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).

![Image](image.png)

**Figure 2**

6. For this Access Log, configure the Upload Client as type “Custom Client” and ‘Save the log file as:’ a ‘text file’.
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.
9. For the log’s upload schedule, specify to upload continuously.

![Figure 5](image5)

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

![Figure 6](image6)
11. In the Access Logging object, enable logging to your new access log.

![Add Access Logging Object](image)

### 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**.

![Syslog Configuration](image)

**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**

![Figure 9](image)

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. Click **Apply**.
### Event Logging Level Options

<table>
<thead>
<tr>
<th>Event Logging Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severe errors</td>
<td>Writes only severe error messages to the event log.</td>
</tr>
<tr>
<td>Configuration events</td>
<td>Writes severe and configuration change error messages to the event log.</td>
</tr>
<tr>
<td>Policy messages</td>
<td>Writes severe, configuration change, and policy event error messages to the event log.</td>
</tr>
<tr>
<td>Informational</td>
<td>Writes severe, configuration change, policy event, and information error messages to the event log.</td>
</tr>
<tr>
<td>Verbose</td>
<td>Writes all error messages to the event log.</td>
</tr>
</tbody>
</table>

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

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

![Figure 12](image1.png)

![Figure 13](image2.png)
The **Advanced Log Search** result is displayed.

![Advanced Log Search](image)

**Figure 14**

---

**EventTracker Knowledge Pack (KP)**

Once logs are received into 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 ProxySG: Web access allowed** - This category-based report provides information related to web access allowed.

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

**Alerts**

- **Blue Coat ProxySG: 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.

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.
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.

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.

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.

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.

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

![Message from webpage](image)

**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.

![Token-Value Groups](image)

**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.
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

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>User Name</th>
<th>Client IP Address</th>
<th>Method</th>
<th>Size in Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/17/2014</td>
<td>21:56:26</td>
<td>ut1v9</td>
<td>11.146.143.19</td>
<td>CONNECT</td>
<td>58856</td>
</tr>
<tr>
<td>4/17/2014</td>
<td>21:56:25</td>
<td>ut1v9</td>
<td>11.146.143.40</td>
<td>GET</td>
<td>58027</td>
</tr>
<tr>
<td>4/17/2014</td>
<td>21:56:25</td>
<td>ut1v6</td>
<td>11.146.143.130</td>
<td>CONNECT</td>
<td>6715</td>
</tr>
<tr>
<td>4/17/2014</td>
<td>21:56:25</td>
<td>john</td>
<td>11.146.143.35</td>
<td>GET</td>
<td>54401</td>
</tr>
<tr>
<td>4/17/2014</td>
<td>21:56:25</td>
<td>ut1v9</td>
<td>11.146.143.40</td>
<td>CONNECT</td>
<td>58865</td>
</tr>
<tr>
<td>4/17/2014</td>
<td>21:56:25</td>
<td>ut1v9</td>
<td>11.146.143.19</td>
<td>GET</td>
<td>60027</td>
</tr>
<tr>
<td>4/17/2014</td>
<td>21:56:25</td>
<td>rohn</td>
<td>11.146.143.120</td>
<td>CONNECT</td>
<td>6767</td>
</tr>
<tr>
<td>4/17/2014</td>
<td>21:56:25</td>
<td>melon</td>
<td>11.146.143.34</td>
<td>GET</td>
<td>402</td>
</tr>
<tr>
<td>4/17/2014</td>
<td>21:56:25</td>
<td>john</td>
<td>11.146.143.78</td>
<td>GET</td>
<td>54401</td>
</tr>
<tr>
<td>4/17/2014</td>
<td>21:56:25</td>
<td>ut1v9</td>
<td>11.146.143.35</td>
<td>GET</td>
<td>60027</td>
</tr>
</tbody>
</table>