Monitoring the Wireless Network

The Meraki Cloud makes it easy to monitor the status of many Access Points within a network as well as the traffic passing on the wireless network. Larger distributed customers will likely have multiple organizations. Meraki offers a number of Organization level monitoring tools in addition to the monitoring tools available at the network level that are discussed in this article.

Wireless Summary Report

A network administrator can obtain rich network analytics from the Summary Report page under the Monitor tab. This report provides information about the Meraki wireless network since its inception, including some of the following statistics:

- Top 10 APs by data consumption and number of client logins
- Top 10 clients by data consumption
- Usage breakdown by SSID and AP model
- Top client device manufacturers and OS types by number of client logins and data consumption
The report can be customized and viewed for statistics over a certain time period to allow for statistical analytics for a specific day, week or month.

The report can be e-mailed on a configurable schedule for constant visibility. Administrators can configure one or more e-mail addresses under the 'Schedule monthly e-mails' tab if they wish to send the summary report to multiple people. They can also add their organization’s logo to the report. More information on this feature is found here.

Traffic Analytics and Layer 7 Visibility

Meraki Enterprise networks offer powerful application visibility and control tools. Packet inspection engines running custom parsers in each AP provide this information by fingerprinting and identifying applications and application groups. Traffic Shaper then provides the ability to create custom per-user shaping policies based on this application-level visibility. Since Meraki’s parsers are designed to run at line rate, there is no performance decrease when enabling Traffic Analysis or Traffic Shaping.

Next to the usage graph at the top of the screen is a pie chart that can display a breakdown of the traffic currently displayed on the page by application, HTTP content type, port number or custom criteria. The gray arrows flip from one chart to the next. Custom pie charts can be configured on the Network-wide Settings page under the Configure tab.

Clicking on either the pie chart itself or the “More” link underneath the pie chart will open up the Traffic Analysis Details page, showing a detailed list of the specific applications and content types that make up the data shown in the pie chart. The applications have been assigned to groups to make classifying applications and creating shaping policies simpler.
Clicking on a particular application or content type within the Traffic Analysis Details page will take you to the Rule Details page, where you will find detailed information about that particular application or content type rule, including which users are contributing to usage of this type and details such as which application group that item belongs to, port number, description of the application or rule and links to additional information.

For broad categories such as ‘Miscellaneous secure web’, it is now possible to get a more granular breakdown of hostnames and IP addresses that comprise this category. This functionality can be enabled by enabling the more detailed ‘Traffic Analytics’ capability under the Network-wide settings page. More information is available on the Traffic Analytics page.

Client List

The Clients page shows how the network is being used and by which client devices. The page includes the following features:

• Displays clients that have associated on any SSID advertised by the wireless network, or only those clients that have associated on a given SSID. This can be selected using the SSID drop down menu at the top of the screen.
• Search for clients by MAC, OS, device type or NetBIOS/Bonjour name. (Using Search)
• Zoom control, which enables the administrator to see only those clients that have associated within the specified time span.
• The administrator can also click on the “blocked list” to view only those clients on the MAC blacklist.
• Like the Access Points page, the Clients page has a list that can be customized (adding, removing, and reordering columns) and sorted (by clicking on a column header).
• The “Description” column shows the device name, if it can be determined (i.e., through NetBIOS); otherwise, it simply displays the device’s MAC address.
• The “Operating system” column shows the operating system of the device, which is determined through OS fingerprinting (the unique pattern by which a particular operating system requests an IP address via DHCP).
• An administrator can mouse over a row in the device list to see a new line appear in the usage graph, which depicts the fraction of total bandwidth that the highlighted device used.

More information on client visibility can be found here.

---

**Access Point List**

The Access Point list is a convenient way to make it easier to find, sort and filter APs in a large network with hundreds or thousands of APs is using AP tagging.

---

**AP Tagging**

Lphanumeric tags can be assigned to access points to create groups of APs by location (e.g. Building_1, Floor_4, West_Campus, etc.) or by other criteria. The Access Points page is searchable by tag to make filtering for specific groups of APs fast and easy.

AP’s can be tagged individually on the AP details page, or in the AP page by selecting multiple AP’s and choosing Action->Add Tags.

---

**Export Access Point Data**

List data on the Access Points pages can be exported in XML format for further processing and analysis. An administrator can click on the “Download as XML” link to retrieve the data. Most spreadsheet programs, such as Microsoft Excel, can open an XML file.

---

**Maps and Floor Plans**

The aerial map shows the latest information about the APs in the network. The options in the upper-right corner enable an administrator to view the APs on top of a graphical map, a satellite image, or a hybrid view. In the upper-left corner, the arrow controls enable the administrator to pan. Panning can also be achieved by clicking-and-dragging the map. Below the arrow controls, a scale control enables the administrator to adjust the zoom level. The zoom level can also be controlled with the magnifying glass next to the arrow controls, or by double-clicking on a particular region to zoom into.

An administrator can click on an AP to get its name, its mesh mode (mesh gateway or mesh repeater), the number of users that have associated to it in the last 24 hours (also indicated by the number inside the AP), and the amount of data that it has transferred in the last 24 hours. Gray lines between APs represent mesh links. Mousing over a mesh repeater highlights a line that shows the path that the AP is taking through the mesh network to reach a mesh gateway (and the LAN).
The “Gear” box in the upper right part of the map lets users select what the numbers in the APs represent (e.g., number of clients connected or mesh hops to gateway), as well as preferences about how to display mesh links.

The “Current clients” link under the network name in the upper left corner, when clicked, will open up a table showing a summary of the distribution of current clients at that moment across the various SSIDs and channels in the network.

Clicking on the link directly above the network name in the upper left corner or selecting the All-network Overview option under the Network drop-down selector at the top of the screen will take the administrator to the All Network Overview page.

More information on setting up the Map is found in this KB article.

---

**AP Color Codes**

On the map and in the list the status of the AP is indicated by its color:

- Green: The AP is not reporting any problems.
• Yellow: The AP is up, but experienced a problem recently. In some cases, the administrator may be able to clear this alert on the Access Points page.
• Red: The AP is currently down.
• Gray: The AP has been down for more than 7 days.

SNMP Polling

It is also possible to use SNMP to monitor certain parameters on your network with 3rd party monitoring systems such as Solarwinds. Meraki supports SNMP polling of both the Meraki Cloud as well as the Meraki APs directly.

Configuration info on these two polling methods is as follows:

SNMP Polling the Meraki Cloud

More information on Polling the Meraki cloud is on the Organization overview article and the SNMP Overview and Configuration article.

SNMP Polling Meraki APs directly

At the network level Access Points may be polled directly. SNMP polling can be enabled on the Configuration > Network-wide settings page. Detailed configuration instructions, including a list of the OID parameters that can be polled, is available here.

Syslog

MR access points can be configured to send syslog data to any server that accepts Syslog traffic on the Network-wide > General settings page. Currently, the following information is supported:

• Event logs
• URL logs
• Traffic flows
Sample Syslog Post

May 05 13:54:44 24.136.237.228 logger:  <134>1 0.0 pavan events type=disassociation radio='0' vap='0' channel='1' reason='8' instigator='1' duration='60706.779996820' full_conn='0.150005690' ip_resp='0.170005003' ip_src='10.111.191.59' http_resp='0.150005690' arp_src='10.111.191.59' aid='1664629283' dns_server='10.128.128.128' dns_req_rtt='0.039998076' dns_resp='0.099997939' session='0' xid='0.010009056' arp_resp='0.010009056' aid='1664629283' mac='E4:CE:8F:29:6E:5A' source='10.111.191.59' xid='0.010009056' session='0' xid='0.010009056'
May 05 13:54:44 24.136.237.228 logger:  <134>1 0.0 pavan events type=association radio='0' vap='0' channel='1' rssi='22' aid='532435667'
May 05 13:54:44 24.136.237.228 logger:  <134>1 0.0 pavan flows allow src=10.111.191.59 dst=23.1.61.15 mac=E4:CE:8F:29:6E:5A protocol=tcp sport=61289 dport=80