Alerts and Notifications

Overview

There are a number of options available in the Meraki dashboard for email alerts to be sent when certain network or device events occur. This article outlines which options are available for each product and provides additional considerations when using network alerts and organization-wide notifications throughout the dashboard.

Configuring Network Alerts

Network alerts can be configured in the dashboard under Network-wide > Configure > Alerts.

Network alerts can be configured by specifying the default recipients for selected alerts and by configuring additional recipients on a per-alert basis. There are two options to denote who will receive email alerts:

- **All network admins**
  This will send email alerts to both full and read-only network admins. This does not include organization admins.

- **Other email addresses**
  This allows for a custom list of recipients, where email alerts are sent to all email addresses listed. To specify other email addresses, type an email address into the default recipients field and hit enter.

All network alerts will be sourced from the same email address. To ensure that alerts are not being lost to a spam filter, please be sure to add alerts-noreply@meraki.com as a trusted email source.

Network-Wide Alerts

The following alerts can be configured on multiple Cisco Meraki products when:

- **Configuration settings are changed**
  Available on all platforms; sends an email if any configuration change is made in the dashboard.

- **A VPN connection comes up or goes down**
  Available on both the MR and MX platforms; sends an email if a configured VPN tunnel goes up or down.
  Note: for MX, only AutoVPN connections are monitored for alerts. The connectivity status of non-Meraki site-to-site VPN cannot be monitored from both sides of the tunnel.

- **A rogue AP is detected**
  Sends an alert if a rogue AP is detected on the network.

- **Network usage exceeds (x) KB/MB/GB/TB in 20 minutes/4 hours/1 day**
  Sends an alert if the specified amount of data is seen on the network for the specified time frame.
MR Alerts

Alerts can be configured for the following MR access point events:

- **A gateway goes offline for (x) minutes**
  Sends an email if any gateway AP is unreachable from the dashboard for the configured number of minutes. Please note that the AP may still be functioning, this only indicates that it is unable to contact the dashboard.

- **A repeater goes offline for (x) minutes**
  Sends an email if any repeater AP is unreachable from the dashboard for the configured number of minutes.

- **A gateway becomes a repeater**
  Sends an email if a gateway AP loses its link to the network and comes online as a repeater. For more information on this behavior, please refer to our documentation regarding Gateway AP Switches to Repeater.

Additional alerts can be configured to maintain visibility on wireless Bluetooth® clients:

Detected devices will be displayed in the Wireless > Monitor > Bluetooth clients page. The name of the Bluetooth® client can also be edited for easier tracking. Email alerts can be enabled to trigger when the device becomes visible by the access point and when the device is no longer visible.
Alerts

Send an email when a device becomes visible again: Off
Send an email when a device is no longer visible: Off
edit alerts »

MX Alerts

Alerts can be configured for the following MX security appliance events:

• **A security appliance goes offline for (x) minutes**
  Sends an email if the MX is unreachable from the dashboard for the configured number of minutes. Please note that the MX may still be functioning, this only indicates that it is unable to contact the dashboard.

• **The primary uplink status changes**
  Sends an email if the status of the primary uplink changes, which could be a failover event or downed link.

  **Note:** It is not recommended to configure this alert if you are running an appliance with only a cellular uplink, as you may see false alerts about failing over to a cellular uplink if the node reboots or experiences an issue with connectivity. In such situations, it’s recommended to use the cellular connection state alerts.

• **The DHCP lease pool is exhausted**
  Indicates that the MX has run out of available IPs in one or more of its configured DHCP scopes and is unable to provide an IP address to a requesting client.

• **An IP conflict is detected**
  Sends an email if the MX has observed traffic from multiple MAC addresses using the same IP address. **Note:** Due to the nature of certain device types, this event may occur as a result of normal network behavior. For a common example, please refer to our documentation regarding IP Conflict Events Triggered by iOS Devices.

• **Cellular connection state changes**
  Sends an email if the appliance establishes or loses its connection to the cellular network.

• **A rogue DHCP server is detected**
  Sends an email if the MX observes multiple MAC addresses responding to DHCP Discover or DHCP Request messages. This can occur if a DHCP relay server is configured on a VLAN where the MX is configured to respond to DHCP. For more information, please refer to our documentation regarding DHCP configuration in the dashboard.

• **A warm spare failover occurs**
  Sends an email if the primary MX of a high-availability pair fails over to the spare, or vice versa. For more information, please refer to our documentation regarding Troubleshooting MX Warm Spare.

• **Malware is blocked**
  This alert will be triggered when a malicious file download is blocked.

• **Malware is downloaded**
  This alert will be triggered when a file previously downloaded on your network is determined to be malicious in retrospect.

• **Clients connect or disconnect from the LAN**
Sends an email if select clients connect or disconnect from the LAN, as observed by the MX. The MX sends an ARP request to the client approximately every ten seconds to monitor its connectivity status. If the MX does not receive an ARP reply from the client after approximately 35 seconds, it considers the client to be disconnected. Once the client begins sending data through the MX and responding to ARP requests, it will again be marked as connected.

**Note:** This alert is not available on MX security appliance networks that are set to track clients by IP address. Client tracking can be configured in Security & SD-WAN > Addressing & VLANS > Client tracking.

- **HTTPS inspection certificate error occurs**
  This error may occur when the security appliance has been factory reset. Re-upload the certificate to restore HTTPS inspection functionality.

**Wireless MX/Z-Series Alerts**

The following additional alert is available for wireless MX devices or the Z-series teleworker gateway:

- **A rogue AP is detected**
  Sends an alert if a rogue AP is detected on the network

**MS Alerts**

Alerts can be configured for the following MS switch events:

- **A switch goes offline for (x) minutes**
  Sends an email if a switch is unreachable from the dashboard for the configured number of minutes. Please note that the switch may still be functioning, this only indicates that it is unable to contact the dashboard.

- **A new DHCP server is detected on the network**
  Sends an email if a DHCP offer, ACK, or NACK message from a new MAC address (not seen in the last month) is observed by the switch.

- **A client is detected sharing its IP address via NAT**
  Sends an email if the switch detects a device that appears to be using Network Address Translation (NAT). For more information on this behavior, please refer to our documentation regarding [NAT Detection on MS Switches](#).

- **Any/specific port(s) goes down for more than (x) minutes**
  Sends an email if the switch port(s) specified goes down for more than the configured number of minutes.

- **Any/specific port detects a cable error**
  Sends an email if the switch port specified detects an issue with the connected cable.

- **Any/specific port changes link speed**
  Sends an email if the switch port specified renegotiates or fails over to another link speed.

**Note:** Alerting for a specific port (or ports) requires the port(s) to be tagged under Switch > Switch ports. If no ports are tagged, "any port" will be the only option in the drop-down menu. Please note that multiple ports can share the same tag.

- **A power supply goes down**
  Sends an email if one of the removable power supplies on the MS fails.

- **A redundant power supply is powering a switch**
  This alert will be triggered if redundant (not modular) power supplies are providing power to a switch.
• **Unidirectional link detection (UDLD) errors exist on a port**
  This alert will be triggered if UDLD errors are seen on a switch port.

• **A switch is operating at critical temperature**
  This alert will be triggered if a switch detects that it is operating at critical temperature. Critical temperature is a serious scenario requiring consideration of the operating environment of the switch. This alert is supported for the MS120 series, MS220-24P, MS210 series, MS225 series, MS250 series, MS320 series, MS350 series, MS410 series, and MS425 series.

The Switch > Monitor > DHCP Servers page displays information about any DHCP servers seen by Meraki switches on the LAN. From this page, administrators can configure email alerts.

The Email Alerts drop-down menu can be used to send alerts to administrators when a switch detects a new DHCP server on the network. This can also be configured from the Network-wide > Configure > Alerts page, under the Switch heading.

---

**SM Alerts**

Systems Manager offers a number of advanced alert options, unique from the rest of the Meraki product line.

Several alerts can be configured to inform you and other network administrators of modifications made to your Systems Manager network. On a standalone Systems Manager network, these can be configured under Systems Manager > Configure > Alerts. In a combined network, all alerts are configured under Network-wide > Configure > Alerts and administration.

• **Software Alerts**

  Checking this option will enable the Meraki cloud to send a nightly email to the network administrators listed in the “Delivery Settings” section regarding Systems Manager clients that have software installed matching the listed regular expression*.

  *The expression field must be a valid POSIX regular expression, and the search is performed case insensitive. For example, if you want to receive a complete list of all software installed in the last day, you would enter “.*” (without quotes). If instead you wanted to be alerted when Starcraft or Warcraft is installed, you would enter “starcraft|warcraft” (without quotes).

• **Connectivity Alerts**

  Checking this option will enable the Meraki cloud to send an email* whenever a client device with a specific tag stops checking-in for more than the determined time threshold. This will alert an administrator of any abnormal client outage.

  *You will also receive an email when the client comes back online.

  Client tags can be set by clicking on a client from the Monitor > Clients tab, clicking edit, and then editing the tags field. Please see Tagging Devices for more information.

• **Geofencing Alerts**

  This section gives you the option to enable the Meraki cloud to send an e-mail whenever a client device violates a geofencing policy. You can also check the option to have an e-mail sent when a client re-enters their geofencing region after violating a geofencing policy.

• **Enrollment Alerts**

  Checking this option will enable the Meraki cloud to send an email when a client device enrolls in a network. This will alert an administrator when a device is added to a network.

• **Mobile Device Management**

  If a client device managed by Systems Manager has its Meraki Management profile removed, checking this option will allow the MCC to send an email to the network administrators listed in the “Delivery Settings” section.
It is very important to ensure that your managed devices retain the Meraki management profile, as this is the way your client devices check in to the Meraki cloud.

For iOS devices, there is currently no way to password-protect the management profile from being deleted. From the end user perspective, removing the management profile will result in the possible loss of wireless connectivity, apps, and any enhancements gained from being managed by a Systems Manager network.

**Delivery Settings**

There are three options for selecting the recipient of an e-mail alert. E-mail alerts can be sent to a network owner, all network owners, or a specified e-mail list.

*The “Other e-mail addresses” option will accept one email per line.*

---

**MV Alerts**

Network-wide alerts can be configured for the following MV camera event:

- **A camera goes offline for (x) minutes**
  Sends an email if a camera is unreachable from the dashboard for the configured number of minutes. Please note that the camera may still be functioning, this only indicates that it is unable to contact the dashboard.

- **A camera has a potential issue with Cloud Archive**
  Sends an email if one or more cameras in the network are detected to have an issue with video upload to Cloud Archive. The email is only sent once for the entire network and not for each individual camera. This alert is enabled by default on all networks which include cameras with cloud archive licenses.

**Motion Alerts**

Motion events get triggered when a portion of an area in the MV’s field of view is changed, causing motion to be detected. When this occurs, an alert will be generated which will be directly sent to the configured email address. An example of what the email alert looks like is shown below:
By default, your motion alert email will include a motion recap image that corresponds to the relevant event. [More on Motion Recap here](#). However, if you have [Restricted Bandwidth Mode](#) enabled, you will not see an image.

If you are unable to see a Motion Recap image and you do not have Restricted Bandwidth Mode enabled, it is likely that SSL inspection is utilized upstream of a Meraki security camera. If so, please disable this to ensure you can view Motion Recap images.
Configuring Motion Alerts

1. Navigate to Cameras > Monitor > Cameras
2. Select a node from the camera list page
3. Navigate to Settings > Motion Alerts to configure alerts for this specific node

• Alert scheduling

   Motion alerts can be configured to be sent whenever an alert is triggered or as a summary on a schedule. Templates can be used for schedule-based recording or new schedules can be created. Increasing minimum event duration will reduce noise from various minor events that may be inconsequential.

• Areas of interest

   Allows you to select specific portions of the frame that you want to receive motion alerts for.

• Motion sensitivity

   Higher motion sensitivity means that relatively smaller objects passing in front of the camera will generate an alert. On the other hand, lower sensitivity means that only larger objects passing in front of the camera will generate an alert.

• People detection

   Alerts from a camera can be minimized by only triggering alerts when a person is detected by the camera anywhere in its field of view.

For an overview of this feature, along with additional configuration parameters, please see our Motion Alerts article.

MT Alerts

The MT line of sensors have robust and easy-to-set-up alerts in order to notify a user in the event of configured threshold violations. This is accomplished through the creation and assignment of alert profiles.

For information on setting up MT alert profiles, see the Sensor Alert Profiles article.

Organization-Wide Alerts/Notifications

Organization alerts can be configured in the dashboard under Organization > Settings.

Licensing Notifications management
This document describes options listed in Manage alerts section.

**Special Announcements**

Special announcements are notifications that may not be network-specific. Example: Scheduled maintenance notification for Meraki dashboard.

### Administration

- Licensing notifications
- Send licensing notifications only to organization admins
- Special announcements
- All organization admins with full access
- A mailing list you manage...

> All organization-wide alerts will be sourced from the same email address. To ensure that alerts are not being lost to a spam filter, please be sure to add alerts-noreply@meraki.com and noreply-support@meraki.com as trusted email sources.

---

**Meraki Insight (MI)**

Utilizing Meraki Insight, an MX can be configured to monitor and track traffic associated with specific web applications. This data is tracked on a per-flow basis at the MX, then the relevant flows are aggregated into categorical groups based on their associated application and sent over an encrypted connection to the Meraki Cloud Controller for further analysis before populating that flow data into the Insight feature on the dashboard.

For a detailed overview of this feature please see our MI Web App Health article.

---

**Alert Configuration**

---

**Additional Alert Considerations**

### SPAM Filters

- All network alerts will be sourced from the same email address. To ensure that alerts are not being lost to a spam filter, please be sure to add alerts-noreply@meraki.com as a trusted email source.
- All organization-wide alerts will be sourced from the same email address. To ensure that alerts are not being lost to a spam filter, please be sure to add noreply@meraki.com, and noreply-support@meraki.com as trusted email sources.
Receiving Email Alerts via SMS

It is possible to have email alerts forwarded as an SMS to a phone number. When configuring email recipients, follow the best practices below:

- Alltel: phonenumber@message.alltel.com
- AT&T: phonenumber@txt.att.net
- T-Mobile: phonenumber@tmomail.net
- Virgin Mobile: phonenumber@vmobl.com
- Sprint: phonenumber@messaging.sprintpcs.com
- Verizon: phonenumber@vtext.com
- Nextel: phonenumber@messaging.nextel.com
- US Cellular: phonenumber@mms.uscc.net

Alert Rate Limiting

All alerts are logged to the Network-wide > Monitor > Event Log and are sent as emails depending on the settings outlined in this article. The alerts listed below are rate limited to 25 alerts per 10 minutes, per event type, per dashboard organization. This means that if 35 alerts for "Client IP conflict detected" are triggered at the same time in your organization, they will all be logged to the event log, but only the first 25 will be sent to your organizations' administrators. This rate-limit also applies to Webhooks.

Alert events that are rate limited:

- DHCP leases exhausted
- Client IP conflict detected
- Cellular came up
- Cellular went down
- Client connectivity changed
- Failover event detected
- Rogue DHCP server detected
- VPN connectivity changed
- Devices operating at critical temperature
- UPS output source changed
- HTTPS inspection certificate error
- Uplink status changed
- Client connected to another network

Syslog, API, Webhooks, and SNMP

Syslog, API, and SNMP each have their own benefits for network and device reporting. Below is a list comparing each option with their possible use-cases.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Meraki</th>
<th>SNMP</th>
<th>API</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detailed information for network events</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>(device flows, client connectivity, config changes, etc.)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real-time information gathering</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Real-time network statistics</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Device information gathering</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Detailed device statistics</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Network-wide information gathering</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Organization-wide information gathering</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Proactive alerts for critical events</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Automation capabilities</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Application integration</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cloud-centric</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Scalability</td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

A detailed overview and configuration guide of the reporting options in the table above can be found in our [Meraki Device Reporting - Syslog, SNMP, and API](#) article.