Integrate Meraki Switch

EventTracker v8.x and above

Publication Date: June 28, 2017
Abstract

This guide provides instructions to configure a **Meraki Switch** to send its syslog to EventTracker Enterprise

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version v8.x or above and Meraki Switch MS series.

Audience

Administrators who are assigned the task to monitor Meraki Switch events using EventTracker.
# Table of Contents

Abstract .................................................................................................................................................................... 1  
Scope ..................................................................................................................................................................... 1  
Audience .................................................................................................................................................................. 1  
Overview ............................................................................................................................................................... 3  
Prerequisites .......................................................................................................................................................... 3  
Integration of Meraki Switch with EventTracker manager ................................................................................. 3  
   Configuring Log Delivery ................................................................................................................................ 3  
   EventTracker Knowledge Pack .......................................................................................................................... 4  
   Flex Reports ....................................................................................................................................................... 4  
   Alerts .................................................................................................................................................................. 6  
   Knowledge Objects .......................................................................................................................................... 6  
Import Meraki Switch knowledge pack into EventTracker .................................................................................. 6  
   Alerts ................................................................................................................................................................ 7  
   Token Templates .............................................................................................................................................. 8  
   Knowledge Objects .......................................................................................................................................... 8  
   Flex Reports ................................................................................................................................................... 9  
Verify Meraki Switch knowledge pack in EventTracker ..................................................................................... 11  
   Alerts .............................................................................................................................................................. 11  
   Token Template ............................................................................................................................................ 12  
   Knowledge Objects ........................................................................................................................................ 12  
   Flex Reports .................................................................................................................................................. 13
Overview

Cisco Meraki offers a broad range of switches, built from the ground up to be easy to manage without compromising any of the power and flexibility traditionally found in traditional enterprise-class switches. The Meraki dashboard provides unified policies, event logs, and monitoring, making it easy to manage network deployments.

EventTracker helps to monitor events from Meraki Switches. It will trigger alerts whenever it detects an error or port block. It’s knowledge object and flex reports will help you to analyze STP changes, port changes and 802.1x authentications.

Prerequisites

- EventTracker v8.x or above should be installed.
- Meraki Switch MS series should be configured for forwarding logs.

Integration of Meraki Switch with EventTracker manager

Configuring Log Delivery

To configure a Meraki Switch to forward logs to a syslog server,

- Logon to Meraki Dashboard Login.
- From the Dashboard, navigate to Network-wide > Configure > General.

- Click Add a syslog server under logging.

Figure 1
Integrate Meraki Switch

• Set the **Server IP** to the IP address of the EventTracker.
• Set the **Port** to **514** (the default port for syslog).
• Add the role **Switch event log** to the **Roles** field in order to enable logging for those role.

---

**EventTracker Knowledge Pack**

Once logs are received by EventTracker manager, knowledge packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Meraki Switch.

**Flex Reports**

- **Meraki Switch-SP port role changes** – This report gives the information about switch port role which changes due to STP.
Sample logs:

<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>8/20/2017 4:38:38 PM</td>
<td>3333</td>
<td>ET-KP-1</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: Jun 15 07:54:54 10.101.116.23 1 1497527709.946035526 FrDodge1016_switch events Port 9 changed STP role from disabled to designated

---

• **Meraki Switch-Port status** – This report gives the information about the switch port changes.

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Port Number</th>
<th>Old Value</th>
<th>New Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/20/2017 04:38:38 PM</td>
<td>Webster_switch</td>
<td>11</td>
<td>100fdx</td>
<td>down</td>
</tr>
<tr>
<td>06/20/2017 04:38:38 PM</td>
<td>F1016_switch</td>
<td>9</td>
<td>down</td>
<td>1Gfdx</td>
</tr>
<tr>
<td>06/20/2017 04:38:38 PM</td>
<td>F1016_switch</td>
<td>9</td>
<td>1Gfdx</td>
<td>down</td>
</tr>
<tr>
<td>06/20/2017 04:38:38 PM</td>
<td>Logan_switch</td>
<td>11</td>
<td>down</td>
<td>1Gfdx</td>
</tr>
<tr>
<td>06/20/2017 04:38:38 PM</td>
<td>Meeting-Hall_switch</td>
<td>11</td>
<td>100fdx</td>
<td>down</td>
</tr>
<tr>
<td>06/20/2017 04:38:38 PM</td>
<td>Logan_switch</td>
<td>9</td>
<td>down</td>
<td>1Gfdx</td>
</tr>
<tr>
<td>06/20/2017 04:38:38 PM</td>
<td>F1016_switch</td>
<td>9</td>
<td>1Gfdx</td>
<td>down</td>
</tr>
<tr>
<td>06/20/2017 04:38:38 PM</td>
<td>Clarion_1029_switch</td>
<td>11</td>
<td>1Gfdx</td>
<td>down</td>
</tr>
</tbody>
</table>

---

Sample logs:

<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>8/20/2017 4:38:38 PM</td>
<td>3333</td>
<td>ET-KP-1</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: Jun 15 07:54:50 10.101.116.23 1 1497527705.841091862 FrDodge1016_switch events port 9 status changed from 1Gfdx to down

---

• **Meraki Switch-802.1x authentication details** – This report provides the information about the 802.1x authentication and de-authentication details.

---

Figure 5

Figure 6

Figure 7

Figure 8
Integrate Meraki Switch

Alerts

- **Meraki Switch: DHCP response blocked** - This alert will trigger when switch blocks the DHCP response from server.
- **Meraki Switch: STP port blocked** - This alert will generate when switch port role changes to blocked by STP.
- **Meraki Switch: VRRP errors** - This alert will generate when VRRP backup doesn’t receive a packet from VRRP master or when switch receives VRRP packet with incompatible configuration.

Knowledge Objects

- **Meraki Switch-802.1x authentication details** – This knowledge object will help us to analyze the log related with Meraki Switch’s 802.1x authentication and de-authentication details.
- **Meraki Switch-Port status** – This knowledge object will help us to analyze the log related to Meraki Switch’s port status.
- **Meraki Switch-STP port role changes** – This knowledge object will help us to analyze the log related to Meraki Switch’s port role changes due to STP.

Import Meraki Switch knowledge pack into EventTracker

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

- Categories
- Alerts
- Token templates
- Knowledge Objects
- Flex Reports

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

**Alerts**

1. Click **Alert** option, and then click the browse button.
2. Locate All alerts for meraki switch.isalt file, and then click the Open button.

3. To import alerts, click the Import button.

Token Templates

1. Click Parsing rules under Admin option in the EventTracker manager page.

2. Move to Template and click on import configuration icon on the top right corner.

3. In the popup window browse the file named All token template for meraki switch.ettd.

4. Now select all the check box and then click on ‘Import’ option.

![Figure 11]

Knowledge Objects

1. Click Knowledge objects under Admin option in the EventTracker manager page.

2. Locate the file named Meraki Switch Knowledge Object.etko.
3. Now select all the check box and then click on ‘Import’ option.

![Figure 12](image12)

4. Knowledge objects are now imported successfully.

![Figure 13](image13)

**Flex Reports**

1. Click Reports option, and select new(etcrx) from the option.
2. Locate the file named **All reports for meraki switch.etcrx**, and select all the check box.
3. Click the **Import** button to import the reports. EventTracker displays success message.

![Export Import Utility](image17.png)

**Figure 17**

**Verify Meraki Switch knowledge pack in EventTracker**

**Alerts**

1. In the EventTracker Enterprise web interface, click the **Admin** dropdown, and then click **Alerts**.

2. In search box enter **Meraki Switch** and then click the **Search** button. EventTracker displays alert of **Meraki Switch**.

![Alert Management](image18.png)

**Figure 18**
Token Template

1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Parsing rules.
2. On Template tab, click on the Meraki Switch group folder to view the imported Templates.

Knowledge Objects

1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Knowledge Objects.

2. In the Knowledge Object tree, expand Meraki Switch group folder to view the imported Knowledge objects.
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. Click on the Meraki Switch group folder to view the imported Meraki Switch reports.
Figure 21