EventTracker

Actionable Security Intelligence

# Integrate Aerohive Wireless Access Point

Publication Date: November 15, 2016

## 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.

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

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

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

*EventTracker 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 EventTracker, 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.*

# 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**.

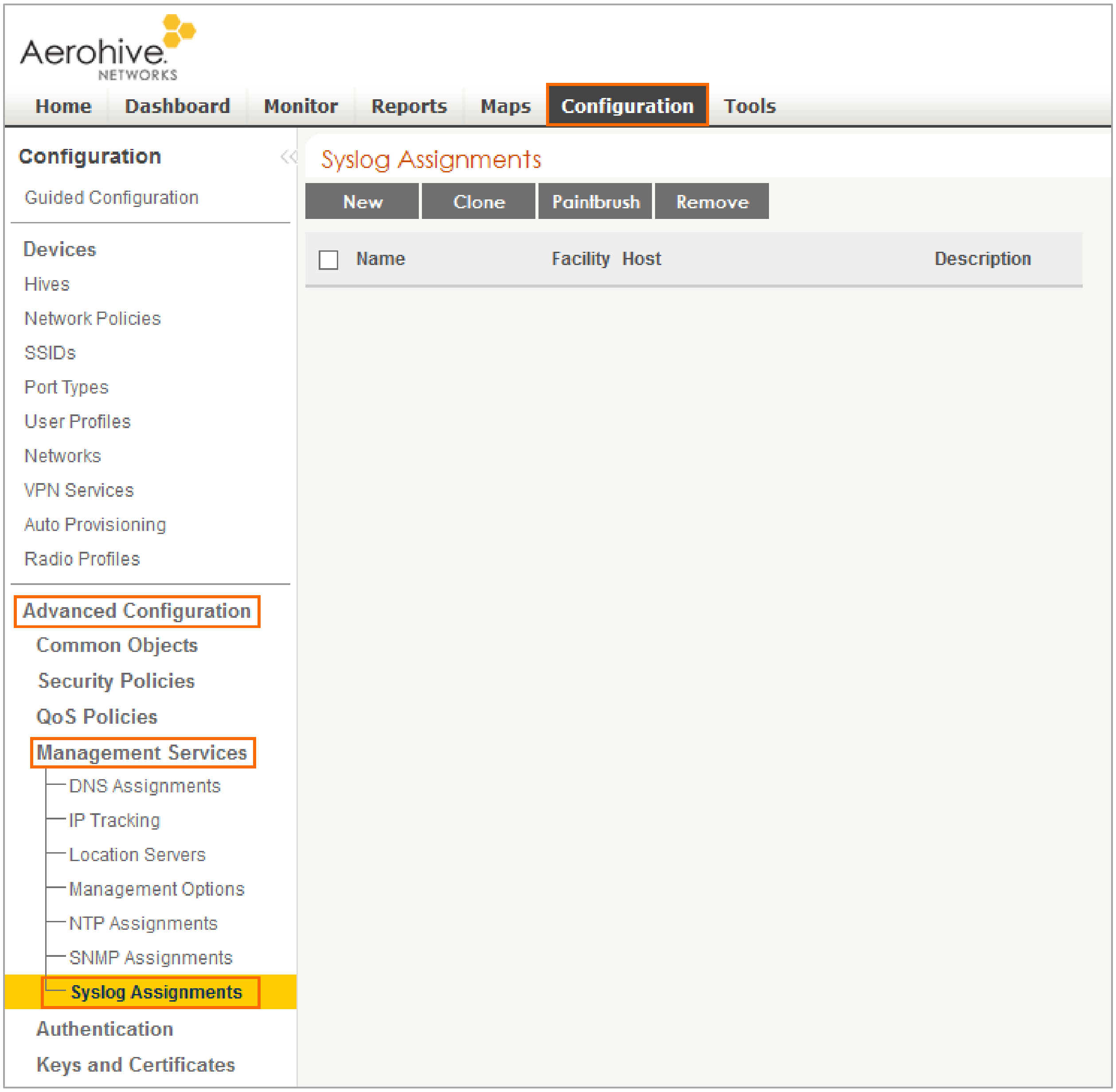
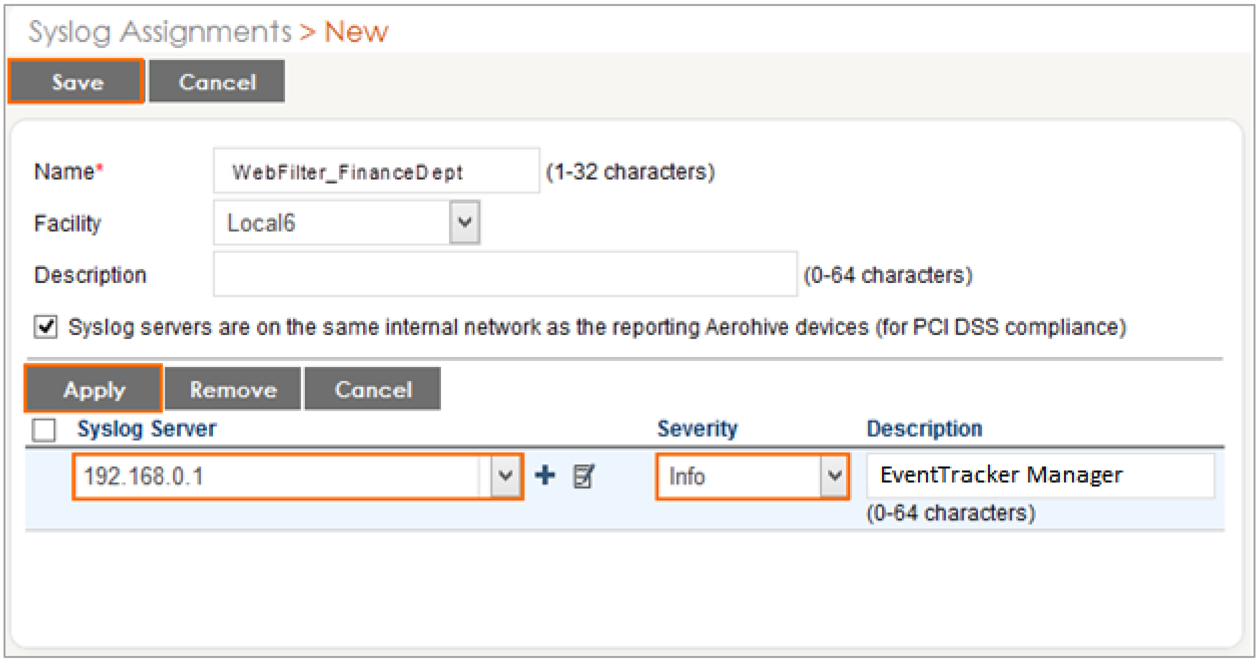


Figure 1

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**.



Syslog Assignments > New

Name* WebFilter_FinanceDept (1-32 characters)

Facility Local6

Description (0-64 characters)

☑ Syslog servers are on the same internal network as the reporting Aerohive devices (for PCI DSS compliance)

| □ Syslog Server | Severity | Description |
|---|---|---|
| 192.168.0.1 | Info | EventTracker Manager<br>(0-64 characters) |

Figure 2

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

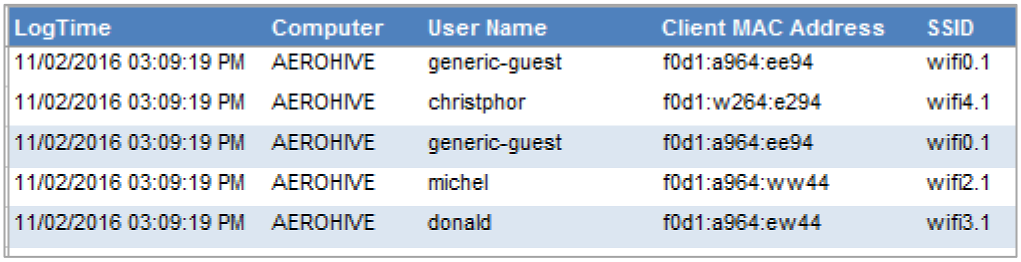
- **Aerohive WAP: User login success**
  This category provides information related to user login successfully into Aerohive WAP.
- **Aerohive WAP: Client activity**
  This category provides information related to client activity in the Aerohive WAP.
- **Aerohive WAP: DHCP activity**
  This category 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.

## Alerts

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

## Flex Reports

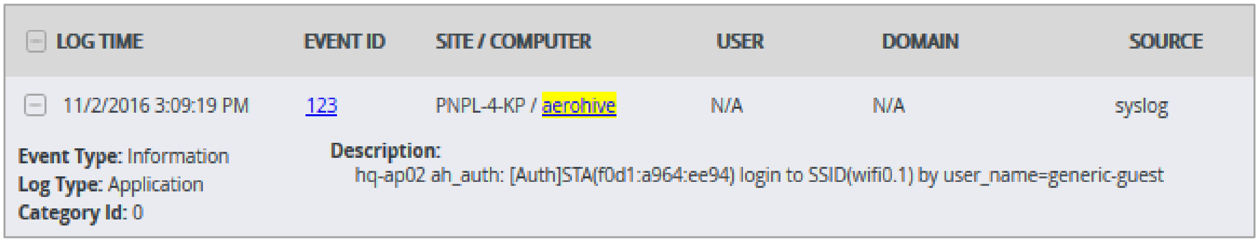
- **Aerohive WAP-User login success**
  This report provides the information related to user login successfully into Aerohive WAP.
  **Sample Report:**



| LogTime | Computer | User Name | Client MAC Address | SSID |
|---|---|---|---|---|
| 11/02/2016 03:09:19 PM | AEROHIVE | generic-guest | f0d1:a964:ee94 | wifi0.1 |
| 11/02/2016 03:09:19 PM | AEROHIVE | christphor | f0d1:w264:e294 | wifi4.1 |
| 11/02/2016 03:09:19 PM | AEROHIVE | generic-guest | f0d1:a964:ee94 | wifi0.1 |
| 11/02/2016 03:09:19 PM | AEROHIVE | michel | f0d1:a964:ww44 | wifi2.1 |
| 11/02/2016 03:09:19 PM | AEROHIVE | donald | f0d1:a964:ew44 | wifi3.1 |

Figure 3

**Logs Considered:**



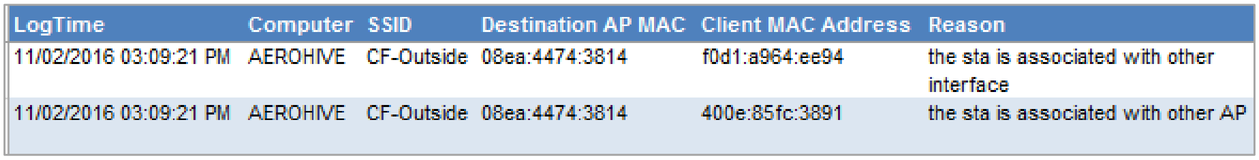
| LOG TIME | EVENT ID | SITE / COMPUTER | USER | DOMAIN | SOURCE |
|---|---|---|---|---|---|
| 11/2/2016 3:09:19 PM | 123 | PNPL-4-KP / aerohive | N/A | N/A | syslog |

**Event Type:** Information
**Log Type:** Application
**Category Id:** 0

**Description:**
hq-ap02 ah_auth: [Auth]STA(f0d1:a964:ee94) login to SSID(wifi0.1) by user_name=generic-guest

Figure 4

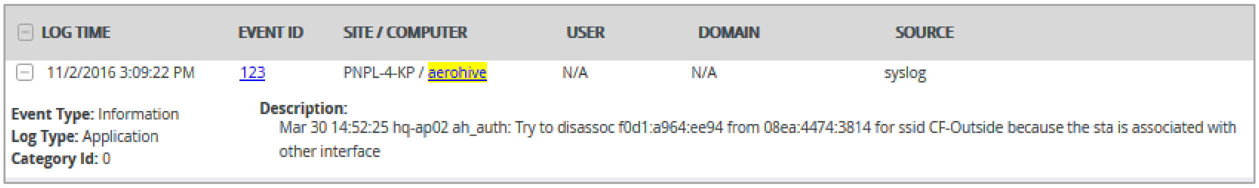
- **Aerohive WAP-Client activity**
  This report provides the information related to client activities for which they are associated in Aerohive WAP.
  **Sample Report:**



| LogTime | Computer | SSID | Destination AP MAC | Client MAC Address | Reason |
|---|---|---|---|---|---|
| 11/02/2016 03:09:21 PM | AEROHIVE | CF-Outside | 08ea:4474:3814 | f0d1:a964:ee94 | the sta is associated with other interface |
| 11/02/2016 03:09:21 PM | AEROHIVE | CF-Outside | 08ea:4474:3814 | 400e:85fc:3891 | the sta is associated with other AP |

Figure 5

**Logs Considered:**



| LOG TIME | EVENT ID | SITE / COMPUTER | USER | DOMAIN | SOURCE |
|---|---|---|---|---|---|
| 11/2/2016 3:09:22 PM | 123 | PNPL-4-KP / aerohive | N/A | N/A | syslog |

**Event Type:** Information
**Log Type:** Application
**Category Id:** 0

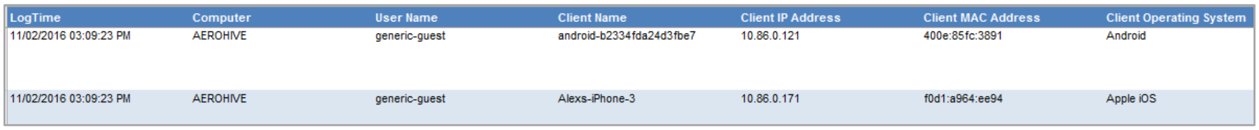
**Description:**
Mar 30 14:52:25 hq-ap02 ah_auth: Try to disassoc f0d1:a964:ee94 from 08ea:4474:3814 for ssid CF-Outside because the sta is associated with other interface

Figure 6

- **Aerohive WAP: DHCP activity**

This report provides the information related to DHCP activities into Aerohive WAP.

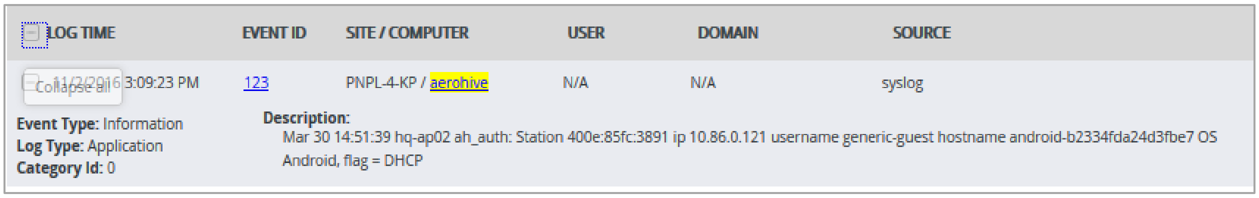
**Sample Report:**



| LogTime | Computer | User Name | Client Name | Client IP Address | Client MAC Address | Client Operating System |
|---|---|---|---|---|---|---|
| 11/02/2016 03:09:23 PM | AEROHIVE | generic-guest | android-b2334fda24d3fbe7 | 10.86.0.121 | 400e:85fc:3891 | Android |
| 11/02/2016 03:09:23 PM | AEROHIVE | generic-guest | Alexs-iPhone-3 | 10.86.0.171 | f0d1:a964:ee94 | Apple iOS |

Figure 7

**Logs Considered:**



| LOG TIME | EVENT ID | SITE / COMPUTER | USER | DOMAIN | SOURCE |
|---|---|---|---|---|---|
| 11/2/2016 3:09:23 PM | 123 | PNPL-4-KP / aerohive | N/A | N/A | syslog |

**Event Type:** Information
**Log Type:** Application
**Category Id:** 0

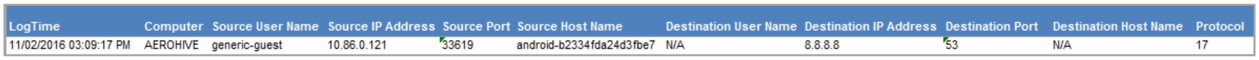
**Description:**
Mar 30 14:51:39 hq-ap02 ah_auth: Station 400e:85fc:3891 ip 10.86.0.121 username generic-guest hostname android-b2334fda24d3fbe7 OS Android, flag = DHCP

Figure 8

- **Aerohive WAP: IP traffic details**

This report provides the information related to IP traffic details into Aerohive WAP.

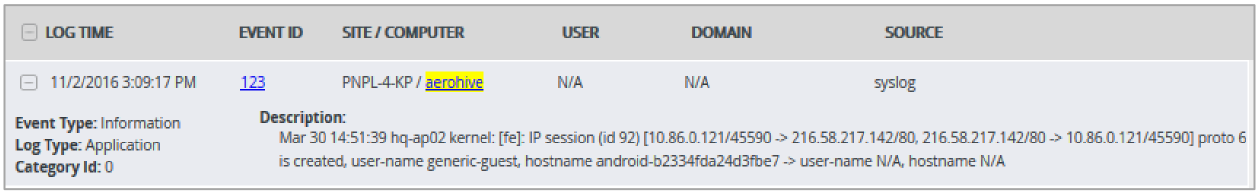
**Sample Report:**



| LogTime | Computer | Source User Name | Source IP Address | Source Port | Source Host Name | Destination User Name | Destination IP Address | Destination Port | Destination Host Name | Protocol |
|---|---|---|---|---|---|---|---|---|---|---|
| 11/02/2016 03:09:17 PM | AEROHIVE | generic-guest | 10.86.0.121 | 33619 | android-b2334fda24d3fbe7 | N/A | 8.8.8.8 | 53 | N/A | 17 |

Figure 9

**Logs Considered:**



| LOG TIME | EVENT ID | SITE / COMPUTER | USER | DOMAIN | SOURCE |
|---|---|---|---|---|---|
| 11/2/2016 3:09:17 PM | 123 | PNPL-4-KP / aerohive | N/A | N/A | syslog |

**Event Type:** Information
**Log Type:** Application
**Category Id:** 0

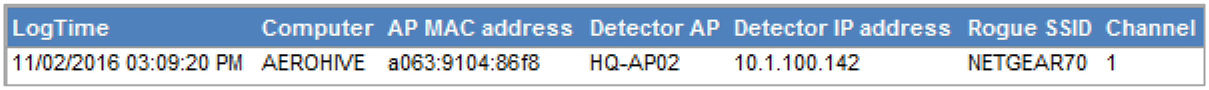
**Description:**
Mar 30 14:51:39 hq-ap02 kernel: [fe]: IP session (id 92) [10.86.0.121/45590 -> 216.58.217.142/80, 216.58.217.142/80 -> 10.86.0.121/45590] proto 6 is created, user-name generic-guest, hostname android-b2334fda24d3fbe7 -> user-name N/A, hostname N/A

Figure 10

- **Aerohive WAP: Rogue AP detected**

  This report provides the information related to a rogue AP that has been detected into Aerohive WAP.

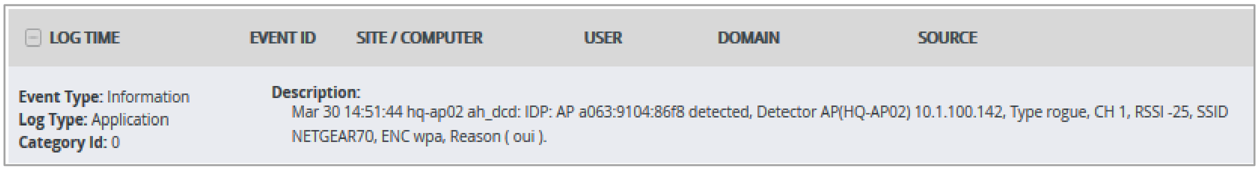
  **Sample Report:**



| LogTime | Computer | AP MAC address | Detector AP | Detector IP address | Rogue SSID | Channel |
|---|---|---|---|---|---|---|
| 11/02/2016 03:09:20 PM | AEROHIVE | a063:9104:86f8 | HQ-AP02 | 10.1.100.142 | NETGEAR70 | 1 |

Figure 11

**Logs Considered:**



| LOG TIME | EVENT ID | SITE / COMPUTER | USER | DOMAIN | SOURCE |
|---|---|---|---|---|---|

**Event Type:** Information
**Log Type:** Application
**Category Id:** 0

**Description:**
Mar 30 14:51:44 hq-ap02 ah_dcd: IDP: AP a063:9104:86f8 detected, Detector AP(HQ-AP02) 10.1.100.142, Type rogue, CH 1, RSSI -25, SSID NETGEAR70, ENC wpa, Reason ( oui ).

Figure 12

# 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**.

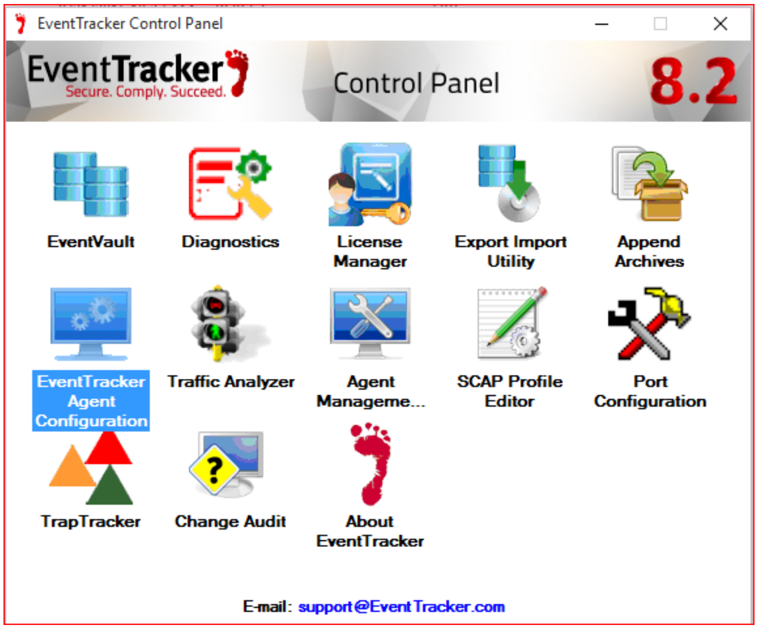
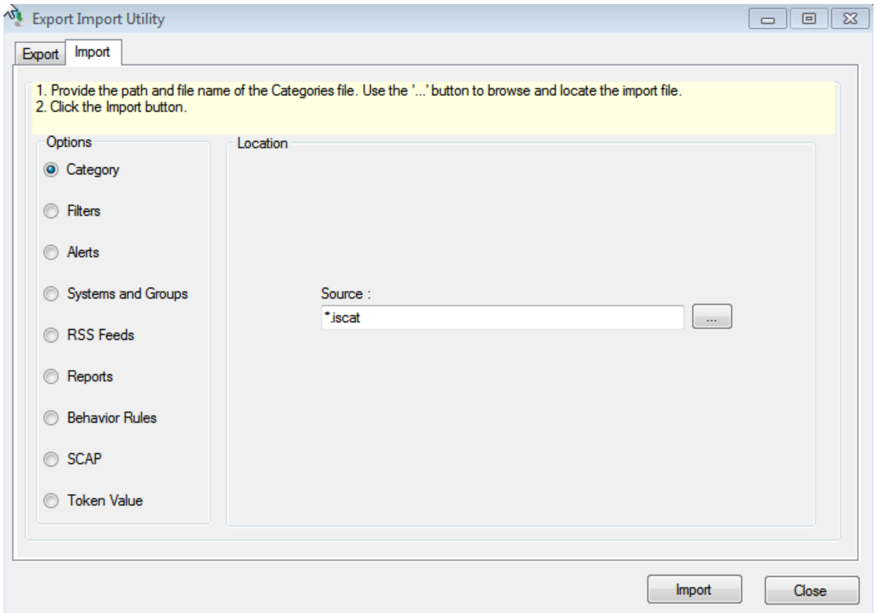


Figure 13

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.

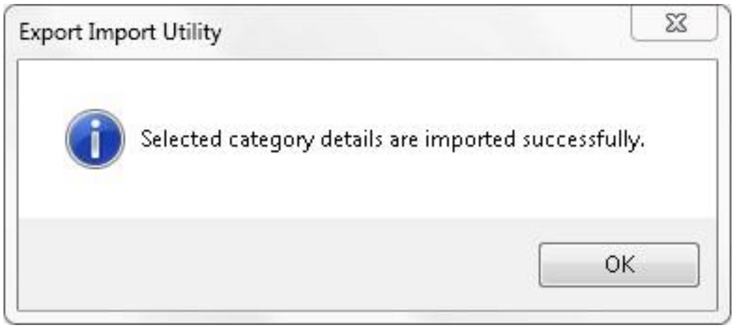


1. Provide the path and file name of the Categories file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Source : *.iscat

Figure 14

3. To import categories, click the **Import** button.
   EventTracker displays success message.



Export Import Utility

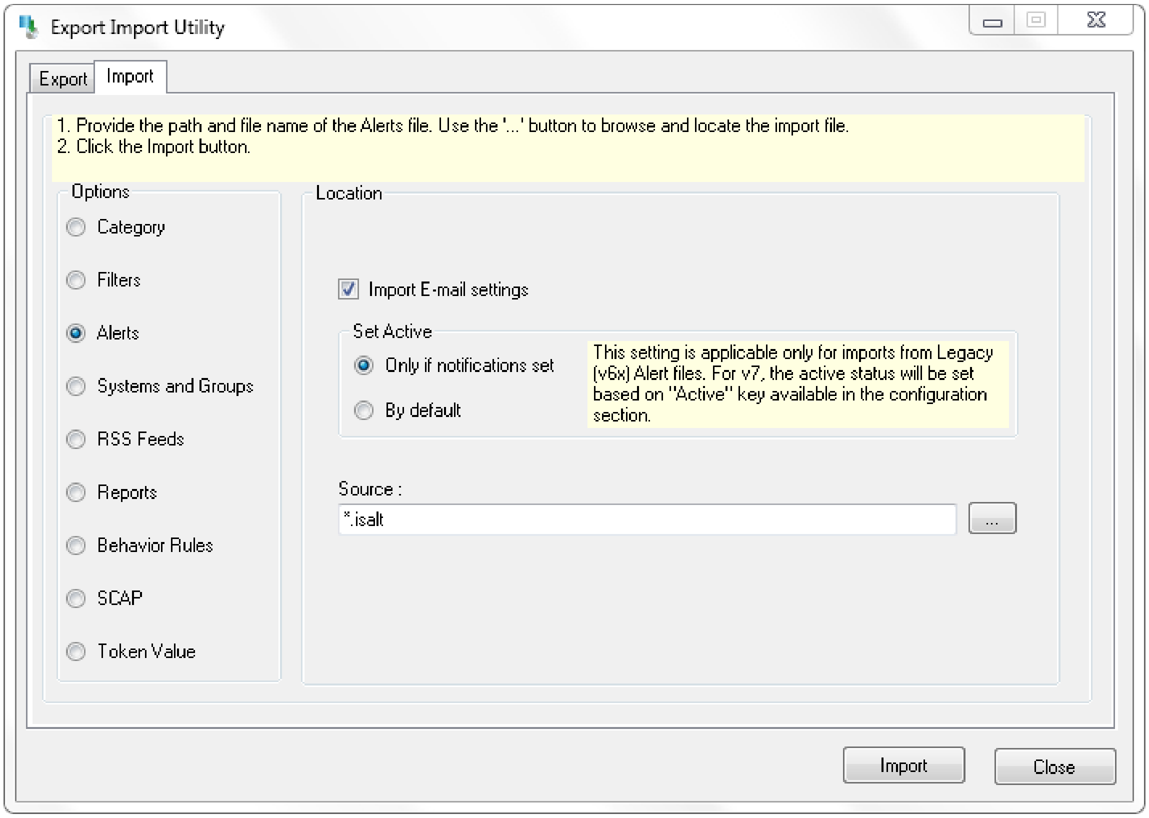
Selected category details are imported successfully.

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

1. Provide the path and file name of the Alerts file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Options

○ Category
○ Filters
● Alerts
○ Systems and Groups
○ RSS Feeds
○ Reports
○ Behavior Rules
○ SCAP
○ Token Value

Location

☑ Import E-mail settings

Set Active

● Only if notifications set
○ By default

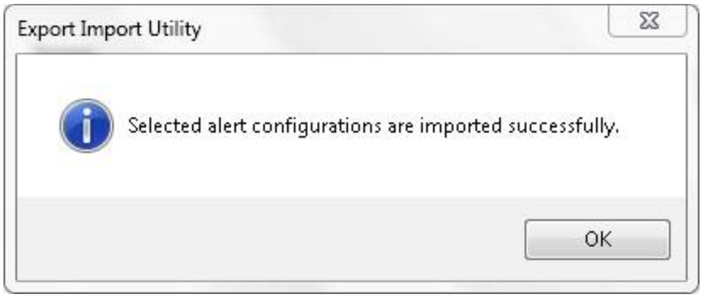
This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.

Source : *.isalt

Figure 16

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

   EventTracker displays success message.



Export Import Utility

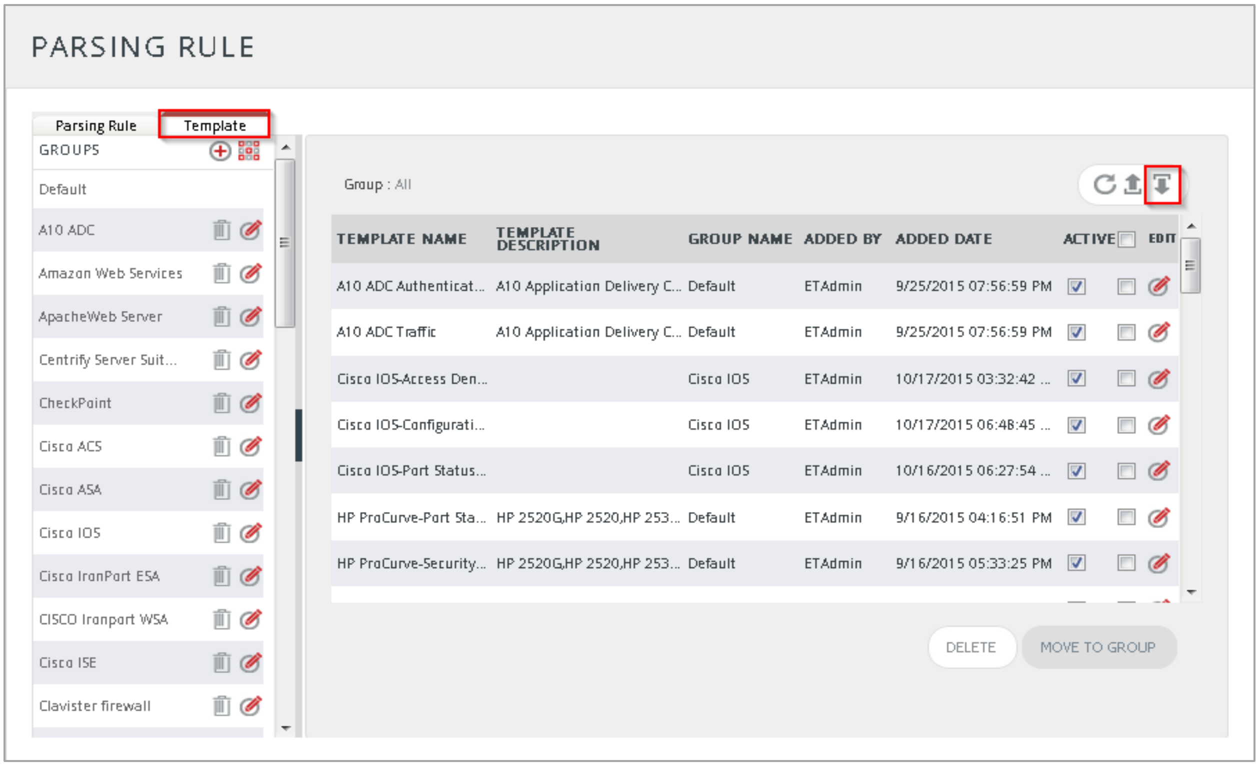
Selected alert configurations are imported successfully.

Figure 17

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.

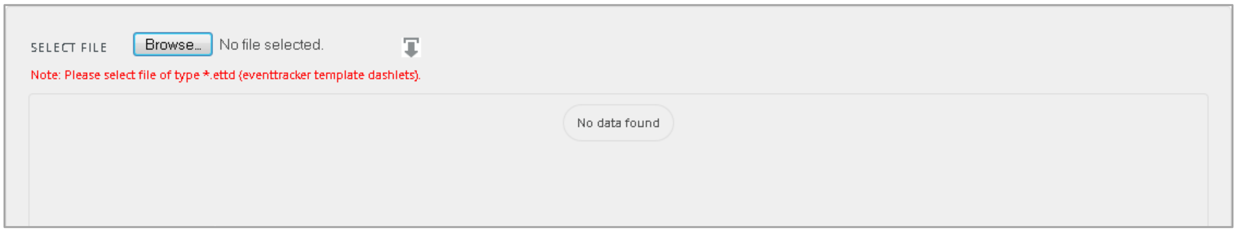


PARSING RULE

| TEMPLATE NAME | TEMPLATE DESCRIPTION | GROUP NAME | ADDED BY | ADDED DATE | ACTIVE □ | EDIT |
|---|---|---|---|---|---|---|
| A10 ADC Authenticat... | A10 Application Delivery C... | Default | ETAdmin | 9/25/2015 07:56:59 PM | ☑ | □ |
| A10 ADC Traffic | A10 Application Delivery C... | Default | ETAdmin | 9/25/2015 07:56:59 PM | ☑ | □ |
| Cisco IOS-Access Den... | | Cisco IOS | ETAdmin | 10/17/2015 03:32:42 ... | ☑ | □ |
| Cisco IOS-Configurati... | | Cisco IOS | ETAdmin | 10/17/2015 06:48:45 ... | ☑ | □ |
| Cisco IOS-Port Status... | | Cisco IOS | ETAdmin | 10/16/2015 06:27:54 ... | ☑ | □ |
| HP ProCurve-Port Sta... | HP 2520G,HP 2520,HP 253... | Default | ETAdmin | 9/16/2015 04:16:51 PM | ☑ | □ |
| HP ProCurve-Security... | HP 2520G,HP 2520,HP 253... | Default | ETAdmin | 9/16/2015 05:33:25 PM | ☑ | □ |

Figure 18

3. Click on **Browse** button.



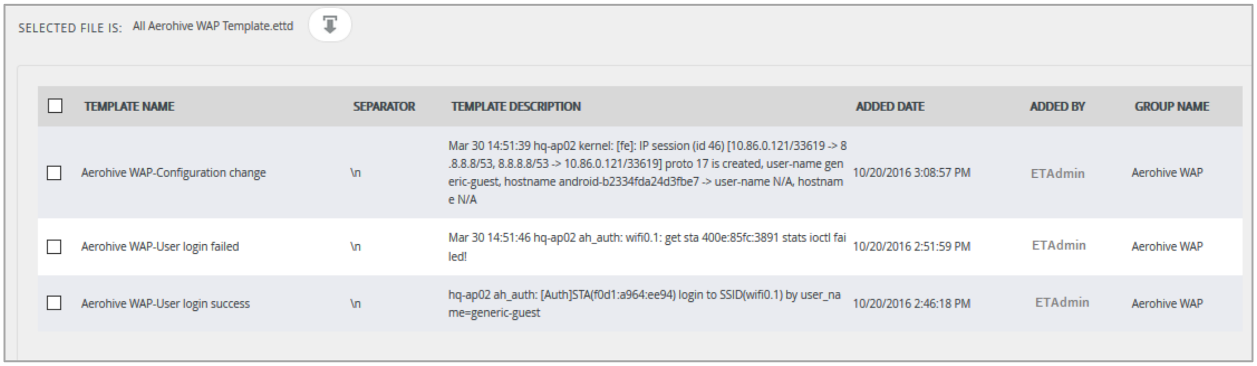
SELECT FILE No file selected.

Note: Please select file of type *.ettd (eventtracker template dashlets).

No data found

Figure 19

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

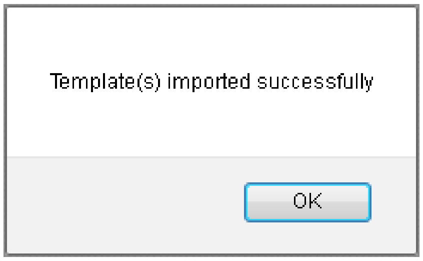


SELECTED FILE IS: All Aerohive WAP Template.ettd

| □ | TEMPLATE NAME | SEPARATOR | TEMPLATE DESCRIPTION | ADDED DATE | ADDED BY | GROUP NAME |
|---|---|---|---|---|---|---|
| □ | Aerohive WAP-Configuration change | \n | Mar 30 14:51:39 hq-ap02 kernel: [fe]: IP session (id 46) [10.86.0.121/33619 -> 8.8.8.8/53, 8.8.8.8/53 -> 10.86.0.121/33619] proto 17 is created, user-name generic-guest, hostname android-b2334fda24d3fbe7 -> user-name N/A, hostname N/A | 10/20/2016 3:08:57 PM | ETAdmin | Aerohive WAP |
| □ | Aerohive WAP-User login failed | \n | Mar 30 14:51:46 hq-ap02 ah_auth: wifi0.1: get sta 400e:85fc:3891 stats ioctl failed! | 10/20/2016 2:51:59 PM | ETAdmin | Aerohive WAP |
| □ | Aerohive WAP-User login success | \n | hq-ap02 ah_auth: [Auth]STA(f0d1:a964:ee94) login to SSID(wifi0.1) by user_name=generic-guest | 10/20/2016 2:46:18 PM | ETAdmin | Aerohive WAP |

Figure 20

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



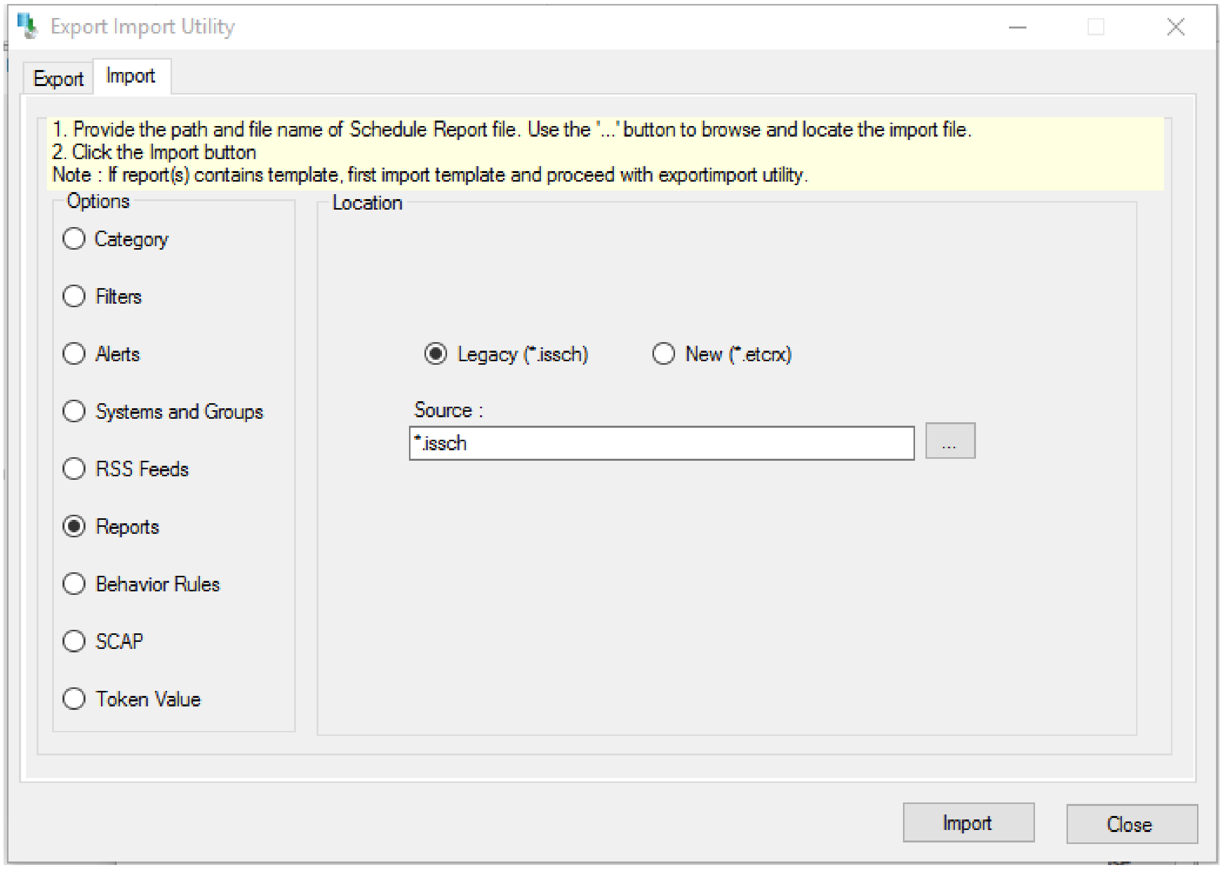
Template(s) imported successfully

Figure 21

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.

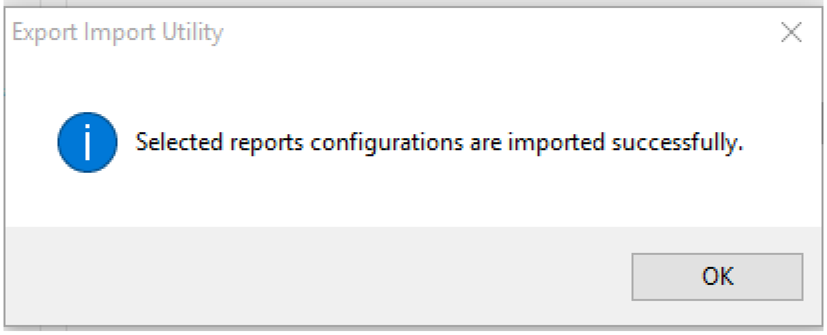


1. Provide the path and file name of Schedule Report file. Use the '...' button to browse and locate the import file.
2. Click the Import button
Note : If report(s) contains template, first import template and proceed with exportimport utility.

Source : *.issch

Figure 22

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



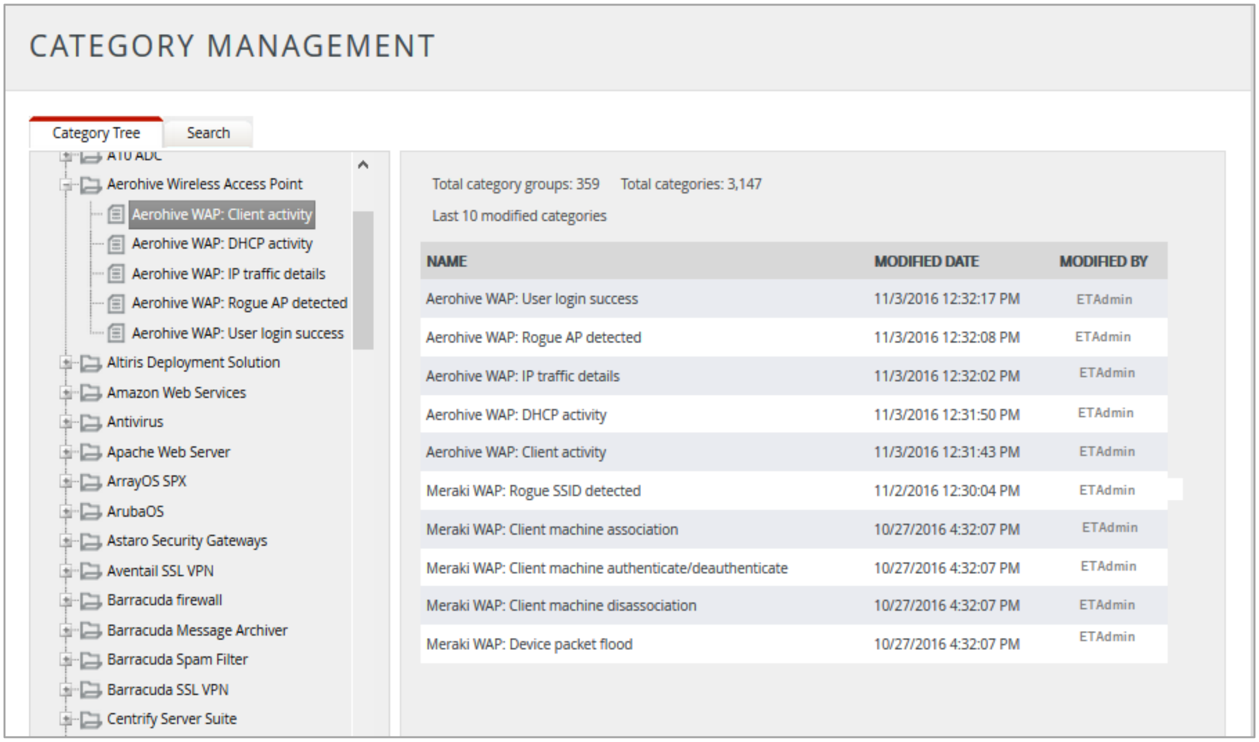
Selected reports configurations are imported successfully.

Figure 23

# 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

- A10 ADC
- Aerohive Wireless Access Point
  - Aerohive WAP: Client activity
  - Aerohive WAP: DHCP activity
  - Aerohive WAP: IP traffic details
  - Aerohive WAP: Rogue AP detected
  - Aerohive WAP: User login success
- Altiris Deployment Solution
- Amazon Web Services
- Antivirus
- Apache Web Server
- ArrayOS SPX
- ArubaOS
- Astaro Security Gateways
- Aventail SSL VPN
- Barracuda firewall
- Barracuda Message Archiver
- Barracuda Spam Filter
- Barracuda SSL VPN
- Centrify Server Suite

Total category groups: 359 Total categories: 3,147

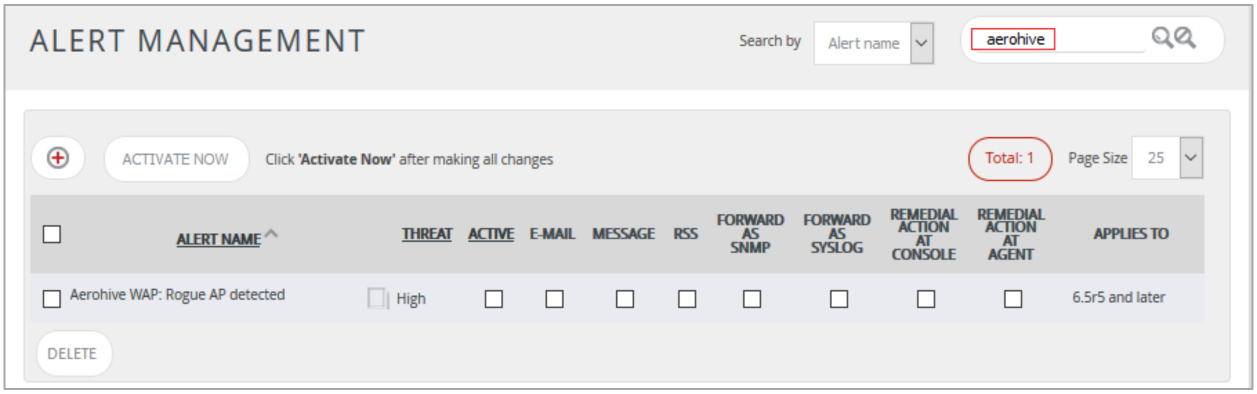
Last 10 modified categories

| NAME | MODIFIED DATE | MODIFIED BY |
|---|---|---|
| Aerohive WAP: User login success | 11/3/2016 12:32:17 PM | ETAdmin |
| Aerohive WAP: Rogue AP detected | 11/3/2016 12:32:08 PM | ETAdmin |
| Aerohive WAP: IP traffic details | 11/3/2016 12:32:02 PM | ETAdmin |
| Aerohive WAP: DHCP activity | 11/3/2016 12:31:50 PM | ETAdmin |
| Aerohive WAP: Client activity | 11/3/2016 12:31:43 PM | ETAdmin |
| Meraki WAP: Rogue SSID detected | 11/2/2016 12:30:04 PM | ETAdmin |
| Meraki WAP: Client machine association | 10/27/2016 4:32:07 PM | ETAdmin |
| Meraki WAP: Client machine authenticate/deauthenticate | 10/27/2016 4:32:07 PM | ETAdmin |
| Meraki WAP: Client machine disassociation | 10/27/2016 4:32:07 PM | ETAdmin |
| Meraki WAP: Device packet flood | 10/27/2016 4:32:07 PM | ETAdmin |

Figure 24

## 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.



ALERT MANAGEMENT

Search by Alert name aerohive

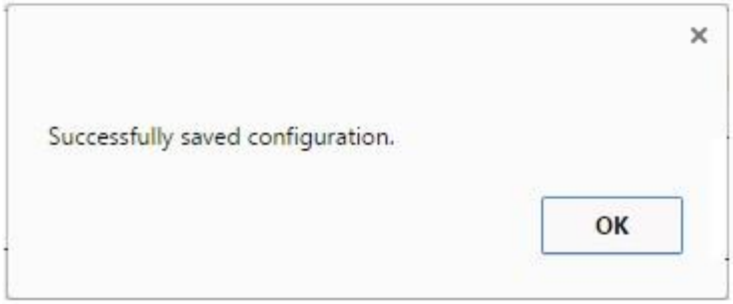
Click **'Activate Now'** after making all changes

Total: 1 Page Size 25

| □ | ALERT NAME | THREAT | ACTIVE | E-MAIL | MESSAGE | RSS | FORWARD AS SNMP | FORWARD AS SYSLOG | REMEDIAL ACTION AT CONSOLE | REMEDIAL ACTION AT AGENT | APPLIES TO |
|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | Aerohive WAP: Rogue AP detected | High | □ | □ | □ | □ | □ | □ | □ | □ | 6.5r5 and later |

Figure 25

3. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.



Successfully saved configuration.

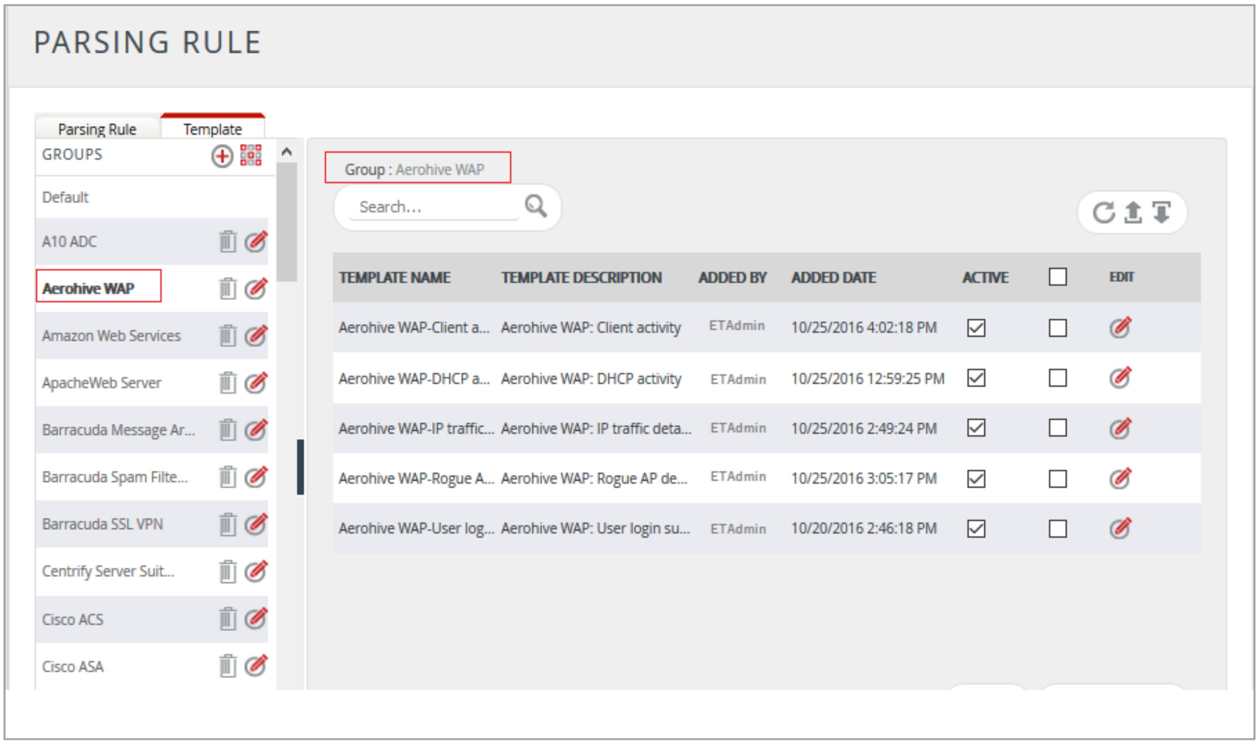
Figure 26

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**.

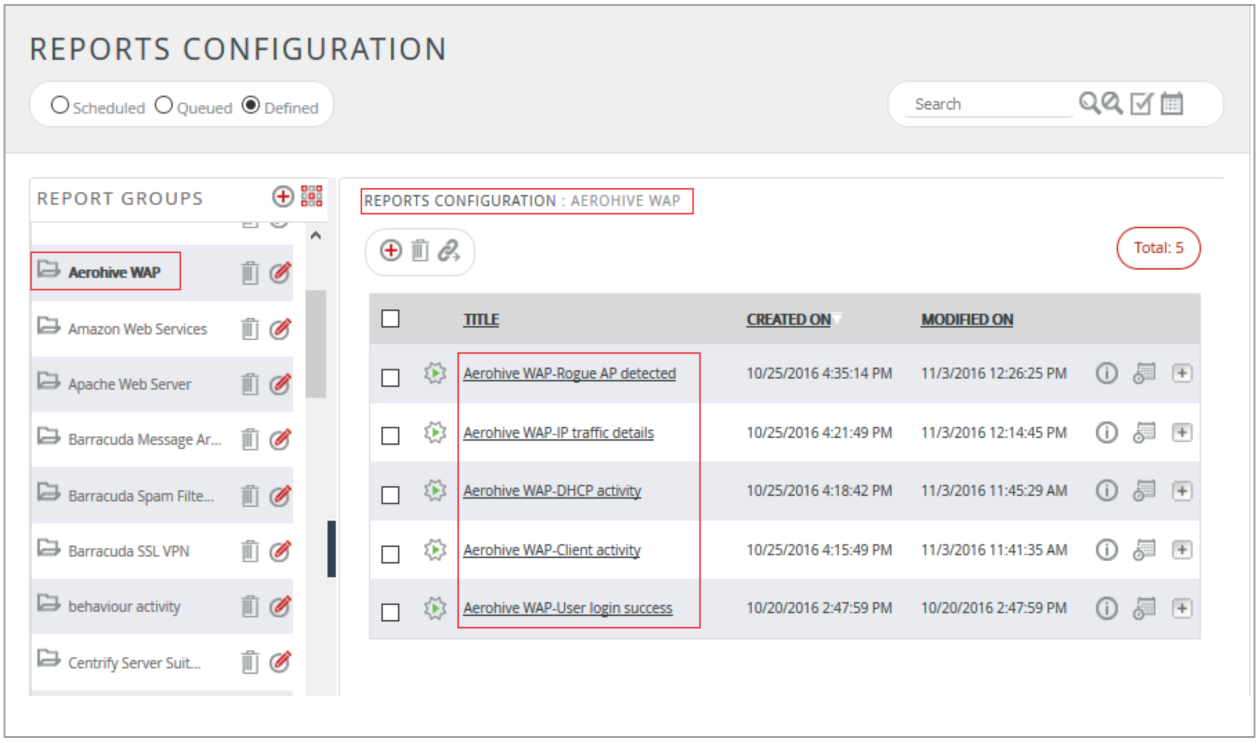


| TEMPLATE NAME | TEMPLATE DESCRIPTION | ADDED BY | ADDED DATE | ACTIVE | □ | EDIT |
|---|---|---|---|---|---|---|
| Aerohive WAP-Client a... | Aerohive WAP: Client activity | ETAdmin | 10/25/2016 4:02:18 PM | ☑ | □ | |
| Aerohive WAP-DHCP a... | Aerohive WAP: DHCP activity | ETAdmin | 10/25/2016 12:59:25 PM | ☑ | □ | |
| Aerohive WAP-IP traffic... | Aerohive WAP: IP traffic deta... | ETAdmin | 10/25/2016 2:49:24 PM | ☑ | □ | |
| Aerohive WAP-Rogue A... | Aerohive WAP: Rogue AP de... | ETAdmin | 10/25/2016 3:05:17 PM | ☑ | □ | |
| Aerohive WAP-User log... | Aerohive WAP: User login su... | ETAdmin | 10/20/2016 2:46:18 PM | ☑ | □ | |

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.**



REPORTS CONFIGURATION

○ Scheduled ○ Queued ● Defined

Search

REPORT GROUPS

- Aerohive WAP
- Amazon Web Services
- Apache Web Server
- Barracuda Message Ar...
- Barracuda Spam Filte...
- Barracuda SSL VPN
- behaviour activity
- Centrify Server Suit...

REPORTS CONFIGURATION : AEROHIVE WAP

Total: 5

| □ | | TITLE | CREATED ON | MODIFIED ON |
|---|---|---|---|---|
| □ | | Aerohive WAP-Rogue AP detected | 10/25/2016 4:35:14 PM | 11/3/2016 12:26:25 PM |
| □ | | Aerohive WAP-IP traffic details | 10/25/2016 4:21:49 PM | 11/3/2016 12:14:45 PM |
| □ | | Aerohive WAP-DHCP activity | 10/25/2016 4:18:42 PM | 11/3/2016 11:45:29 AM |
| □ | | Aerohive WAP-Client activity | 10/25/2016 4:15:49 PM | 11/3/2016 11:41:35 AM |
| □ | | Aerohive WAP-User login success | 10/20/2016 2:47:59 PM | 10/20/2016 2:47:59 PM |

Figure 28

# 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.

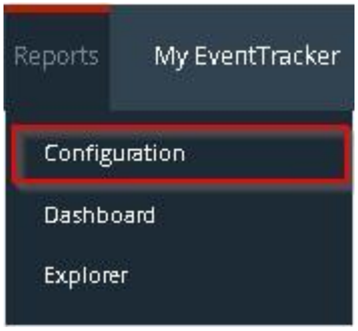
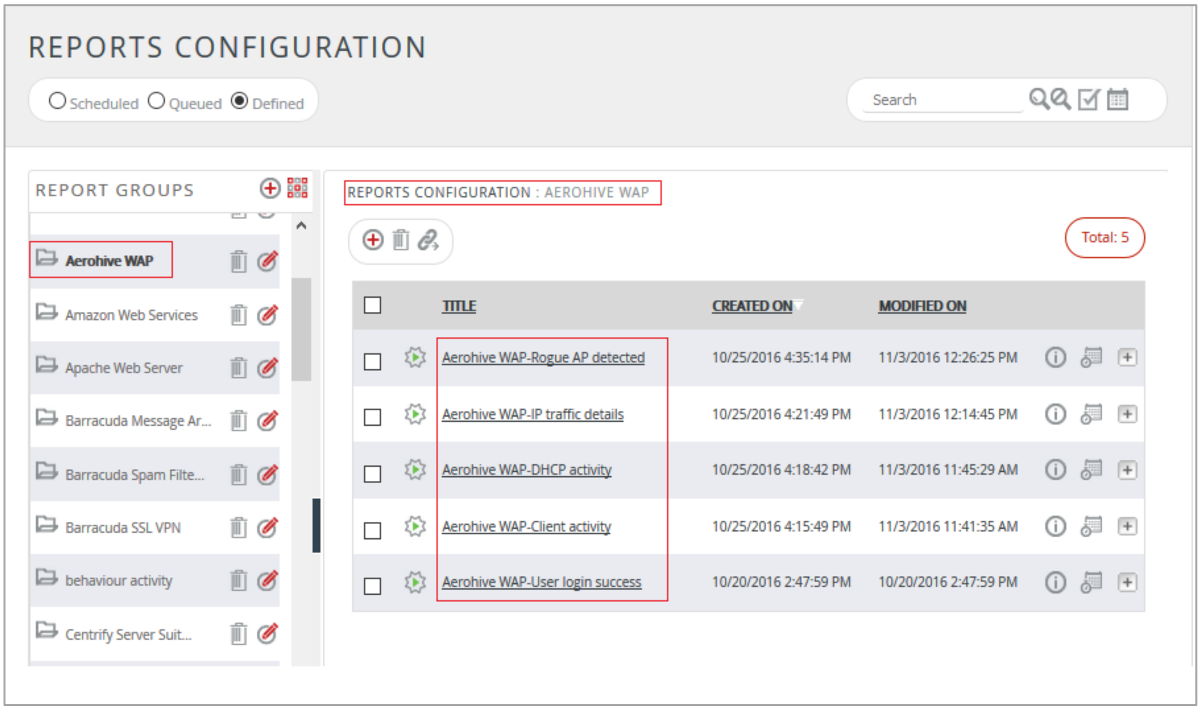


Figure 29

2. Navigate to **Reports>Configuration**.

3. Select **Aerohive** in report groups. Check **Defined** dialog box.



REPORTS CONFIGURATION

○ Scheduled ○ Queued ● Defined

Search

REPORT GROUPS

- Aerohive WAP
- Amazon Web Services
- Apache Web Server
- Barracuda Message Ar...
- Barracuda Spam Filte...
- Barracuda SSL VPN
- behaviour activity
- Centrify Server Suit...

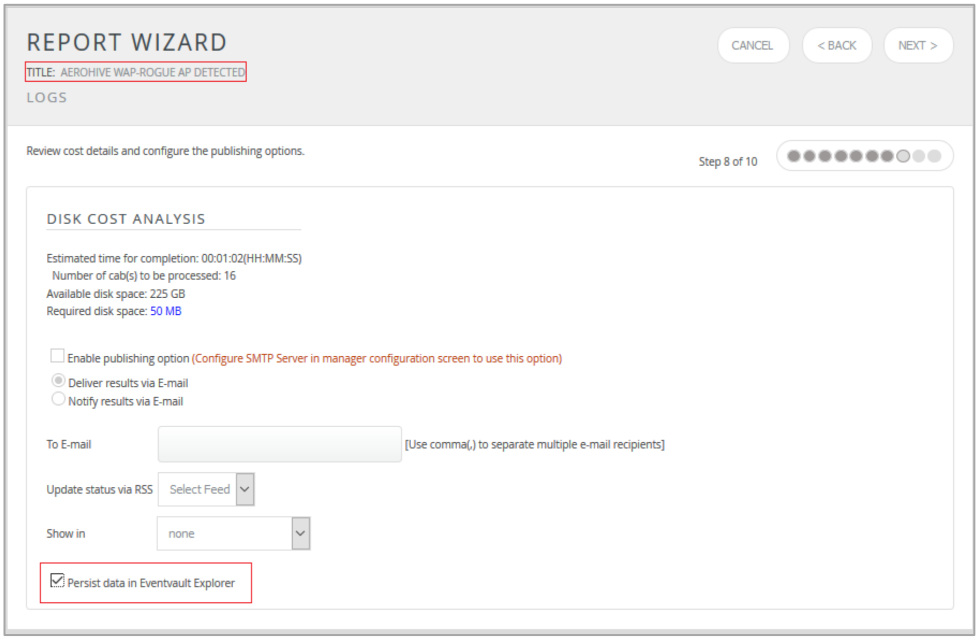
REPORTS CONFIGURATION : AEROHIVE WAP

Total: 5

| □ | | TITLE | CREATED ON | MODIFIED ON |
|---|---|---|---|---|
| □ | | Aerohive WAP-Rogue AP detected | 10/25/2016 4:35:14 PM | 11/3/2016 12:26:25 PM |
| □ | | Aerohive WAP-IP traffic details | 10/25/2016 4:21:49 PM | 11/3/2016 12:14:45 PM |
| □ | | Aerohive WAP-DHCP activity | 10/25/2016 4:18:42 PM | 11/3/2016 11:45:29 AM |
| □ | | Aerohive WAP-Client activity | 10/25/2016 4:15:49 PM | 11/3/2016 11:41:35 AM |
| □ | | Aerohive WAP-User login success | 10/20/2016 2:47:59 PM | 10/20/2016 2:47:59 PM |

Figure 30

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.



REPORT WIZARD

CANCEL < BACK NEXT >

TITLE: AEROHIVE WAP-ROGUE AP DETECTED

LOGS

Review cost details and configure the publishing options.

Step 8 of 10

DISK COST ANALYSIS

Estimated time for completion: 00:01:02(HH:MM:SS)
Number of cab(s) to be processed: 16
Available disk space: 225 GB
Required disk space: 50 MB

□ Enable publishing option (Configure SMTP Server in manager configuration screen to use this option)

● Deliver results via E-mail
○ Notify results via E-mail

To E-mail [Use comma(,) to separate multiple e-mail recipients]

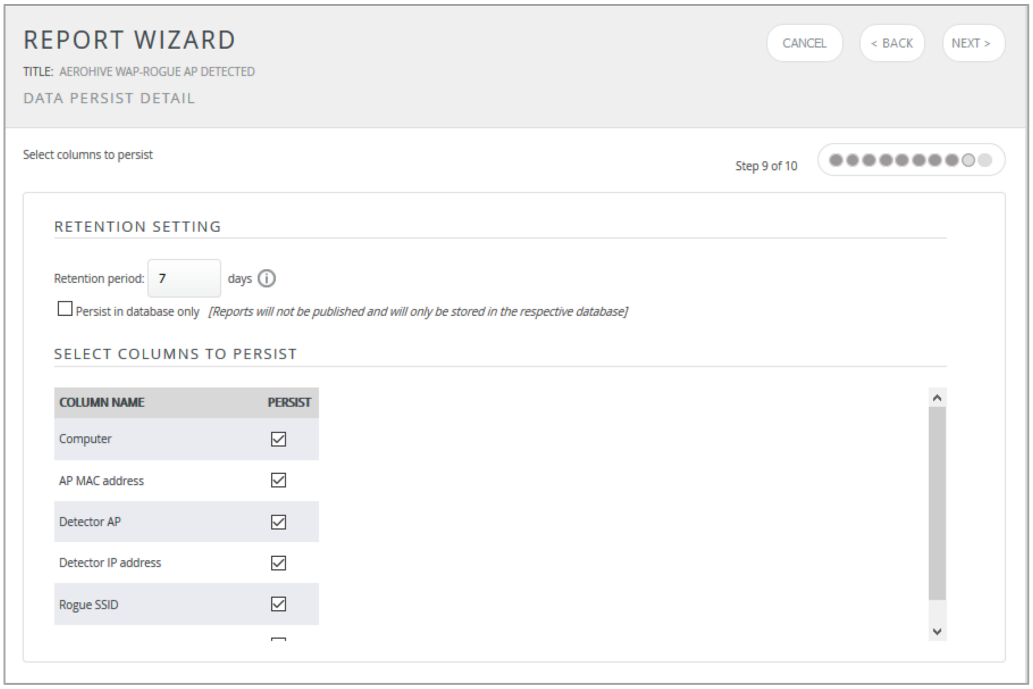
Update status via RSS: Select Feed

Show in: none

☑ Persist data in Eventvault Explorer

Figure 31

7. In next page, check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.



REPORT WIZARD

TITLE: AEROHIVE WAP-ROGUE AP DETECTED

DATA PERSIST DETAIL

Select columns to persist

Step 9 of 10

RETENTION SETTING

Retention period: 7 days

□ Persist in database only *[Reports will not be published and will only be stored in the respective database]*

SELECT COLUMNS TO PERSIST

| COLUMN NAME | PERSIST |
|---|---|
| Computer | ☑ |
| AP MAC address | ☑ |
| Detector AP | ☑ |
| Detector IP address | ☑ |
| Rogue SSID | ☑ |

Figure 32

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.

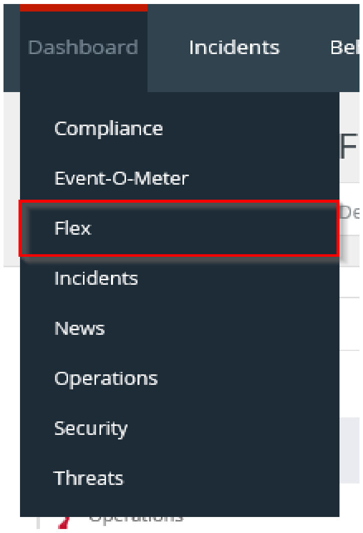
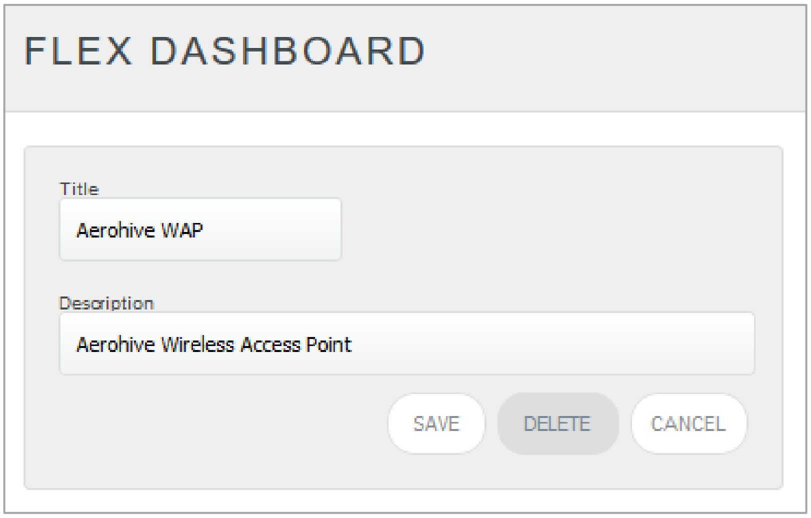


Figure 33

2. Navigate to **Dashboard>Flex**.
   Flex Dashboard pane is shown.



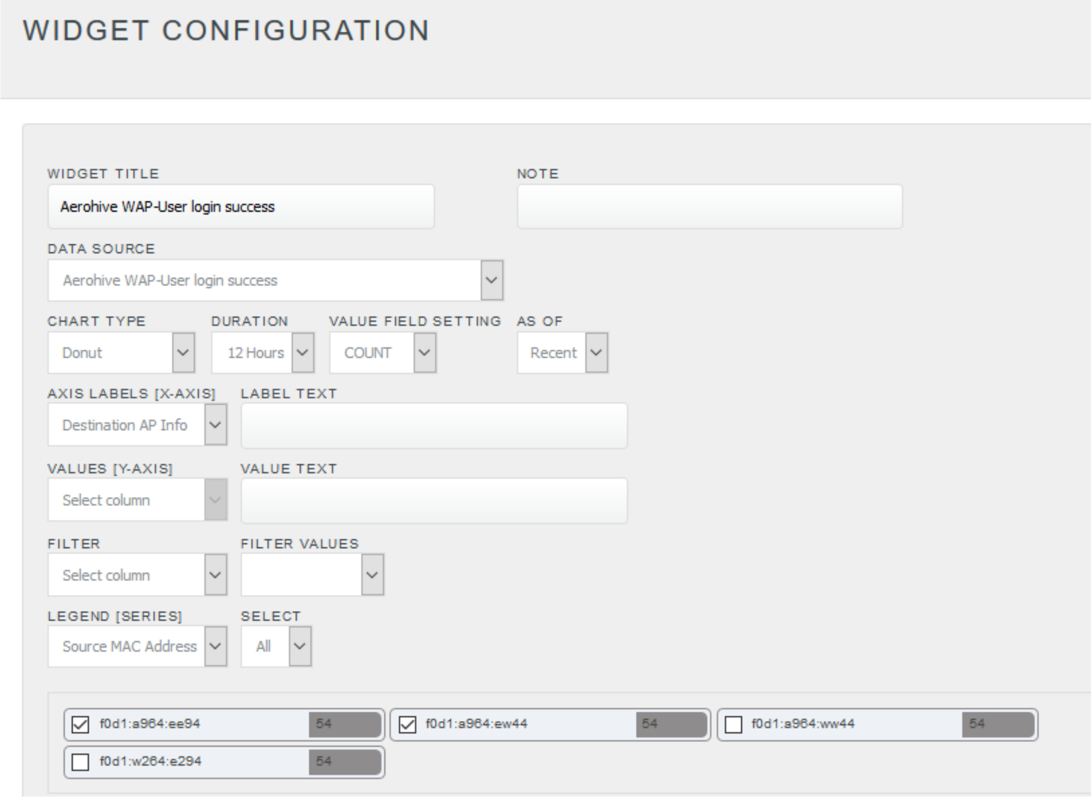
FLEX DASHBOARD

Title: Aerohive WAP

Description: Aerohive Wireless Access Point

Figure 34

3. Fill suitable title and description and click **Save** button.
4. Click ⚙ to configure a new flex dashlet. Widget configuration pane is shown.



WIDGET CONFIGURATION

WIDGET TITLE: Aerohive WAP-User login success

NOTE:

DATA SOURCE: Aerohive WAP-User login success

CHART TYPE: Donut

DURATION: 12 Hours

VALUE FIELD SETTING: COUNT

AS OF: Recent

AXIS LABELS [X-AXIS]: Destination AP Info

LABEL TEXT:

VALUES [Y-AXIS]: Select column

VALUE TEXT:

FILTER: Select column

FILTER VALUES:

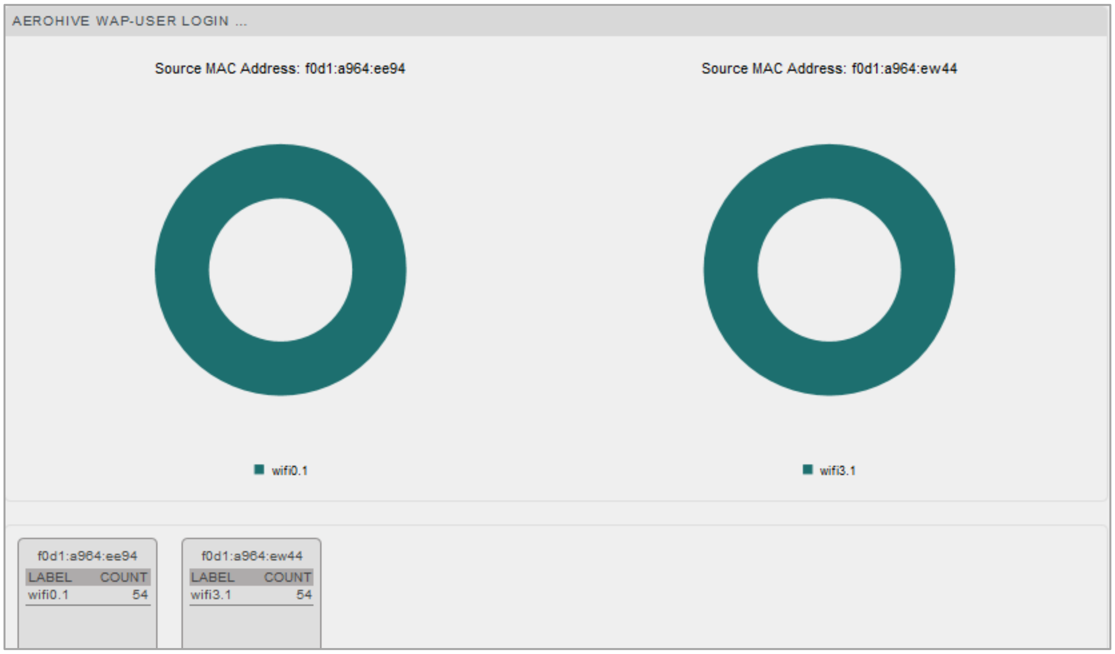
LEGEND [SERIES]: Source MAC Address

SELECT: All

☑ f0d1:a964:ee94 54
☑ f0d1:a964:ew44 54
□ f0d1:a964:ww44 54
□ f0d1:w264:e294 54

Figure 35

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.


AEROHIVE WAP-USER LOGIN ...
Source MAC Address: f0d1:a964:ee94
Source MAC Address: f0d1:a964:ew44
■ wifi0.1
■ wifi3.1

f0d1:a964:ee94

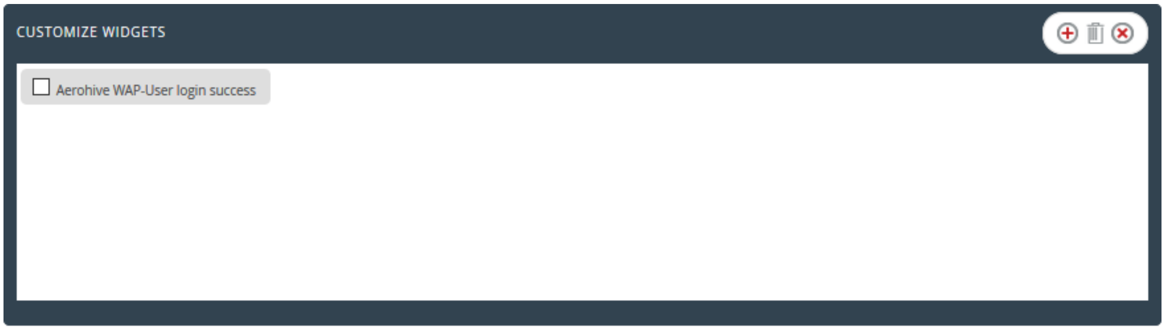
| LABEL | COUNT |
|---|---|
| wifi0.1 | 54 |

f0d1:a964:ew44

| LABEL | COUNT |
|---|---|
| wifi3.1 | 54 |

Figure 36

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



☐ Aerohive WAP-User login success

Figure 37

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

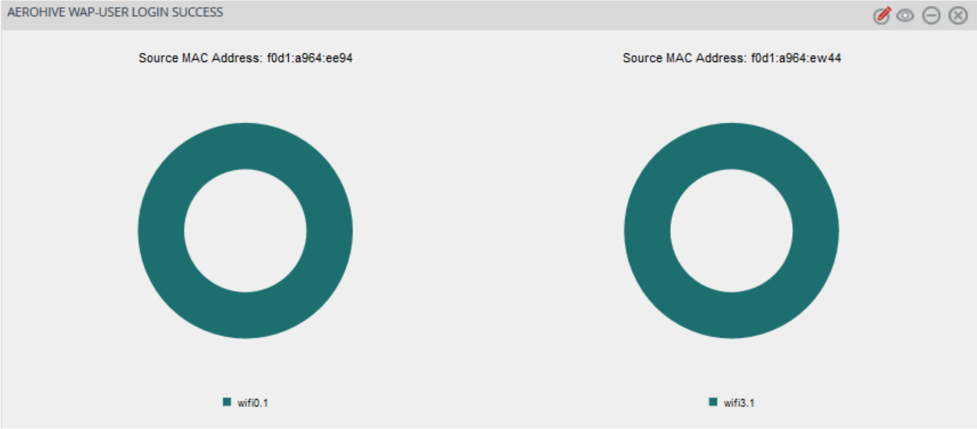

AEROHIVE WAP-USER LOGIN SUCCESS
Source MAC Address: f0d1:a964:ee94
Source MAC Address: f0d1:a964:ew44
■ wifi0.1
■ wifi3.1

Figure 38

- **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

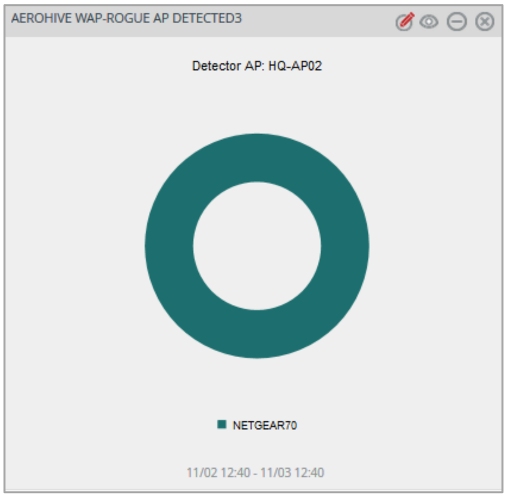


Figure 39