Abstract

This guide provides instructions to configure a Meraki Wireless Access Point (WAP) to send its syslog to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 7.x and later, and Meraki Wireless Access Point (WAP) MR series.

Audience

Administrators, who wish to monitor Meraki Wireless Access Point (WAP) using EventTracker Enterprise.
Table of Contents

Abstract.................................................................................................................................................. 1
  Scope.................................................................................................................................................. 1
  Audience............................................................................................................................................. 1
Introduction ........................................................................................................................................... 3
Pre-requisites........................................................................................................................................ 3
Enable syslog logging............................................................................................................................ 3
EventTracker Knowledge Pack (KP)....................................................................................................... 5
  Categories .......................................................................................................................................... 5
  Alerts................................................................................................................................................ 5
  Reports............................................................................................................................................... 5
Import Meraki WAP Knowledge Pack into EventTracker................................................................. 8
  Categories .......................................................................................................................................... 9
  Alerts................................................................................................................................................ 11
  Flex Reports .................................................................................................................................... 12
  Templates ........................................................................................................................................ 13
Verifying Meraki WAP knowledge pack in EventTracker................................................................. 14
  Categories .......................................................................................................................................... 14
  Alerts................................................................................................................................................ 15
  Flex Reports .................................................................................................................................... 16
  Template .......................................................................................................................................... 17
Create Flex Dashboards in EventTracker............................................................................................ 18
  Schedule Reports ............................................................................................................................. 18
  Create Dashlets ................................................................................................................................. 21
Sample Flex Dashboards..................................................................................................................... 24
Introduction

The Meraki MR series is the world’s first enterprise-grade line of cloud-managed WLAN access points. Designed for challenging enterprise environments, the MR access points use advanced 802.11ac and 802.11n technologies including MIMO, beam forming and channel bonding to deliver the throughput and reliable coverage required by demanding business applications.

EventTracker amasses and examines logs generated by Meraki WAP to help an administrator to monitor IP traffic, Rogue AP, SSID spoofing etc.

Pre-requisites

1. EventTracker 7.x and later should be installed.
2. Administrative access to Meraki Dashboard.
3. Port 514 must be opened on Meraki WAP.
4. Port 514 must not be used by other services of Meraki WAP.
5. An exception should be added into Windows Firewall on EventTracker machine for Syslog port 514.

Enable syslog logging

To configure a Meraki WAP to forward logs to a syslog server;

1. Logon to Meraki Dashboard Login.
2. Click on Network-Wide at top left and select General under Configure tab.
3. At the General page scroll down to the Logging section.
4. Click on **Add a syslog server** link.

   **Figure 2**

5. Type the IP address or name of **EventTracker Manager** Machine in **Server IP** field.
6. Type **514** in the **Port** field. (Recommended Port no. is 514)
7. Choose roles which you want to monitor like **Airmarshal events, Flows, URLs, Wireless event log** in **Roles** field.
   
   Mentioned log types are detailed below:

<table>
<thead>
<tr>
<th>Log Type</th>
<th>Log Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Event Log</td>
<td>Messages under Monitor &gt; Event log</td>
</tr>
<tr>
<td>Flows</td>
<td>Inbound and outbound traffic flows</td>
</tr>
<tr>
<td>URLs</td>
<td>HTTP/HTTPS GET requests</td>
</tr>
<tr>
<td>Airmarshal events</td>
<td>Alerts generated by IDS</td>
</tr>
</tbody>
</table>

   **Table 1**

Sample syslog configuration is shown below.
EventTracker Knowledge Pack (KP)

Once logs are received into EventTracker; Categories, Alerts, Reports can be configured into EventTracker. The following Knowledge Packs are available in EventTracker to support Meraki WAP monitoring.

Categories

- **Meraki WAP: Client machine association** - This category provides information related to client machine getting associated to one of the AP of Meraki WAP.
- **Meraki WAP: Client machine authenticate/deauthenticate** - This category provides information related to client machine trying to authenticate or deauthenticate to one of the AP of Meraki WAP.
- **Meraki WAP: Client machine disassociation** - This category provides information related to Client machine trying to disassociate from one of the AP of Meraki WAP.
- **Meraki WAP: Rogue SSID detected** - This category provides information related to rogue SSID which has been detected in AP of Meraki WAP.
- **Meraki WAP: SSID spoofing detected** - This category provides information related to SSID spoofing that has been detected in AP of Meraki WAP.

Alerts

- **Meraki WAP: Client deauthentication** - This alert is generated when client tries to login to the AP but due to wrong credentials it gets deauthenticated.
• **Meraki WAP: Rogue SSID detected**- This alert is generated when rogue SSID has been detected.

• **Meraki WAP: SSID spoofing detected**- This alert is generated when SSID spoofing has been detected.

### Reports

• **Meraki WAP-Rogue SSID detected**- This report provides information related to Rogue SSID that has been detected.

**Sample Report:**

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>BSID</th>
<th>Wired MAC Address</th>
<th>SSID Name</th>
<th>Channel</th>
<th>RSI</th>
<th>VLAN ID</th>
</tr>
</thead>
</table>

**Logs Considered:**

<table>
<thead>
<tr>
<th>LOG TIME</th>
<th>EVENT ID</th>
<th>SITE / COMPUTER</th>
<th>USER</th>
<th>DOMAIN</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/2/2016 5:08:14 PM</td>
<td>123</td>
<td>FNPL-4 KP / MerakiWAP</td>
<td>N/A</td>
<td>N/A</td>
<td>syslog</td>
</tr>
</tbody>
</table>

• **Meraki WAP-Client machine disassociation**- This report provides information related to client machine that is getting disassociated from the AP.

**Sample Report:**

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Client IP Address</th>
<th>Client MAC Address</th>
<th>Virtual AP</th>
<th>Channel</th>
<th>Radio</th>
<th>DHCP Server IP Address</th>
<th>DHCP Server MAC Address</th>
<th>DNS Server</th>
<th>Total duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>19/20/2016 24:55:16 PM</td>
<td>MERAKIWAP</td>
<td>10.100.1.236</td>
<td>54:4E:95:39:6D:61</td>
<td>1</td>
<td>11</td>
<td>0</td>
<td>10.100.1.1</td>
<td>88.15.44.88.40.90</td>
<td>206.67.222.222</td>
<td>60.64</td>
</tr>
</tbody>
</table>

**Logs Considered:**

<table>
<thead>
<tr>
<th>LOG TIME</th>
<th>EVENT ID</th>
<th>SITE / COMPUTER</th>
<th>USER</th>
<th>DOMAIN</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/2/2016 5:08:14 PM</td>
<td>123</td>
<td>FNPL-4 KP / MerakiWAP</td>
<td>N/A</td>
<td>N/A</td>
<td>syslog</td>
</tr>
</tbody>
</table>

• **Meraki WAP-Client machine association**- This report provides information related to client machine getting associated to one of the APs.
Sample Report:

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Event Type</th>
<th>Client IP address</th>
<th>Client MAC Address</th>
<th>Virtual AP</th>
<th>Channel</th>
<th>Radio</th>
<th>RSSI</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/20/2016 03:58:18 PM</td>
<td>MERAKIWAP</td>
<td>association</td>
<td>0.0.0.0</td>
<td>DC:2B:2A:01:5D:4A</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>39</td>
</tr>
</tbody>
</table>

Logs Considered:

- **Meraki WAP-Client machine authenticate deauthenticate** - This report provides information related to client machine getting authentication or deauthenticated during connectivity.

Sample Report:

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Event Type</th>
<th>Client IP address</th>
<th>Client MAC Address</th>
<th>Host Name</th>
<th>Virtual AP</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/20/2016 02:36:19 PM</td>
<td>MERAKIWAP</td>
<td>wpa_deauth</td>
<td>0.0.0.0</td>
<td>DC:2B:2A:01:5D:4A</td>
<td><a href="mailto:host9W7@badger.nomic.com">host9W7@badger.nomic.com</a></td>
<td>1</td>
</tr>
<tr>
<td>10/20/2016 02:36:19 PM</td>
<td>MERAKIWAP</td>
<td>wpa_auth</td>
<td>0.0.0.0</td>
<td>DC:2B:2A:01:5D:4A</td>
<td><a href="mailto:host9W7@badger.nomic.com">host9W7@badger.nomic.com</a></td>
<td>1</td>
</tr>
</tbody>
</table>

Logs Considered:

- **Meraki WAP-SSID spoofing detected** - This report provides information related to SSID spoofing that has been detected.

Sample Report:

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Source MAC Address</th>
<th>Channel</th>
<th>SSID</th>
<th>RSSI</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/02/2016 12:00:57 PM</td>
<td>MERAKIWAP</td>
<td>5C:F5:DA:97:0E:87</td>
<td>44</td>
<td>Envoy</td>
<td>7</td>
</tr>
</tbody>
</table>
EventTracker: Integrate Meraki WAP

Logs Considered:

<table>
<thead>
<tr>
<th>LOG TIME</th>
<th>EVENT ID</th>
<th>SITE / COMPUTER</th>
<th>USER</th>
<th>DOMAIN</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/2/2016 5:08:13 PM</td>
<td>123</td>
<td>PN-FL-4 AP / Meraki WA</td>
<td>N/A</td>
<td>N/A</td>
<td>syslog</td>
</tr>
</tbody>
</table>

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

Description:
Sep 23 12:55:13 10.4.4.12 1:0:0 1st_Floor_NE IS1 armchair_events type:ssid spoofing detected ssid:"Envoy" vapid:71 bssid:FF:FF:FF:FF:FF:
src:"5C5S0A09D0E87" dst:"FF:FF:FF:FF:FF:FF" channel:"44" rc:"7" fc_type:"0" fc_subtype:"4"

Import Meraki WAP 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, and then click the Import tab.
Categories

1. Click **Category** option, and then click the **browse** button.
2. Locate All Meraki WAP categories.iscat file, and then click the Open button.

3. To import categories, click the Import button.

   EventTracker displays success message.

   Figure 15

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

   Figure 16
Alerts

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

![Figure 17](image1.png)

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

   EventTracker displays success message.

![Figure 18](image2.png)

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

1. Click **Reports** option, and then click the 'browse' button.
2. Locate **All Meraki WAP reports.issch** file, and then click the **Open** button.

![Figure 19](image1.png)

3. To import scheduled reports, click the **Import** button.

   EventTracker displays success message.

![Figure 20](image2.png)

4. 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.

3. Click on **Browse** button.

4. Locate **All Meraki WAP Template.ettd** file, and then click the **Open** button.
5. Now select the check box and then click on 'Import' option. EventTracker displays success message.

![Template(s) imported successfully](image)

6. Click on OK button.

**Verifying Meraki WAP knowledge pack in EventTracker Categories**

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Categories.
3. In the Category Tree, navigate to Meraki->Meraki WAP group folder.
Alerts

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and select Alerts.
3. In Search field, type ‘Meraki WAP’, and then click the button.

Alert Management page will display all the imported Meraki WAP alerts.
4. To activate the imported alerts, select the respective checkbox in the **Active** column.

   EventTracker displays message box.

   ![Message Box](image)

   **Figure 27**

   ![Alert Management](image)

   **Figure 28**

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

   **NOTE**: Please specify appropriate systems in alert configuration for better performance.

### Flex Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports** menu and select **Configuration**.
3. Select **Defined** in report type.

   Imported reports are displayed on the right pane.
1. Logon to EventTracker Enterprise web interface.

2. Click the Admin menu, and then click Parsing Rules and click Template.
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 **Meraki WAP** in report groups. Check **Defined** dialog box.

![Figure 30](image)

1. Click on ‘**schedule**’ to plan a report for later execution.
2. Click **Next** button to proceed.
3. In review page, check **Persist data in EventVault Explorer** option.
4. In next page, check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.
EventTracker: Integrate Meraki WAP

5. Proceed to next step and click **Schedule** button.
6. 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.

![Figure 34](image)
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.
14. If satisfied, click **Configure** button.

4. Click 'customize' to locate and choose created dashlet.
5. Click to add dashlet to earlier created dashboard.
Sample Flex Dashboards

For below dashboard **DATA SOURCE: Meraki WAP: Rogue SSID detected**

**Meraki WAP: Rogue SSID detected**
**WIDGET TITLE:** Meraki WAP: Rogue SSID detected
**CHART TYPE:** Donut
**AXIS LABELS [X-AXIS]:** Broadcast SSID
**FILTER:** Event type
**LEGEND [SERIES]:** Destination MAC Address

![Figure 38](image-url)