Integrate Akamai Web Application Firewall
EventTracker v8.x and above
Abstract

This guide helps you in configuring Akamai WAF and EventTracker to receive events. In this guide, you will find the detailed procedures required for monitoring Akamai WAF logs.

Audience

Administrators who are assigned the task to monitor Akamai WAF events using EventTracker.

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
Audience .................................................................................................................................................................. 1
Overview ............................................................................................................................................................. 3
Prerequisites .......................................................................................................................................................... 3
Integration of Akamai WAF to EventTracker manager ...................................................................................... 3
  Configuring Log Delivery ................................................................................................................................. 3
  EventTracker Knowledge Pack ...................................................................................................................... 6
    Flex Reports ............................................................................................................................................... 7
    Knowledge Object ....................................................................................................................................... 8
Import Akamai WAF knowledge pack into EventTracker ................................................................................... 8
  Knowledge Objects ........................................................................................................................................ 9
  Flex Reports ................................................................................................................................................. 10
Verify Akamai WAF knowledge pack in EventTracker ..................................................................................... 11
  Knowledge Objects ....................................................................................................................................... 11
  Flex Reports ................................................................................................................................................. 11
Create Flex Dashboards in EventTracker ......................................................................................................... 12
  Schedule Reports ......................................................................................................................................... 12
  Create Dashlets .......................................................................................................................................... 14
  Sample Flex Dashboards ............................................................................................................................. 18
Overview

Kona Web Application Firewall from Akamai offers effective protection against web application attacks. Globally-distributed across the Akamai Intelligent Platform™, Kona WAF can easily scale to defend against massive application attacks. Kona WAF can identify and mitigate suspicious traffic without affecting performance or availability of the origin server. Security rules for Kona WAF are continuously refined by Akamai’s Threat Intelligence Team to protect against known attacks and respond to emerging threats.

EventTracker helps you to monitor event activities in Akamai WAF. Its knowledge object will help you make the log search easier and informative. And it can generate flex reports, flex dashboards for Akamai WAF.

Prerequisites

- EventTracker v8.x should be installed.
- Kona Web Application Firewall.

Integration of Akamai WAF to EventTracker manager

Configuring Log Delivery

1. Log Delivery Service can be configured through the Akamai Luna Control Center.
2. Click the Configure tab.
3. Select Log Delivery.
4. On the Select Product page, click the radio button next to the Akamai WAF.
5. Click Continue to view the Log Delivery Service page.
6. The Log Delivery Service page shows the CP codes that are associated with the Akamai service that you selected.
7. Find the CP code/service pair on the Log Delivery Service page.
8. Click the Begin Log Delivery link for a service that lacks a current LDS configuration. The Begin Log Delivery page appears.
9. Select the Create a new configuration tab.
10. Define the options for your log delivery configuration, including:
    - Time Frame: start (required) and end (optional) dates.
    - Type of Delivery: FTP
    - Type of aggregation: log arrival time
    - Log identifier string: [Identifier String]
11. You will click Next three times before completing all options.
12. On the Verify Configuration page, review the details of the configuration you created for accuracy, clicking Edit if it’s necessary to make further changes.
13. Click Save to retain this Log Delivery Service configuration. Because it is difficult to time the LDS provisioning process, a best practice is to set the start date to two days before you need the service enabled.
14. For FTP login, you will need the FTP server name, the login, the password, and the directory path (if the account used for LDS does not automatically default to this directory) for FTP login. Before accepting a new configuration, Akamai Luna Control Center runs a series of tests against your FTP server. It can be used in conjunction with Akamai’s Net Storage product.
15. Once FTP has conjunction with Akamai’s Net Storage product, collect the Akamai integrator from the support team.
16. Extract the Akamai integrator.zip in any folder.
17. Run Akamai Integrator.bat with admin privileges.

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>?zip</td>
<td>5/17/2017 2:37 PM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>akamai logs</td>
<td>5/17/2017 2:40 PM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>icon</td>
<td>5/17/2017 2:38 PM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>public key</td>
<td>5/17/2017 2:37 PM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>waf_zipfiles</td>
<td>5/17/2017 2:37 PM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>WinSCP-5.9.5-Automation</td>
<td>5/17/2017 2:37 PM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Akamai integrator</td>
<td></td>
<td>Windows Batch File</td>
<td>1 KB</td>
</tr>
<tr>
<td>Akamai integrator.config</td>
<td></td>
<td>Windows PowerShell</td>
<td>7 KB</td>
</tr>
<tr>
<td>config</td>
<td></td>
<td>Microsoft Excel C</td>
<td>1 KB</td>
</tr>
<tr>
<td>Get akamai logs</td>
<td></td>
<td>Windows PowerShell</td>
<td>3 KB</td>
</tr>
</tbody>
</table>

Figure 1
18. Enter the following details in the form.

![Akamai WAF Integrator](image)

**Client ID**: username  
**Client Secret**: User password (if any)  
**Host link**: Link to cloud storage “prefix with ‘@’ “  
**SSH Host key**: SSH Public host key  
**SSH Private key**: Private key file .ppk format  
**Source folder**: source folder location in cloud storage.

![Figure 2](image)

19. Now a task scheduler trigger pop-up window appears as shown in below image.

![Figure 3](image)

20. In this task scheduler window, you need to choose how you want to schedule the Akamai WAF reports on a Daily, Weekly or Monthly basis.

21. Once Clicked on OK, an authentication pop up window will appear asking for Username and password as shown below:
22. Please enter your System Username and Password to proceed with the Task Scheduling.

23. Click on OK to continue.

24. Click on OK once the scheduling period is chosen.

25. Click on OK.

**EventTracker Knowledge Pack**

Once logs are received into EventTracker, reports and knowledge objects can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Akamai WAF.
Integrate Akamai Web Application Firewall Flex Reports

- **Akamai WAF-Traffic report** – This report provides information about the web traffic on Akamai WAF.

Sample logs:

- **Akamai WAF – Web Traffic Errors** – This report provides the failures and errors in Web traffic.
Sample logs:

<table>
<thead>
<tr>
<th>Event Type: Information</th>
<th>Log Type: System</th>
<th>Category ID: 2</th>
</tr>
</thead>
</table>

**Event Time:** 5/16/2017 13:02:27 AM  
**Log ID:** 92347  
**Log Server:** WAFSERVER...  
**Category Name:** SYSTEM  
**Severity:** NT AUTHORITY  
**Service:** WAF  

**Log Description:**  
Client IP: 70.198.205.88  
Failed 1 times.  
Failed 2 times.  
Date Time: 09/May/2017: 13:53:54 +0000  
URI User Requested: GET /origins/www1.talbots.com/ori/nextgen_p2p/CA23bg/ljsq0_600550131014.js HTTP/1.1  
Akamai Response Code: 302  
Number of Bytes Not Relevant: 77  
HTTP Referer: https://www.talbots.com/online/tr/browse/m_category_landing_galleryview.jsp?N=3321363485&dc=cat59037&rootCategoryId=4&conceptName=Regular&conceptId=UnderSale&colorOverride:  
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 10_0_2 like Mac OS X) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Mobile/14A46 Safari/602.1  
Cookie:  
WAF Policy: TAD_4407 | |  

**Knowledge Object**

- **Akamai WAF Web traffic errors** – This knowledge object will help us to analyze the log related with Akamai WAF’s web traffic errors.
- **Akamai WAF Traffic Details** – This knowledge object will help us to analyze the log related to Akamai WAF’s Traffic.

**Import Akamai WAF knowledge pack into EventTracker**

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

![EventTracker Control Panel](image)  
**Figure 6**
3. Click the **Import** tab.

### Knowledge Objects

1. Click **Knowledge objects** under **Admin** option in the EventTracker manager page.
2. Locate the **Akamai WAF Knowledge Object**, and then click **Import** button.

![Figure 7](image)

3. Choose the Knowledge objects that needs to be imported and click on **upload**.

![Figure 8](image)

Knowledge objects are now imported successfully.

![Figure 9](image)
Flex Reports

1. Click Reports option, and select New from the option.

   ![Figure 10](image)

2. Locate the Akamai WAF Reports.etcrx file, and then click the Open button.

   ![Figure 11](image)
3. Click the **Import** button to import the reports. EventTracker displays success message.

![Figure 12](image)

**Verify Akamai WAF knowledge pack in EventTracker**

**Knowledge Objects**

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Knowledge Objects**

In the **Knowledge Object tree**, expand **Akamai WAF** group folder to see the imported Knowledge objects

![Figure 13](image)

**Flex Reports**

1. In the **EventTracker** web interface, click the **Reports** menu, and then select **Configuration**.
2. In **Reports Configuration** pane, select **Defined** option.
3. In search box enter **Akamai WAF** and then click the **Search** button.
   EventTracker displays Flex reports of 'Akamai WAF

### 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.

   ![EventTracker](image)

   **Figure 15**

2. Navigate to **Reports>Configuration**.
3. Select **Akamai WAF** 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.

![REPORT WIZARD](image)

Select columns to persist.

![RETENTION SETTING](image)

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](image)

<table>
<thead>
<tr>
<th>COLUMN NAME</th>
<th>PERSIST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer</td>
<td></td>
</tr>
<tr>
<td>Date and Time</td>
<td></td>
</tr>
<tr>
<td>Client IP Address</td>
<td></td>
</tr>
<tr>
<td>URL Request</td>
<td></td>
</tr>
<tr>
<td>Akamai Response Code</td>
<td></td>
</tr>
<tr>
<td>HTTP referer</td>
<td></td>
</tr>
</tbody>
</table>

Figure 18

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

3. Fill suitable title and description and click **Save** button.

4. Click 🔄 to configure a new flex dashlet. Widget configuration pane is shown.
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.
14. If satisfied, click **Configure** button.

15. Click ‘customize’ to locate and choose created dashlet.

16. Click to add dashlet to earlier created dashboard.
Sample Flex Dashboards

1. **WIDGET TITLE:** Akamai WAF Web Response codes  
**DATA SOURCE:** Akamai WAF-Traffic report  
**CHART TYPE:** Donut  
**AXIS LABELS [X-AXIS]:** Akamai Response Code

![AKAMAI WAF RESPONSE CODES](image)

*Figure 24*
2. **WIDGET TITLE:** Akamai HTTP errors  
**DATA SOURCE:** Akamai WAF-Web Traffic errors  
**CHART TYPE:** Column  
**AXIS LABELS [X-AXIS]:** Status Code  
**LEGEND:** URL Request Method

![Diagram of Akamai HTTP errors](image)

*Figure 25*
3. **WIDGET TITLE**: Akamai WAF – 404 Errors  
**DATA SOURCE**: Akamai WAF-Web Traffic errors  
**CHART TYPE**: Donut  
**AXIS LABELS [X-AXIS]**: Client IP Address  
**FILTER**: status Code  
**FILTER VALUES**: 404

![Akamai WAF - 404 Errors Chart](image)

*Figure 26*