

How to - Configure Fastly CDN/WAF

EventTracker v9.x and later

Abstract

This guide provides instructions to configure/ retrieve **Fastly CDN/WAF** events by “Syslog” logging for access events collection and REST API for Fastly internal/ operational event collection. Once **EventTracker** is configured to collect and parse these logs, dashboard and reports can be configured to monitor **Fastly CDN/WAF**.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x or above and **Fastly CDN/WAF**.

Audience

Administrators who are assigned the task to monitor **Fastly CDN/WAF** events using EventTracker.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright of FastlyCDN/WAF is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion 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 Netsurion, 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.

© 2020 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

1. Overview	3
2. Prerequisites	3
3. Integrating Fastly CDN/WAF with EventTracker	4
3.1 Collecting API Key	4
3.2 Forwarding logs from “Fastly audit and syslog”	6

1. Overview

Fastly is a **Content Delivery Network (CDN) and Web Application Firewall (WAF)**. **Fastly CDN** makes content available through

- Users/organizations websites.
- Internet-accessible (hosted) application programming interfaces (APIs).

Fastly's CDN/WAF Service then makes the transmission of that content (which we sometimes refer to as "content objects") more efficient by automatically storing copies at intermediate locations on a temporary basis.

Fastly WAF protects your applications from malicious attacks designed to compromise web servers. It protects against injection attacks, cross site scripting, HTTP protocols violations, and more. The Fastly WAF provides rules that detect and block potential attacks. The rules are collected into a policy and deployed within your Fastly service at the edge.

EventTracker, when integrated with Fastly CDN/WAF, collects log from Fastly CDN/WAF and creates a detailed reports, alerts, dashboards and saved searches. These attributes of EventTracker help users to view the most critical and important information on a single platform.

Flex reports will contain detailed overview of activities like, Fastly user login/ logout, Fastly login failed, user management events, Fastly service management events, devices, Fastly access events by success and failure, blocked URL and IP and its reason.

Alerts are provided as soon as any critical event triggered by Fastly CDN/WAF. With alerts users will be able to get real time events such as, login failed, service or service version deletion in their email services. From visual representation/ overview of top activities being performed in Fastly CDN/WAF to unauthorized user access (failed) can be viewed on EventTracker 'dashboard'. For e.g. "Fastly CDN/WAF - Access events by user agent" dashlet displays the user-agents trying to access any specific domain/ URL. "Fastly CDN/WAF - User login fail (Audit events by region)" dashlet displays the Login failure occurring in Fastly account in a world map by country. Dashlets associated with WAF activity will display information such as, PHP Injections attacks, SQL injection attacks, Application attack Session fixation, Application attack RCE (Remote code execution), etc.

2. Prerequisites

- EventTracker manager v9.x is required.
- EventTracker knowledge packs are required.
- Syslog port of the EventTracker console should be open with public IP address.
- API token of a user must be with at least Engineer permissions.

Note: To enable Fastly WAF logging, contact Fastly WAF support.

3. Integrating Fastly CDN/WAF with EventTracker

Although there are various methods to export the Fastly logs, EventTracker recommends using syslog.

Note - The syslog method will require a public IP address to be assigned to syslog port of the EventTracker console.

3.1 Collecting API Key

To configure EventTracker to receive logs from Fastly, we need API key with at-least engineer permissions. To do so, follow the below steps to collect the API key:

1. Go to your **“Fastly”** home page and click on user account:

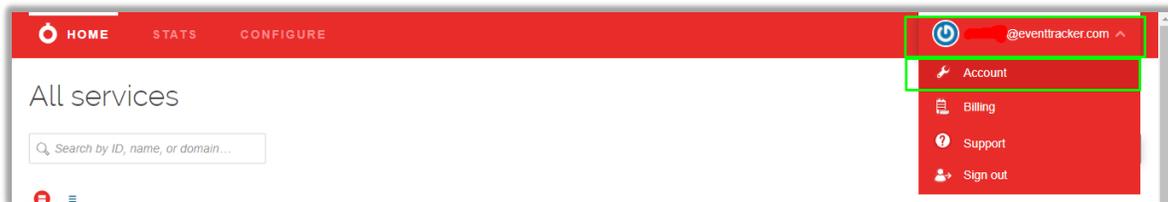


Figure 1

2. On the left panel, click **“Personal API token”** and then click **“Create Token”**

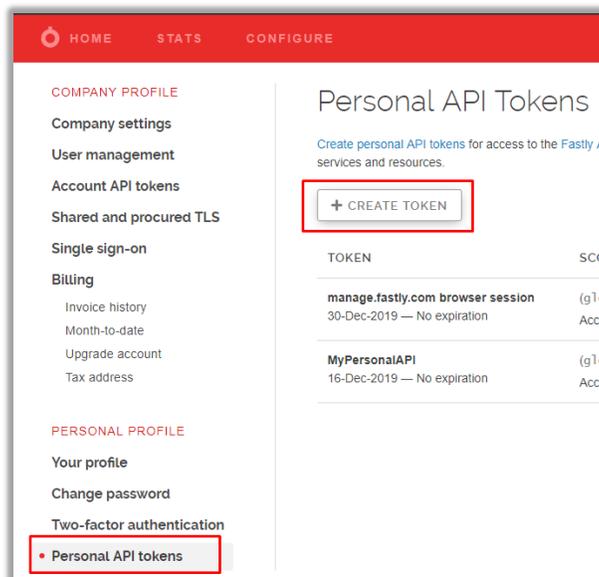


Figure 2

3. Enter the given required fields:
 - **Password** – Enter the password of your Fastly account.
 - **Name** – Give a name to the API. E.g. EventTrackerAPI.
 - **Apply to** – Set it to “All services”.
 - **Set a scope** – Set it to “Global API access(global)”.
 - **Set a token expiration** – Set it to “Never expire”.
4. Click “create” to generate a new key.

The screenshot shows the 'Create a Token' form with the following details:

- Password:** A text input field with a masked password and a 'Required' star icon.
- Name:** A text input field containing 'EventTrackerAPI' and a 'Required' star icon. Below it is a prompt: 'Describe what this token is going to be used for'.
- Apply to:** A radio button selection with 'All Services' selected. Below it is the text: 'Limiting service access does not prevent access to non-service related capabilities'.
- Set a scope:** A list of checkboxes:
 - Global API access (global) — Full control over service, purging and account
 - Purge full cache (purge_all) — Purge all assets in cache
 - Purge select content (purge_select) — Purge by URL or surrogate key
 - Read-only access (global:read) — Read account information, configuration and stats
 Below this list is the text: 'Scopes can be used to limit a token's access'.
- Set a token expiration:** A radio button selection with 'Never expire' selected. Below it is the text: 'Set expiration date'.
- Buttons:** A blue 'CREATE' button (highlighted with a red box) and a grey 'CANCEL' button.

Figure 3

5. A pop-up screen will be triggered for new token creation. Note down the API Key and click “Okay”

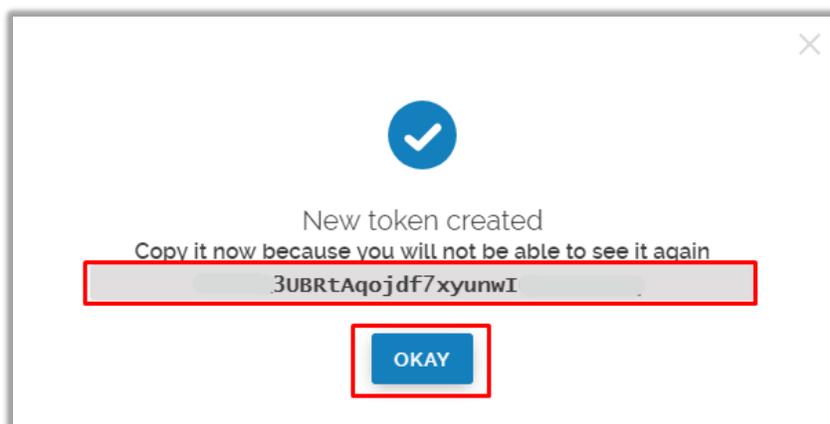


Figure 4

3.2 Forwarding logs from “Fastly audit and syslog”

1. Contact the [EventTracker support](#) team and get the “**FASTLY_CDN_Integrator**” executable file.
2. Once the executable application is received, right click on the file and select “**Run as Administrator**”.
3. Upon Running the Integrator, fill-in the given fields.

Follow the below procedures to configure Fastly CDN/WAF for EventTracker:

1. Right click the “**EventTracker (Fastly_CDN)**” executable file and “Run as administrator”.
2. Enter the **Fastly API key** and click “**Validate**”

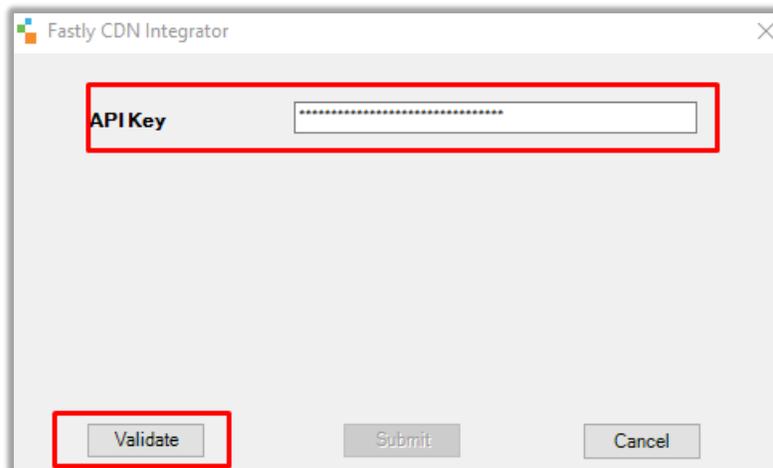


Figure 5

3. Once credentials have been successfully verified, a pop-up message will be triggered for successful validation. Else, pop-up will be triggered for validation failure.
4. Next,
 - Select the service/s “**Active Service Name/ Version**” that needs to be monitored.
 - In “**Syslog IP Address**” field enter the EventTracker Public Ip address.
 - In “**Syslog Port**” enter the EventTracker syslog port. E.g. “**514**”.

Fastly CDN Integrator

APIKey

Active Service Name/Version

- (Service_Name - "My_Service") (Version - "
- (Service_Name - "Production_ESX01") (Vers

Syslog IP Address

198.17.xxx.xxx

Syslog Endpoint Name

EventTracker Syslog VCP

Syslog Port

514

Validate Submit Cancel

Figure 6

5. Click **“Submit”**. When successfully configured, a pop-up message will be triggered for successful integration.

Fastly CDN Integrator

APIKey

Active Service Name/Version

Syslog IP Address

Syslog Endpoint Name

Syslog Port

Validate Submit Cancel

Information

Fastly CDN Integration configured successfully

OK

Figure 7