Integrating Imperva SecureSphere
Abstract
This guide provides instructions to configure Imperva SecureSphere to send the syslog events to EventTracker.

Scope
The configurations detailed in this guide are consistent with EventTracker version 7.X and later, and Imperva SecureSphere 8 and later.

Audience
Imperva SecureSphere users, who wish to forward syslog events to EventTracker manager.
# Table of Contents

Abstract ................................................................................................................................................. 1

Pre-requisites .......................................................................................................................................... 3

Configurations ......................................................................................................................................... 3
  To create audit events action set ........................................................................................................... 3
  To create security events action set ...................................................................................................... 6

Configure audit policies to send the events to EventTracker ................................................................. 9

Configure security policies to send the events to EventTracker ............................................................. 10

Import Imperva Knowledge Pack into EventTracker ........................................................................... 11
  To import Category ............................................................................................................................... 11
  To import Alerts .................................................................................................................................. 12
  To import Scheduled Reports ............................................................................................................... 14

Verify Imperva Knowledge Pack in EventTracker ............................................................................... 15
  Verify Imperva categories .................................................................................................................... 15
  Verify Imperva alerts ........................................................................................................................... 16
  Verify Imperva Scheduled Reports ...................................................................................................... 17
Pre-requisites

- EventTracker should be installed
- Imperva SecureSphere 8 (or later) should be installed.
- Per Imperva console needs one ‘Syslog Device’ license.

Configurations

SecureSphere can send security events and audit events to EventTracker. The following section describes how to configure SecureSphere to send syslog messages to EventTracker. For this, the required configurations are as below:

- Create Audit Events action set
- Create Security Events action set
- Configure Audit policies
- Configure security policies

To create audit events action set

1. Log on to IMPERVA SECURE SPHERE.
2. Click the Policy tab, and select Action Sets.
3. Click Create new icon on the Action Set pane.
   IMPERVA opens Action set dialog box.

   ![Figure 1](image)

4. Enter the Name of the action set.
   For example: Forward audit events to EventTracker.

5. From the Apply to event type dropdown, select an event type as Audit, and then click the Create button.
   The newly created action set appears in the Action Set pane.
6. Click the green arrow to expand **Gateway Syslog > Log audit events to System Log (Gateway Syslog)** action interface.

7. Expand **Selected Actions**, and type EventTracker in the **Name** field.

8. Configure the action parameters as given in below table.
### Parameter name

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Select UDP\TCP option</td>
</tr>
<tr>
<td>Primary Host</td>
<td>IP address of EventTracker server.</td>
</tr>
<tr>
<td>Primary Port</td>
<td>By default, EventTracker will listen to port number 514.</td>
</tr>
<tr>
<td>Secondary Host</td>
<td>Optional</td>
</tr>
<tr>
<td>Secondary Port</td>
<td>Optional</td>
</tr>
<tr>
<td>Syslog Log Level</td>
<td>Select log level from the dropdown.</td>
</tr>
<tr>
<td></td>
<td>In case of ‘Audit’ event, enter the placeholder as below:</td>
</tr>
<tr>
<td></td>
<td>Imperva Inc.</td>
</tr>
<tr>
<td></td>
<td>Time=${Event.createTime}; Event Type=${Event.struct.eventType}; Server</td>
</tr>
<tr>
<td></td>
<td>Group=${Event.serverGroup}; Service Name=${Event.serviceName}; Application</td>
</tr>
<tr>
<td></td>
<td>Name=${Event.applicationName}; Database UserName=${Event.struct.user.user}; User Group=${Event.struct.userGroup}; User Authentication=${Event.struct.user.authenticated}; Application UserName=${Event.struct.applicationUser}; Source IP=${Event.sourceInfo.sourcelp}; Source Port=${Event.sourceInfo.sourcePort}; Source Application=${Event.struct.application.application}; OS UserName=${Event.struct.osUser.osUser}; Source HostName=${Event.struct.host.host}; Service Type=${Event.struct.serviceType}; Destination IP=${Event.destInfo.serverIp}; Destination Port=${Event.destInfo.serverPort}; Operation=${Event.struct.operations.name}; Operation Type=${Event.struct.operations.operationType}; Object Name=${Event.struct.operations.objects.name}; Object Type=${Event.struct.operations.objectType}; Subject=${Event.struct.operations.subjects.name}; Database Name=${Event.struct.databases.databaseName}; Schema Name=${Event.struct.databases.schemaName}; Table Group=${Event.struct.tableGroups.displayName}; Sensitive Operation=${Event.struct.tableGroups.sensitive}; Privileged Operation=${Event.struct.operations.privileged}; Stored Procedure=${Event.struct.operations.storedProcedure}; Exception=${Event.struct.complete.completeSuccessful}; Response size=${Event.struct.complete.responseSize}; Response time=${Event.struct.complete.responseTime}; Effected rows=${Event.struct.query.affectedRows}; Exception Message=${Event.struct.complete.errorValue}; Parsed</td>
</tr>
<tr>
<td>Query=Event.struct.query.parsedQuery; Raw Query=Event.struct.rawData.rawData</td>
<td>Facility</td>
</tr>
</tbody>
</table>

9. Click the **Save** icon.
10. Click the **Save** icon.

The settings are saved and newly created action set will appear under **Selected Actions**.

![Figure 4](image)

**To create security events action set**

1. Log on to IMPERVA SECURE SPHERE.
2. Click the **Policy** tab, and select **Action Sets**.
3. Click **Create new** icon on the **Action Set** pane.
   IMPERVA opens Action set dialog box.
4. Enter the name of the action set.
   For example: **Forward security events to EventTracker**.
5. From the **Apply to event type** dropdown, select an event type as **Security**, and then click the **Create** button.
   The newly created action set appears in the **Action Set** pane.
6. Click the green arrow to expand Log to System Log (syslog) (System Log > EventTracker) action interface.

7. Expand Selected Actions, and type EventTracker in the Name field.

8. Configure the action parameters as given in below table.
### Integrate Imperva SecureSphere

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syslog Host</strong></td>
<td>IP address of EventTracker server.</td>
</tr>
<tr>
<td><strong>Syslog Log Level</strong></td>
<td>Select log level from the dropdown.</td>
</tr>
<tr>
<td><strong>Message</strong></td>
<td>In case of 'Security' event, enter the placeholder as below:</td>
</tr>
<tr>
<td></td>
<td>Imperva Inc.</td>
</tr>
<tr>
<td><strong>Facility</strong></td>
<td>Select appropriate option from the dropdown.</td>
</tr>
<tr>
<td><strong>Run on Every Event</strong></td>
<td>Click this checkbox, to get the notification on every security alert.</td>
</tr>
</tbody>
</table>

9. Click the **Save** icon.
10. Click the **Save** icon.

The settings are saved and newly created action set will appear under **Selected Actions**.

![Figure 7](image-url)
Integrate Imperva SecureSphere

Configure audit policies to send the events to EventTracker

1. Click the **Policy** tab, and select **Audit**.

2. In the **Audit Policies** pane, select **Default Rule – All Events** option.

3. Move to right pane, and click **Apply to** tab.

4. Select the **systems/sites**, for which you wish to send the events.

5. Click **External logger** tab.

6. Select the newly created audit event action set (Ex. **Forward audit events to EventTracker**) in the dropdown.

7. Click **Save** icon to save the settings.
Configure security policies to send the events to EventTracker

The Syslog message can be sent with the following action upon the occurrence of a security or an audit event. The action set defined for audit/security events, will be used as following action.

1. Click the Policy tab, and select Security.
2. In the Policies pane, select the policy for which you wish to enable following action.
3. In the Policy Rules tab, select the appropriate policy rule.
4. Click the Enabled checkbox next to the policy rule.
5. Select the Severity level.
6. Select Action from the dropdown.
7. In the Followed Action dropdown, select the custom created action set for audit/security events.

8. Click Save icon to save the settings.
Import Imperva Knowledge Pack into EventTracker

1. Launch EventTracker Control Panel.
2. Double click Import Export Utility icon, and then click the Import tab.
3. Import Category/Alert/Reports as given below.

To import Category

1. Click Category option, and then click the browse button.

2. Locate the All Imperva DAM group of categories.iscat file, and then click the Open button.
3. Click the **Import** button to import the categories. EventTracker displays success message.

![Export Import Utility](image)

*Figure 11*

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

**To import Alerts**

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

![Export Import Utility](image)

*Figure 13*
2. Locate the **All Imperva DAM group of alerts.isalt** file, and then click the **Open** button.
3. Click the **Import** button to import the alerts.
   EventTracker displays a success message.

![Export Import Utility](image)

**Figure 14**

4. Click the **OK** button and then click the **Close** button.
To import Scheduled Reports

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

![Export Import Utility](image)

Figure 15

2. Locate the *All Imperva DAM defined analysis report.issch* file, and then click the **Open** button.

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

![Export Import Utility](image)

Figure 16

4. Click the **OK** button, and then click the **Close** button.
Verify Imperva Knowledge Pack in EventTracker

Verify Imperva categories

1. Logon to EventTracker Enterprise.
2. Click the Admin dropdown, and then click Categories.
3. In the Category Tree, expand Imperva group folder to see the imported categories.
Verify Imperva alerts

1. Logon to EventTracker Enterprise.
2. Click the Admin dropdown, and then click Alerts.
3. In the Search field, type ‘Imperva’, and then click the Go button.

Alert Management page will display all the imported Imperva alerts.

4. To activate the imported alerts, select the respective checkbox in the Active column.

EventTracker displays message box.
Integrate Imperva SecureSphere

5. 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.

Verify Imperva Scheduled Reports

1. Logon to EventTracker Enterprise.
2. Go to Reports.
3. Click the Defined option.
   EventTracker displays the Defined reports.

Here you can find imported scheduled reports such as ‘Imperva DAM-Database native auditing change’ report.

4. Search ‘Imperva’ in search box.
5. EventTracker displays Flex reports of all Imperva reports.