Meraki Event Log

The event log can be used to track a number of events occurring across a network. This article describes how to navigate the event log and filter out extraneous information for troubleshooting and monitoring purposes.

Using the Event Log

Each Meraki network has its own event log, accessible under Network-wide > Monitor > Event log. In a combined network, click the drop-down menu at the top of the page and select the event log for one of the following options:

- for security appliances to display information about the MX security appliance in this network.
- for access points to display information about all MR wireless access points in the network.
- for devices to display information about all managed SM clients in the network.
- for switches to display information about all MS switches in the network.
- for cameras to display information about all MV cameras in the network.

Filtering the Event Log

While the event log provides a thorough timeline of events on the network, it is usually unnecessary to view all events across all devices. The following options are available to filter down the event log as needed:

Filtering by Client or Cisco Meraki Device

Filtering events to a specific client can help troubleshoot individual connectivity issues, including IP addressing and network authentication. Entering the MAC address, hostname, or custom name in the Client field will display only events affecting that client, excluding other client information and device events.

An additional, product-specific field can be used to filter to events relevant to a specific device in the network. This can be helpful when troubleshooting a particular Meraki device on the network, or a client connected directly to a specific device.

Filtering by Date and Time

The event log shows all events for clients and devices, starting with the most recent event by default. This time frame can be adjusted using the Before field, displaying only events that happened at or before the specified time.

The event log time shares the time zone set for the network itself. More information on changing this time zone can be found here.

Filtering by Event Type

Even when filtering by a single device or client, there can be quite a few events. Selecting specific events to display or excluding specific event types can significantly decrease the amount of data to sort through.
Each Meraki product offers a different variety of reported events, as listed below:

**MX Security Appliance**

The following types of events will be reported by MX security appliances:

- Auth: Splash page authentication
- BGP: BGP notification and session events
- Cellular: 3G/4G connectivity
- Client Status: Client connectivity
- DHCP: DHCP leases and related errors
- Events dropped: Too many events were generated too quickly, creating an Events Dropped event
- Filtering: Content filtering blocks
- Intrusion Detection: IDS (Advanced Security only)
- IP conflict: Detected IP conflicts on the network
- Appliance status: Primary uplink events
- Status: Device status events
- OSPF: Events related to OSPF routing
- Route tracking: Route connection change and network test events
- Meraki VPN: AutoVPN connectivity events
- VRRP: Warm spare transition
- Web caching: Web cache events
- Non-Meraki / Client VPN: Non-Meraki and Client VPN connectivity events

**MR Access Points**

The following types of events will be reported by MR access points:

- 802.11: Wireless association and disassociations
- 802.1X: RADIUS authentication and deauthentications
- Auth: Splash page authentication
- AutoRF: Channel scans and TX power changes
- DFS: Events related to Dynamic Frequency Selection
- DHCP: DHCP leases and related errors
- Events dropped: Too many events were generated too quickly, creating an Events Dropped event
- L3 roaming: Events related to Layer 3 Roaming
- Status: Device status events
- Meraki VPN: VPN tunnel drops and connectivity events
- Air Marshal: Packet floods and wireless security events
- WPA: WPA authentication and deauthentications

Learn more about Common wireless event log messages.
SM Clients
The following types of events will be reported by managed SM clients:

- Command Line: Command line request events
- Live Tools: Recent usage of live tools on client devices
- MDM: Detailed information about changes in device management
- Remote Desktop: Usage of the remote desktop tool

MS Switch
The following types of events will be reported by MS switches:

- 802.1X: RADIUS authentication and deauthentications
- Auth: Splash page authentication
- DHCP: DHCP blocked and no leases available events
- Events dropped: Too many events were generated too quickly, creating an Events Dropped event
- Status: Device status events
- OSPF: Events related to OSPF routing
- Switch port: Port status and STP information
- Switch status: Power and temperature events
- VRRP: Warm spare transition

Learn more about MS event log entries and definitions.

MV Cameras
The following types of events will be reported by MV cameras:

- Camera: Events related to camera components
- DHCP: DHCP leases and related errors
- Events dropped: Too many events were generated too quickly, creating an Events Dropped event
- Status: Device status events