Integrate Aerohive Wireless Access Point
Abstract
This guide provides instructions to configure Aerohive Wireless Access Point to send the syslog events to EventTracker.

Scope
The configurations detailed in this guide are consistent with EventTracker version 7.x and later, and Aerohive Wireless Access Point 6.5r5.

Audience
Administrators, who are responsible for monitoring Aerohive Wireless Access Point using EventTracker.
# Table of Contents

Abstract .......................................................................................................................... 1
Overview .......................................................................................................................... 3
Pre-requisites .................................................................................................................. 3
Integration Method for Aerohive Wireless Access Point ................................................ 3
EventTracker Knowledge Pack (KP) ............................................................................... 5
  Categories ...................................................................................................................... 5
  Alerts ............................................................................................................................. 6
  Flex Reports .................................................................................................................. 6
Import Aerohive Wireless Access Point knowledge pack into EventTracker .................. 8
  Category ...................................................................................................................... 9
  Alerts ............................................................................................................................. 10
  Templates ..................................................................................................................... 11
  Flex Reports ................................................................................................................ 13
Verify Aerohive Wireless Access Point knowledge pack in EventTracker .................... 14
  Category ...................................................................................................................... 14
  Alerts ............................................................................................................................. 14
  Template ....................................................................................................................... 16
  Flex Reports ................................................................................................................ 16

Create Flex Dashboards in EventTracker ..................................................................... 17
  Schedule Reports ........................................................................................................ 17
  Create Dashlets .......................................................................................................... 19
Sample Flex Dashboards ............................................................................................... 22
Overview

The AP230 set a new performance standard for 802.11ac APs. By combining the latest in 3x3, 3-stream 802.11ac Gigabit Wi-Fi technology and advanced security and mobility management together into an economical package, it allows you to deploy 802.11ac into every part of the network infrastructure.

EventTracker collects the logs, helps administrator to analyze the events and generate the reports.

Pre-requisites

- EventTracker v7.x or later should be installed.
- An exception should be added into windows firewall on EventTracker machine for syslog port 514.
- Aerohive Wireless Access Point version 6.5r5 and later must be installed and configured.

Integration Method for Aerohive Wireless Access Point

1. Log into the Aerohive Networks HiveManager.
2. Go to Configuration > Advanced Configuration > Management Services > Syslog Assignments.
3. Click **New** and configure syslog streaming:
4. In **Syslog Server** – Select the IP address of the EventTracker manager from the dropdown.
5. In **Severity** – Select Info from the dropdown.
6. Click **Apply** and **Save**.
7. Verify that the EventTracker is receiving the syslog data.

**EventTracker Knowledge Pack (KP)**

Once logs are received in to EventTracker, Alerts and Reports can be configured into EventTracker. The following Knowledge Packs are applicable in EventTracker v7.x and later to support Aerohive.

**Categories**

- **Aerohive WAP: User login success**
  This category provides information related to user login successfully into Aerohive WAP.
- **Aerohive WAP: Client activity**
  This category provides information related to client activity in the Aerohive WAP.
- **Aerohive WAP: DHCP activity**
  This category provides information related to DHCP activity in the Aerohive WAP.
- **Aerohive WAP: IP traffic details**
  This category provides information related to IP traffic details in the Aerohive WAP.
- **Aerohive WAP: Rogue AP detected**
  This category provides information related to rogue AP detected in the Aerohive WAP.
Integrate Aerohive Wireless Access Point

Alerts

- **Aerohive WAP: Rogue AP detected**
  This alert is generated when rogue AP has been detected in the Aerohive WAP.

Flex Reports

- **Aerohive WAP-User login success**
  This report provides the information related to user login successfully into Aerohive WAP.
  **Sample Report:**

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>User Name</th>
<th>Client MAC Address</th>
<th>SSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/02/2016 03:09:19 PM</td>
<td>AEROHIVE</td>
<td>generic-guest</td>
<td>f0d1:a964:ee94</td>
<td>wifi0.1</td>
</tr>
<tr>
<td>11/02/2016 03:09:19 PM</td>
<td>AEROHIVE</td>
<td>christpor</td>
<td>f0d1:w254:e294</td>
<td>wifi4.1</td>
</tr>
<tr>
<td>11/02/2016 03:09:19 PM</td>
<td>AEROHIVE</td>
<td>generic-guest</td>
<td>f0d1:a964:ee94</td>
<td>wifi0.1</td>
</tr>
<tr>
<td>11/02/2016 03:09:19 PM</td>
<td>AEROHIVE</td>
<td>michel</td>
<td>f0d1:a964:ww44</td>
<td>wifi2.1</td>
</tr>
<tr>
<td>11/02/2016 03:09:19 PM</td>
<td>AEROHIVE</td>
<td>donald</td>
<td>f0d1:a964:ew44</td>
<td>wifi3.1</td>
</tr>
</tbody>
</table>

  **Figure 3**

- **Aerohive WAP-Client activity**
  This report provides the information related to client activities for which they are associated in Aerohive WAP.
  **Sample Report:**

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>SSID</th>
<th>Destination AP MAC</th>
<th>Client MAC Address</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/02/2016 03:09:21 PM</td>
<td>AEROHIVE</td>
<td>CF-Outside</td>
<td>08ea:4474:3314</td>
<td>f0d1:a964:ee94</td>
<td>the sta is associated with other interface</td>
</tr>
<tr>
<td>11/02/2016 03:09:21 PM</td>
<td>AEROHIVE</td>
<td>CF-Outside</td>
<td>08ea:4474:3314</td>
<td>400e:85fc:3891</td>
<td>the sta is associated with other AP</td>
</tr>
</tbody>
</table>

  **Figure 5**
Logs Considered:

- **Aerohive WAP: DHCP activity**
  This report provides the information related to DHCP activities into Aerohive WAP.
  Sample Report:

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Event ID</th>
<th>Site / Computer</th>
<th>User Name</th>
<th>Source IP Address</th>
<th>Client MAC Address</th>
<th>Client Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>03:09:23 PM</td>
<td>123</td>
<td>PNPL-4-KP / Aerohive</td>
<td>N/A</td>
<td>10.86.0.121</td>
<td>00:16:6f:0e:07:00</td>
<td>Android</td>
</tr>
</tbody>
</table>

Logs Considered:

- **Aerohive WAP: IP traffic details**
  This report provides the information related to IP traffic details into Aerohive WAP.
  Sample Report:

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Event ID</th>
<th>Site / Computer</th>
<th>Source User Name</th>
<th>Source IP Address</th>
<th>Source Port</th>
<th>Source Host Name</th>
<th>Destination User Name</th>
<th>Destination IP Address</th>
<th>Destination Port</th>
<th>Destination Host Name</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/22/2016 03:09:23 PM</td>
<td>123</td>
<td>PNPL-4-KP / Aerohive</td>
<td>generic-guest</td>
<td>10.86.0.121</td>
<td>50219</td>
<td>android-0233fa2a435b0e7</td>
<td>N/A</td>
<td>0.0.0.0</td>
<td>50</td>
<td>N/A</td>
<td>17</td>
</tr>
</tbody>
</table>
- **Aerohive WAP: Rogue AP detected**
  This report provides the information related to a rogue AP that has been detected into Aerohive WAP.

  **Sample Report:**

  ![Figure 11](image)

  **Logs Considered:**

  ![Figure 12](image)

**Import Aerohive Wireless Access Point knowledge pack into EventTracker**

**NOTE:** Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Parsing Rule
- Knowledge Objects
- Flex Reports

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.
3. Click the **Import** tab.

### Category

1. Click **Category** option, and then click the browse button.
2. Locate the **All Aerohive WAP group of categories.iscat** file, and then click **Open** button.
3. To import categories, click the **Import** button. EventTracker displays success message.

![Export Import Utility](image)

**Figure 15**

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

**Alerts**

1. Click **Alerts** option, and then click the browse button.
2. Locate the **All Aerohive WAP group of alerts.isalt** file, and then click the **Open** button.

![Export Import Utility](image)

**Figure 16**
2. To import alerts, click the **Import** button.

EventTracker displays success message.

![Figure 17](image)

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

**Templates**

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab, and then click on **Import** option.

![Figure 18](image)
3. Click on **Browse** button.

![Figure 19](image1.png)

4. Locate **All Aerohive WAP group of Template.ettd** file, and then click the **Open** button.

![Figure 20](image2.png)

5. Now select the check box and then click on **Import** option. EventTracker displays success message.

![Figure 21](image3.png)

6. Click on **OK** button.
Flex Reports

1. Click **Reports** option, and then click the browse button.
2. Locate the **All Aerohive WAP group of flex reports.issch** file, and then click the **Open** button.

![Figure 22](image)

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

![Figure 23](image)
Verify Aerohive Wireless Access Point knowledge pack in EventTracker

**Category**

1. In the *EventTracker Enterprise* web interface, click the *Admin* dropdown, and then click *Categories*.
2. In the *Category Tree*, expand *Aerohive* group folder to see the imported categories.

![Category Management](image)

**Alerts**

1. In the *EventTracker Enterprise* web interface, click the *Admin* dropdown, and then click *Alerts*.
2. In the *Search* field, type *Aerohive*, and then click *Go* button.

   Alert Management page will display the imported *Aerohive* alert.
3. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

![Figure 25]

4. 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.
Template

1. Logon to EventTracker Enterprise web interface.
2. Click the Admin menu, and then click Parsing Rules and click Template.

![Parsing Rule](image)

**Figure 27**

Flex Reports

1. In the EventTracker Enterprise web interface, click the Reports menu, and then select Configuration.
2. In Reports Configuration pane, select Defined option.
3. In search box enter 'Aerohive', and then click the Search button.

EventTracker displays Flex reports of Aerohive.
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.

2. Navigate to Reports>Configuration.
3. Select **Aerohive** 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**.

![Figure 32](image)

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.

![Figure 33](image)
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.

![Figure 36](image)

14. If satisfied, click **Configure** button.

![Figure 37](image)

15. Click ‘customize’ 🔄 to locate and choose created dashlet.
16. Click ✪ to add dashlet to earlier created dashboard.
Sample Flex Dashboards

For below dashboard **DATA SOURCE: Aerohive WAP-User login success**

- **Aerohive WAP-User login success**
  - **WIDGET TITLE:** Aerohive WAP-User login success
  - **CHART TYPE:** Donut
  - **AXIS LABELS [X-AXIS]:** SSID
  - **LEGEND [SERIES]:** Source MAC Address

![Figure 38](image1.png)

- **Aerohive WAP-Rogue AP detected**
  - **WIDGET TITLE:** Aerohive WAP-Rogue AP detected
  - **CHART TYPE:** Donut
  - **AXIS LABELS [X-AXIS]:** Rogue SSID
  - **LEGEND [SERIES]:** Detector AP

![Figure 39](image2.png)