

Integrate Meraki WAP EventTracker Enterprise

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.

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

This document is for informational purposes only. Prism Microsystems 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 Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems 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 Prism Microsystems, 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.

© 2016 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

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..... | 6 |
| 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.

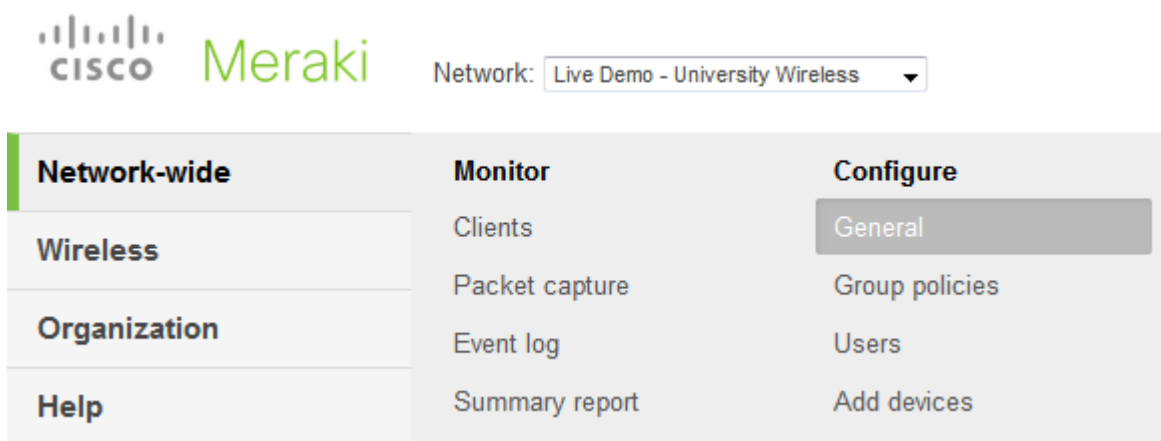


Figure 1

3. At the **General** page scroll down to the **Logging** section.

Logging

Syslog servers

There are no syslog servers for this network.
[Add a syslog server](#)

Figure 2

- Click on **Add a syslog server** link.

Logging

Syslog servers

| Server IP | Port | Roles | Actions |
|----------------------|------|---------------------|---------|
| <input type="text"/> | 514 | Select Some Options | X |

[Add a syslog server](#)

Figure 3

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

| Log Type | Log Details |
|--------------------|--|
| Wireless Event Log | Messages under Monitor > Event log |
| Flows | Inbound and outbound traffic flows |
| URLs | HTTP/HTTPS GET requests |
| Airmarshal events | Alerts generated by IDS |

Table 1

Sample syslog configuration is shown below.

Logging

Syslog servers

| Server IP | Port | Roles | Actions |
|-----------|------|--|---------|
| 10.10.1.5 | 514 | <div> <div>Airmarshal events x</div> <div>Flows x</div> <div>URLs x</div> <div>Wireless event log x</div> </div> | X |

[Add a syslog server](#)

Figure 4

Integrated device can be verified in systems pane of EventTracker advanced log search.

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:

| LogTime | Computer | BSSID | Wired MAC Address | SSID Name | Channel | RSSI | VLAN ID |
|------------------------|-----------|-------------------|-------------------|-----------|---------|------|---------|
| 10/28/2016 06:18:12 PM | MERAKIWAP | E0:91:F5:5E:F2:92 | E0:91:F5:5E:F2:93 | WLAN | 1 | 20 | 38656 |

Logs Considered:

| LOG TIME | EVENT ID | SITE / COMPUTER | USER | DOMAIN | SOURCE |
|----------------------|---------------------|---|------|--------|--------|
| 11/2/2016 5:08:14 PM | 123 | PNPL-4-KP / MerakiWA... | N/A | N/A | syslog |

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

Description:
 Sep 23 12:14:51 10.4.4.22 1 0.0 1st_Floor_NW_Room_122 airmarshal_events type= rogue_ssid_detected ssid="WLAN" bssid="E0:91:F5:5E:F2:92" src="E0:91:F5:5E:F2:92" dst="FF:FF:FF:FF:FF:FF" wired_mac="E0:91:F5:5E:F2:93" vlan_id="38656" channel="1" rssi="20" fc_type="0" fc_subtype="8"

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

Sample Report:

| LogTime | Computer | Client IP address | Client MAC Address | Virtual AP | Channel | Radio | DHCP Server IP Address | DHCP Server MAC address | DNS Server | Total duration |
|------------------------|-----------|-------------------|--------------------|------------|---------|-------|------------------------|-------------------------|----------------|----------------|
| 10/28/2016 04:55:16 PM | MERAKIWAP | 10.100.1.236 | 54:4E:90:59:6D:61 | 1 | 11 | 0 | 10.100.1.1 | 88:15:44:08:A8:90 | 208.67.222.222 | 60.64 |

Logs Considered:

| LOG TIME | EVENT ID | SITE / COMPUTER | USER | DOMAIN | SOURCE |
|----------------------|---------------------|---|------|--------|--------|
| 11/2/2016 5:08:15 PM | 123 | PNPL-4-KP / MerakiWA... | N/A | N/A | syslog |

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

Description:
 Sep 23 12:58:21 10.4.4.22 1 0.0 1st_Floor_NW_Room_122 events type=disassociation radio="0" vap="1" client_mac="54:4E:90:59:6D:61" channel="11" reason="8" instigator="2" duration="60.640000003" auth_neg_dur="0.010000001" last_auth_ago="60.620000" is_wpa="1" full_conn="30.589999999" ip_resp="30.589999999" ip_src="10.100.1.236" arp_resp="0.6000000" arp_src="10.100.1.236" dns_server="208.67.222.222" dns_req_rtt="0.010000001" dns_resp="1.210000001" dhcp_lease_completed="0.630000" dhcp_ip="10.100.1.236" dhcp_server="10.100.1.1" dhcp_server_mac="88:15:44:08:A8:90" dhcp_resp="0.630000" aid="2066782231"

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

Sample Report:

| LogTime | Computer | Event Type | Client IP address | Client MAC Address | Virtual AP | Channel | Radio | RSSID |
|------------------------|-----------|-------------|-------------------|--------------------|------------|---------|-------|-------|
| 10/28/2016 03:58:18 PM | MERAKIWAP | association | 0.0.0.0 | DC:2B:2A:01:5D:4A | 1 | 1 | 0 | 39 |

Logs Considered:

| LOG TIME | EVENT ID | SITE / COMPUTER | USER | DOMAIN | SOURCE |
|--|----------|-------------------------|------|--------|--------|
| 10/28/2016 5:08:19 PM | 123 | PNPL-4-KP / MerakiWA... | N/A | N/A | syslog |
| Event Type: Information Log Type: Application Category Id: 0 | | | | | |
| Description: Sep 23 12:58:08 10.4.4.16 1 0.0 2nd_Floor_NW_ICSC events type=association radio="0" vap="1" client_mac="DC:2B:2A:01:5D:4A" client_ip="0.0.0.0" channel="1" rssi="39" aid="1409706221" | | | | | |

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

Sample Report:

| LogTime | Computer | Event Type | Client IP address | Client MAC Address | Host Name | Virtual AP |
|------------------------|-----------|--------------|-------------------|--------------------|---------------------------|------------|
| 10/28/2016 02:36:19 PM | MERAKIWAP | 8021x_deauth | 0.0.0.0 | 00:24:D7:90:03:B8 | host/w7-jbadger.ncmic.com | 0 |
| 10/28/2016 02:36:19 PM | MERAKIWAP | wpa_auth | 0.0.0.0 | DC:2B:2A:01:5D:4A | | 1 |
| 10/28/2016 02:36:19 PM | MERAKIWAP | wpa_auth | 0.0.0.0 | DC:2B:2A:01:5D:4A | | 1 |

Logs Considered:

| LOG TIME | EVENT ID | SITE / COMPUTER | USER | DOMAIN | SOURCE |
|---|----------|-------------------------|------|--------|--------|
| 10/28/2016 5:08:18 PM | 123 | PNPL-4-KP / MerakiWA... | N/A | N/A | syslog |
| Event Type: Information Log Type: Application Category Id: 0 | | | | | |
| Description: Sep 23 08:02:42 10.4.4.14 1 0.0 2nd_Floor_NE_Claims events type=8021x_deauth radio="1" vap="0" client_mac="00:24:D7:90:03:B8" client_ip="0.0.0.0" identity="host/w7-jbadger.ncmic.com" aid="868665516" | | | | | |
| 11/2/2016 5:08:18 PM | 123 | PNPL-4-KP / MerakiWA... | N/A | N/A | syslog |
| Event Type: Information Log Type: Application Category Id: 0 | | | | | |
| Description: Sep 23 12:58:09 10.4.4.16 1 0.0 2nd_Floor_NW_ICSC events type=wpa_auth radio="0" vap="1" client_mac="DC:2B:2A:01:5D:4A" client_ip="0.0.0.0" aid="1409706221" | | | | | |

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

Sample Report:

| LogTime | Computer | Source MAC Address | Channel | SSID | RSSI |
|------------------------|-----------|--------------------|---------|-------|------|
| 11/02/2016 12:00:57 PM | MERAKIWAP | 5C:F5:DA:97:0E:87 | 44 | Envoy | 7 |

Logs Considered:

| <input type="checkbox"/> LOG TIME | EVENT ID | SITE / COMPUTER | USER | DOMAIN | SOURCE |
|---|---------------------|--|------|--------|--------|
| <input type="checkbox"/> 11/2/2016 5:08:13 PM | 123 | PNPL-4-KP / MerakiWA... | N/A | N/A | syslog |
| 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_JS_1 airmarshal_events type=ssid_spoofing_detected ssid="Envoy" vap="7" bssid="FF:FF:FF:FF:FF:FF" src="5C:F5:DA:97:0E:87" dst="FF:FF:FF:FF:FF:FF" channel="44" rssi="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.

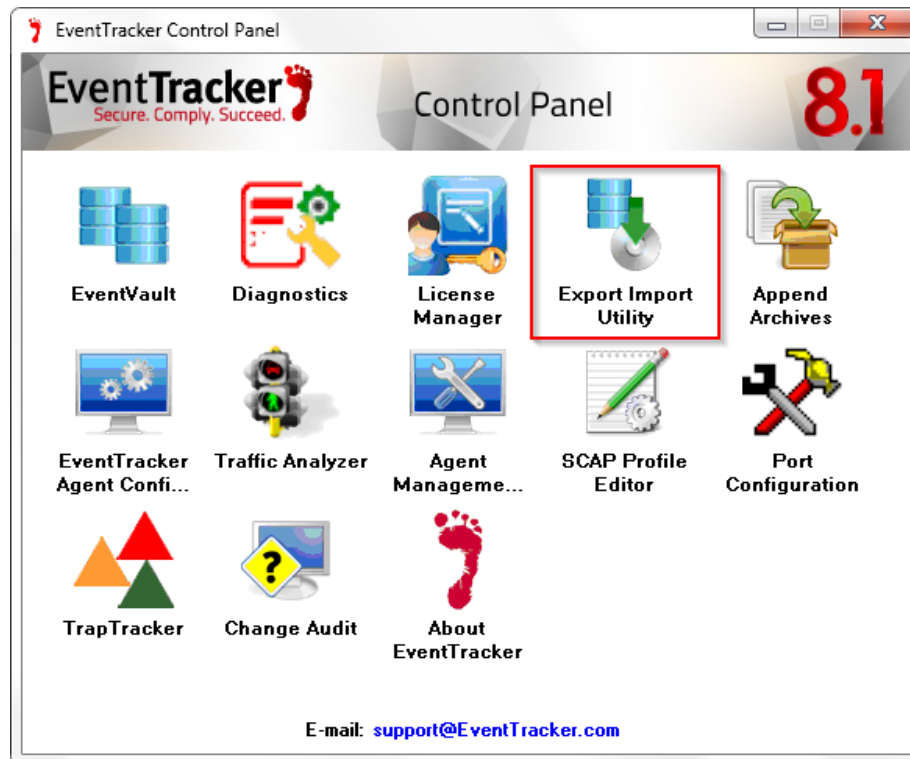


Figure 10

Categories

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

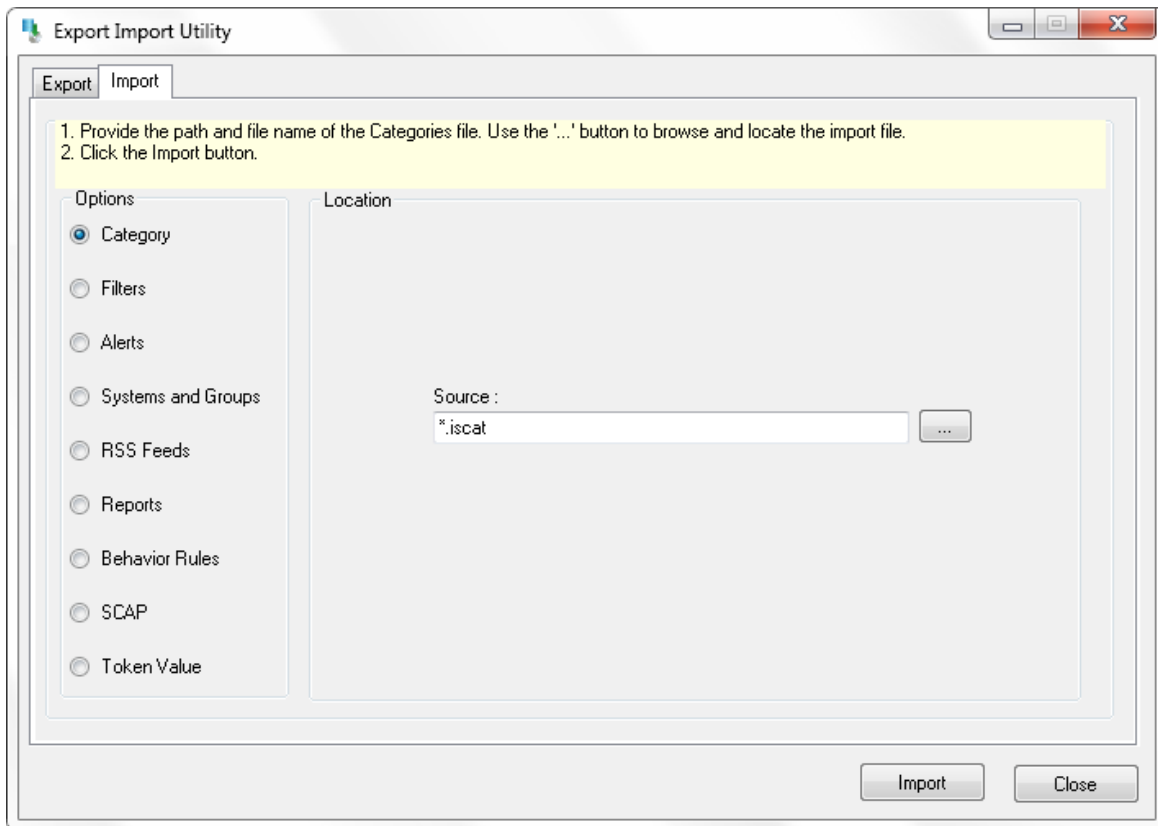


Figure 15

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.

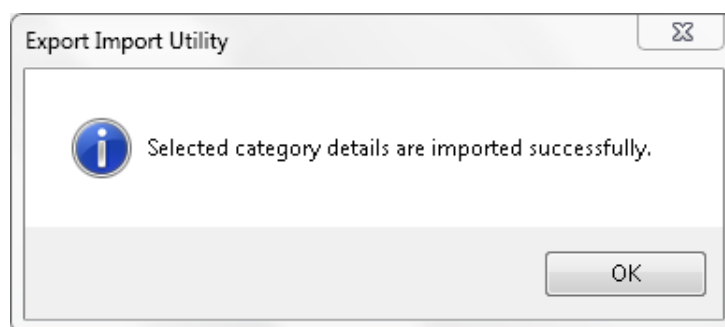



Figure 16

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

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.

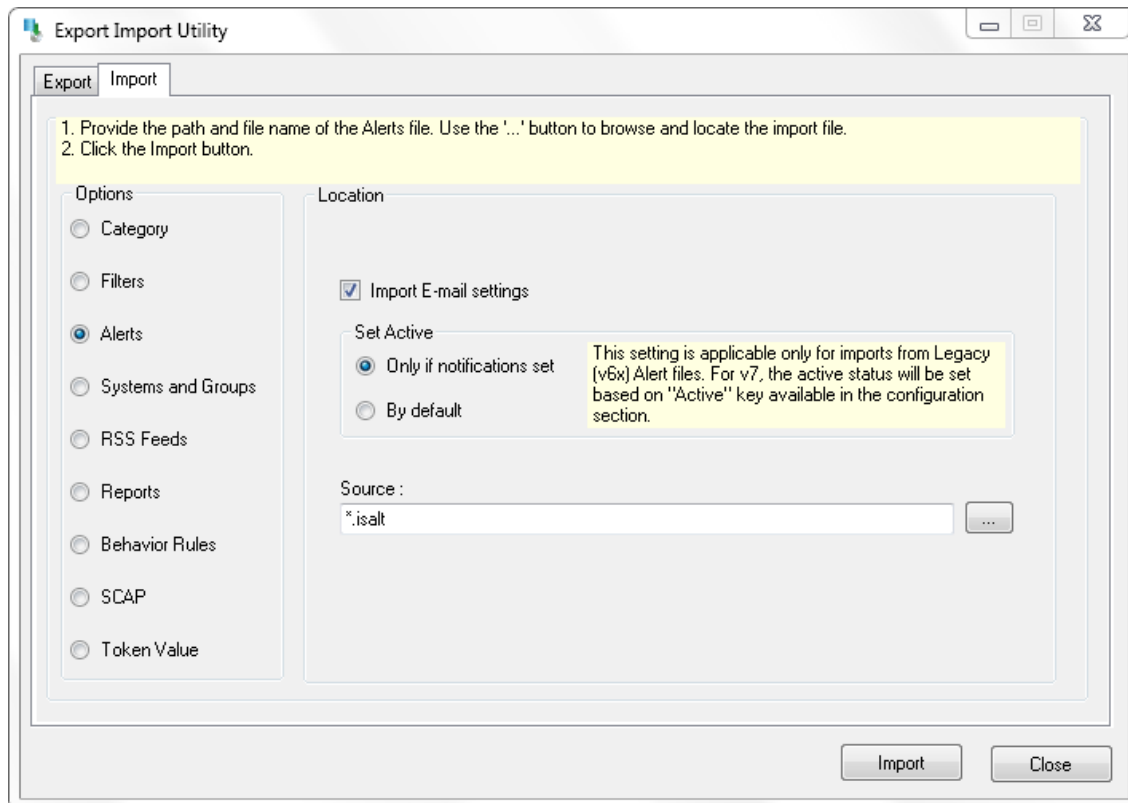


Figure 17

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

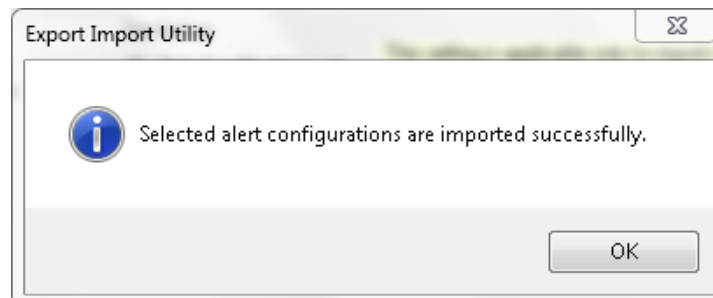



Figure 18

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.

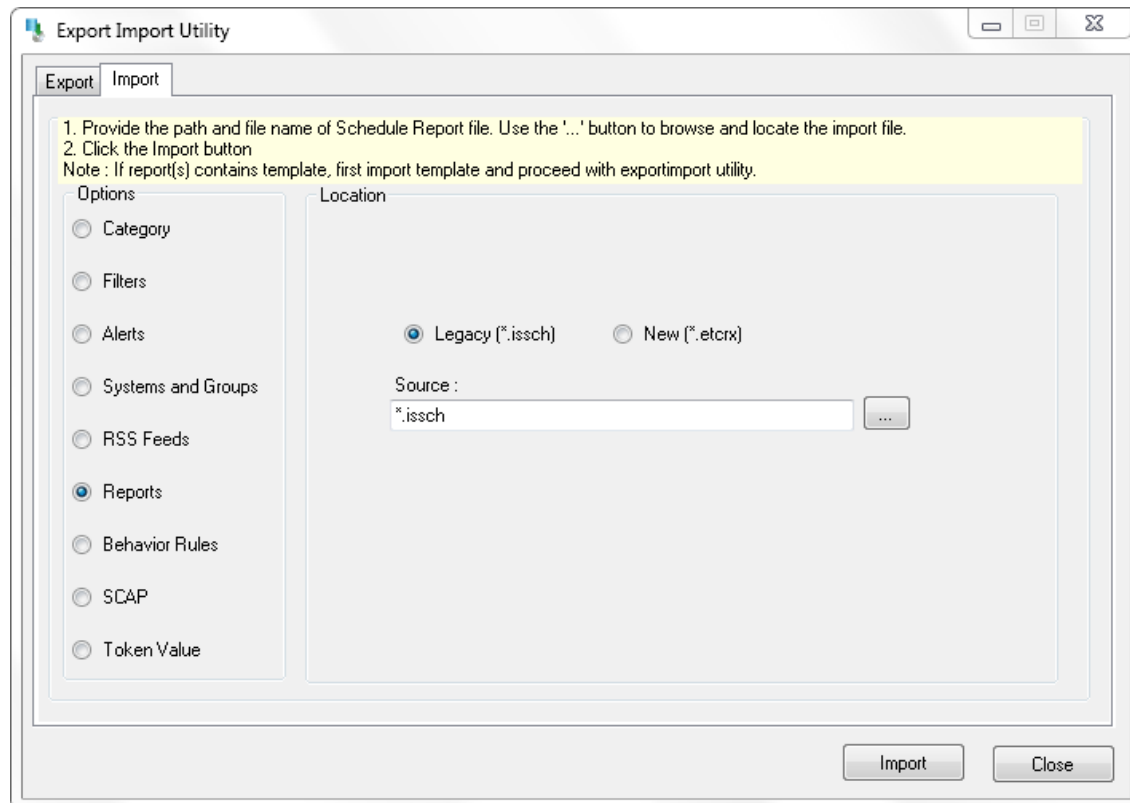


Figure 19

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

EventTracker displays success message.

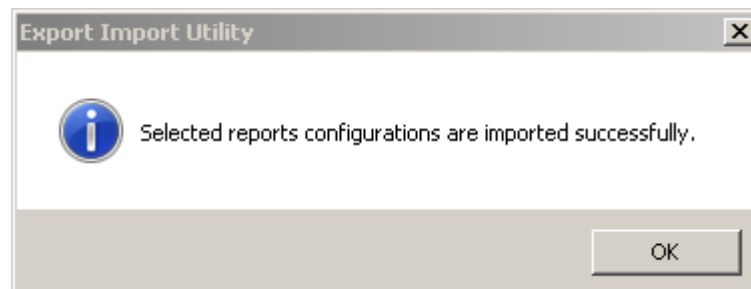



Figure 20

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.

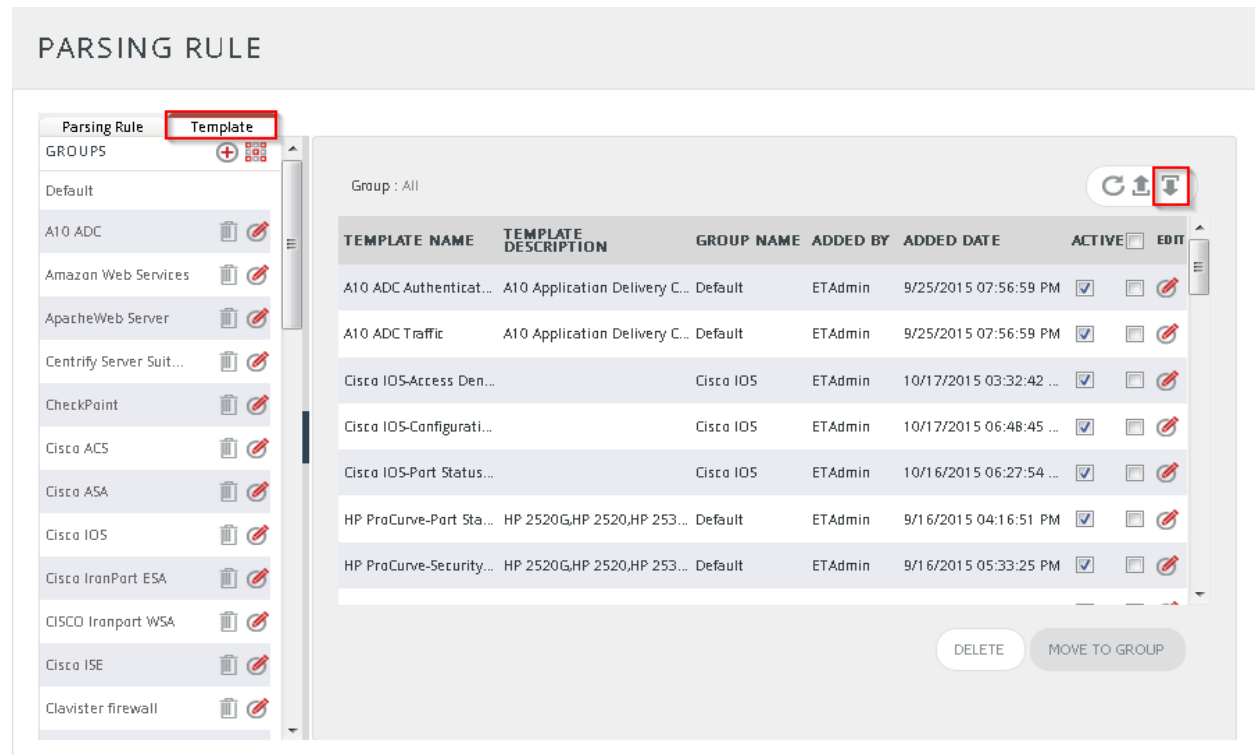


Figure 18

3. Click on **Browse** button.

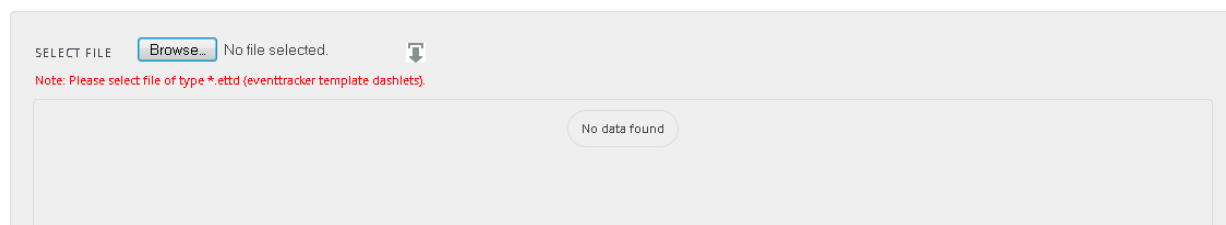



Figure 19

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

SELECTED FILE IS: All Meraki WAP Template.ettid

| <input type="checkbox"/> TEMPLATE NAME | SEPARATOR | TEMPLATE DESCRIPTION | ADDED DATE | ADDED BY | GROUP NAME |
|--|-----------|---|-----------------------|--------------|------------|
| <input type="checkbox"/> Meraki WAP-Client machine association | \n | Sep 23 12:58:08 10.4.4.16 1 0.0 2nd_Floor_NW_ICSC events type=association r adio="0" vap="1" client_mac="DC:2B:2A:01:5D:4A" client_ip="0.0.0.0" channel= "1" rssi="39" aid="1409706221" | 10/28/2016 4:41:29 PM | abhilanchana | Meraki WAP |
| <input type="checkbox"/> Meraki WAP-Client machine authentication deauthentication | \n | Sep 23 08:05:57 10.4.4.12 1 0.0 1st_Floor_NE_IS_1 events type=8021x_auth rad io="1" vap="0" client_mac="4C:EB:42:F3:EF:82" client_ip="0.0.0.0" identity="ho st/w10-tchandavong.ncmic.com" aid="964109866" | 10/28/2016 3:07:29 PM | abhilanchana | Meraki WAP |
| <input type="checkbox"/> Meraki WAP-Client machine disassociation | \n | Sep 23 12:58:21 10.4.4.22 1 0.0 1st_Floor_NW_Room_122 events type=disasso ciation radio="0" vap="1" client_mac="54:4E:90:59:6D:61" channel="11" reaso n="8" instigator="2" duration="60.640000003" auth_neg_dur="0.010000001" l ast_auth_age="60.6200000" is_wpa="1" full_conn="30.5899999999" ip_resp="30. 589999999" ip_src="10.100.1.236" arp_resp="0.6000000" arp_src="10.100.1.236 " dns_server="208.67.222.222" dns_req_rtt="0.010000001" dns_resp="1.21000 0001" dhcp_lease_completed="0.6300000" dhcp_ip="10.100.1.236" dhcp_server ="10.100.1.1" dhcp_server_mac="88:15:44:08:A8:90" dhcp_resp="0.6300000" ai d="2066782231" | 10/28/2016 6:13:29 PM | abhilanchana | Meraki WAP |

Figure 20

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

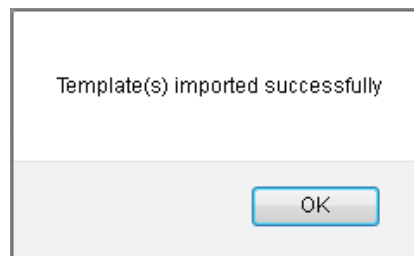


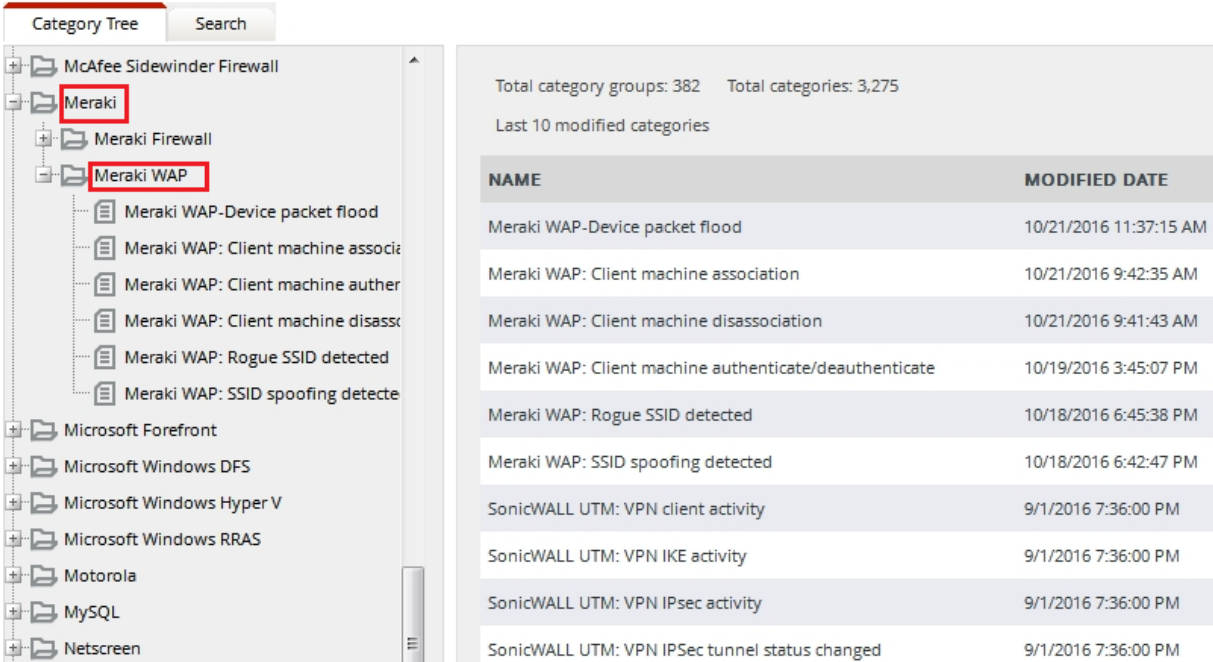
Figure 21

- Click on **OK** button.

Verifying Meraki WAP knowledge pack in EventTracker Categories

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

CATEGORY MANAGEMENT




The screenshot displays the 'Category Management' interface. On the left, a 'Category Tree' shows a hierarchy starting with 'McAfee Sidewinder Firewall', followed by 'Meraki' (highlighted with a red box), 'Meraki Firewall', and 'Meraki WAP' (also highlighted with a red box). Below 'Meraki WAP', several sub-categories are listed, including 'Meraki WAP-Device packet flood', 'Meraki WAP: Client machine associ...', 'Meraki WAP: Client machine auther...', 'Meraki WAP: Client machine disass...', 'Meraki WAP: Rogue SSID detected', and 'Meraki WAP: SSID spoofing detecte...'. Other categories like 'Microsoft Forefront', 'Microsoft Windows DFS', 'Microsoft Windows Hyper V', 'Microsoft Windows RRAS', 'Motorola', 'MySQL', and 'Netscreen' are also visible.

On the right, a summary shows 'Total category groups: 382' and 'Total categories: 3,275'. Below this, a table titled 'Last 10 modified categories' lists the following:

| NAME | MODIFIED DATE |
|--|------------------------|
| Meraki WAP-Device packet flood | 10/21/2016 11:37:15 AM |
| Meraki WAP: Client machine association | 10/21/2016 9:42:35 AM |
| Meraki WAP: Client machine disassociation | 10/21/2016 9:41:43 AM |
| Meraki WAP: Client machine authenticate/deauthenticate | 10/19/2016 3:45:07 PM |
| Meraki WAP: Rogue SSID detected | 10/18/2016 6:45:38 PM |
| Meraki WAP: SSID spoofing detected | 10/18/2016 6:42:47 PM |
| SonicWALL UTM: VPN client activity | 9/1/2016 7:36:00 PM |
| SonicWALL UTM: VPN IKE activity | 9/1/2016 7:36:00 PM |
| SonicWALL UTM: VPN IPsec activity | 9/1/2016 7:36:00 PM |
| SonicWALL UTM: VPN IPsec tunnel status changed | 9/1/2016 7:36:00 PM |

Figure 26

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.

ALERT MANAGEMENT

Search by Alert name

Click 'Activate Now' after making all changes Total: 3 Page Size 25

| <input type="checkbox"/> | ALERT NAME ^ | THREAT | ACTIVE | E-MAIL | MESSAGE | RSS | FORWARD AS SNMP | FORWARD AS SYSLOG | REMEDIAL ACTION AT CONSOLE | REMEDIAL ACTION AT AGENT | APPLIES TO |
|--------------------------|-------------------------------------|---------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|----------------------------|--------------------------|------------|
| <input type="checkbox"/> | Meraki WAP: Client deauthentication | High | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | MR Series |
| <input type="checkbox"/> | Meraki WAP: Rogue SSID detected | Serious | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | MR Series |
| <input type="checkbox"/> | Meraki WAP: SSID spoofing detected | Serious | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | MR Series |

Figure 27

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

EventTracker displays message box.

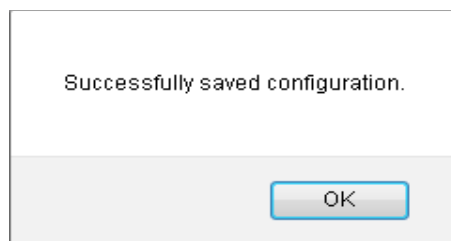


Figure 28

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

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




Flex Reports

- Logon to **EventTracker Enterprise**.
- Click the **Reports** menu and select **Configuration**.
- Select **Defined** in report type.
- In **Report Groups Tree**, select **Meraki WAP group** folder.




Imported reports are displayed on the right pane.




REPORTS CONFIGURATION




☐ Scheduled ☐ Queued ☒ Defined




Search   




REPORT GROUPS




 McAfee  




 Meraki Firewall  




 **Meraki WAP**  




 Microsoft Windows DF...  




 Microsoft Windows RR...  

 MSSQL  




 MySQL  

 Office 365  

 OKTA SSO  

 OpenDNS  

REPORTS CONFIGURATION : MERAKI WAP

Total: 6



































|  | TITLE | CREATED ON | MODIFIED ON |  |  |  |
|---|--|------------------------|------------------------|---|---|---|
|  |  Meraki WAP-Device packet flood details | 10/21/2016 11:57:06 AM | 10/21/2016 11:57:06 AM |  |  |  |
|  |  Meraki WAP-Rogue SSID detected | 10/21/2016 10:26:31 AM | 10/21/2016 10:30:35 AM |  |  |  |
|  |  Meraki WAP-Client machine disassociation | 10/21/2016 10:01:22 AM | 10/21/2016 10:01:22 AM |  |  |  |
|  |  Meraki WAP-Client machine association | 10/21/2016 9:46:31 AM | 10/21/2016 9:48:12 AM |  |  |  |
|  |  Meraki WAP-Client machine authenticate deauthen... | 10/21/2016 9:28:35 AM | 10/21/2016 9:28:35 AM |  |  |  |
|  |  Meraki WAP-SSID spoofing detected | 10/6/2016 10:58:42 AM | 10/21/2016 10:43:52 AM |  |  |  |

Figure 29

Template

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

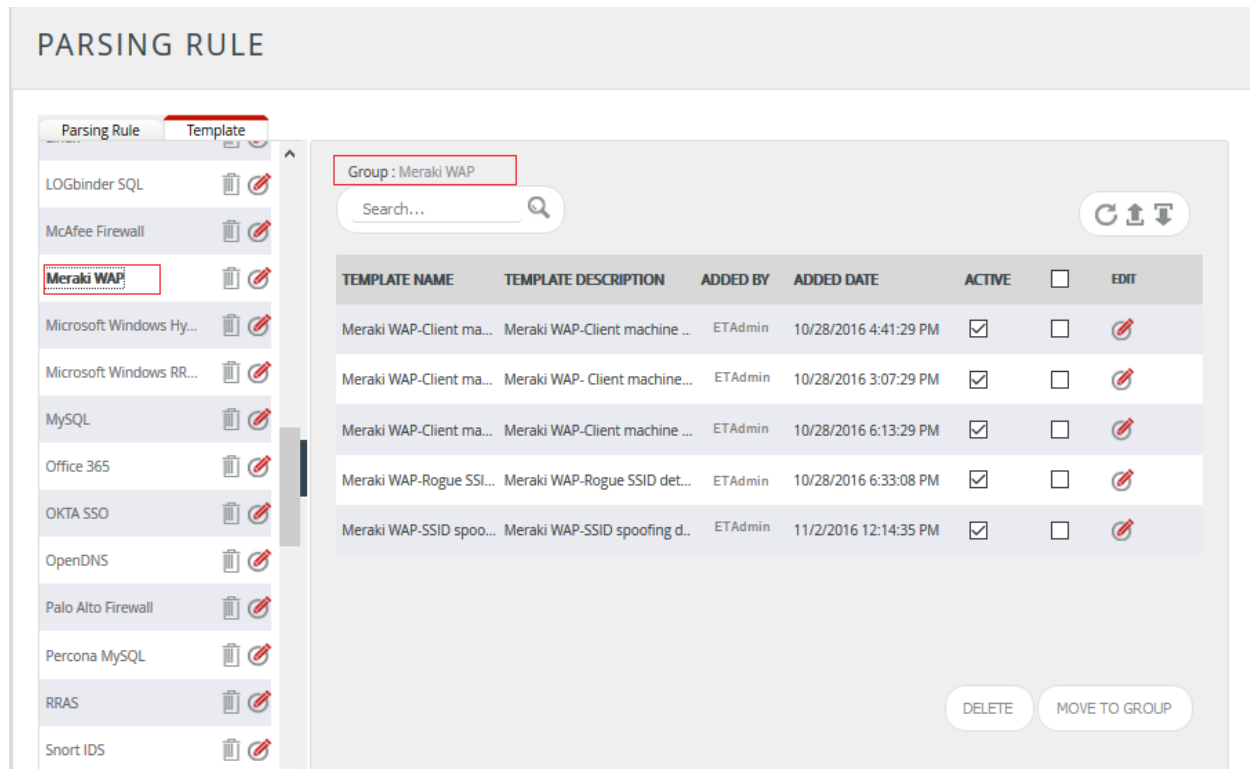


Figure 27

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 login.

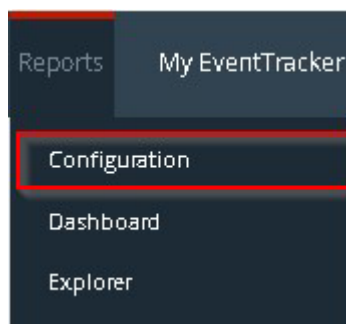





Figure 29

2. Navigate to **Reports>Configuration**.
3. Select **Meraki WAP** in report groups. Check **Defined** dialog box.

REPORTS CONFIGURATION

☐ Scheduled ☐ Queued ☒ Defined

Search   

REPORT GROUPS

- McAfee
- Meraki Firewall
- Meraki WAP**
- Microsoft Windows DF...
- Microsoft Windows RR...
- MSSQL
- MySQL
- Office 365
- OKTA SSO
- OpenDNS

REPORTS CONFIGURATION : MERAKI WAP

Total: 6








| TITLE | CREATED ON | MODIFIED ON |
|--|------------------------|------------------------|
|  Meraki WAP-Device packet flood details | 10/21/2016 11:57:06 AM | 10/21/2016 11:57:06 AM |
|  Meraki WAP-Rogue SSID detected | 10/21/2016 10:26:31 AM | 10/21/2016 10:30:35 AM |
|  Meraki WAP-Client machine disassociation | 10/21/2016 10:01:22 AM | 10/21/2016 10:01:22 AM |
|  Meraki WAP-Client machine association | 10/21/2016 9:46:31 AM | 10/21/2016 9:48:12 AM |
|  Meraki WAP-Client machine authenticate deauthen... | 10/21/2016 9:28:35 AM | 10/21/2016 9:28:35 AM |
|  Meraki WAP-SSID spoofing detected | 10/6/2016 10:58:42 AM | 10/21/2016 10:43:52 AM |

Figure 30

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.

REPORT WIZARD
TITLE: MERAKI WAP-ROGUE SSID DETECTED
LOGS

Review cost details and configure the publishing options. Step 8 of 10

DISK COST ANALYSIS

Estimated time for completion: 00:00:52(HH:MM:SS)
Number of cab(s) to be processed: 11
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

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

REPORT WIZARD
TITLE: MERAKI WAP-ROGUE SSID 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 | <input checked="" type="checkbox"/> |
| Event Type | <input checked="" type="checkbox"/> |
| SSID Name | <input checked="" type="checkbox"/> |
| Broadcast SSID | <input checked="" type="checkbox"/> |
| VLAN ID | <input checked="" type="checkbox"/> |

Figure 32

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.

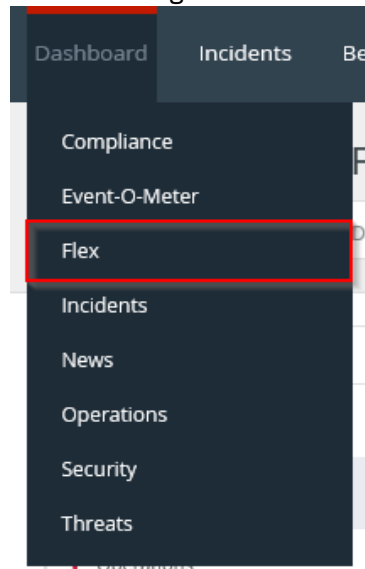


Figure 33

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

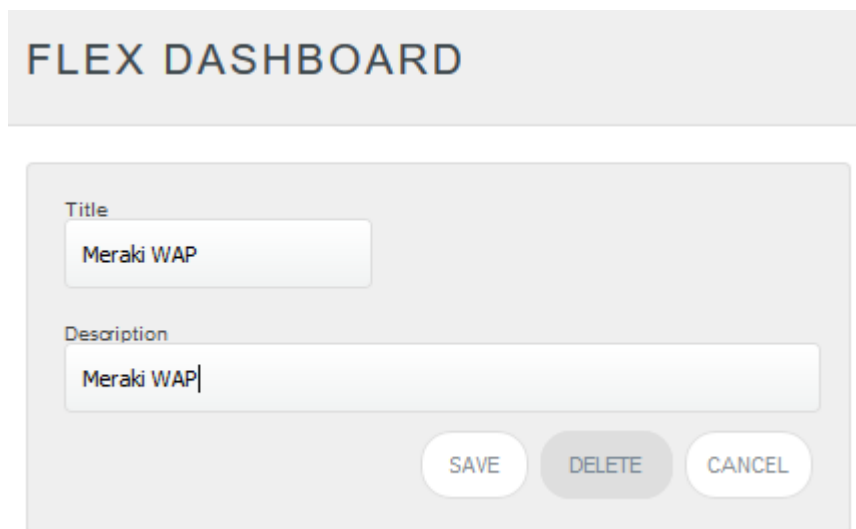

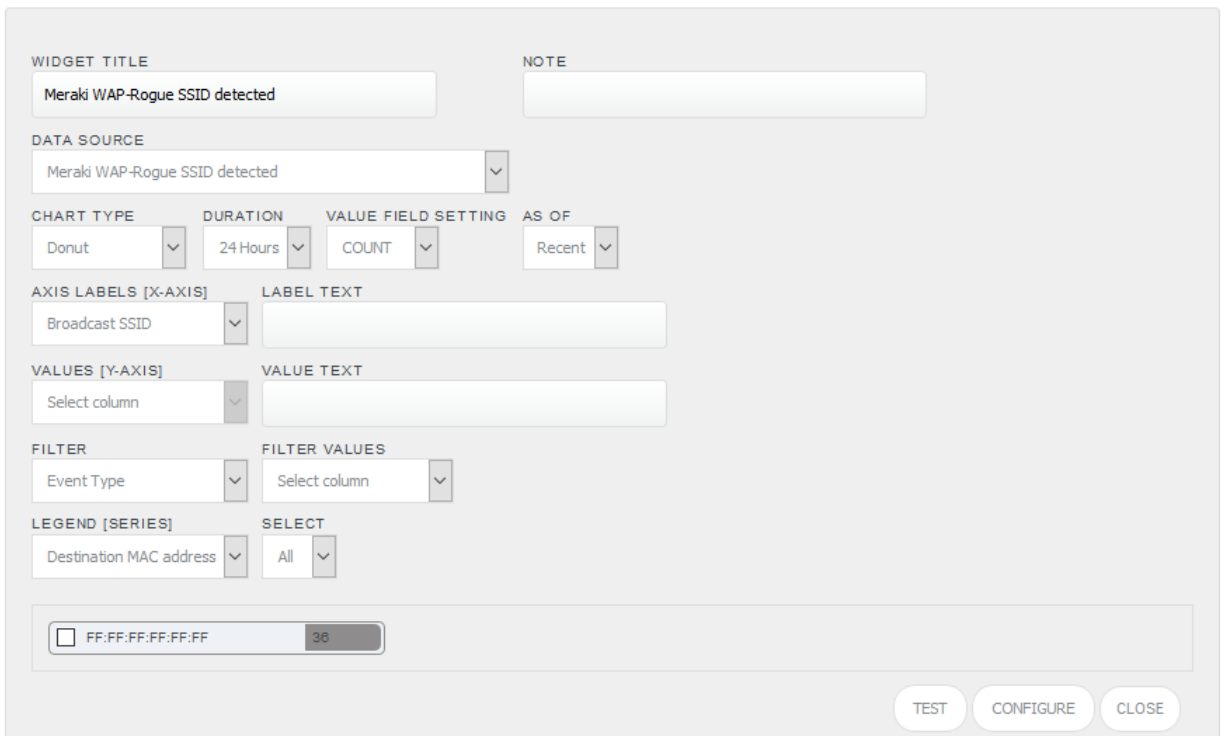
A screenshot of the 'FLEX DASHBOARD' form. The title 'FLEX DASHBOARD' is at the top in a light gray box. Below it, there is a form with two input fields: 'Title' and 'Description'. Both fields contain the text 'Meraki WAP'. At the bottom right of the form, there are three buttons: 'SAVE', 'DELETE', and 'CANCEL'.

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



The Widget Configuration pane is a form for configuring a flex dashlet. It includes the following sections:

- WIDGET TITLE:** A text input field containing "Meraki WAP-Rogue SSID detected".
- NOTE:** A text input field.
- DATA SOURCE:** A dropdown menu showing "Meraki WAP-Rogue SSID detected".
- CHART TYPE:** A dropdown menu showing "Donut".
- DURATION:** A dropdown menu showing "24 Hours".
- VALUE FIELD SETTING:** A dropdown menu showing "COUNT".
- AS OF:** A dropdown menu showing "Recent".
- AXIS LABELS [X-AXIS]:** A dropdown menu showing "Broadcast SSID".
- LABEL TEXT:** A text input field.
- VALUES [Y-AXIS]:** A dropdown menu showing "Select column".
- VALUE TEXT:** A text input field.
- FILTER:** A dropdown menu showing "Event Type".
- FILTER VALUES:** A dropdown menu showing "Select column".
- LEGEND [SERIES]:** A dropdown menu showing "Destination MAC address".
- SELECT:** A dropdown menu showing "All".

At the bottom, there is a preview section showing a donut chart with a single segment labeled "FF:FF:FF:FF:FF:FF" and a value of "38".

At the bottom right, there are three buttons: **TEST**, **CONFIGURE**, and **CLOSE**.

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.

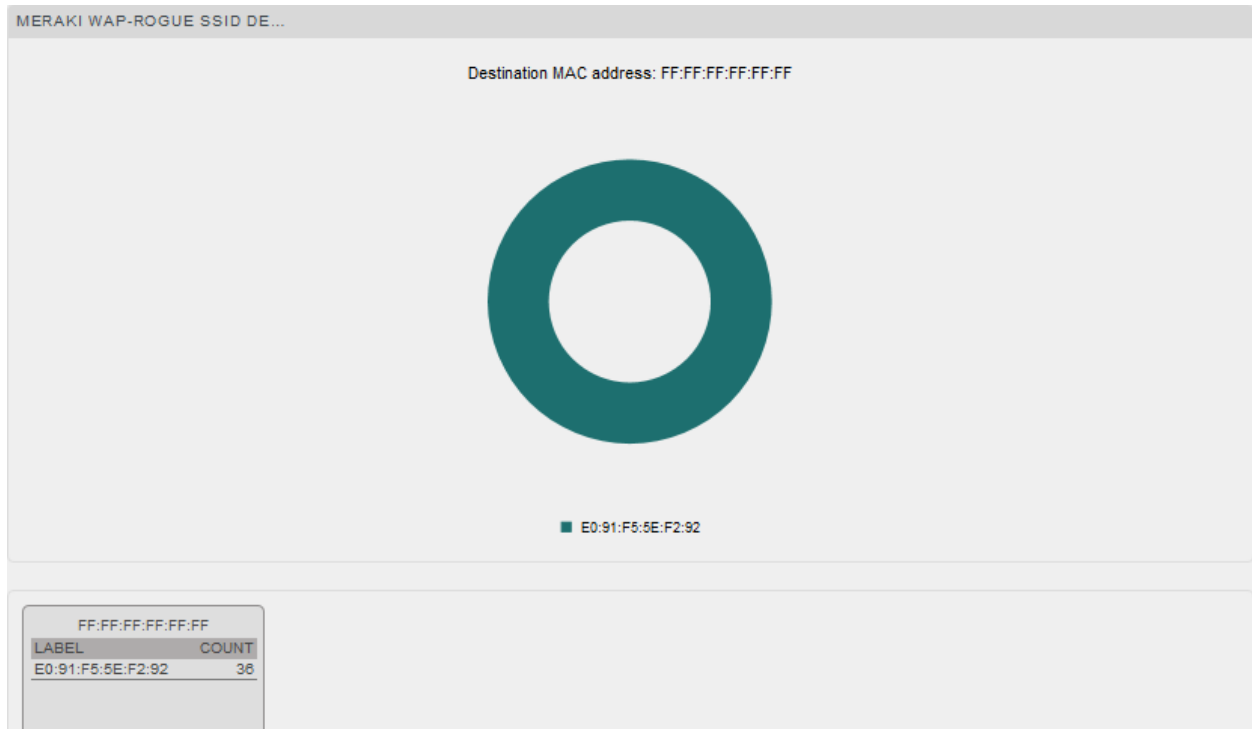


Figure 36

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

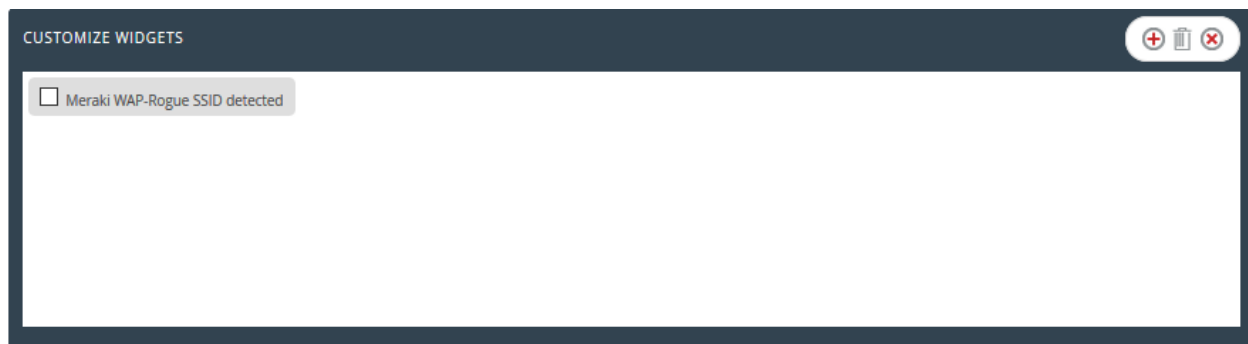




Figure 37

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

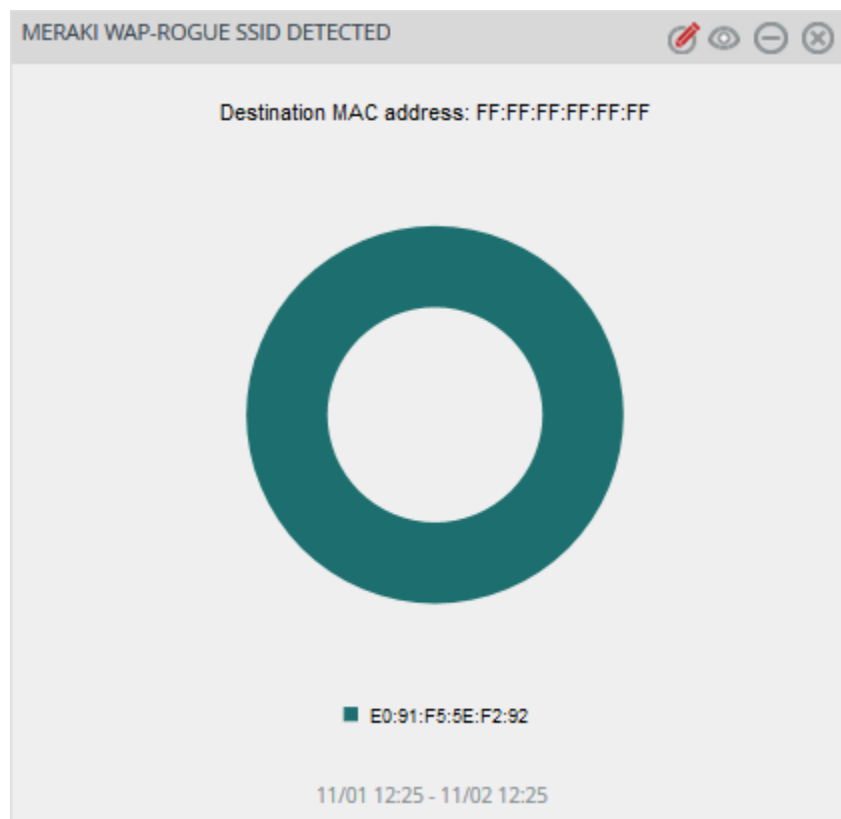


Figure 38