MANAGED NETWORK EDGE

Portal User Guide - Cisco® Meraki®
# Table of contents

**Introduction** ...................................................................................................................................................................... 3

**Goals of this document** .................................................................................................................................................. 3

**Supported browsers** ....................................................................................................................................................... 4

**Account access** ................................................................................................................................................................. 4

**Security and SD-WAN** .......................................................................................................................................................... 6

**Use case summary** ........................................................................................................................................................ 6

**Security and SD-WAN monitoring** ............................................................................................................................. 7

**VPN status page** .............................................................................................................................................................. 7

**Security center** ................................................................................................................................................................. 9

**Security and SD-WAN configuration** .......................................................................................................................... 11

**Addressing and VLANS** .................................................................................................................................................. 11

**Firewall** ............................................................................................................................................................................ 14

**Client VPN** ......................................................................................................................................................................... 16

**SD-WAN and traffic shaping** ....................................................................................................................................... 17

**Additional references** .................................................................................................................................................... 18

**Wireless (WiFi)** .............................................................................................................................................................. 19

**Use case summary** ........................................................................................................................................................ 19

**Wireless monitoring** ..................................................................................................................................................... 20

**Air Marshal** ................................................................................................................................................................. 20

**Wireless Health** ........................................................................................................................................................... 22

**Wireless configuration** ................................................................................................................................................ 23

**SSID and SSID availability** ............................................................................................................................................ 23

**Additional references** ................................................................................................................................................... 27

**Switch** ............................................................................................................................................................................. 28

**Use case summary** ........................................................................................................................................................ 28

**Switch monitoring** ....................................................................................................................................................... 28

**Network-wide topology** ................................................................................................................................................ 28

**Switch ports** ................................................................................................................................................................. 29
Introduction
Managed Network Edge (MNE) is powered by the Cisco Meraki cloud, enabling secure, cloud-based management of modular MNE services (including security, routing, SD-WAN WiFi and switching options). The MNE portal allows you to monitor, manage and control your MNE services—all from one place.

This document is designed to help you use the main sections of the MNE portal, including the Security and SD-WAN, Wireless (WiFi) and Switch sections. You’ll also learn about 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 the main components of the Security and SD-WAN, Wireless and Switch sections of the MNE portal.

• Provide sample use cases and user-level details to assist in the training of 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.
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

<table>
<thead>
<tr>
<th>Action</th>
<th>Page</th>
<th>Common use cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addressing and VLANs</td>
<td></td>
<td>- Set up VLAN and port configurations, as well as static routes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Check if a port and its associated VLANs and routes are configured correctly.</td>
</tr>
<tr>
<td>Firewall</td>
<td></td>
<td>- Set up firewall rules (access /deny), and 1-to-1 NAT rules.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Check if a firewall rule is configured appropriately.</td>
</tr>
<tr>
<td>Client VPN</td>
<td></td>
<td>- Set up the client VPN interface to enable remote workers to access your network resources.</td>
</tr>
<tr>
<td>SD-WAN and traffic shaping</td>
<td></td>
<td>- Set up QoS policies, load balancing and prioritization based on traffic types and applications.</td>
</tr>
<tr>
<td>Monitor</td>
<td></td>
<td>- Check on the VPN connectivity between different sites.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- View traffic flow and specific VPN connections in detail.</td>
</tr>
<tr>
<td>Security Center</td>
<td></td>
<td>- View information and insights related to security filtering events and threats.</td>
</tr>
</tbody>
</table>
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.

- Clicking on a peer will refresh the page and set the focus to that peer’s device. This makes it easier to troubleshoot any problems the MNE device could be having communicating or establishing a connection to another MNE peer.
- Hovering the mouse over a peer will display the two peers’ graphs in an overlapping manner for an easier comparison.

For the selected uplink latency, jitter, loss and MOS score metrics are provided. For each metric, the average, minimum detected value and maximum detected value are also presented.
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.

![Events over time chart](chart1.png)

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.

![Top sources of threats map](map1.png)

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.

![Most affected clients table](table1.png)

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

![Most prevalent threats table](table2.png)
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.

   ![Configure a VLAN port](image)

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

   ![Per-port VLAN settings table](image)
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.
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.
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
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**

<table>
<thead>
<tr>
<th>Action</th>
<th>Page</th>
<th>Common use cases</th>
</tr>
</thead>
</table>
| 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. |
| Air Marshal  |                       | • Get insights into your WiFi infrastructure, as well as contain rogue SSIDs and spoofs. |
| Monitor      | 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.

![Whitelist configuration interface](image)

**Contain rogue SSIDs**

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

![Air Marshal interface](image)

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

![Rogue SSIDs interface](image)

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”).

![SSID selection interface](image)
4. The 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 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
**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**

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

**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.”

**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

©Cisco and Meraki are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

**About Spectrum Enterprise**

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving 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.

Spectrum Enterprise’s industry-leading team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. More information about Spectrum Enterprise can be found at enterprise.spectrum.com.