GUIDE

MANAGED NETWORK EDGE

Portal User Guide - Cisco Meraki™

©2022 Charter Communications. All rights reserved.

Spectrum ENTERPRISE

Table of contents

Introduction

The Meraki cloud is the backbone of the Meraki solution, enabling instant onboarding access to all features inside the Managed Network Edge (MNE) Portal. The MNE Portal is a centralized, web browser-based tool used to monitor and configure Meraki devices and services within an organization's network.

This document aims to provide an overview of some of the main features available in the MNE Portal (Meraki Dashboard) as it relates to Meraki's MX appliance and the Security and SD-WAN portal sections, which include common configuration and visualization use cases.

Goals of this document

Our goals for this document are to:

- Present step-by-step guidance on how to navigate to, as well as to understand, the main components of the Security, SD-WAN, WiFi, Switch, and Sensor sections of the MNE Portal.
- Provide best use case and user level details to assist in training internal user groups.
- Highlight key considerations that may improve the reader's understanding of the MNE portal and the overall MNE solution.

This document is also meant to serve as additional reference in assisting knowledge transfer activities.

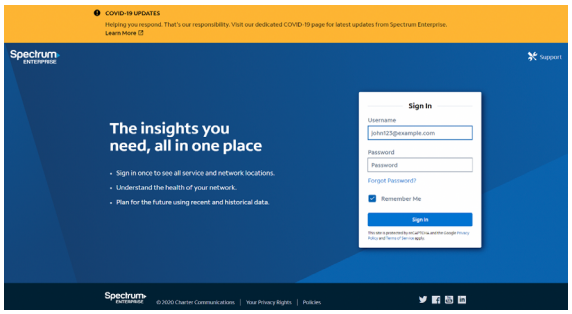
Supported browsers

The MNE portal is best viewed in the following browsers:

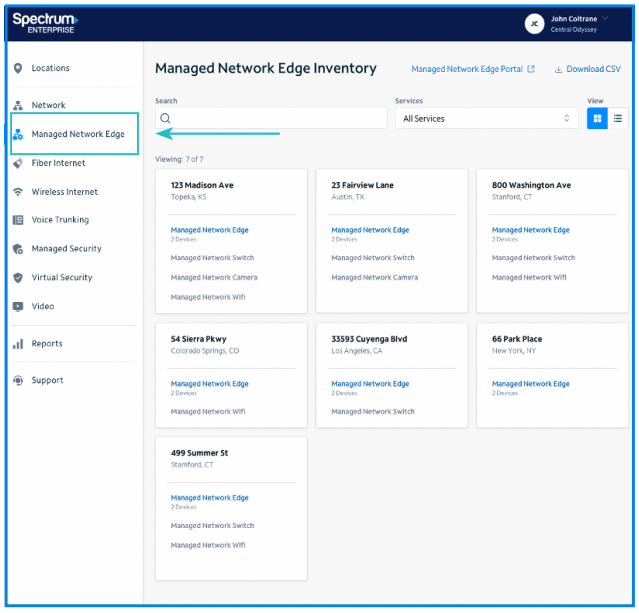
- Chrome®
- Firefox®
- Internet Explorer® (PC only)
- Safari® (MAC only)

Account access

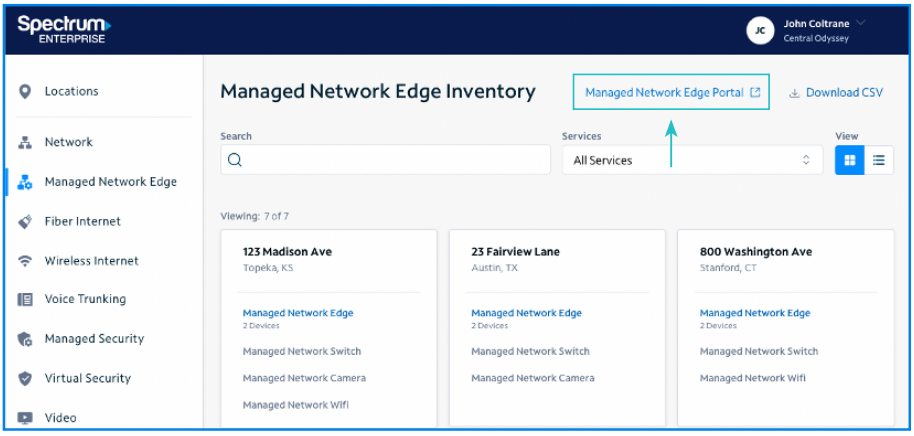
1. Log in with your username and password at SpectrumEnterprise.net.



2. Select Managed Network Edge from the left-hand navigation menu.



3. Click “Managed Network Edge Portal” to open the portal using your single sign-on access.



Note: Users can be configured for read-only or administrative access and can be limited to view only certain locations or circuits.

Spectrum ENTERPRISE

Security and SD-WAN appliance(s)

MNE provides security and routing services via Meraki MX devices, a family of enterprise security and SD-WAN appliances designed for distributed deployments. Their SD-WAN capabilities are designed to maximize network resiliency and bandwidth efficiency.

Use case summary

Action	Page	Common use cases
Configure	Addressing and VLANs	• Set up VLAN and port configurations, as well as static routes. • Check if a port and its associated VLANs and routes are configured correctly.
	Firewall	• Set up firewalll rules (access /deny), and 1-to-1 NAT rules. • Check if a firewall rule is configured appropriately.
	Client VPN	• Set up the client VPN interface to enable remote workers to access your network resources.
	SD-WAN and traffic shaping	• Set up QoS policies, load balancing and prioritization based on traffic types and applications.

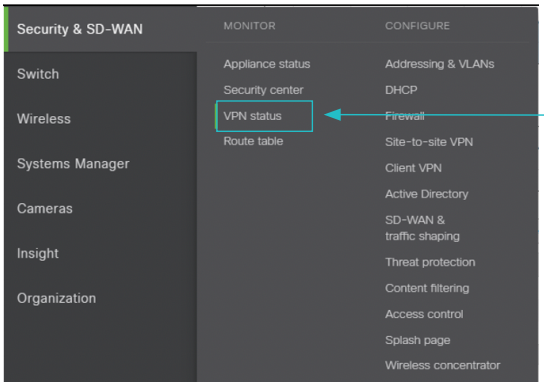
Action	Page	Common use cases
Monitor	VPN status	• Check on the VPN connectivity between different sites. • View traffic flow and specific VPN connections in detail.
	Security Center	• View information and insights related to security filtering events and threats.

Spectrum ENTERPRISE

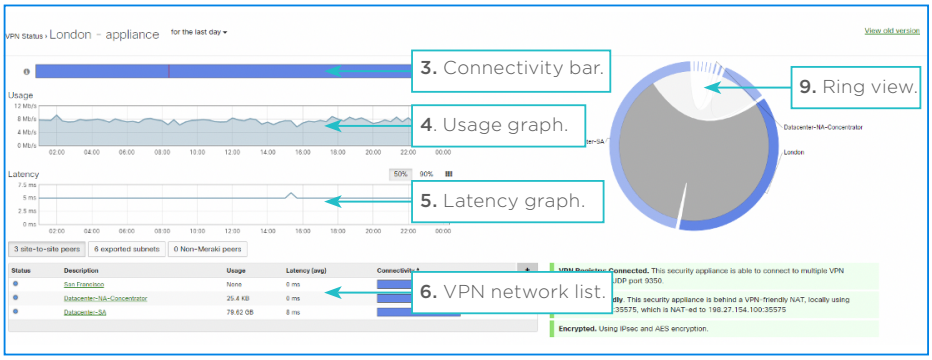
Security and SD-WAN monitoring

VPN status page

1. To review the VPN status, select Security and SD-WAN -> Monitor -> VPN status.



2. The "VPN status" page displays a wealth of information. We've highlighted some key areas to check out.

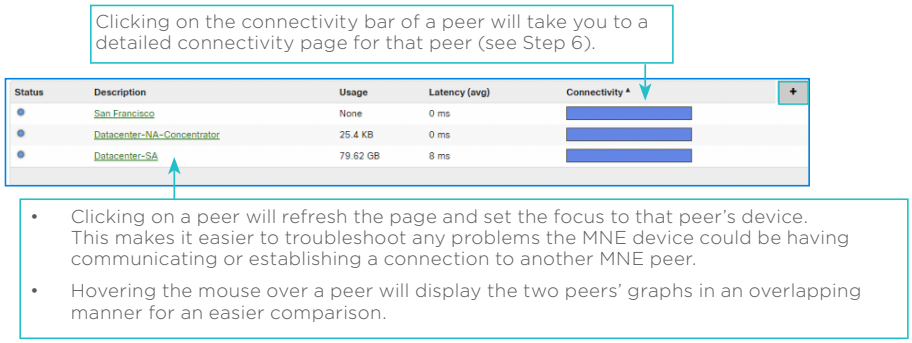


3. The "Connectivity bar" shows connectivity history for the selected MNE device. The bar can display three colors to indicate the VPN status:
   - **Red** – Peer is unreachable.
   - **Yellow** – Some peers are unreachable.
   - **Blue** – All peers are reachable.

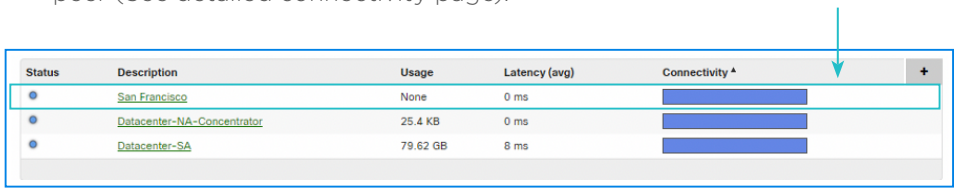
4. The "Usage graph" shows the throughput of the VPN. Use this graph to monitor the throughput of your site-to-site VPN connections.

5. The "Latency graph" shows the latency in a 50th percentile, 90th percentile, or histogram view. Note that:
   - The 50% option is typically useful for viewing the average connectivity for a specific time period.
   - The 90% option is typically useful for viewing spikes in latency over a specific time period.
   - The histogram view is typically useful for viewing detailed data for a specific time period.
   - If there are network problems (like poor voice quality) that can be related to latency, the 90% or histogram views can help you troubleshoot the issues and see if they're truly related to VPN connectivity.

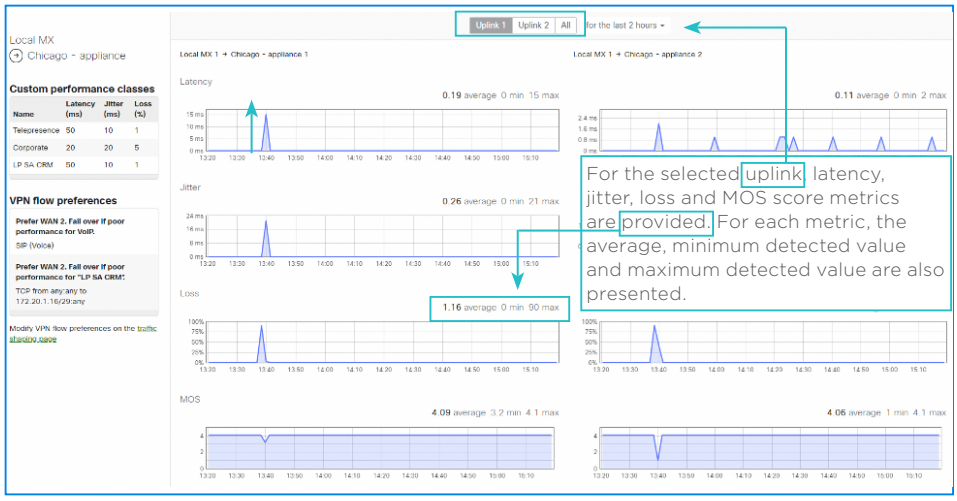
6. The "VPN network list" provides detailed information about an MNE device's VPN peers. Information columns can be added or removed using the "+" icon on the top right of the Networks list.



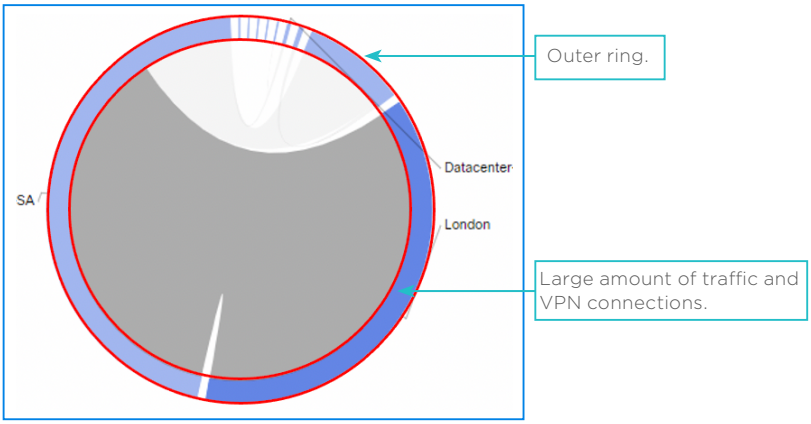
7. By clicking on the "Connectivity bar" of a VPN peer, you can compare the VPN statistics of the current network with the statistics of that remote VPN peer (See detailed connectivity page).



8. The detailed connectivity page displays a wide range of performance metrics.

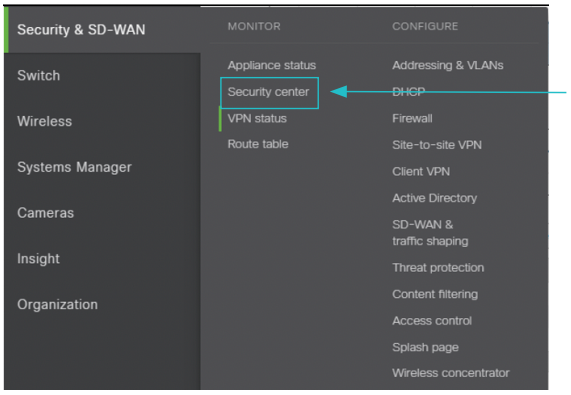


9. The ring view graph visually represents the traffic distribution between VPN peers. Each band or "slice" of color on the outer ring represents a device deployed at a given site. The bandwidth is based on the amount of traffic to or from that site. Wide segments indicate MNE networks that send and receive larger amounts of traffic than thinner segments.

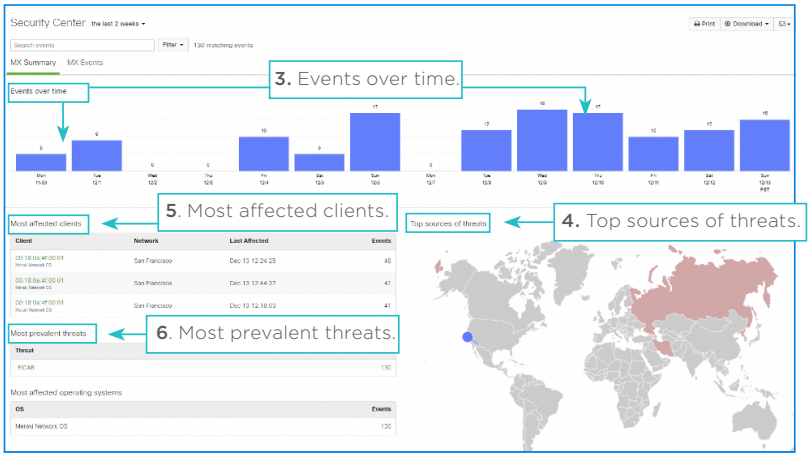


Security center

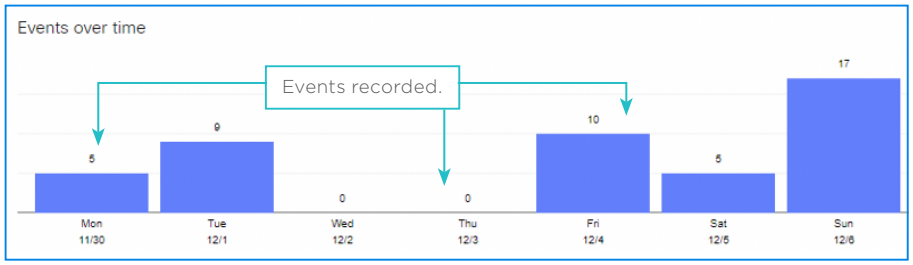
1. To review MNE security events, select Security and SD-WAN -> Monitor -> Security center.



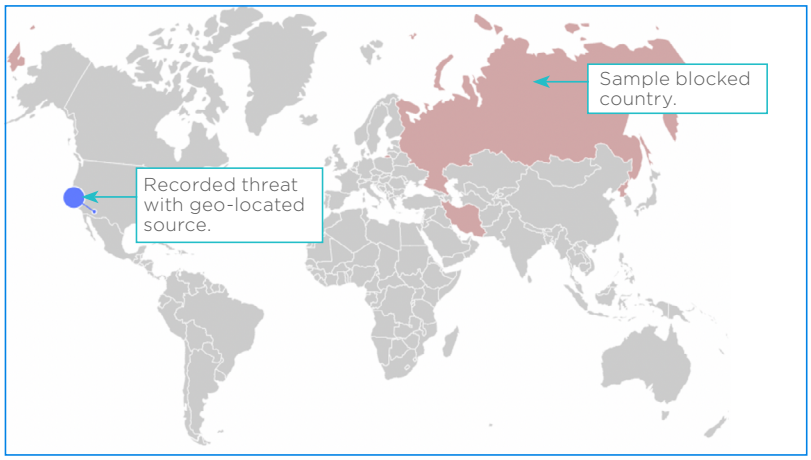
2. The "Security center" page displays the tops security threats impacting your network. We've highlighted some key areas to check out.



3. The “Events over time” chart shows the number of events matching configured filters, over a specific time period.



4. The “Top sources of threats” map shows a visual trajectory of the most common threats, including the location of recorded threats as well as the geo-located sources (that is, IP addresses) associated with them.



5. The “Most affected clients” section provides a breakdown of the clients that have generated the most events for the selected filters. Although the example below only shows Meraki OS events, this list could include other common clients like Windows, Android, iOS, etc.

Client	Network	Last Affected	Events
00:18:0a:4f:00:01 Meraki Network OS	San Francisco	Dec 13 12:24:25	48
00:18:0a:4f:00:01 Meraki Network OS	San Francisco	Dec 13 12:44:37	41
00:18:0a:4f:00:01 Meraki Network OS	San Francisco	Dec 13 12:18:03	41

6. The “Most prevalent threats” table lists the most frequent types of threats that have been detected, scanned or blocked.

Threat	Occurrences
EICAR	130

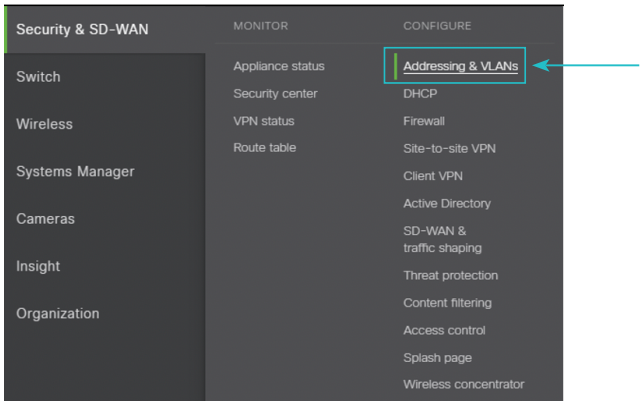
Virus-related vulnerabilities.

Spectrum ENTERPRISE

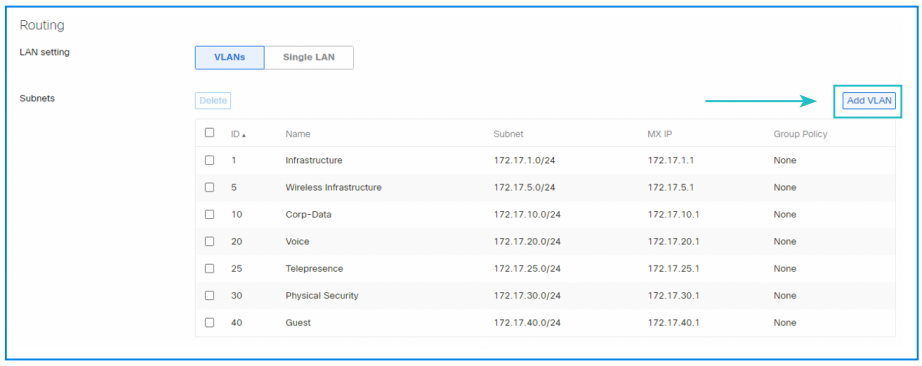
Security and SD-WAN configuration

Addressing and VLANS

1. To create a VLAN, select Security and SD-WAN -> Configure -> Addressing and VLANs.

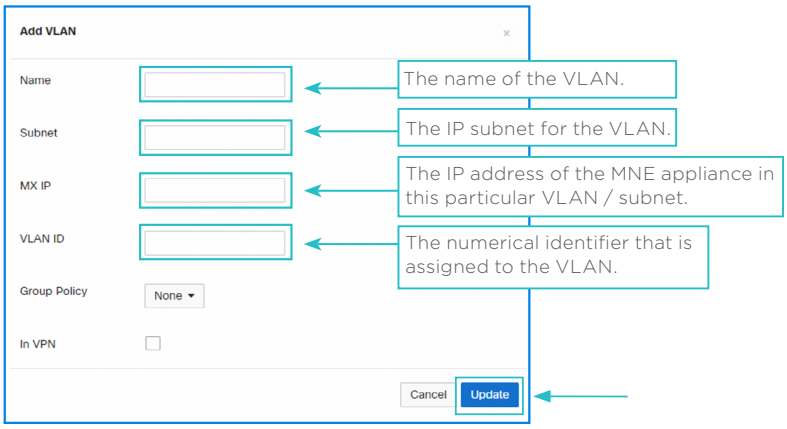


2. Within the "Routing" section, click on the Add VLAN button. The "Add VLAN" window pops up.



3. Within the "Add VLAN" window, enter your:
   - VLAN name.
   - Subnet.
   - MX IP.
   - VLAN ID.

   Click the Update button.



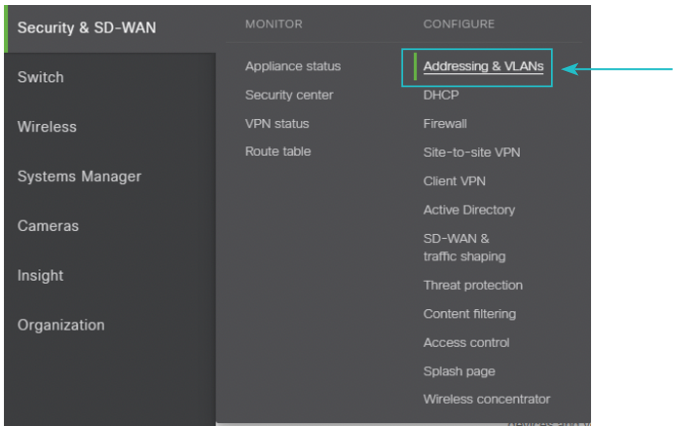
4. Within the “Routing” section, the “Subnets” table should include a new record showing your newly created VLAN.

5. Note that in the “Add VLAN” window, you can also select a “Group” policy (list of rules and settings) to apply to this VLAN, if any.

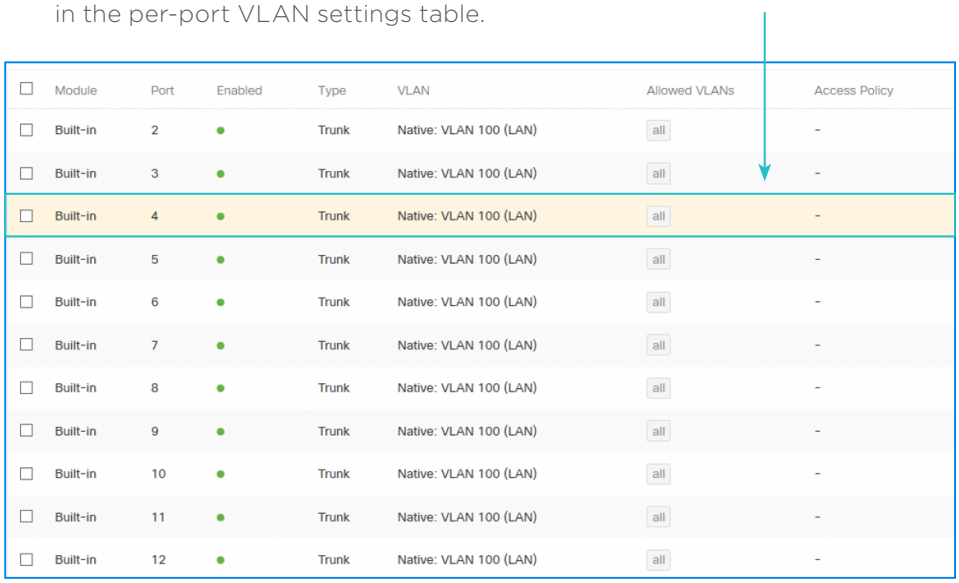
   Plus, you can select the “In VPN” box to specify whether the MNE device should advertise this new VLAN to site-to-site VPN peers.

Configure a VLAN port

1. To configure a port, select Security and SD-WAN -> Configure -> Addressing and VLANs.



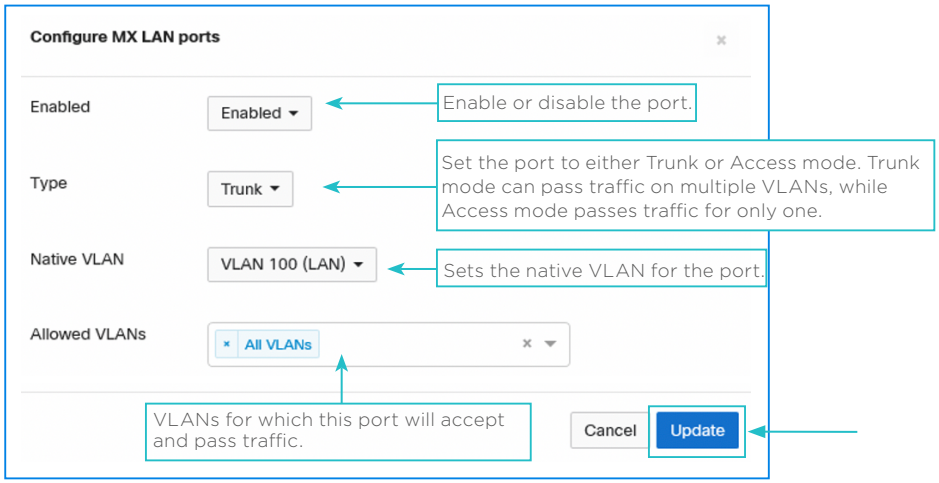
2. Within the “Routing” section, click on the port you would like to configure in the per-port VLAN settings table.



Module	Port	Enabled	Type	VLAN	Allowed VLANs	Access Policy
Built-in	2	●	Trunk	Native: VLAN 100 (LAN)	all	-
Built-in	3	●	Trunk	Native: VLAN 100 (LAN)	all	-
Built-in	4	●	Trunk	Native: VLAN 100 (LAN)	all	-
Built-in	5	●	Trunk	Native: VLAN 100 (LAN)	all	-
Built-in	6	●	Trunk	Native: VLAN 100 (LAN)	all	-
Built-in	7	●	Trunk	Native: VLAN 100 (LAN)	all	-
Built-in	8	●	Trunk	Native: VLAN 100 (LAN)	all	-
Built-in	9	●	Trunk	Native: VLAN 100 (LAN)	all	-
Built-in	10	●	Trunk	Native: VLAN 100 (LAN)	all	-
Built-in	11	●	Trunk	Native: VLAN 100 (LAN)	all	-
Built-in	12	●	Trunk	Native: VLAN 100 (LAN)	all	-

3. Within the "Configure MX LAN ports" window, select your new port's parameters:
   - Enabled or disabled.
   - Type (trunk or access).
   - Native VLAN.
   - Allowed VLANs.

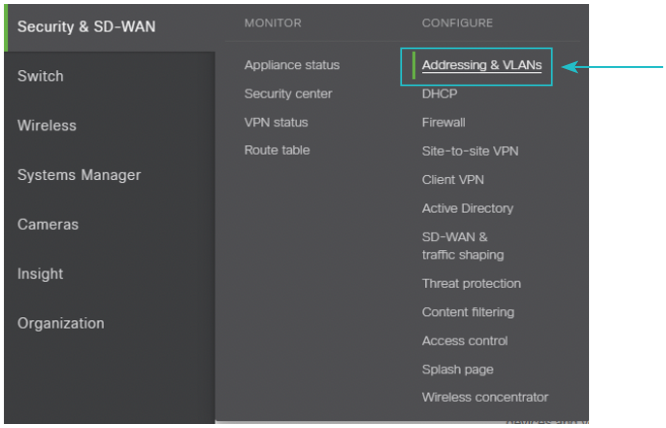
   Click the Update button.



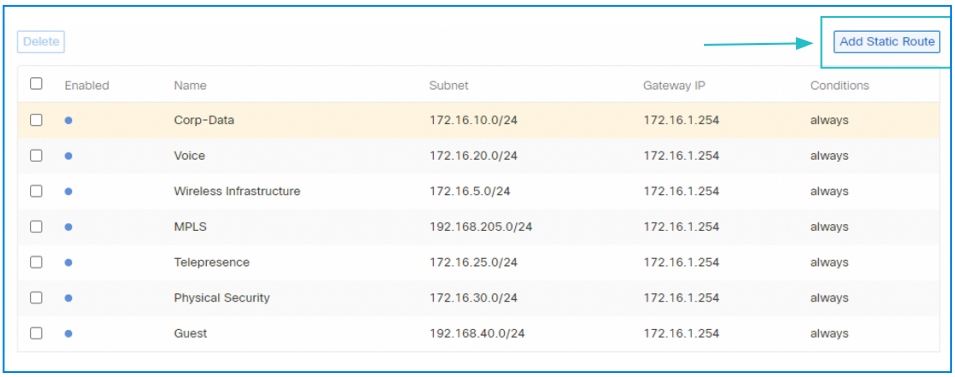
4. Within the "Routing" section, the per-port VLAN settings table should include the new settings for your selected port.

Create a new static route

1. To create a new VPN route, select Security and SD-WAN -> Configure -> Addressing and VLANs.

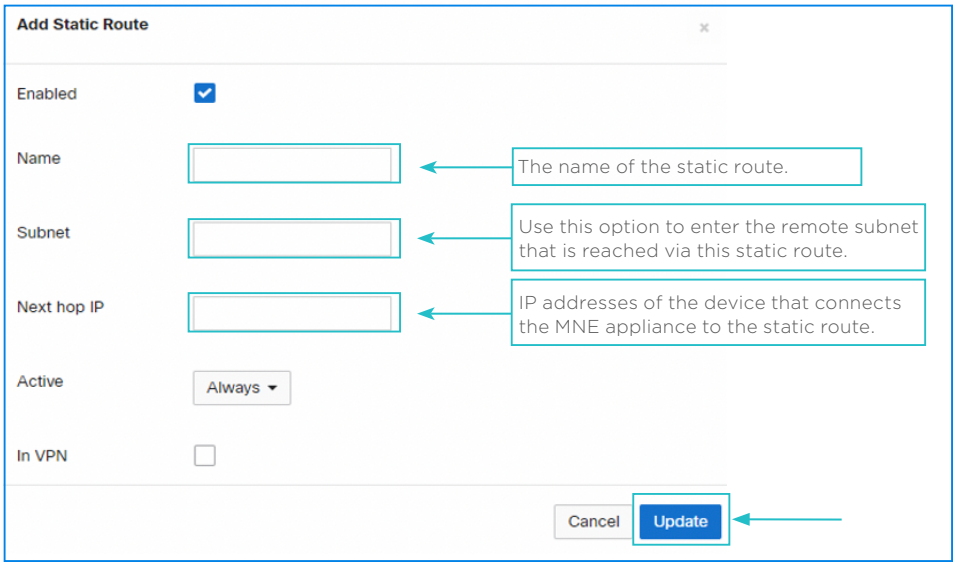


2. Within the "Static Route" section, click on the Add Static Route button. The "Add Static Route" window pops up.



3. Within the "Add Static Route" window, enter your:
   - Route name.
   - Subnet.
   - Next hop IP.

   Select "Always" from the "Active" drop-down list. Click the **Update** button.



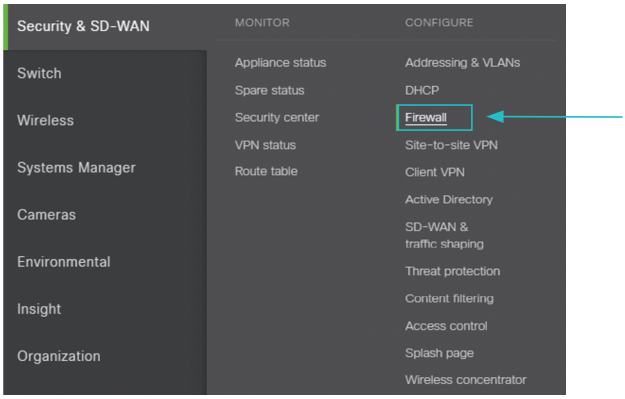
4. Within the "Routing" section, the "Static Route" table should include a new record showing your newly created static route.

5. Note that in the "Add Static Route" window, you can select the "In VPN" box to specify whether the MX device should advertise this new static route to site-to-site VPN peers.

Firewall

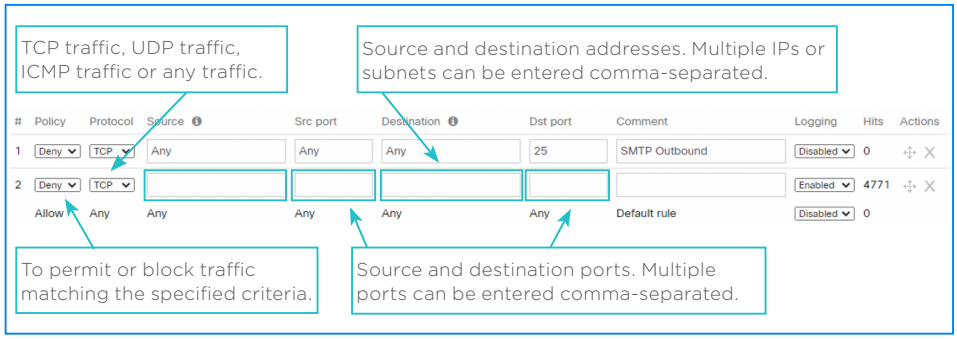
Create a new firewall rule (Layer 3)

1. To create a Layer 3 firewall rule, select Security and SD-WAN -> Configure -> Firewall.



2. Within the "Layer 3" section, click on "Add Rule" in the "Outbound rules" subsection. Then, configure the settings for the new firewall rule, including its:
   - Policy (permit or deny).
   - Protocol(s) impacted.
   - Source address(es).
   - Source port(s).
   - Destination address(es).
   - Destination port(s).

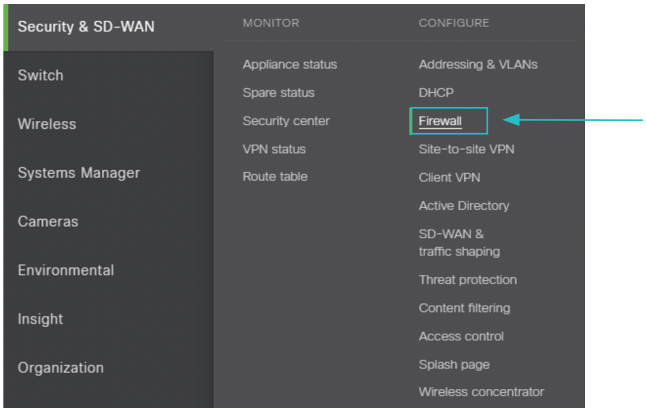
   Save changes.



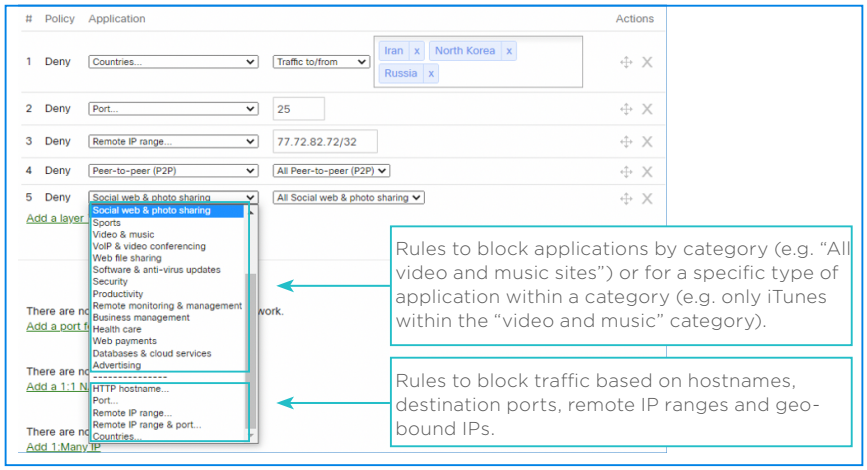
3. Within the "Outbound rules" subsection, the new firewall rule should appear.

Create a new firewall rule (Layer 7)

1. To create a Layer 7 firewall rule, select Security and SD-WAN -> Configure -> Firewall.



2. Within the “Layer 7” section, click on “Add layer 7 firewall rule” in the “Firewall rules” subsection. Then, select the settings for your new firewall rule, using the dynamic choices in the “Application” drop-down list. Save changes.

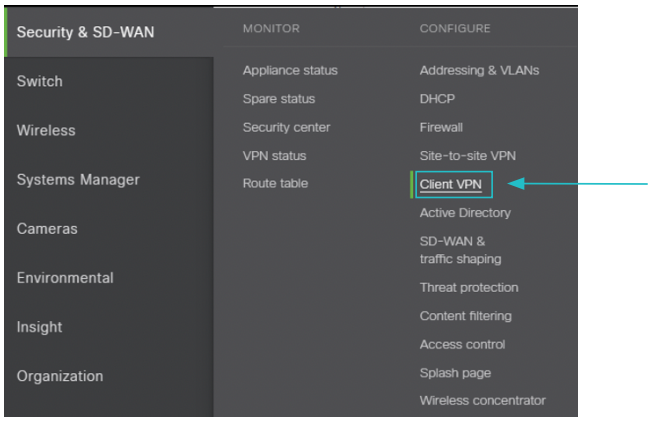


3. Within the “Firewall rules” section, the new firewall rule should appear.

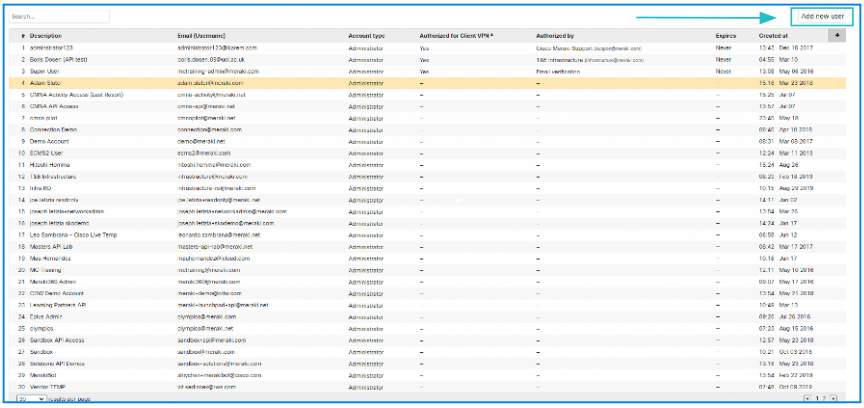
Client VPN

Add new VPN user

1. To add a new VPN user, select Security and SD-WAN -> Configure -> Client VPN.

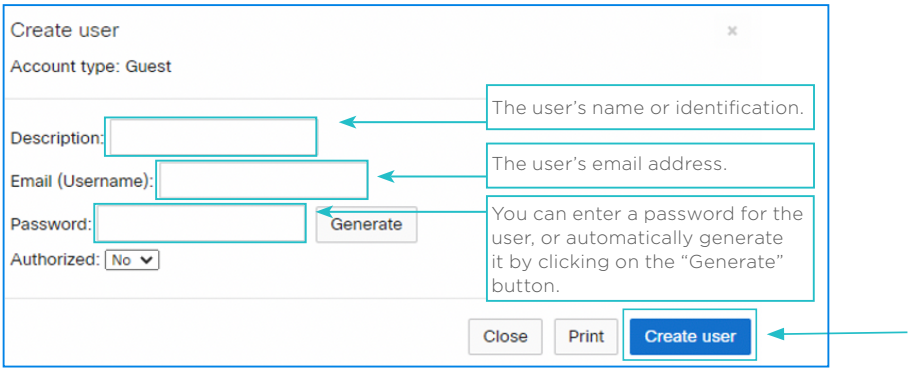


2. Within the “User Management” section, click on the Add new user button. The “Create user” window pops up.



3. Within the "Create user" window, enter your user's:
   - Description.
   - Email address.
   - Password.
   - Authorization (select "Yes," and if applicable, enter an expiration date).

   Click the Create user button.

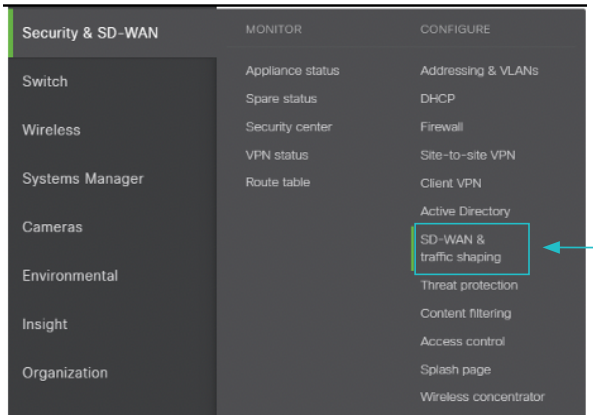


4. Within the "User Management" section, the table of authorized users should include a new record showing your newly added client VPN user.

SD-WAN and traffic shaping

Create a new shaping rule

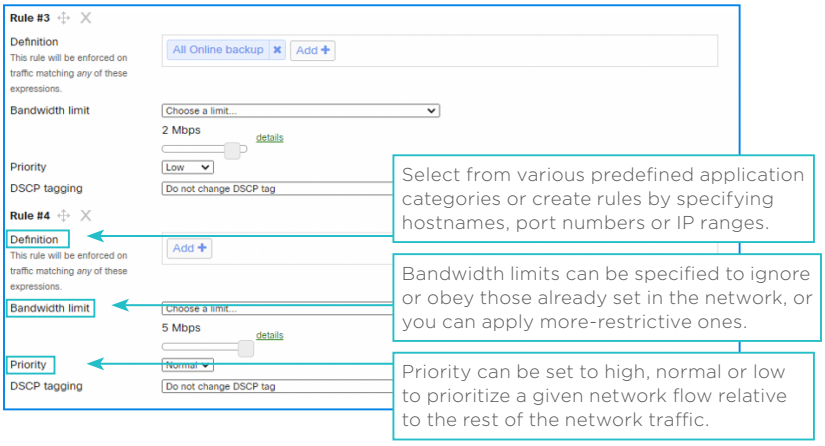
1. To create a new traffic shaping rule, select Security and SD-WAN -> Configure -> SD-WAN and traffic shaping.



Spectrum ENTERPRISE

2. Within the "Traffic Shaping Rules" section, click on "Add New Shaping Rule" at the bottom of the section. Then, configure the settings for your new shaping rule, including its:
   - Definition.
   - Bandwidth limit.
   - Priority.

   Save changes.



3. Within the "Traffic Shaping Rules" section, the new traffic rule should appear.

4. Note that in the rule parameters, you can use DSCP tagging to apply Quality of Service (QoS) prioritization to Layer 3 traffic. Simply select a value to be used for the DSCP tag in the IP header on all incoming and outgoing IP packets.

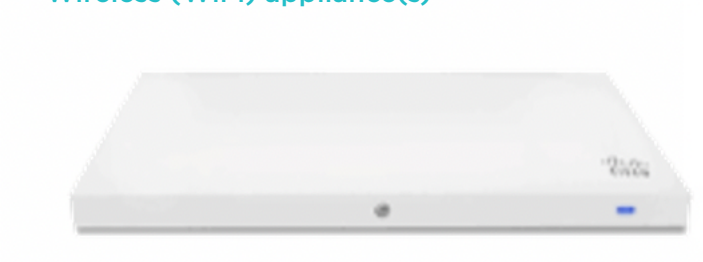
Additional references

To learn more about MX security and SD-WAN, refer to the Meraki documentation on:

- General MX best practices
- MX addressing and VLANS
- MX firewall settings
- VPN status page
- Security center
- SD-WAN traffic shaping
- Client VPN overview

Spectrum ENTERPRISE

Wireless (WiFi) appliance(s)



MNE provides WiFi capabilities via the Meraki MR series, a family of cloud-managed WiFi access points for enterprises. The MR access points use 802.11ac and 802.11n technologies to deliver the throughput and coverage demanded by business applications.

Use case summary

Action	Page	Common use cases
Configure	SSID and SSID availability	• Enable / disable SSID. • Limit SSID availability to certain times, hide it, advertise it or make it available to certain APs.

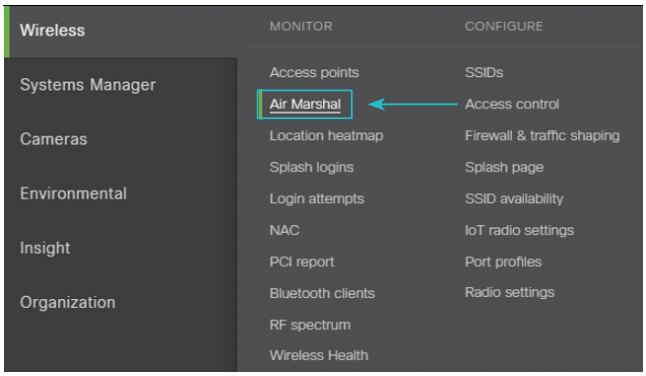
Action	Page	Common use cases
Monitor	Air Marshal	• Get insights into your WiFi infrastructure, as well as contain rogue SSIDs and spoofs.
	Wireless health	• View all of your wireless networks and their status. • Check if a specific client, access point or SSID has had any issues reported.

Wireless monitoring

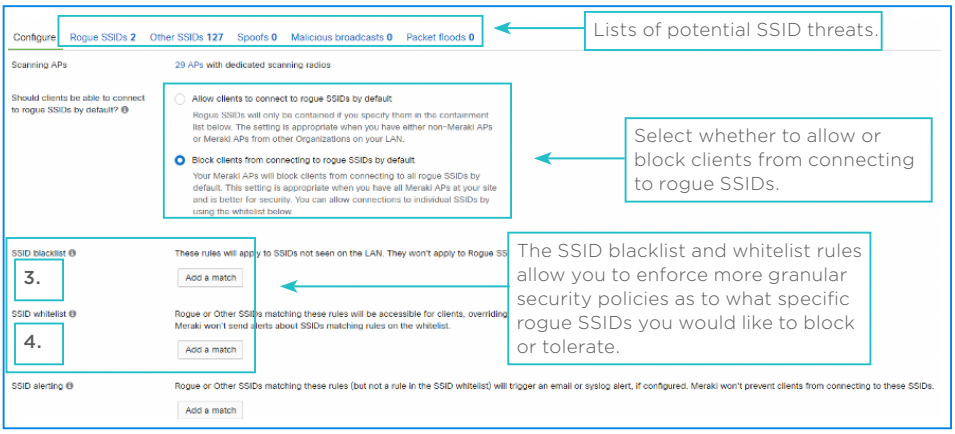
Air Marshal

The Air Marshal is a built-in wireless intrusion prevention system, which can trigger alarms and automatically contain malicious rogue APs.

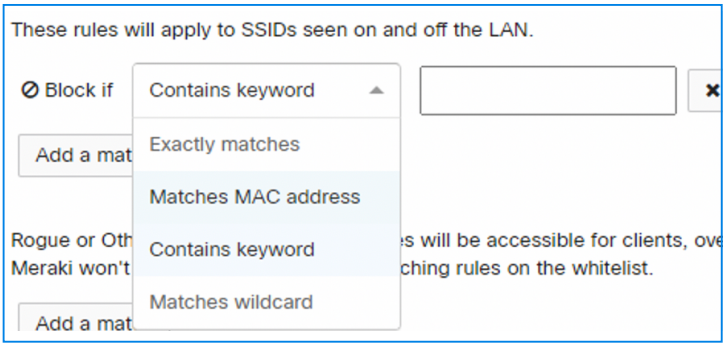
1. To open the Air Marshal, select Wireless -> Monitor -> Air Marshal.



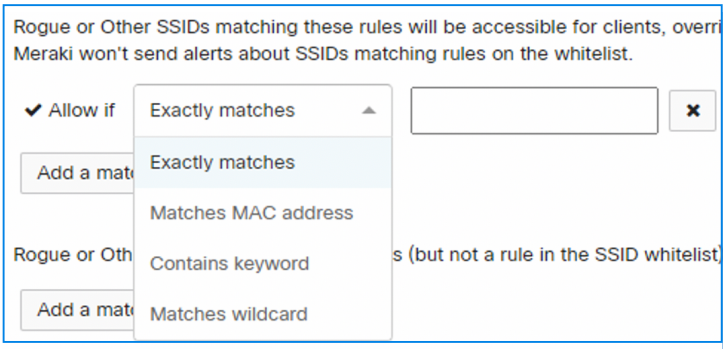
2. The "Air Marshal" page enables you to configure granular WiFi security policies. We've highlighted some key areas to check out.



3. If clients are allowed to connect to rogue SSIDs, you can use the SSID blacklist section to configure more granular policies for certain SSIDs. For example, you can block connections to SSIDs that contain exact words, MAC addresses, keywords or wildcards, as shown below.

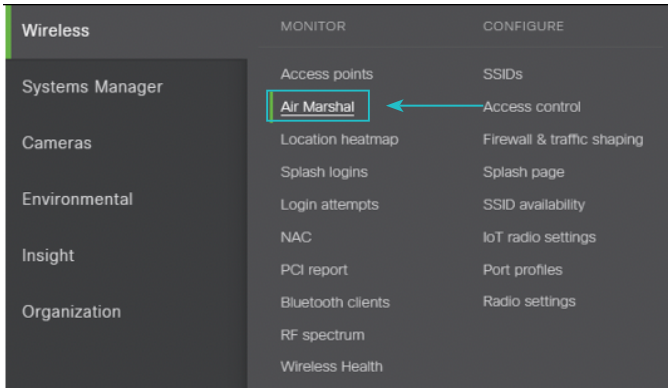


4. Similarly, you can block clients from connecting to rogue SSIDs by configuring whitelists. In the SSID whitelist section, you can specify the SSIDs that are trusted and accessible for clients.

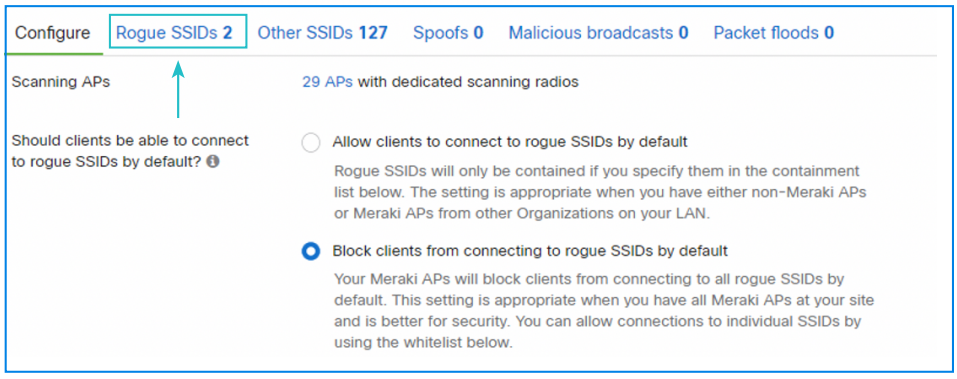


Contain rogue SSIDs

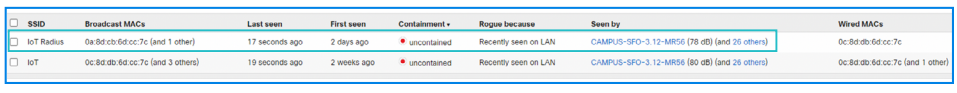
1. To contain rogue SSIDs with the Air Marshal, select Wireless -> Monitor -> Air Marshal.



2. Click on the "Rogue SSIDs" tab at the top of the "Air Marshal" page.

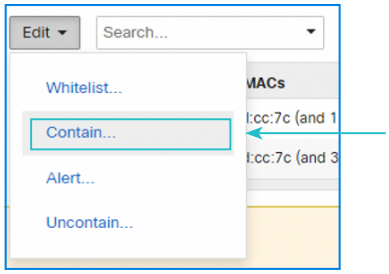


3. Select an SSID record from the "Rogue SSID" table and click on the checkbox to the left of the SSID (in this example, "IoT Radius").

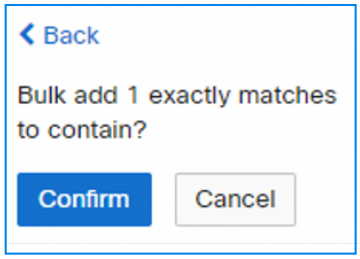


4. The Edit drop-down button is enabled above the Rogue SSID table. Click on it to see a list of actions to choose from, including:
   - Whitelist.
   - Contain.
   - Alert.
   - Uncontain.

Select “Contain” -> “by SSID.”



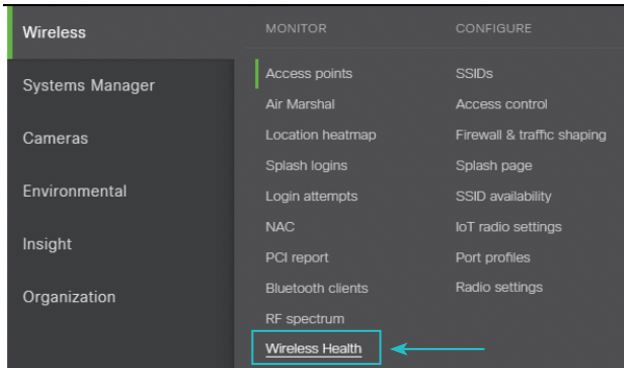
5. Click on the Confirm button. Save changes.



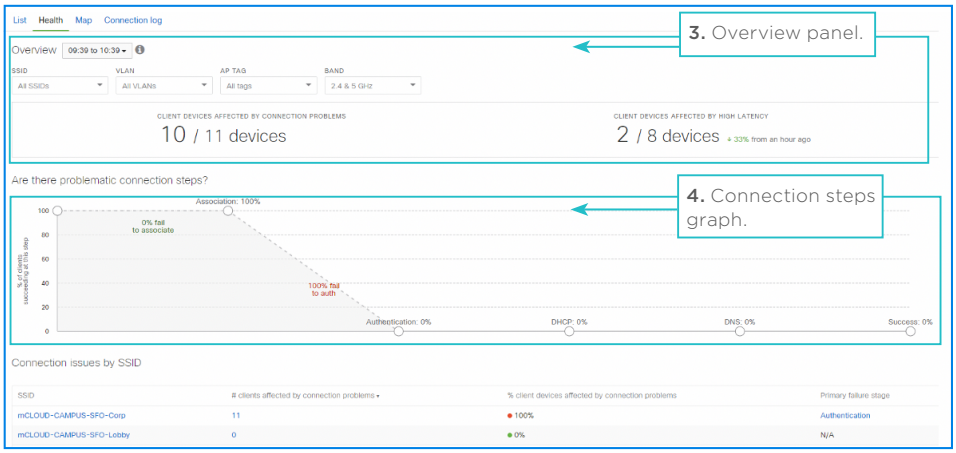
6. The selected SSID “Containment” status should change from “Uncontained” to “Contained.” Clients will now be blocked from connecting to this rogue SSID.

Wireless health

1. To monitor the health of your WiFi network, select Wireless -> Monitor -> Wireless Health.



2. The “Wireless Health” page displays a wealth of information. We’ve highlighted some key areas to check out.



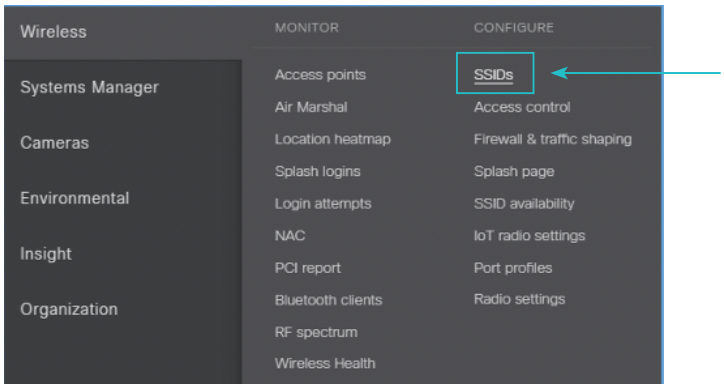
3. The “Overview panel” displays the overall health of the wireless network, including a quick reference for the percentage of failed connection attempts and average packet latency of connected wireless clients.

4. The “Connection steps” graph shows how clients connect to an Access Point, and at what step (association, authentication, etc.) that they might be experiencing issues. You can also view the overall success rate of clients attempting to connect to the wireless network.

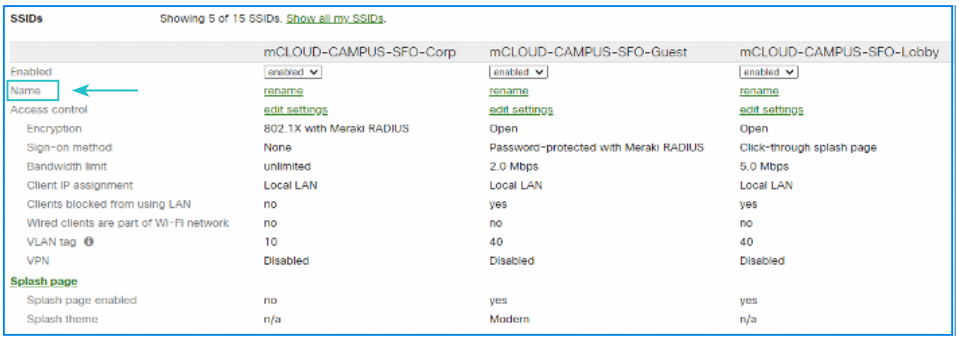
Wireless configuration

SSID and SSID availability

1. To rename or disable an existing SSID, select Wireless -> Configure -> SSIDs.

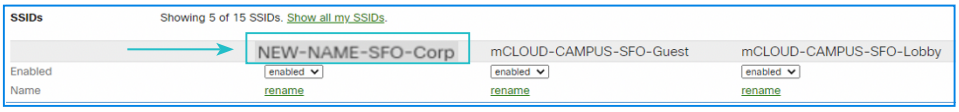


2. Within the “Name” section, click on the “Rename” link for an unused SSID.

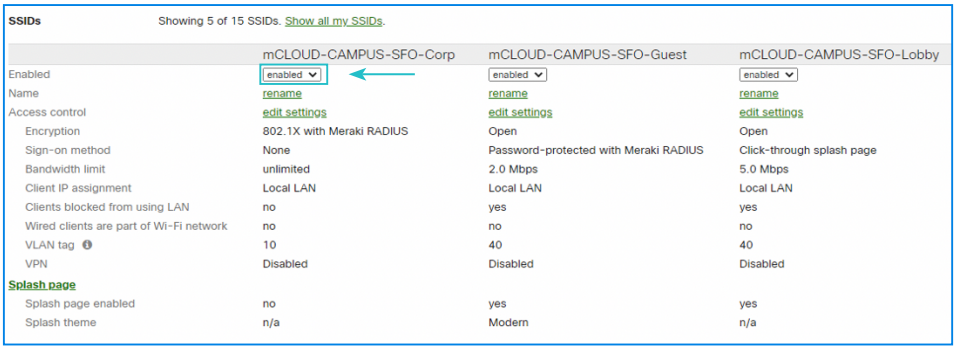


3. In the text field that appears, type in a new name for the SSID and press “Enter.”

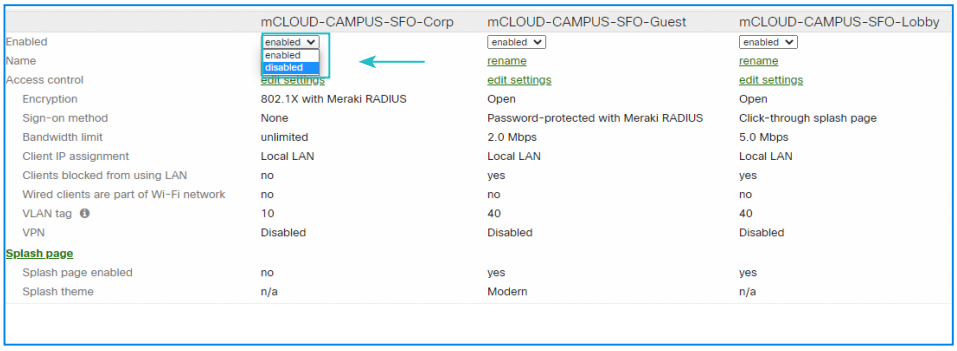
4. Within the “Configuration overview” table, the new SSID name should appear.



5. To disable the SSID, within the “Enabled” section, click on the drop-down list.



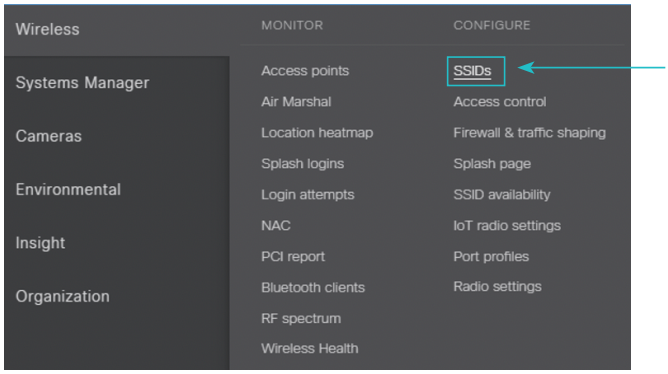
6. Select “Disable.”



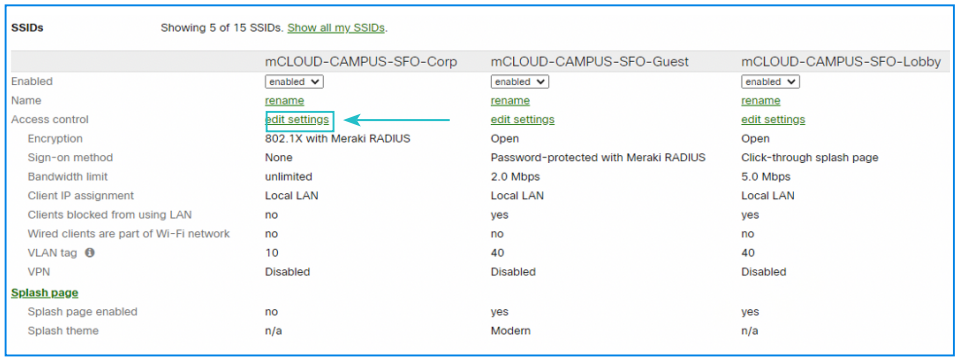
7. Within the “Configuration overview” table, the column for your disabled SSID should be grayed out.

Set the access control for an SSID

1. To set up access control policies for SSIDs, select Wireless -> Configure -> SSIDs.

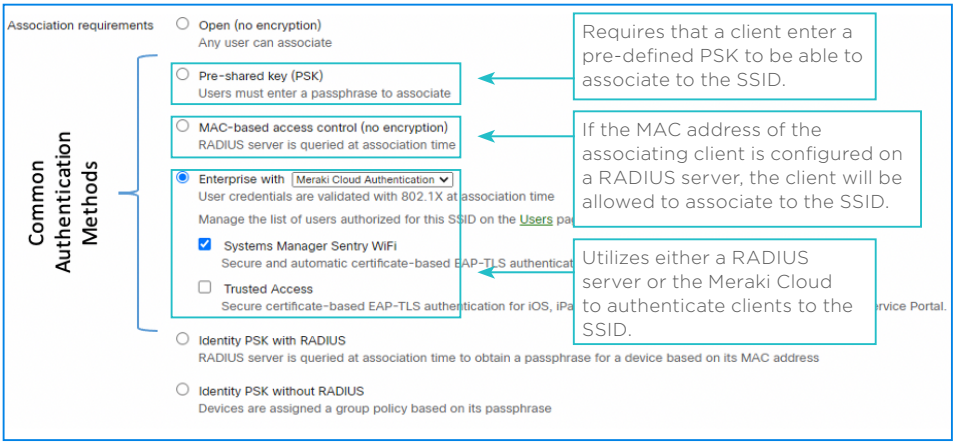


2. Within the “Access control” section, click on the “edit settings” link for an SSID (In this example, “mCloud-Campus-SFO-Corp”).



3. Within the “Network access” section, select a preferred authentication method for the SSID, including:
    - Open (co-encryption).
    - Pre-shared Key (PSK).
    - MAC-based access control.
    - Enterprise:
        - Meraki cloud.
        - Radius.
        - Local.
        - Identity PSK with RADIUS.
        - Identity PSK without RADIUS.

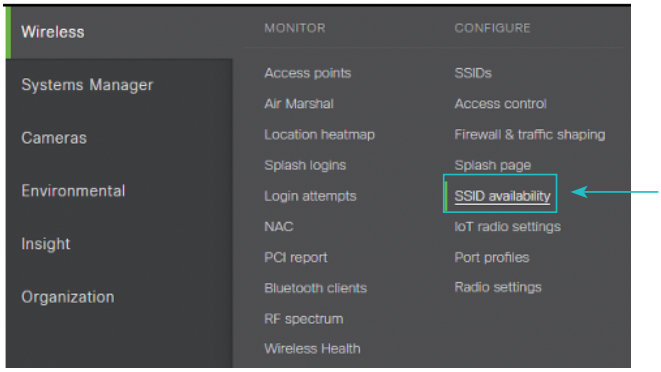
Save changes.



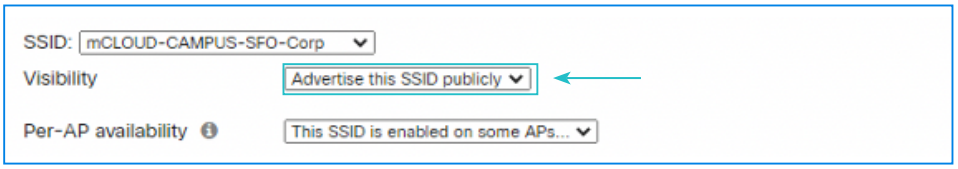
4. The selected authentication method is confirmed.

Configure SSID availability

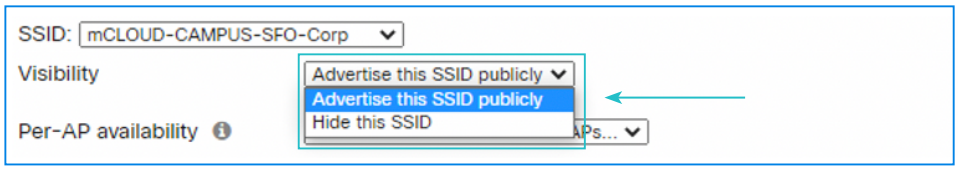
1. To configure SSID availability, select Wireless -> Configure -> SSID availability.



2. To hide or advertise an SSID, within the "SSID availability" section, click on the "Visibility" drop-down list.

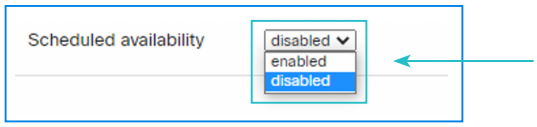


3. Click on "Advertise this SSID publicly" if you would like to make it visible for clients or click on "Hide this SSID" to prevent clients from seeing it.

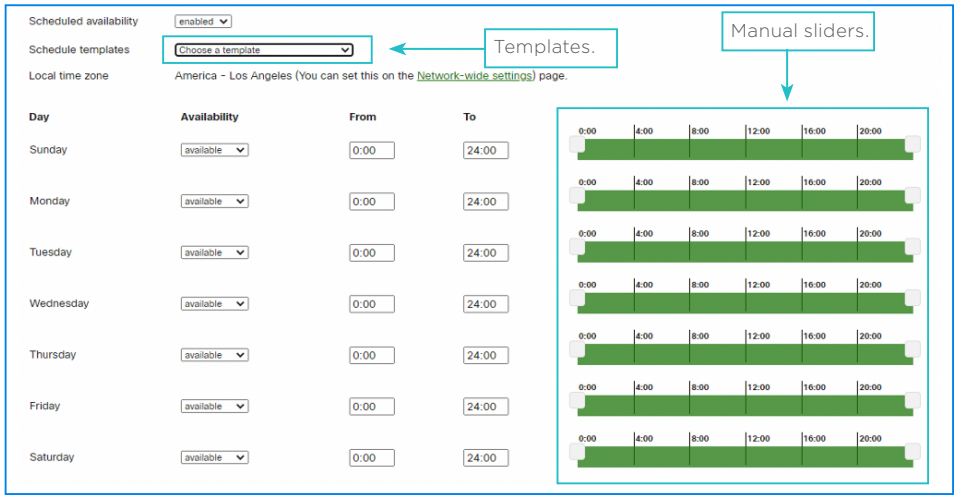


4. If advertised, the SSID should be visible to clients.
   If hidden, the SSID should not be available for clients.

5. To limit an SSID's availability to certain times, within the "SSID availability" section, click on the "Scheduled availability" drop-down list and select "Enabled."



6. A weekly schedule appears. Use the sliders to set an availability schedule, or choose a template from the "Schedule templates" drop-down list (e.g. available only 8 AM to 5 PM). Save changes.



7. The SSID should only be visible and available in the specified time or schedule.

Additional references

To learn more about MNE WiFi, refer to the Meraki documentation on:

- MR Wireless LAN
- Enabling, disabling and changing SSID names
- Air Marshal
- Wireless health

Sensor offers

The Meraki MT sensors are a line of cloud-managed offerings that provides visibility into customer locations. With cloud management, these sensors can be provisioned to alert customers via email and SMS notifications if specific thresholds are exceeded. In this section, you will find the different types of alerts that can be provisioned and customized by customers. Below are the Managed Network Sensors that are offered.

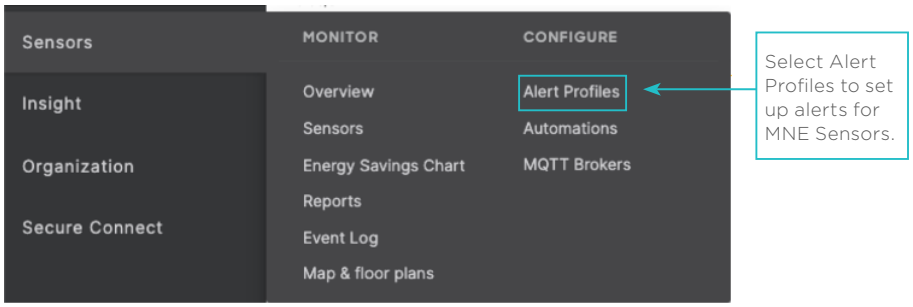
MNE Sensor offers	Device
Temperature and humidity	MT10
Open | Close	MT20
Water detection	MT12
Temperature probe	MT11
Air quality	MT14
Smart button	MT30

Setting up sensor alert profiles

The MT line of sensors has robust and easy-to-set-up alerts to notify users in the event of threshold violation. This section outlines the process of creating an Alert Profile and assigning it to a sensor.

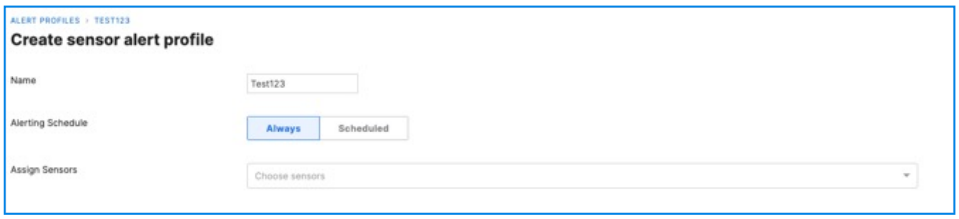
Each alert profile may have multiple sensor thresholds that trigger based on specified conditions. Users can assign multiple email recipients and phone numbers for SMS notifications. Below is how to set up an individual Alert Profile. See the Alert Profiles example section in the document to see what a dashboard looks like with multiple Alert Profiles created.

Begin at the main navigation toolbar and select Sensors>Alert Profiles



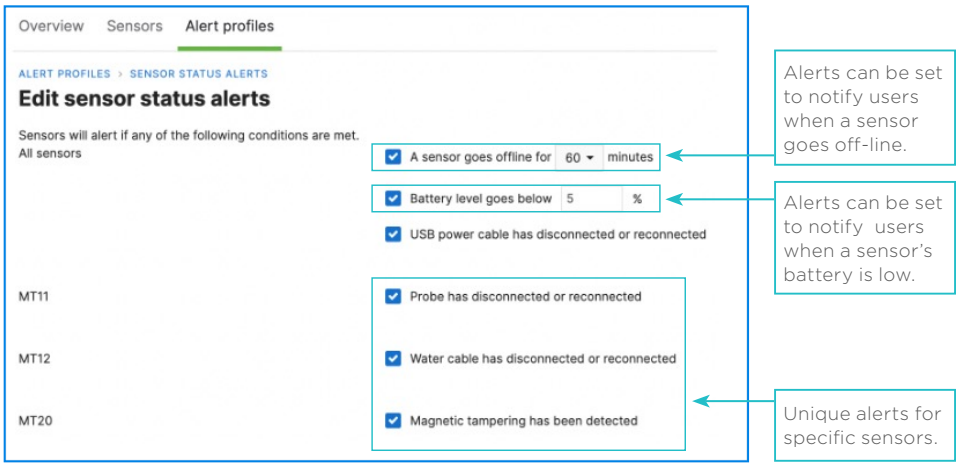
Users create multiple alert profiles with notifications to users based on conditional settings.

Start by creating and naming the Alert Profile and selecting the sensors you want to monitor:

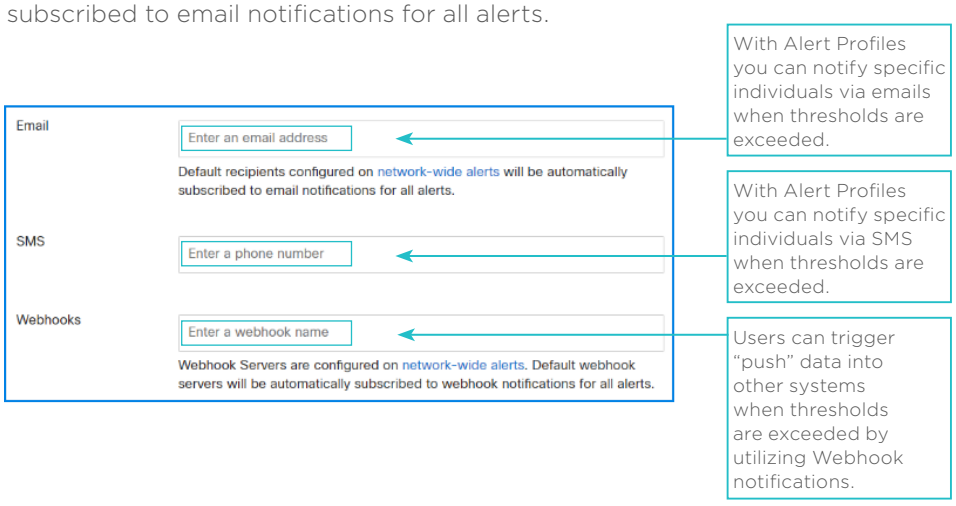


Monitoring alerts

Alert conditions can be set in this profile based on either general device health or model specific to certain devices.



An email or SMS recipient can be added to the field for notifications. Please note that all default recipients in the network-wide alerts will be automatically subscribed to email notifications for all alerts.



Alert conditions

MNE Sensors can be programmed to notify customers of specific conditions within their environments. Below are the thresholds and the view into the Dashboard for setting up these sensor conditions.

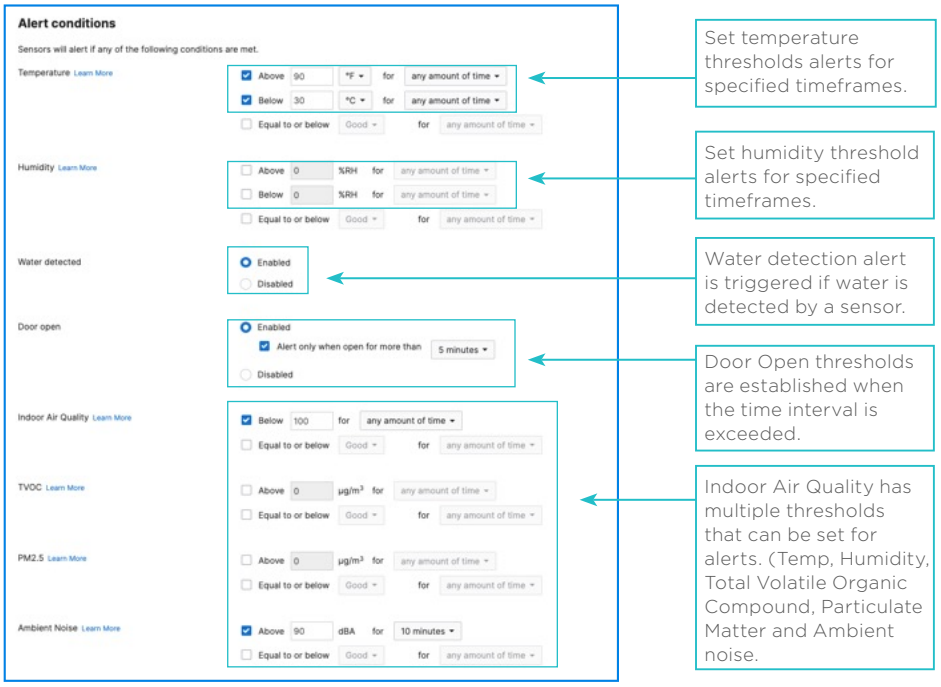
MT sensors	Sensor alerts (alert conditions)	Alert dimensions	Measurement type	Conditions
MT 10 MT 11	Temperature	Above / Below	Celcius or Fahrenheit	Specific timeframe
MT 10	Humidity	Above / Below	% relative humidity	Exceeds threshold
MT 12	Water detection	Alert	Water detection	If a sesor detects water
MT 20	Open | Close	Enabled / Disabled	Alert only when open	Specified timeframe
MT 14	Indoor air quality	Temperature	0C-55C / 32F to 131F	Measured thresholds
		Humidity	0-95% Relative Humidity	
		Total volatile organic compound	300- >10,000 µg/m^{3}*	
		Particulate Matter (PM 2.5)**	0 to 100ug/m^3	
		Ambient noise	20 to 120 dBA***	
MT 30	Smart button	Short Press (less than 1 sec) Long Press (greater than 1 sec)	User-defined	Any

*µg/m3: The concentration of an air pollutant (e.g. ozone) is given in micrograms (one-millionth of a gram) per cubic meter air or µg/m3.

**Particulate Matter 2.5 Requires an External power adapter.

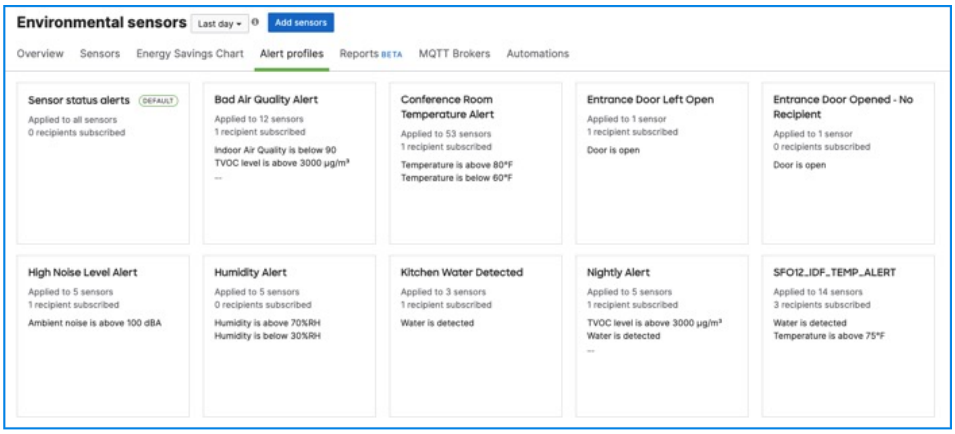
**120 dB is a decibel level that describes extremely loud sounds. In fact, on a decibel chart, 120 dB marks the limit from which sounds become painful and very dangerous to the human ear.

Alert conditions configurations (Dashboard)



Alert Profiles examples

MNE Sensors using Alert Profiles allow customers to organize the sensors to alert specific individuals or multiple individuals at the sensor level. Users can easily modify Alert Profiles to change thresholds, modify users who receive alerts, and change alerts status.



Switch appliance(s)

MNE provides switching capabilities via the Meraki MS series, a family of cloud-managed access and aggregation switches. With cloud management, you can configure and monitor switch ports via a secure portal. You can also provision remote sites without on-site IT, and deploy network-wide configuration changes.

Use case summary

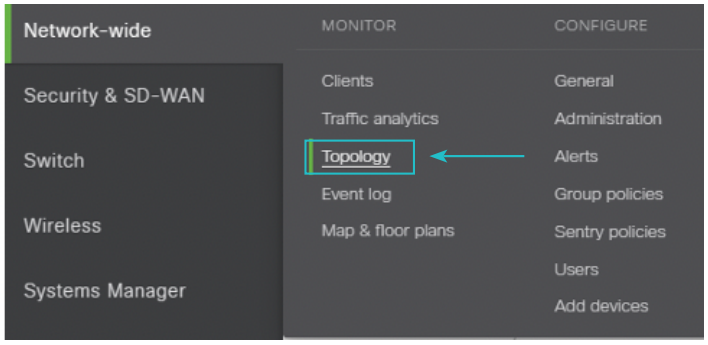
Action	Page	Common use cases
Monitor	Network-wide topology	• View switching alerts using a visual representation of your network.
	Switch ports	• Name ports, turn ports on / off, define port types and specify VLANs.

Spectrum ENTERPRISE

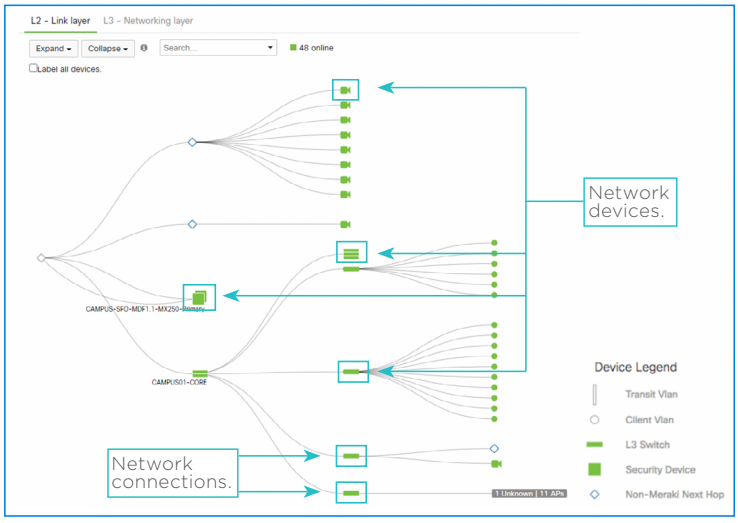
Switch monitoring

Network-wide topology

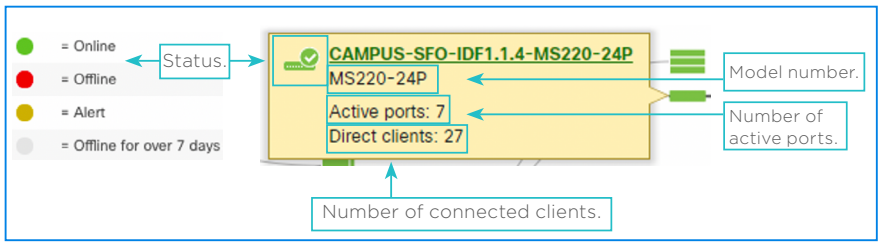
1. To check the status of a switch, select Network -> Monitor -> Topology.



2. The "Topology" page enables you to quickly become familiar with a network environment. By hovering over different elements of the topology, data points are instantly available. While hovering over a node—for example—Subnets, Node IPs on each specific Subnet, and Static Routes for that particular node are listed. In addition to the L2 Topology, the L3 Topology view allows you to visualize the L3 network connectivity.



3. To check the status of a switch, within the "Topology" section hover the mouse over a specific switch appliance. In this example, we selected "CAMPUS-SFO-IDF1.1.4."

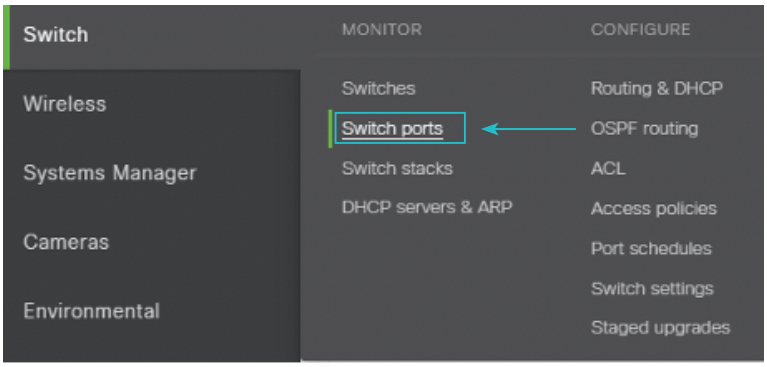


Spectrum ENTERPRISE

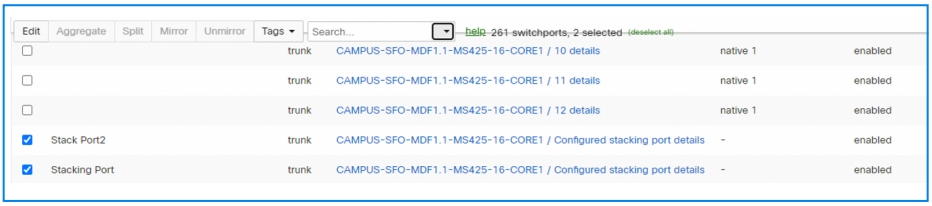
Switch ports

Edit switch ports

1. To edit a group of switch ports, select Network -> Monitor -> Switch ports.

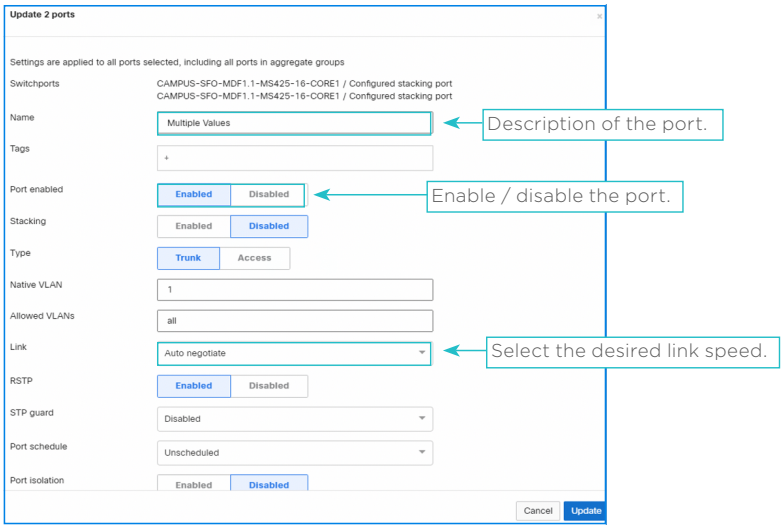


2. Within the “Switch ports” section, click on one or more port records (in this example, “Stack Port 2” and “Stacking Port”).



3. The Edit button is enabled above the Switch Ports table. Click on it to see the configurable port parameters, including:
    - Name.
    - Tags.
    - Port enabled.
    - Stacking.
    - Type.
    - Native VLAN.
    - Link.
    - RSTP.
    - STP guard.
    - Port schedule.
    - Port isolation.

Select “Disabled” in the “Port enabled” section. Click the Update button.



4. The selected ports should appear as “Disabled” in the “Switch Ports” table.

Additional references

To learn more about Meraki MS switches, refer to the Meraki documentation on:

- MS switches
- Network topology
- Switch stacks
- Switch ports

“Spectrum Enterprise” is a trademark of Charter Communications. All other trademarks are and remain the property of their respective owners.

About Spectrum Enterprise

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America’s largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions. The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. For more information, visit enterprise.spectrum.com.

Not all products, pricing and services are available in all areas. Pricing and actual speeds may vary.
Restrictions may apply. Subject to change without notice. ©2022 Charter Communications. All rights reserved.