How-To Guide

Configuring Imperva WAF to Forward Logs to EventTracker

Publication Date:

December 19, 2021

Abstract

This guide provides instructions to retrieve the **Imperva WAF** events via the API to forward the logs to EventTracker. After EventTracker receives the logs from the API, the reports, dashboard, alerts, and saved searches can be configured.

Scope

The configuration details in this guide are consistent with EventTracker version 9.3 or above and **Imperva WAF.**

Audience

The Administrators who are assigned the task to monitor the **Imperva WAF** events using EventTracker.

Table of Contents

1. Overview

Imperva WAF is a Cloud-based **Web Application Firewall** (**WAF**) platform that protects application layers from malicious activities. **Imperva WAF** safeguards your cloud application from Open Web Application Security Project (OWASP) top 10 threats such as Cross-Site Scripting (XSS), SQL injection, illegal access, Remote file inclusion (RFI), and many others.

EventTracker helps to monitor events from the Imperva WAF. Its dashboard and reports will help you track traffic, block traffic, attack activities, allow traffic and trigger alerts for SQL Injection, Cross-Site Scripting, and more.

2. Prerequisites

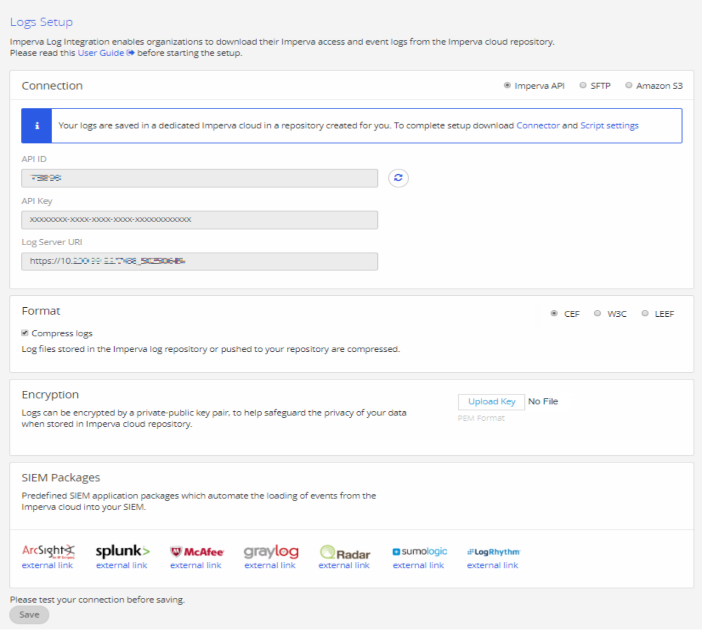
- EventTracker Agent should be installed in a host system/ server.
- PowerShell 5.0 should be installed on the host system/ server.
- Users should have administrative privilege on the host system/ server to run PowerShell.
- Administrative/root access to Imperva WAF UI.

3. Configuring Imperva WAF to Forward Logs to EventTracker

The steps provided below will help configure EventTracker to receive the Imperva WAF events using the REST API.

3.1 Configuration Imperva WAF log integration

1. Log into your **my.imperva.com** account and navigate to the **Logs Setup** page.
2. On the top menu bar, click **Account > Account Management**.
3. On the sidebar, click **SIEM Logs Setup > Logs Setup**.



Logs Setup

Imperva Log Integration enables organizations to download their Imperva access and event logs from the Imperva cloud repository.
Please read this User Guide before starting the setup.

Connection ● Imperva API ○ SFTP ○ Amazon S3

Your logs are saved in a dedicated Imperva cloud in a repository created for you. To complete setup download Connector and Script settings

API ID: [redacted]

API Key: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

Log Server URI: https://10.[redacted]

Format ● CEF ○ W3C ○ LEEF

☑ Compress logs

Log files stored in the Imperva log repository or pushed to your repository are compressed.

Encryption

Logs can be encrypted by a private-public key pair, to help safeguard the privacy of your data when stored in Imperva cloud repository.

Upload Key No File

PEM Format

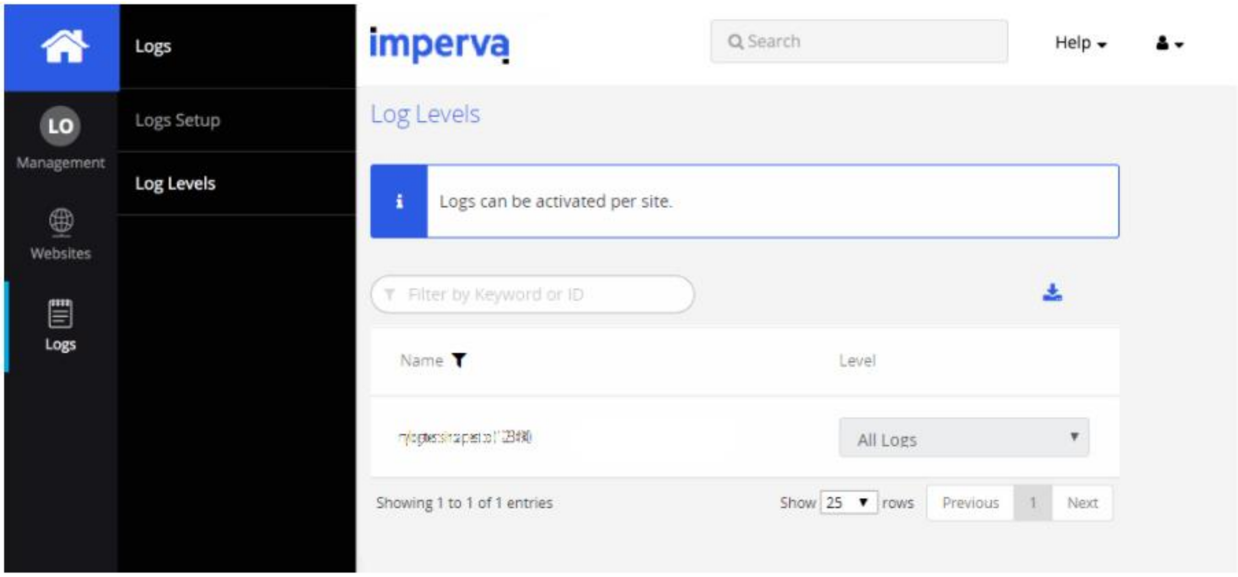
SIEM Packages

Predefined SIEM application packages which automate the loading of events from the Imperva cloud into your SIEM.

Please test your connection before saving.

a. Select **Imperva API**.
b. Uncheck **Compress logs.**
c. Under **Connection**, copy the **API Key** before exiting the window. You will need it later. If you forget to copy the key, you can come back to this window later and click **Generate API Key** to create a new key.
d. Copy the **Log Server URL** and **API ID**.
e. Click **Save.**

4. On the sidebar, click **Log Levels**. The following window displays:



Log Levels

Logs can be activated per site.

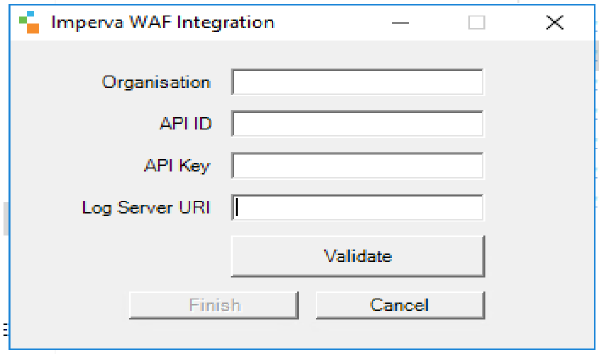
Name	Level
[illegible]	All Logs

Showing 1 to 1 of 1 entries

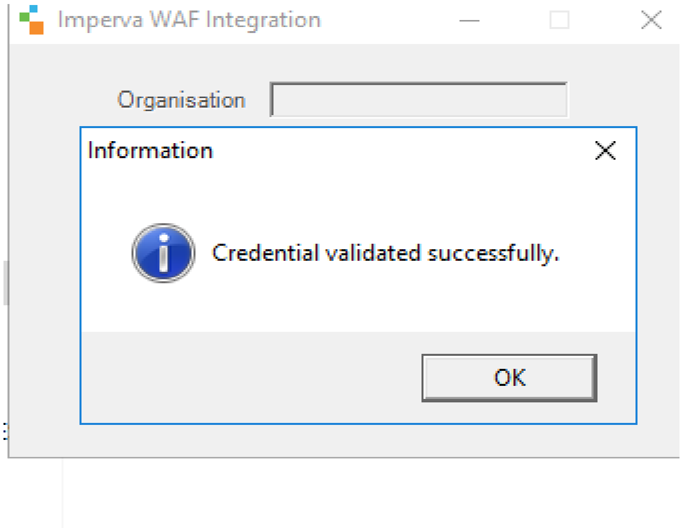
5. Select a log level for each site to enable logging or leave it disabled. There are two levels of logs:
   - **Security Logs** include the Imperva security events log.
   - **All Logs** comprise a comprehensive log of every request and response (access logs), as well as the security events log.

3.2 Configuring Imperva WAF with EventTracker

1. Download the Imperva integrator from https://downloads.eventtracker.com/kp-integrator/ImpervaWAFIntegrator.exe
2. Open the Imperva Integrator.
3. Enter the following details obtained from step 1 and provide the organization name.



4. Validate the details provided.



Credential validated successfully.

5. After successful validation, click **Finish** and Imperva WAF is configured with the EventTracker.

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's EventTracker cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's BranchSDO delivers purpose-built technology with optional levels of managed services to multi-location businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn. Netsurion is #23 among MSSP Alert's 2021 Top 250 MSSPs.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)
EventTracker Enterprise for MSPs SOC: 877-333-1433 (Option 3)
EventTracker Essentials SOC: 877-333-1433 (Option 4)
EventTracker Software Support: 877-333-1433 (Option 5)
https://www.netsurion.com/eventtracker-support