Netsurion®
Powering Secure and Agile Networks

Integration Guide

Integrating Imperva WAF Service with EventTracker

Publication Date:

December 19, 2021

© Copyright Netsurion. All Rights Reserved.

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.

© Copyright Netsurion. All Rights Reserved.

Table of Contents

© Copyright Netsurion. All Rights Reserved.

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

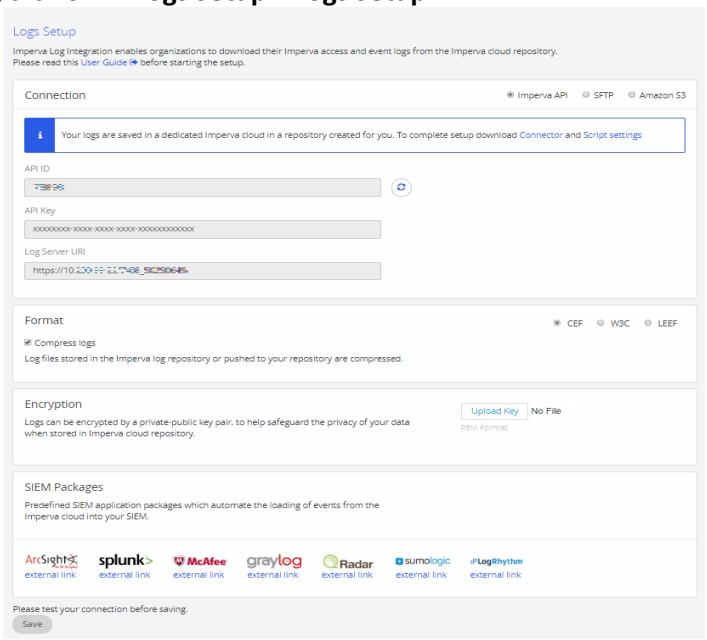
- EventTracker Agent should be installed in a host system/ server.
- PowerShell 5.0 should be installed on the host system/ server.
- Users should have administrative privilege on the host system/ server to run PowerShell.
- Administrative/root access to Imperva WAF UI.

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

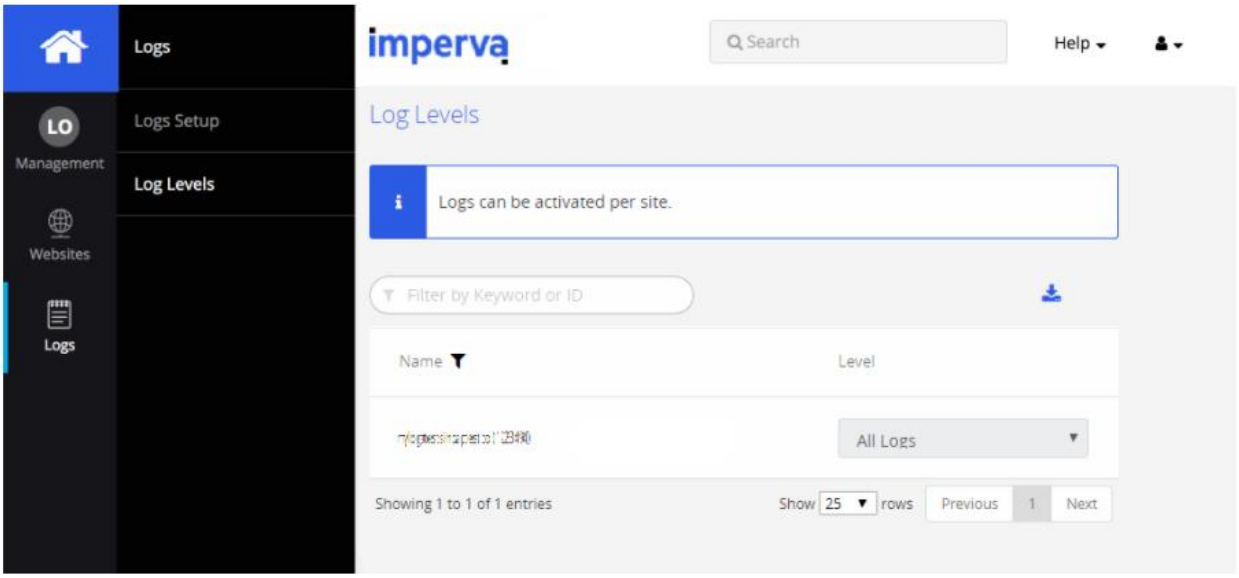
1. Log into your **my.imperva.com** account and navigate to the **Logs Setup** page.
2. On the top menu bar, click **Account > Account Management**.
3. On the sidebar, click **SIEM Logs Setup > Logs Setup**.



© Copyright Netsurion. All Rights Reserved.

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.**

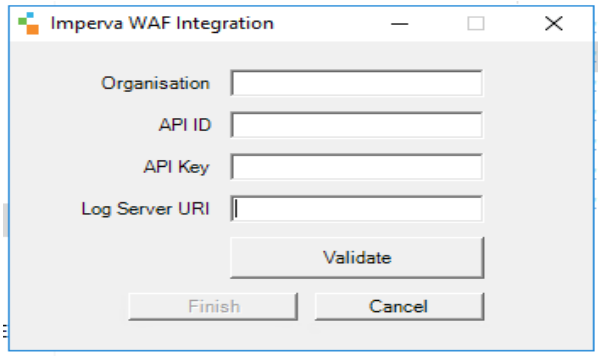
4. On the sidebar, click **Log Levels**. The following window displays:



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.

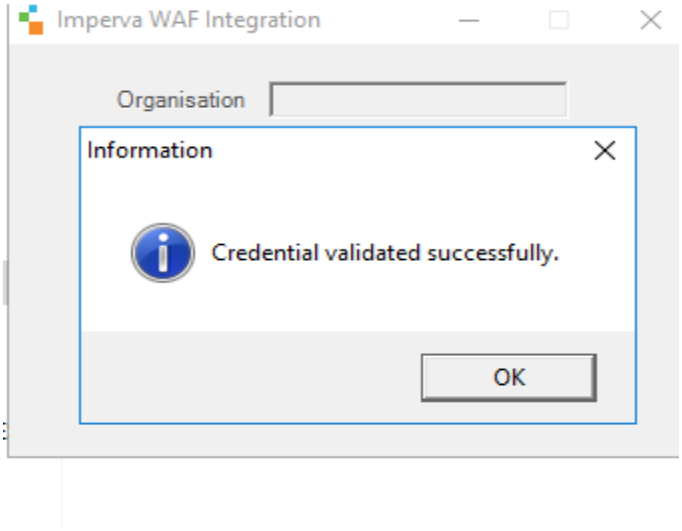
3.2 Configuring Imperva WAF with EventTracker

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.



© Copyright Netsurion. All Rights Reserved.

4. Validate the details provided.



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

4. EventTracker Knowledge Packs

After the logs are received by the EventTracker Manager, then the Knowledge Packs can be configured into EventTracker.

The following Knowledge Packs (KPs) are available in EventTracker to support the Imperva WAF.

4.1 Alerts

- **Imperva WAF: Account Takeover Detected:** Account takeover is a form of identity theft and fraud, where a malicious third party successfully gains access to the user's account credentials. By appearing as a real user, cyber-criminals can change account details, send phishing emails, steal financial information or sensitive data, or access stolen information to access more accounts in the organization. As soon as such attacks are detected these are alerted to admin.
- **Imperva WAF: ACL Detected:** The Access Control List (ACL) contains rules that deny or deny access to digital environments. Depending upon the list kept in the Imperva Environment as soon as the rule is triggered an alert is generated regarding the same.
- **Imperva WAF: Advanced Bot Detected:** Advanced bots are attacks beyond the simple scripts; these attacks are using advanced tactics such as headless browsers. Such advanced bot attacks when detected are sent as an alert from EventTracker.
- **Imperva WAF: API Specification Detected:** Vulnerabilities related to poor authentication, lack of encryption, business logic malfunctions, and insecure endpoints are detected under this alert. These vulnerabilities lead to cyber-attack such as man-in-middle attacks. This alert will trigger whenever such activity is detected.
- **Imperva WAF: Backdoor Detected:** Backdoor is a type of malware that defies common authentication mechanisms to access the system. As a result, remote access is allowed to resource within an

© Copyright Netsurion. All Rights Reserved.

application, such as databases and file servers, giving corrupters the ability to remove system commands and update malware. This alert will trigger whenever such activity is detected.

- **Imperva WAF: Bot Access Control Detected:** Devices that are infected under the bot's command control are detected, these devices are controlled under the command and used for attacks such as DDoS, etc. This alert will trigger whenever such activity is detected.
- **Imperva WAF: Remote File Inclusion Detected:** Remote File Inclusion (RFI) is an attack, targeting bugs in that web application that dynamically renders external scripts. The purpose of the offender is to exploit the function in an application for uploading the malware (for example, backdoor shell) within a domain separate from the remote URL. The results of a successful RFI attack include theft, a compromised server, and running a site that allows for content modification. This alert will trigger whenever such activity is detected.
- **Imperva WAF: Cross-Site Scripting Detected:** Cross-site scripting (XSS) attacks are a type of injection in which scripts are otherwise inserted into random and trusted websites. XSS instances occur when an attacker uses a web application to send malicious code, usually in the form of scripts by the browser, to different end-users. The flaws that allow these attacks to succeed are widely available and anywhere validated or encoded by a web application user using their input. This alert will trigger whenever such activity is detected.
- **Imperva WAF: DDoS Detected:** Distribution Denial of Service (DDoS) attack is a malicious attempt to distort the normal traffic of the target server, service, or network by flooding the Internet traffic or affecting its surrounding infrastructure. This alert will trigger whenever such activity is detected.
- **Imperva WAF: Illegal Resource Access Detected:** An Illegal Resource Access attack attempts to access private or restricted pages or attempts to view or process system files. This is mostly done using URL fuzzing, directory trajectories or command injection techniques. This alert will trigger whenever such activity is detected.
- **Imperva WAF: SQL Injection Detected:** This alert will trigger when a user execution statement contains a SQL Injection parse. SQL injection is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into the entry field for execution (for example to dump the contents of the database to the attacker). SQL injection must exploit security vulnerabilities in an application's software.

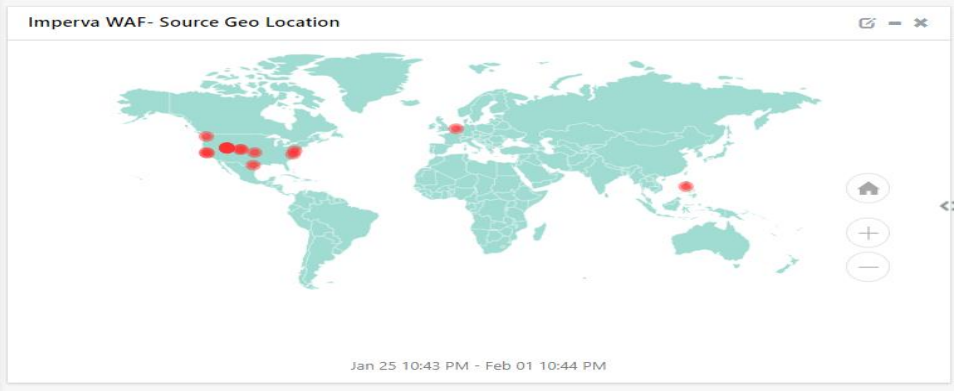
4.2 Reports

- **Imperva WAF – Attack Activities** - This report allows the user to extract the detailed summary of events that are specific to web attacks such as Cross-site scripting, SQL injection, etc.
- **Imperva WAF – Blocked Traffic** - This report allows the user to extract the detailed summary of events that are blocked by Imperva WAF.
- **Imperva WAF – Allowed Traffic** - This report allows the user to extract the detailed summary of events allowed by Imperva WAF.

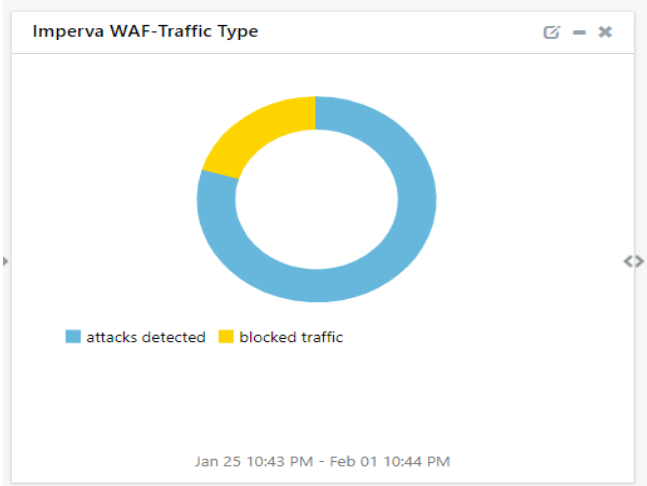
© Copyright Netsurion. All Rights Reserved.

4.3 Dashboards

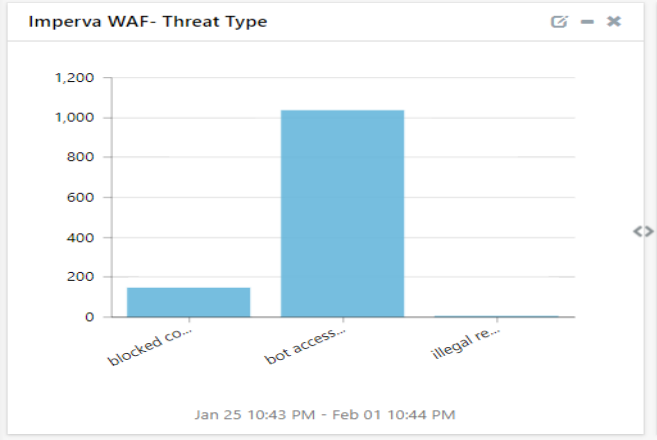
- **Imperva WAF – Source Geo Location**



- **Imperva WAF – Traffic Type**

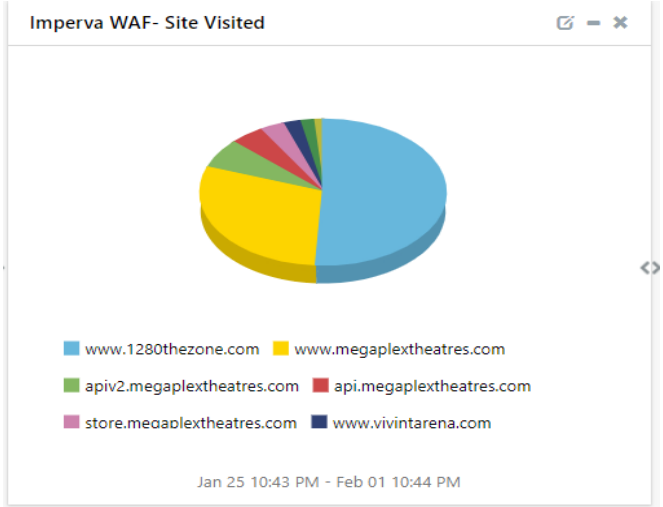


- **Imperva WAF – Threat Type**

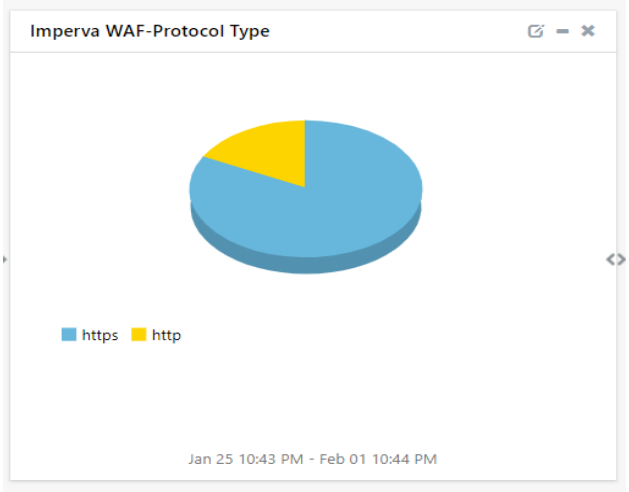


© Copyright Netsurion. All Rights Reserved.

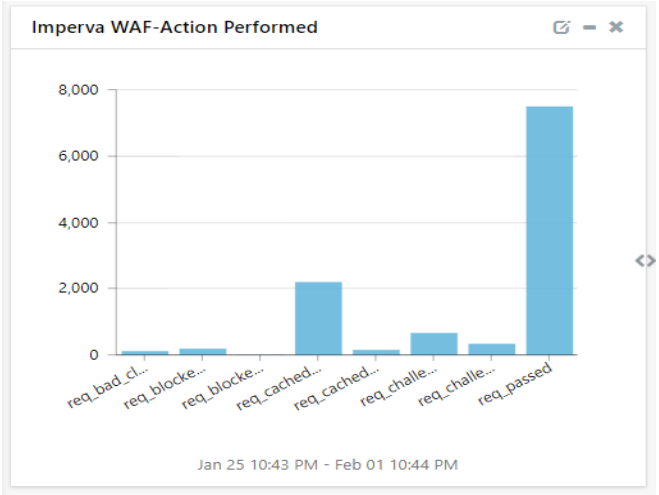
- **Imperva WAF – Site Visited**



- **Imperva WAF – Protocol Type**

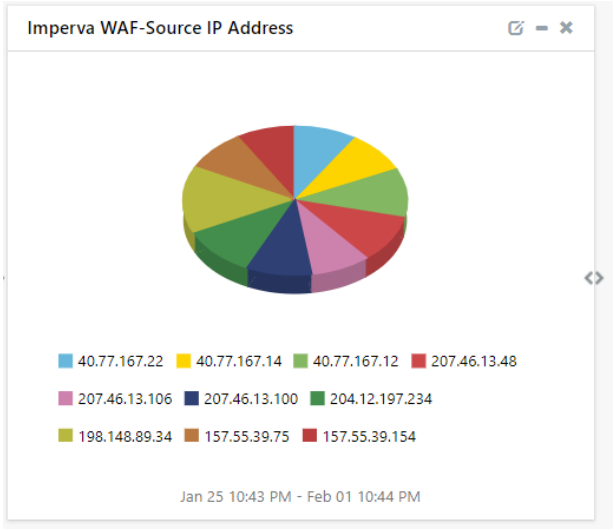


- **Imperva WAF – Action Performed**



© Copyright Netsurion. All Rights Reserved.

- **Imperva WAF – Source IP Address**

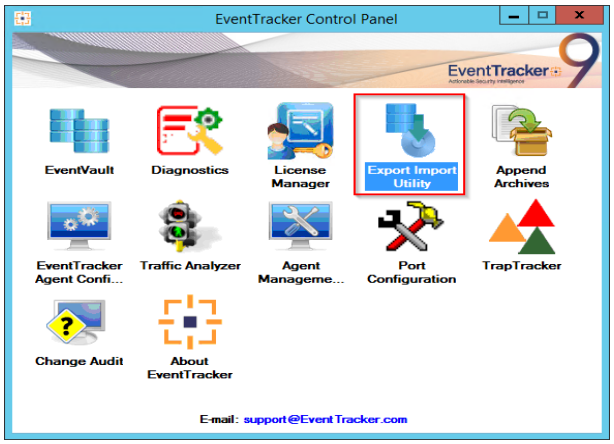


5. Importing Imperva WAF Knowledge Packs into EventTracker

NOTE: Import the Knowledge Pack items in the following sequence:

- Categories
- Alerts
- Knowledge Objects
- Reports
- Dashboards

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

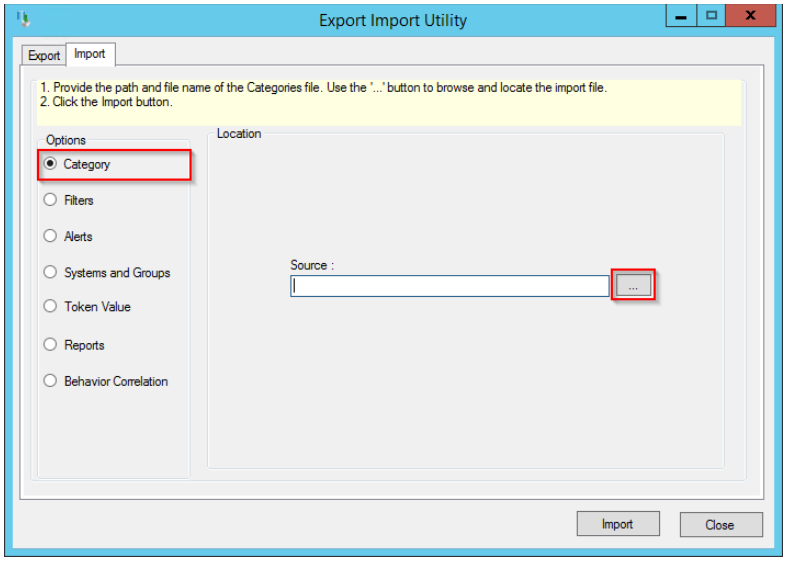


3. Click the **Import** tab.

© Copyright Netsurion. All Rights Reserved.

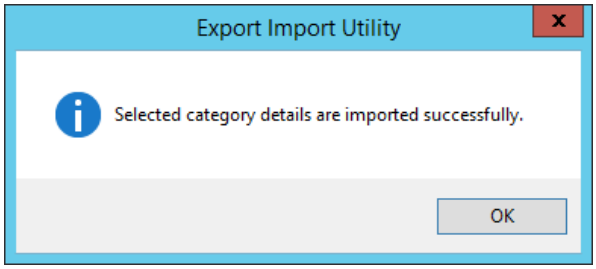
5.1 Categories

1. Click the **Category** option, and then click the **Browse** button.



2. Locate the **Categories_Imperva_WAF.iscat** file, and then click the **Open** button.
3. To import the categories, click the **Import** button.

EventTracker displays a success message.

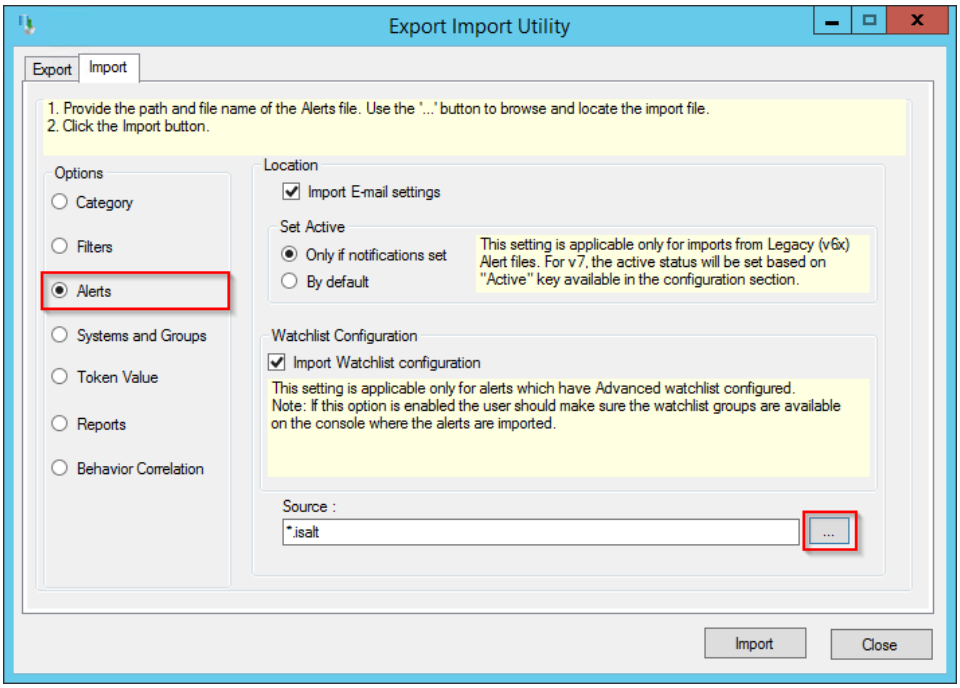


4. Click **OK,** and then click the **Close** button.

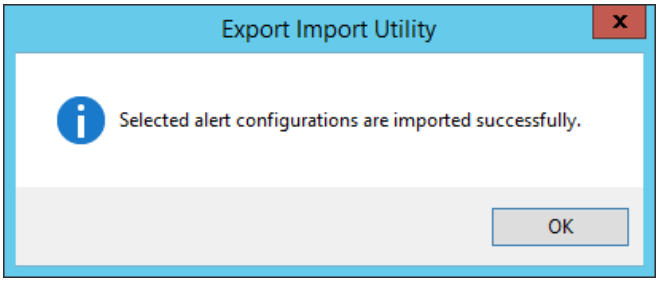
5.2 Alerts

1. Click the **Alert** option, and then click the **Browse** button.

© Copyright Netsurion. All Rights Reserved.



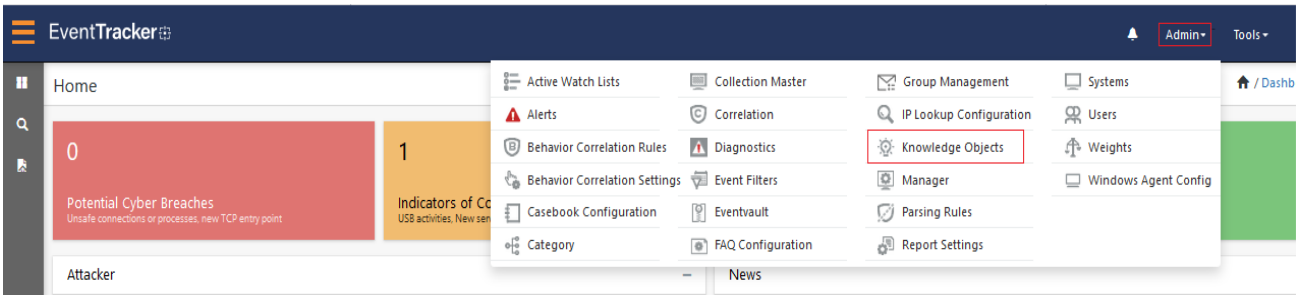
2. Locate the **Alerts_Imperva_WAF.isalt** file, and then click the **Open** button.
3. To import the alerts, click the **Import** button.
   EventTracker displays a success message.



4. Click **OK**, and then click **Close**.

5.3 Knowledge Objects

1. Click **Knowledge Objects** under the **Admin** option on the EventTracker Manager page.

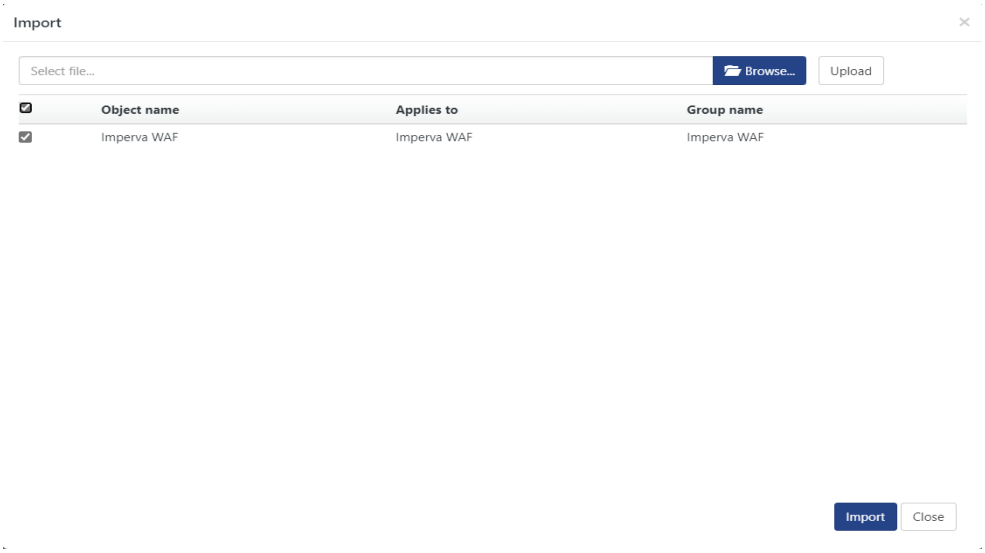


© Copyright Netsurion. All Rights Reserved.

2. Click the **Import** button as highlighted in the below image.

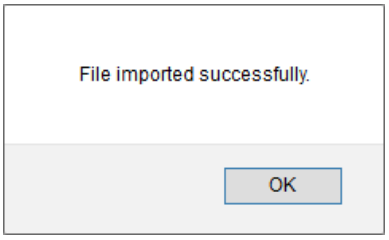
3. Click **Browse**.

4. Locate the file named **KO_Imperva_WAF.etko**.
5. Select the check box and then click the **Import** option.



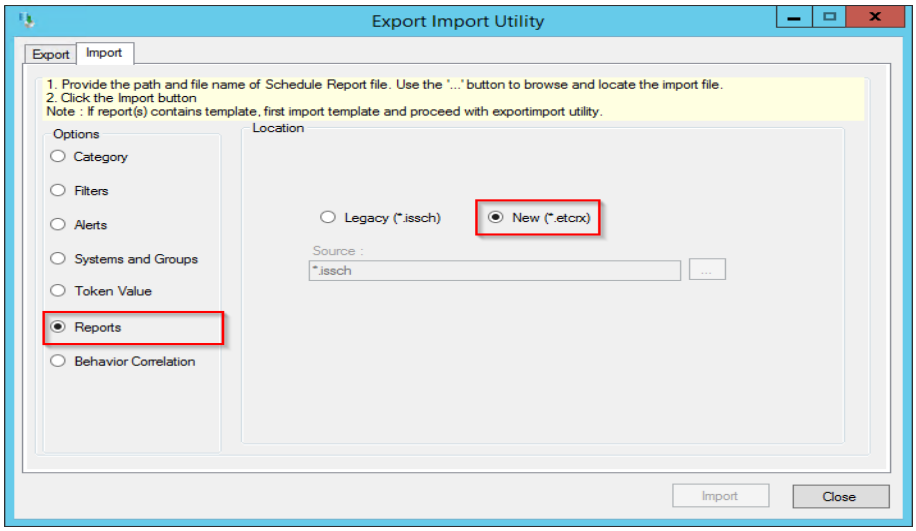
© Copyright Netsurion. All Rights Reserved.

6. The Knowledge Objects (KO) are now imported successfully.

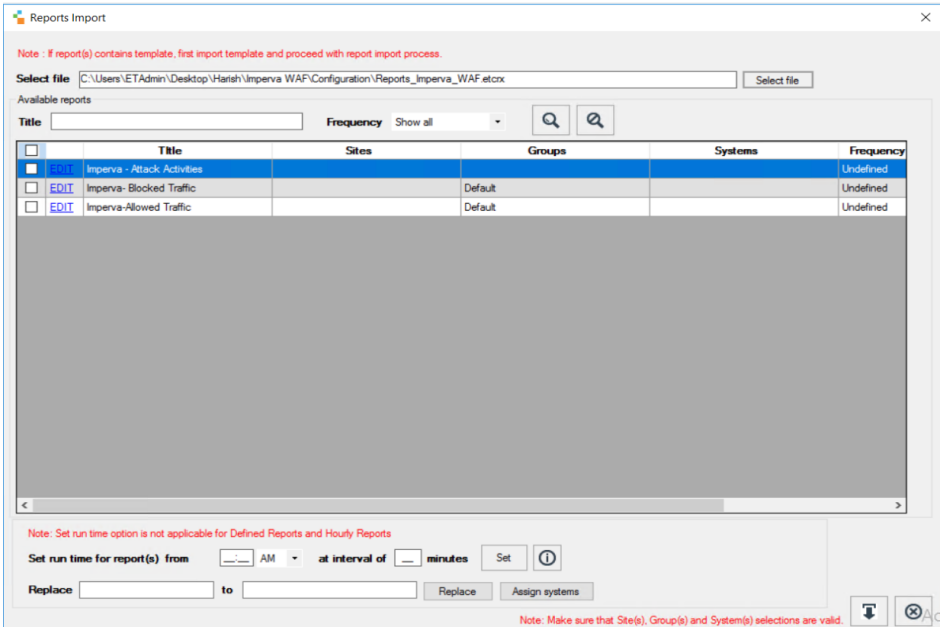


5.4 Reports

1. Click the **Reports** option and select the **New (*.etcrx)** option.

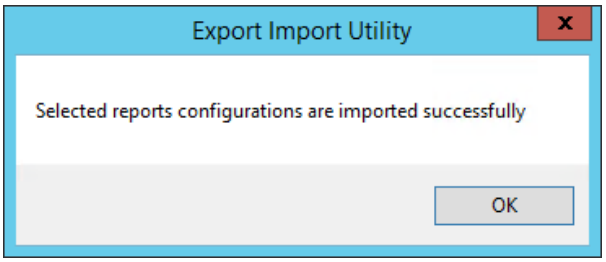


2. Locate the file named **Reports_ Imperva_WAF.etcrx** and select all the check boxes.



© Copyright Netsurion. All Rights Reserved.

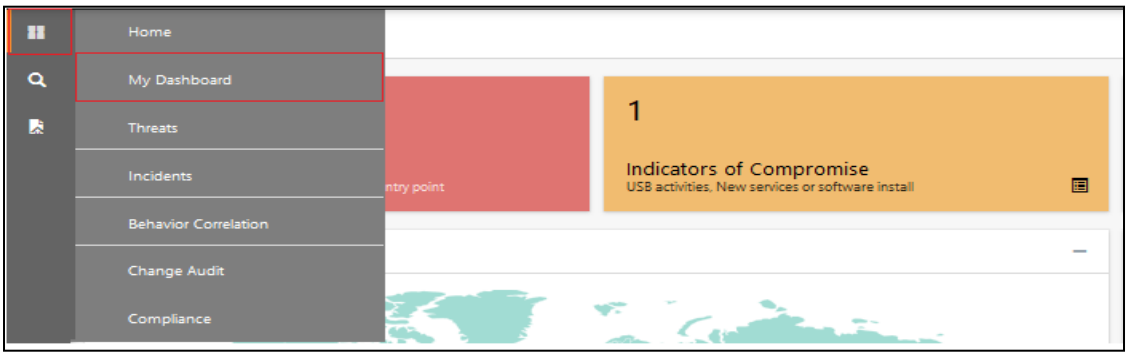
3. Click the **Import** button to import the report. EventTracker displays a success message.



5.5 Dashboards

NOTE: Below steps given are specific to EventTracker 9 and later.

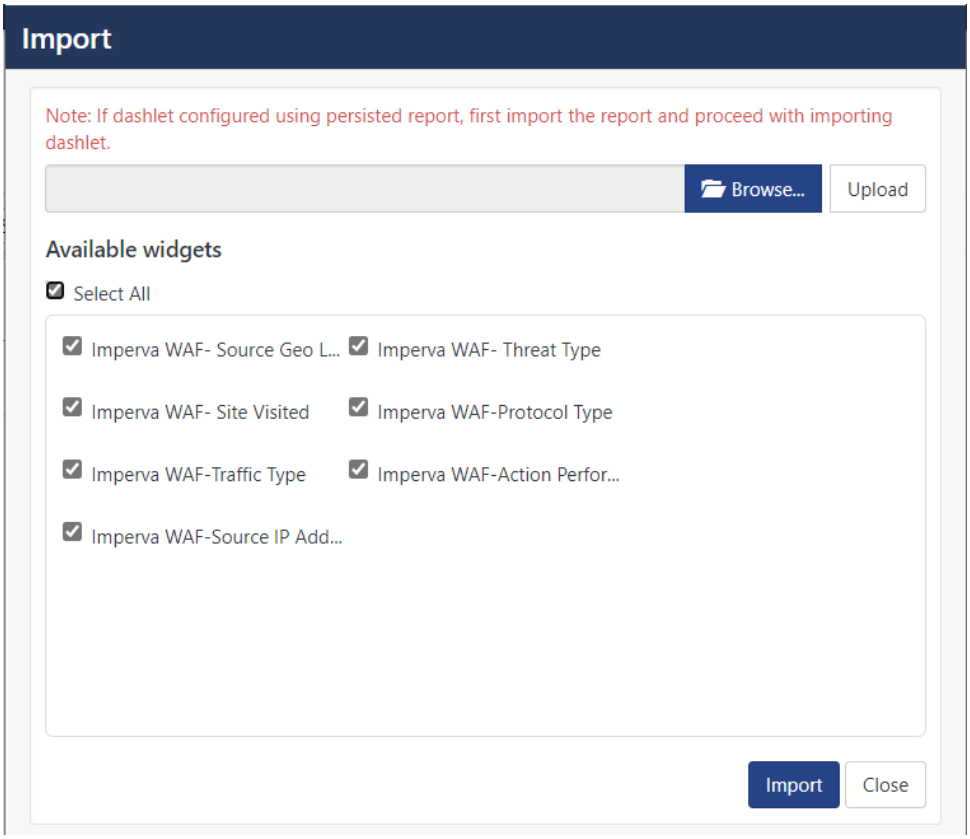
1. Open **EventTracker** in a browser and log on.



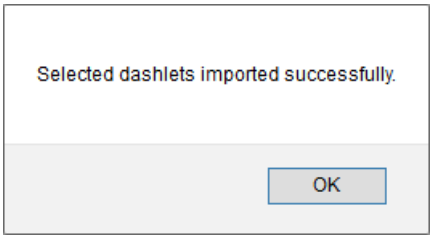
2. Navigate to the **My Dashboard** option.
3. Click the **Import** button as shown below.

4. Import the dashboard file **Dashboards_Imperva_WAF.etwd** and select the **Select All** checkbox.
5. Click **Import** as shown below.

© Copyright Netsurion. All Rights Reserved.



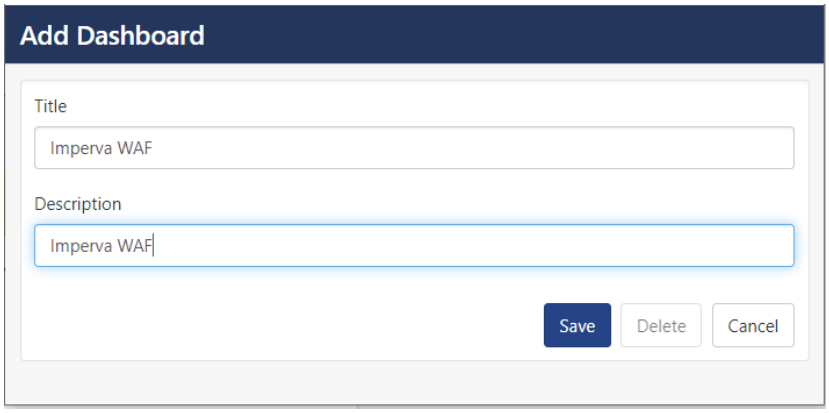
6. Import is now completed successfully.



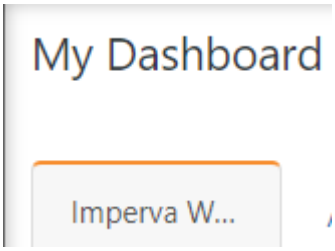
7. In the **My Dashboard** page select ⊕ to add dashboard.

8. Choose the appropriate name for the **Title** and **Description**. Click **Save**.

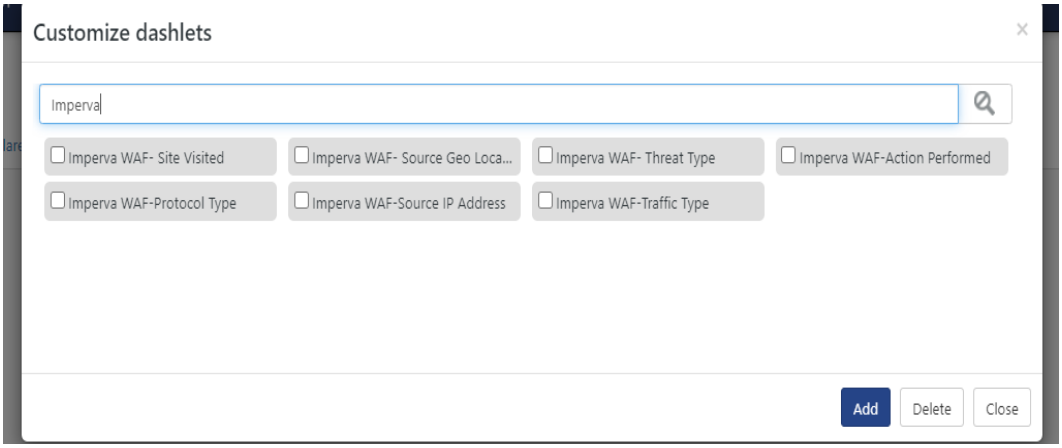
© Copyright Netsurion. All Rights Reserved.



9. On the **My Dashboard** page select to add dashlets.



10. Select the imported dashlets and click **Add**.

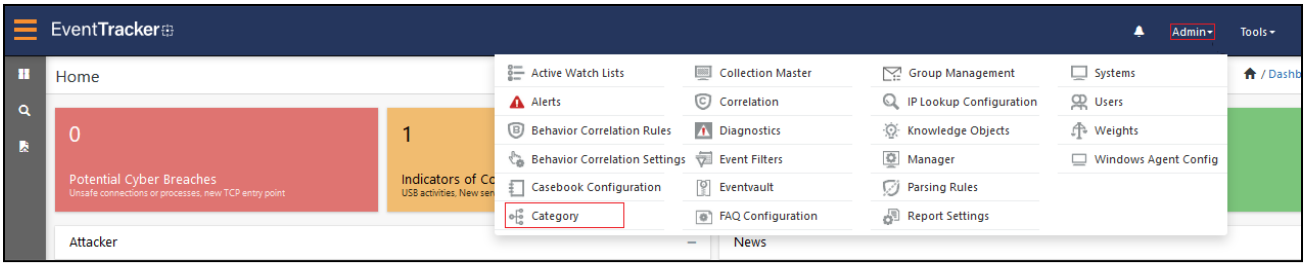


6. Verifying Imperva WAF Knowledge Packs in EventTracker

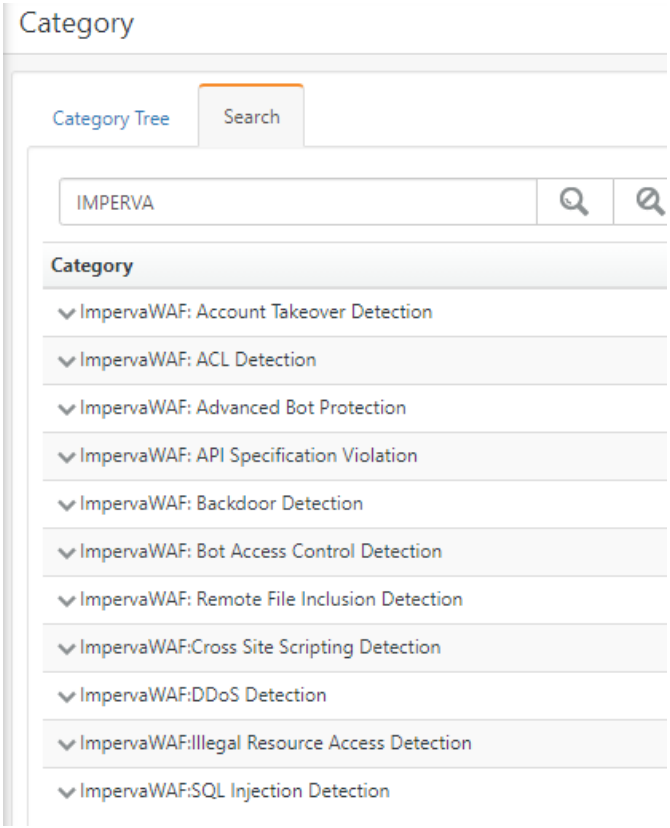
6.1 Categories

1. Log onto **EventTracker**.
2. Click the **Admin** dropdown, and then click **Category**.

© Copyright Netsurion. All Rights Reserved.



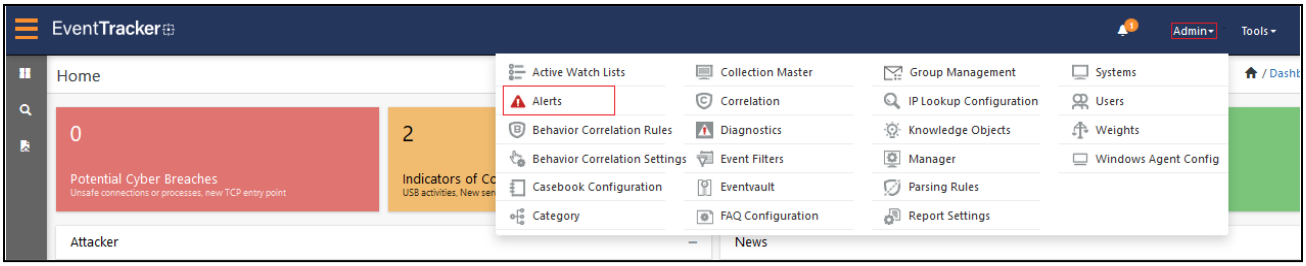
3. In the **Category Tree**, scroll down and expand the **Imperva WAF** group folder to view the imported category.



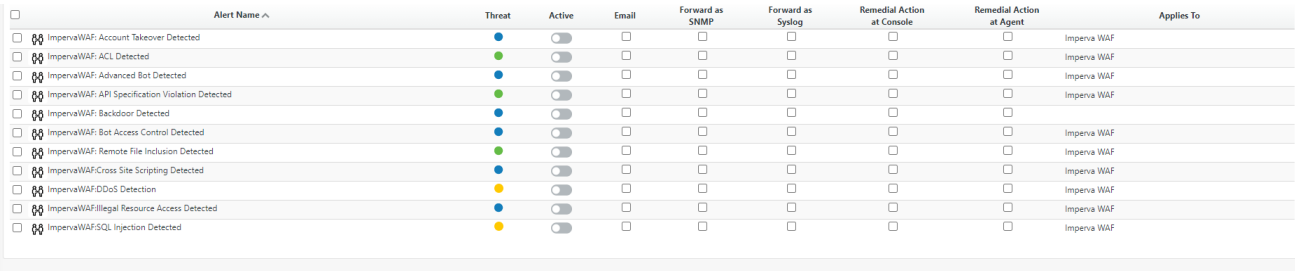
6.2 Alerts

1. Logon to **EventTracker**.
2. Click the **Admin** menu, and then click **Alerts**.

© Copyright Netsurion. All Rights Reserved.

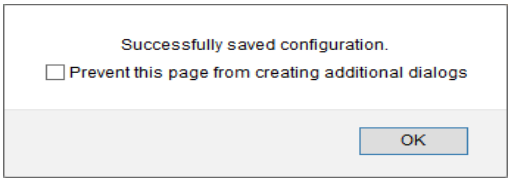


3. In the **Search** box, type **Imperva WAF**, and then click the **Go** button.
   The Alert Management page will display the imported alert.



4. To activate the imported alert, toggle the **Active** switch.

   EventTracker displays a message box.

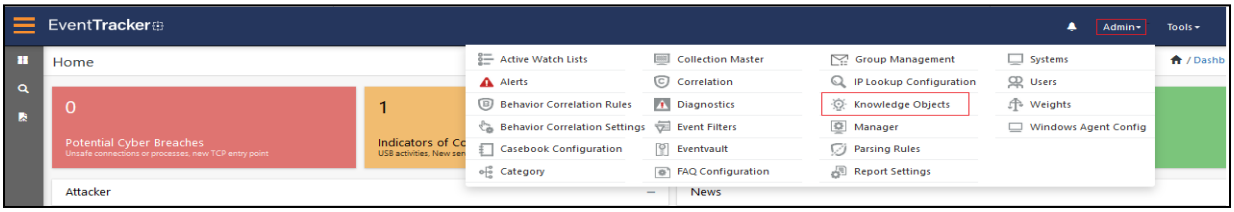


5. Click **OK**, and then click the **Activate Now** button.

NOTE: Specify the appropriate **system** in **alert configuration** for better performance.

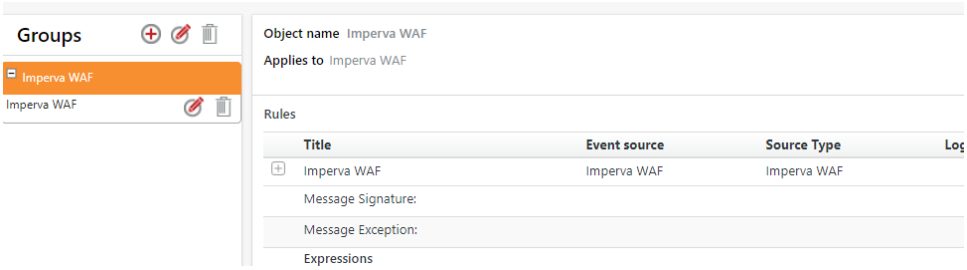
6.3 Knowledge Objects

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



2. In the Knowledge Object tree, expand the **Imperva WAF group** folder to view the imported Knowledge Objects.

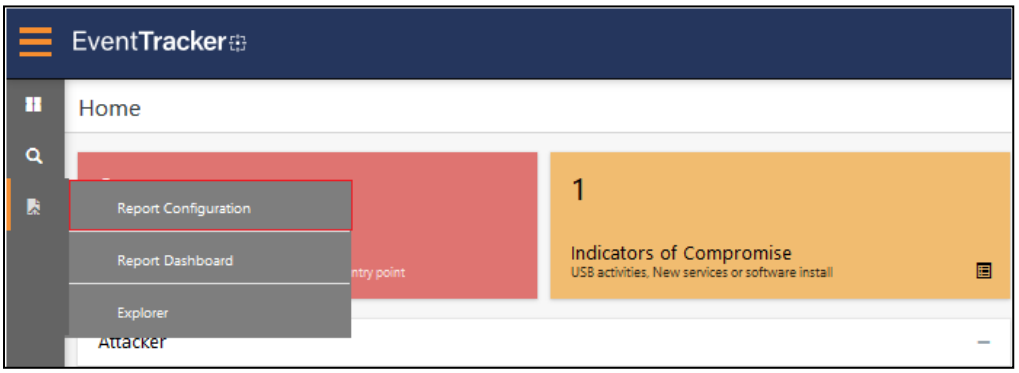
© Copyright Netsurion. All Rights Reserved.



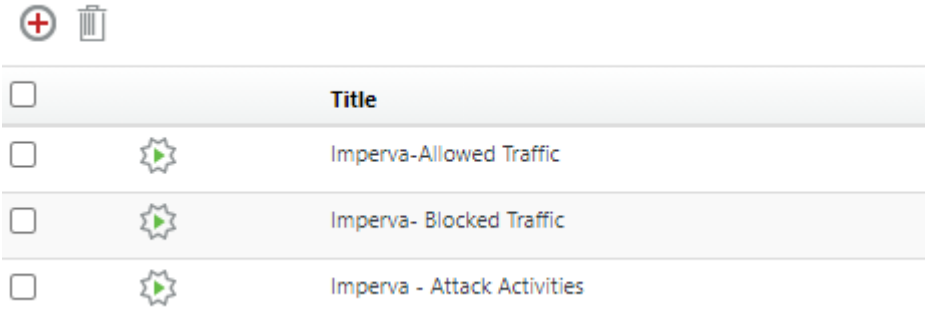
3. Click **Activate Now** to apply the imported Knowledge Objects.

6.4 Reports

1. In the **EventTracker** web interface, click the **Reports** menu, and then select **Report Configuration**.



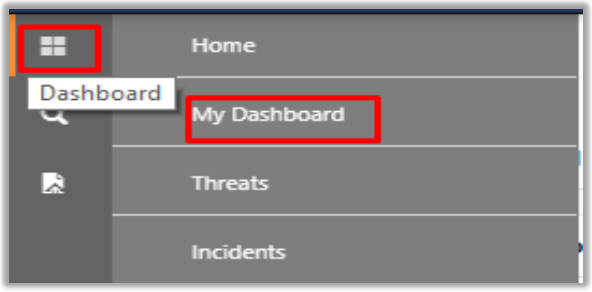
2. In the **Reports Configuration** pane, select the **Defined** option.
3. Click the **Imperva WAF** group folder to view the imported reports.



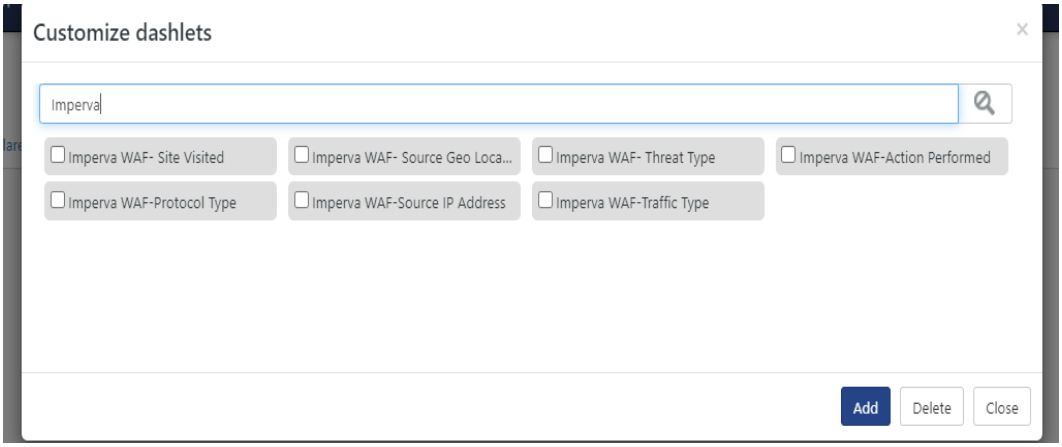
6.5 Dashboards

1. In the EventTracker web interface, click the **Home** Button and select **My Dashboard**.

© Copyright Netsurion. All Rights Reserved.



2. Click **Search** for the **Imperva WAF.** You will see the following screen.



© Copyright Netsurion. All Rights Reserved.

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

© Copyright Netsurion. All Rights Reserved.