Integrate Meraki Firewall
EventTracker v8.x and above

Publication Date: March 6, 2019
Abstract

This guide provides instructions to configure a Meraki Firewall to report its logs to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 8.x and later, and Meraki security appliance MX series.

Audience

Administrators, who wish to monitor Meraki Firewall using EventTracker Enterprise.
# Table of Contents

Abstract ........................................................................................................................................... 1  
Scope ............................................................................................................................................... 1  
Audience .......................................................................................................................................... 1  
Overview ......................................................................................................................................... 3  
Prerequisites .................................................................................................................................... 3  
Configure Meraki Firewall to forward logs to EventTracker ......................................................... 3  
  To configure the Meraki Firewall to forward logs to a syslog server .......................................... 3  
EventTracker Knowledge Pack .......................................................................................................... 5  
  Flex Reports .................................................................................................................................. 5  
  Alerts ............................................................................................................................................ 9  
  Categories and Saved searches ....................................................................................................... 9  
  Knowledge Objects ......................................................................................................................... 10  
Import Meraki Firewall knowledge pack into EventTracker ............................................................ 10  
  Category ....................................................................................................................................... 11  
  Alerts ............................................................................................................................................ 13  
  Knowledge Objects ......................................................................................................................... 14  
  Flex Reports .................................................................................................................................. 16  
Verify Meraki Firewall knowledge pack in EventTracker ............................................................... 18  
  Categories ..................................................................................................................................... 18  
  Alerts ............................................................................................................................................ 18  
  Token Templates ............................................................................................................................ 19  
  Knowledge Objects ......................................................................................................................... 19  
  Flex Reports .................................................................................................................................. 20
Overview

Meraki Firewalls are cloud-managed network security appliances designed to make distributed networks fast, secure, manageable by employing stateful inspection and auto-configuring VPN options.

EventTracker amasses and examines logs generated by Meraki Firewall to help an administration to monitor ids, alerts, VPN sessions, web traffic etc.

Prerequisites

- Administrative access to Meraki Dashboard.

Configure Meraki Firewall to forward logs to EventTracker

To configure the Meraki Firewall to forward logs to a syslog server

In your Meraki Dashboard:

1. Go to Network-wide.
2. On Configure tab, click on General.
3. At the General page, scroll down to the Logging section.
4. Click the Add a syslog server link to define a new server.
5. Click on the Add a syslog server link and type the IP address or name of EventTracker Manager in Server IP field.
6. Type Eventtracker Manager Port in the Port field.
7. Choose Appliance event Log, Security events, IDS Alerts, Flows and URLs; in Roles field. Mentioned log types are detailed below:

8. Click Save Changes at the bottom of the page.

Integrated device can be verified in the Systems pane of EventTracker advanced log search.
EventTracker Knowledge Pack

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

Flex Reports

- **Meraki Firewall- Blocked web content details**: This report provides information related to web content blocked by content filter.

Report Sample:

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Device Name</th>
<th>Server Address</th>
<th>Server Port</th>
<th>Blocked Category</th>
<th>Blocked URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/30/2016 07:53:40 PM</td>
<td>MX54</td>
<td>174.76.226.03</td>
<td>80</td>
<td>User-defined Blacklist</td>
<td><img src="http://img2.imagesbn.com/2940043b7533_p0_v2_s600_e404.png" alt="Image" />;</td>
</tr>
<tr>
<td>03/30/2016 07:53:49 PM</td>
<td>MX54</td>
<td>184.105.82.3</td>
<td>443</td>
<td>User-defined Blacklist</td>
<td><img src="http://q85.info/wp-content/uploads/2013/12/costed-the-wizard-saturday-july-48000.jpg" alt="Image" />;</td>
</tr>
<tr>
<td>03/30/2016 07:54:01 PM</td>
<td>MX54</td>
<td>67.215.65.130</td>
<td>80</td>
<td>Proxy Avoidance and Anonymizers</td>
<td><img src="http://api.gotmister.com/..." alt="Image" />;</td>
</tr>
<tr>
<td>04/01/2016 04:54:46 PM</td>
<td>MX54</td>
<td>52.86.88.235</td>
<td>443</td>
<td>Dating</td>
<td><img src="http://img2.imagesbn.com/2940043b7533_p0_v2_s600_e404.png" alt="Image" />;</td>
</tr>
<tr>
<td>04/04/2016 10:30:07 AM</td>
<td>MX54</td>
<td>174.76.226.93</td>
<td>80</td>
<td>User-defined Blacklist</td>
<td><img src="http://img2.imagesbn.com/2940043b7533_p0_v2_s600_e404.png" alt="Image" />;</td>
</tr>
</tbody>
</table>

Sample Log:

```
<table>
<thead>
<tr>
<th>event_computer</th>
<th>event_description</th>
<th>event_id</th>
<th>event_log_type</th>
<th>event_name</th>
<th>event_type</th>
<th>event_user_domain</th>
<th>event_user_name</th>
<th>log_source</th>
<th>svc_name</th>
<th>src_device_name</th>
<th>src_ip_address</th>
<th>src_port</th>
<th>srv_name</th>
<th>tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meraki 001</td>
<td>Meraki 001</td>
<td>10399</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User-defined Blacklist</td>
<td>Meraki 001</td>
<td>Meraki 001</td>
<td>10399</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

```
Figure 5
```

- **Meraki Firewall- VPN session details**: This report provides information related to VPN sessions establishment, connection or disconnection.

```
<table>
<thead>
<tr>
<th>event_computer</th>
<th>event_description</th>
<th>event_id</th>
<th>event_log_type</th>
<th>event_name</th>
<th>event_type</th>
<th>event_user_domain</th>
<th>event_user_name</th>
<th>log_source</th>
<th>svc_name</th>
<th>src_device_name</th>
<th>src_ip_address</th>
<th>src_port</th>
<th>srv_name</th>
<th>tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meraki 001</td>
<td>Meraki 001</td>
<td>10399</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User-defined Blacklist</td>
<td>Meraki 001</td>
<td>Meraki 001</td>
<td>10399</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

```
Figure 6
```
Integrate Meraki Firewall

**Report Sample:**

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Device Name</th>
<th>VPN Type</th>
<th>VPN Status</th>
<th>User Name</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/30/2016 07:10:26 PM</td>
<td>MX60</td>
<td>Site-to-site VPN</td>
<td>established</td>
<td>24.248.102.115</td>
<td>4500</td>
<td>70.168.84.32</td>
<td>4500</td>
<td>70.168.84.32</td>
</tr>
<tr>
<td>03/30/2016 07:10:36 PM</td>
<td>MX60</td>
<td>clientvpn</td>
<td>vpn_connect</td>
<td>astonia</td>
<td>70.168.64.32</td>
<td>119.168.251.122</td>
<td>119.168.251.122</td>
<td></td>
</tr>
<tr>
<td>03/30/2016 07:10:46 PM</td>
<td>MX60</td>
<td>clientvpn</td>
<td>vpn_disconnect</td>
<td>astonia</td>
<td>70.168.64.32</td>
<td>119.168.251.122</td>
<td>119.168.251.122</td>
<td></td>
</tr>
</tbody>
</table>

**Sample Log:**

```
<134>3 119.168.64.32 Meraki_Security_Appliance events Site-to-site VPN established ESPTransport 24.248.102.115[6500] => 70.168.64.32[4100]
```

- **Meraki Firewall - User authentication details:** This report provides information related to local user authentication attempt.

**Report Sample:**

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Device Name</th>
<th>Host MAC</th>
<th>User Name</th>
<th>User Details</th>
<th>Group Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/30/2016 03:36:33 PM</td>
<td>MX64</td>
<td>00:1E:0B:3E:42:CD</td>
<td>Tobey</td>
<td>CN=Teacher,OU=Teachers,OU=Users - Domain,DC=egales,DC=ocacadey,DC=org</td>
<td>CN=Teacher,OU=Teachers,OU=Users - Domain,DC=egales,DC=ocacadey,DC=org</td>
</tr>
<tr>
<td>03/30/2016 03:38:43 PM</td>
<td>MX64</td>
<td>90:B1:7C:79:1C:50</td>
<td>Janet</td>
<td>CN=Teacher,OU=Teachers,OU=Users - Domain,DC=egales,DC=ocacadey,DC=org</td>
<td>CN=Teacher,OU=Teachers,OU=Users - Domain,DC=egales,DC=ocacadey,DC=org</td>
</tr>
<tr>
<td>03/30/2016 03:36:54 PM</td>
<td>MX64</td>
<td>00:0C:DB:73:F1:70</td>
<td>student</td>
<td>CN=Student, OU=Students, OU=Users - Domain,DC=egales,DC=ocacadey,DC=org</td>
<td>CN=Student, OU=Students, OU=Users - Domain,DC=egales,DC=ocacadey,DC=org</td>
</tr>
</tbody>
</table>
Integrate Meraki Firewall

Sample Log:

- New 21-31/4/2016 PM
- User "Meraki2016"
- Client: 10.10.10.12 10.10.10.13 10.10.10.14

- DHCP Leases
  - Meraki Firewall - DHCP IP lease details: This report provides information related to IPs leased by DHCP.

  **Report Sample:**

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Device Name</th>
<th>Server MAC</th>
<th>Client MAC</th>
<th>Leased IP</th>
<th>Allocated DNS</th>
<th>Router IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/31/2016 06:03:47 PM M6X00</td>
<td>00:18:0A:02:85:88</td>
<td>00:16:0A:78:F9:79</td>
<td>172.16.37.220</td>
<td>172.16.1.200, 172.16.1.1, 172.16.1.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>03/31/2016 06:03:20 PM M6X00</td>
<td>00:18:0A:02:85:88</td>
<td>00:18:08:06:3F:88</td>
<td>172.16.37.210</td>
<td>172.16.1.200, 172.16.1.1, 172.16.1.2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Meraki Firewall - IDS alert details: This report provides information related to threats detected by IDS.

  **Report Sample:**

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Device Name</th>
<th>Source MAC</th>
<th>Source IP</th>
<th>Destination MAC</th>
<th>Destination IP</th>
<th>Protocol</th>
<th>Alert</th>
<th>Alert Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/29/2016 06:45:33 PM N6X00</td>
<td>00:19:0E:03:FF:CC</td>
<td>10.10.10.251</td>
<td>120.10.1.24</td>
<td>172.16.1.50</td>
<td>22</td>
<td>icmpv2</td>
<td>ingress</td>
<td>(icmpv2): Protocol mismatch</td>
</tr>
<tr>
<td>03/29/2016 06:45:23 PM N6X00</td>
<td>70.18.16.32</td>
<td>68B7</td>
<td>00:1B:21:82:73:00</td>
<td>172.16.1.70</td>
<td>9999</td>
<td>icmpv2</td>
<td>ingress</td>
<td>Data sent on stream not accepting data (icmpv2): NTP-RPC: DEFIP-CHAP</td>
</tr>
<tr>
<td>03/29/2016 06:45:34 PM N6X00</td>
<td>24-23:01:22:115</td>
<td>40:86</td>
<td>8.0.0.2</td>
<td>3218</td>
<td>icmpv2</td>
<td>ingress</td>
<td>(icmpv2): Protocol mismatch</td>
<td></td>
</tr>
<tr>
<td>03/29/2016 06:45:43 PM N6X00</td>
<td>72.14.68.70</td>
<td>80</td>
<td>34:15:52:50:00:0C</td>
<td>172.16.25.241</td>
<td>50449</td>
<td>icmpv2</td>
<td>ingress</td>
<td>(icmpv2): Protocol mismatch</td>
</tr>
<tr>
<td>03/29/2016 06:45:54 PM N6X00</td>
<td>20.08:06:0C:68:63</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Sample Log:

- Event ID: 140001971
- Event Type: Web
- Event Source: Meraki Firewall
- Event Source: N/A
- Log Source: Meraki Firewall
- Protocol Type: http
- Source IP: 172.16.1.253
- Destination IP: 172.16.4.65
- Event Type: GET
- Request Type: GET
- Requested URI: http://www.google.com

- Event ID: 140001971
- Event Type: Web
- Event Source: Meraki Firewall
- Event Source: N/A
- Log Source: Meraki Firewall
- Protocol Type: http
- Source IP: 172.16.1.253
- Destination IP: 172.16.4.65
- Event Type: GET
- Requested URI: http://www.google.com

**Meraki Firewall- Web traffic details:** This report provides information related to web traffic.

Report Sample:

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Device Name</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Request Type</th>
<th>Requested URI</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/29/2019 12:43:56 PM</td>
<td>MX600</td>
<td>00:10:0A:17:10:27</td>
<td>172.16.3.1</td>
<td>172.16.3.1</td>
<td>100</td>
<td>GET</td>
<td><a href="http://www.google.com">http://www.google.com</a></td>
</tr>
<tr>
<td>03/29/2019 12:41:07 PM</td>
<td>MX600</td>
<td>00:10:0A:17:10:27</td>
<td>172.16.4.65</td>
<td>172.16.4.65</td>
<td>80</td>
<td>GET</td>
<td><a href="http://www.google.com">http://www.google.com</a></td>
</tr>
</tbody>
</table>

Sample Log:

- Event ID: 140001971
- Event Type: Web
- Event Source: Meraki Firewall
- Event Source: N/A
- Log Source: Meraki Firewall
- Protocol Type: http
- Source IP: 172.16.1.253
- Destination IP: 50.194.23.12
- Event Type: GET
- Requested URI: http://example.com

- Event ID: 140001971
- Event Type: Web
- Event Source: Meraki Firewall
- Event Source: N/A
- Log Source: Meraki Firewall
- Protocol Type: http
- Source IP: 172.16.1.253
- Destination IP: 50.194.23.12
- Event Type: GET
- Requested URI: http://example.com

Figure 13

Figure 14

Figure 15
• **Meraki Firewall: Traffic flow details**: This report provides information related to inbound and outbound traffic flow.

**Report Sample:**

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Device Name</th>
<th>Source MAC</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Protocol Type</th>
<th>Rule Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/28/2016 11:57:00 AM</td>
<td>MX60</td>
<td>39:41:41:35</td>
<td>13943</td>
<td>11:4:18:74:11</td>
<td>16329</td>
<td>udp</td>
<td>1:0</td>
<td></td>
</tr>
</tbody>
</table>

**Sample Log:**

```
- Mar 01 23:49 PM 192.168.10.11 943156996721748587 MX60 flows src=192.168.10.254 dst=0.0.0.0 masq=0.0.0.0 protocol=udp sport=5562 dport=53 pattern=allow all
```

**Alerts**

- **Meraki Firewall: IDS alert detected** - This alert is generated when unusual traffic is detected by IDS.
- **Meraki Firewall: Suspicious content blocked** - This alert is generated when suspicious content is blocked by content filter.

**Categories and Saved searches**

- **Meraki Firewall: Content Filter** - This category provides information related to web content blocked by content filter.
- **Meraki Firewall: IDS** - This category provides information related to threats detected by IDS.
- **Meraki Firewall: Traffic flow** - This category provides information related to ingress and egress traffic flow.
Integrate Meraki Firewall

- **Meraki Firewall: Web traffic** - This category provides information related to inbound and outbound web traffic.
- **Meraki Firewall: Authentication Details** - This category provides information related to local user authentication attempt.
- **Meraki Firewall: VPN session** - This category provides information related to VPN sessions establishment, connection or disconnection.
- **Meraki Firewall: AMP** – This category provides information related to meraki firewall advance malware protection and detection details.

Knowledge Objects

- **Meraki Firewall Advanced Malware Protection** - This knowledge object helps to analyze logs related to meraki firewall advanced malware protection.
- **Meraki Firewall Authentication Details** - This knowledge object helps to analyze logs related to user authentication and authorization activities.
- **Meraki Firewall Content Filter** - This knowledge object helps to analyze logs related to web content blocked by content filter.
- **Meraki Firewall IDS** - This knowledge object helps to analyze logs related to threats detected by IDS.
- **Meraki Firewall Traffic Flow** - This knowledge object helps to analyze logs related to network traffic flow details.
- **Meraki Firewall VPN** - This knowledge object helps to analyze logs related to VPN sessions establishment, connection or disconnection.

**Import Meraki Firewall knowledge pack into EventTracker**

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

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

**Category**

1. Click **Category** option, and then click the browse button.
2. Locate **Category_Cisco Meraki Firewall.iscat** file, and then click the **Open** button.

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

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

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

2. Locate **Alert_Cisco Meraki Firewall.isalt** file, and then click the **Open** button.

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

Figure 21

![Figure 21](image)

Figure 22

![Figure 22](image)
4. Click **OK**, and then click the **Close** 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 **Template_Cisco Meraki Firewall.ettd**.

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

![Figure 23](image)

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

**Knowledge Objects**

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

2. Locate the **KO_Cisco Meraki Firewall.etko** file.
3. Click the ‘Upload’ option.
4. Now select all the check box and then click on ‘Import’ option.

![Figure 25]

5. Knowledge objects are now imported successfully.

![Figure 26]

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

On EventTracker Control Panel,

1. Click **Reports** option, and select new (*.etcrx) from the option.

![Export Import Utility](image)

2. Locate the Flex **Report_Cisco Meraki Firewall.etcrx** file and select all the check box.
3. Click the **Import** button to import the reports. EventTracker displays success message.

4. Click **OK**, and then click the **Close** button.
Verify Meraki Firewall knowledge pack in EventTracker

Categories

1. Logon to EventTracker Enterprise.
2. Click Admin dropdown, and then click Categories.
3. In Category Tree to view imported categories, scroll down and expand Cisco Meraki Firewall group folder to view the imported categories.

![Figure 30](image)

Alerts

1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Alerts.
2. In search box, enter Meraki firewall and then click the Search button.
   EventTracker displays alert of Meraki Firewall.

![Figure 31](image)
Token Templates

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

![Figure 32](image)

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 Firewall group folder to view the imported Knowledge objects.

![Figure 33](image)
Flex Reports

1. In the EventTracker Enterprise web interface, click the Reports menu, and then select Report Configuration.

![Figure 34](image1.png)

2. In Reports Configuration pane, select Defined option.
3. Click on the Meraki Firewall group folder to view the imported Meraki Firewall reports.

![Figure 35](image2.png)