Integrate iboss Secure Web Gateway

EventTracker Enterprise
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.
## Table of Contents

Abstract.................................................................................................................................................. 1  
Scope.................................................................................................................................................... 1  
Audience............................................................................................................................................. 1  
Introduction ........................................................................................................................................... 3  
Pre-requisites...................................................................................................................................... 3  
Integration Method for iboss Secure Web Gateway ............................................................................. 3  
EventTracker Knowledge Pack (KP)......................................................................................................... 6  
  Categories .......................................................................................................................................... 6  
  Alerts .................................................................................................................................................. 7  
  Flex Reports .................................................................................................................................... 7  
Import iboss Secure Web Gateway knowledge pack into EventTracker.............................................. 8  
  Category ........................................................................................................................................... 9  
  Alerts ................................................................................................................................................ 10  
  Parsing Rules ................................................................................................................................... 12  
  Knowledge Object ............................................................................................................................ 13  
  Flex Reports .................................................................................................................................... 14  
Verify iboss Secure Web Gateway knowledge pack in EventTracker .................................................... 15  
  Category .......................................................................................................................................... 15  
  Alerts ................................................................................................................................................ 15  
  Parsing Rules ................................................................................................................................... 16  
  Knowledge Object ............................................................................................................................ 17  
  Flex Reports .................................................................................................................................... 17  
Create Flex Dashboards in EventTracker ............................................................................................... 18  
  Schedule Reports ............................................................................................................................. 18  
  Create Dashlets............................................................................................................................... 20  
Sample Flex Dashboards....................................................................................................................... 24
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.
2. Go to Home ➔ Settings ➔ General
3. Click on **General→Syslog Logging** option is available.

4. Configure **Syslog logging** as given below:
EventTracker: iboss Secure Web Gateway

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.

![Figure 5](image5.png)

**Logs Considered:**

![Figure 6](image6.png)
• **Iboss-Web traffic blocked**

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

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Source IP</th>
<th>Source Workstation</th>
<th>Destination IP</th>
<th>URL Name</th>
<th>Category Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/20/2016 11:49:40 AM</td>
<td>iboss</td>
<td>10.1.45.44</td>
<td>EMPTY</td>
<td>216.115.101.179</td>
<td>Virus&amp;Malware</td>
<td></td>
</tr>
<tr>
<td>09/20/2016 11:52:48 AM</td>
<td>iboss</td>
<td>10.1.45.44</td>
<td>EMPTY</td>
<td>108.160.172.204</td>
<td>client.lb.dropbox.com</td>
<td>Shops, Business</td>
</tr>
<tr>
<td>09/20/2016 11:53:38 AM</td>
<td>iboss</td>
<td>10.1.45.48</td>
<td>EMPTY</td>
<td>192.125.17.3</td>
<td>notify.dropbox.com</td>
<td>File Sharing, Technology</td>
</tr>
</tbody>
</table>

**Figure 7**

Logs Considered:

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

   EventTracker displays success message.

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

EventTracker displays success message.

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

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

![Figure 14](image)

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.

![Figure 15](image)

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.

3. In IMPORT pane, click on Browse button.

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.

![Figure 18](image1.png)

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

![Figure 19](image2.png)
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.

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

![Successfully saved configuration message box](image)

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**.

![Parsing Rule window](image)

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.

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.
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.

2. Navigate to Reports>Configuration.

3. Select iboss in report groups. Check defined dialog box.
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.

7. In next page, check column names to persist using PERSIST checkboxes beside them. Choose suitable Retention period.
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.
3. Navigate to **Dashboard>Flex**.
   Flex Dashboard pane is shown.

![Flex Dashboard]

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

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

![Data Source: iboss: Web traffic blocked](image)

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

![IBOSS WEB TRAFFIC ALLOWED BY SOURCE IP](image)

**Figure 36**
EventTracker: iboss Secure Web Gateway

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

![IBOSS WEB TRAFFIC BLOCKED BY CATEGORY](image)

09/20 05:20 - 09/20 17:20

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

![IBOSS WEB TRAFFIC ALLOWED BY CATEGORY](image)

09/20 02:22 - 09/20 14:22

*Figure 38*