Configuring Wi-Fi Networking Settings

RUCKUS One allows you to configure Wi-Fi networking settings, such as LAN ports for your APs, Mesh networking, Directed Multicast, Cellular options (in venues with M510 APs), Smart Monitor, and RADIUS options, at the venue level.

Complete the following steps to configure the Wi-Fi networking settings for your venue:

1. On the navigation bar, click Venues.
   The Venues page is displayed.

2. Click the check box for a specific venue and click Edit. Alternatively, click on a specific venue name then click the Configure button.

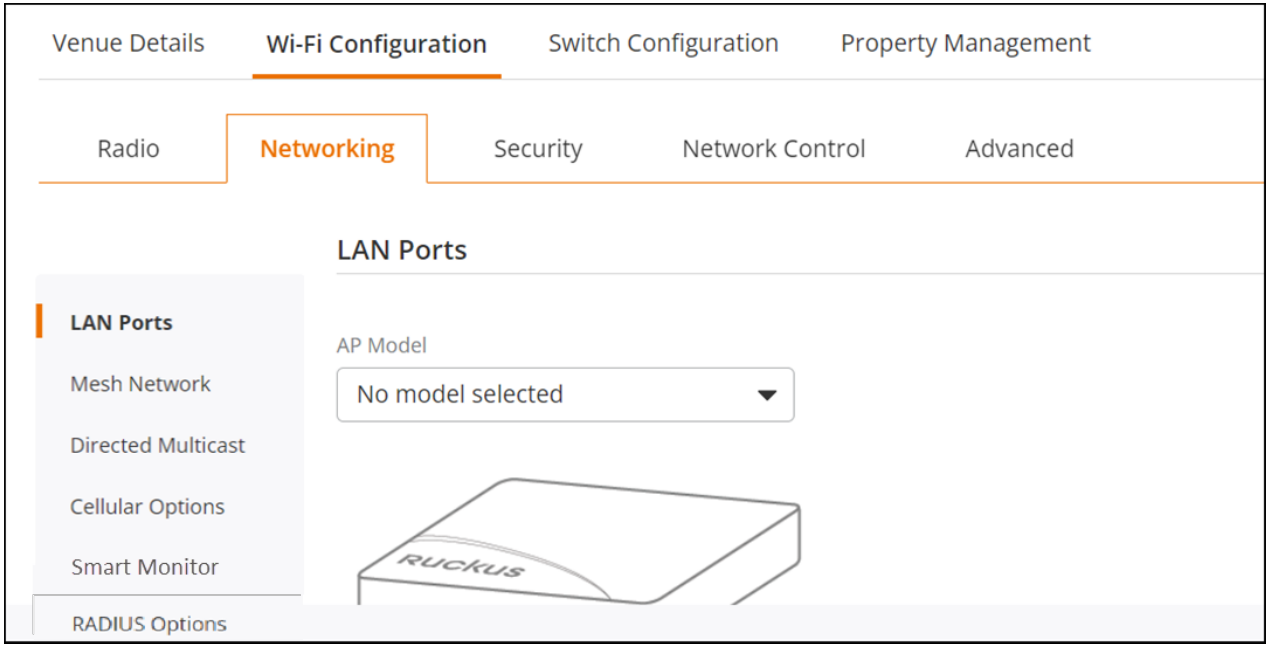
3. Select the Wi-Fi Configuration tab and Networking sub-tab.
   The Networking sub-tab provides several options for configuration, all of which can be accessed by clicking the menu option on the left, or by scrolling down the screen. At the top of the Networking page is the option for configuring LAN Ports on a per-AP model basis.

   Note: The Cellular Options is available only if you have the M510 AP model in your venue.

   Within the Networking sub-tab, customize the services of your preference and click Save. Refer to the following instructions to configure each of the available networking services:
   - *Configuring LAN ports*
   - *Configuring a Mesh network*
   - *Configuring Directed Multicast*

- *Configuring Cellular Options*
- *Configuring Smart Monitor*
- *Configuring RADIUS options*

Networking Configuration



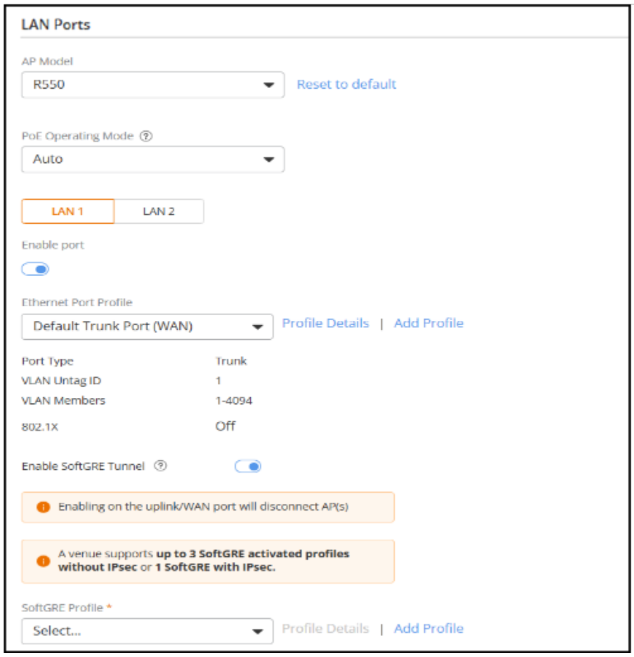
Configuring the LAN Ports

1. Configure the LAN ports for specific AP models. Select an AP from the AP Model drop-down list and configure the following. The screen refreshes, displaying configuration options (per LAN sub-tab) and an image of the selected AP with the ports labeled.

   Note: By default, LAN 1 is applicable for all the AP models and additional LANs are available as applicable to the AP model. For example, the T300 AP has only one LAN port, the R600 model has two LAN ports, and the H550 model has five LAN ports.

   Note: By default, Enable Port is activated for all LAN ports, but you can disable this option by toggling the Enable Port option to OFF.

   LAN Ports Settings



LAN Ports

AP Model: R550

PoE Operating Mode: Auto

Enable port: ON

Ethernet Port Profile: Default Trunk Port (WAN)

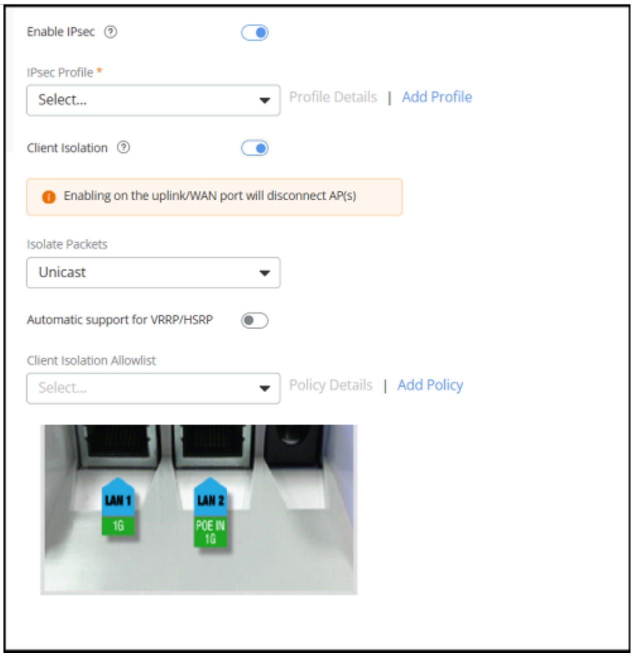
Port Type: Trunk
VLAN Untag ID: 1
VLAN Members: 1-4094
802.1X: Off

Enable SoftGRE Tunnel: ON

Enabling on the uplink/WAN port will disconnect AP(s)

A venue supports **up to 3 SoftGRE activated profiles without IPsec** or **1 SoftGRE with IPsec.**

SoftGRE Profile *: Select...



Enable IPsec: ON

IPsec Profile *: Select...

Client Isolation: ON

Enabling on the uplink/WAN port will disconnect AP(s)

Isolate Packets: Unicast

Automatic support for VRRP/HSRP: OFF

Client Isolation Allowlist: Select...

2. Configure the following settings:
   - PoE Operating Mode: Select the PoE Operating Mode (for specific AP models only) from the drop-down list. By default, Auto is selected. The other options are 802.3af, 802.3at, or 802.3bt/Class 5.

   - Enable PoE Out: By default, the Enable PoE Out option is disabled. You can enable this option by toggling the Enable PoE Out option to ON. This option is available for specific AP models only.

   - Ethernet Port Profile: Manages the configuration settings for Ethernet ports on networking devices. Select an Ethernet port profile from the drop-down list or click Add Profile to create a new Ethernet port profile. Refer to *Adding an Ethernet Port Profile (GUID-F50CE6F1-B253-4C14-820F-C34807BD36AD.html)* for more information.

     Note: For AP firmware 7.0.0.200.6290 and later versions, any changes to the trunk port VLAN untag ID will take effect. However, for APs with firmware versions earlier than 7.0.0.200.6290, the trunk port VLAN untag ID will remain at the default value of 1, even if the configuration has been changed.

   - Enable SoftGRE Tunnel: Tunnels the traffic to a SoftGRE gateway. Toggle the Enable SoftGRE Tunnel switch to ON. Select a SoftGRE profile from the SoftGRE Profile drop-down list or click Add Profile to create a new SoftGRE profile. Refer to *Creating a SoftGRE Profile (GUID-B99FD990-42CF-4297-AAA5-CB91A6691500.html)* for more information.

     Note: The uplink port does not support SoftGRE tunneling, which will cause the AP(s) to disconnect.

Note: SoftGRE tunnel is not supported if you select an Ethernet port profile with 802.1X Role as Supplicant. If SoftGRE tunnel is already enabled and you switch to a profile with the 802.1X Supplicant role, then SoftGRE tunnel will be automatically disabled.

Note: There is no alternative keep-alive detection mechanism between the AP and the SoftGRE server other than ping. As a result, if the primary SoftGRE service goes down but the ping to its IP address still succeeds, then the AP will not fail over to the backup gateway.

- Enable IPsec: Encapsulates data packets within GRE packets and secures them using IPsec. Toggle the Enable IPsec option to enable this feature. Select an IPsec profile from the IPsec Profile drop-down list or click Add Profile to create a new IPsec profile. Refer to *Creating a IPsec Profile (GUID-DB6BFE03-4FAC-4E1B-B80D-DC08B316FA32.html)* for more information.

  Note: A venue supports up to three SoftGRE-activated profiles without IPsec or one SoftGRE profile with IPsec. If a LAN port already has SoftGRE enabled, click the toggle to disable SoftGRE tunneling before enabling SoftGRE with IPsec. Similarly, if SoftGRE with IPsec is enabled, click the toggle to disable SoftGRE with IPsec before enabling SoftGRE tunneling.

  Note: When an Ethernet LAN port for an AP is enabled and configured with both SoftGRE and IPsec, all the wired clients connected to the customized AP LAN port are directed to the SoftGRE tunnel, protected by IPsec.

- Client Isolation: Enabling client isolation enhances network security by preventing devices on the same Wi-Fi network from communicating directly with each other. To apply client isolation, a manual device reboot is necessary. You can choose the specific AP devices from the AP list and click Reboot to restart them.

  Note: Enabling client isolation on the uplink will disconnect the AP.

- Isolate Packets: You can isolate data packets within the network to enhance network security and performance by controlling how data is transmitted and received within the network. Select unicast, multicast, and broadcast packets from the drop-down menu. Isolating unicast packets prevents direct communication between individual devices on the same network. Isolating multicast packets prevents specific devices from receiving data from the same device unless explicitly allowed. Isolating broadcast packets prevents all devices from receiving data from one device.
- Automatic support for VRRP/HSRP: Enabling Automatic support for VRRP and HSRP ensures seamless failover and increased network reliability by dynamically managing router failover without manual intervention. This maintains high availability and reliability in critical network environments.
- Client Isolation Allowlist: Enabling Client Isolation on a specific port for an AP model at a particular venue prevents devices on the same network from communicating with each other. However, the Client Isolation Allowlist permits certain devices to bypass this restriction and

communicate with isolated clients. You can select an allowlist from the drop down menu or click Add Policy to create one. These policies allow specific devices, to communicate with isolated clients despite the isolation settings.
To create a policy, provide the Policy Name, Description and add clients to the policy from the Select from Connected Clients. You can also add clients by clicking Add New Client. Click Policy Details to view information about the policy.

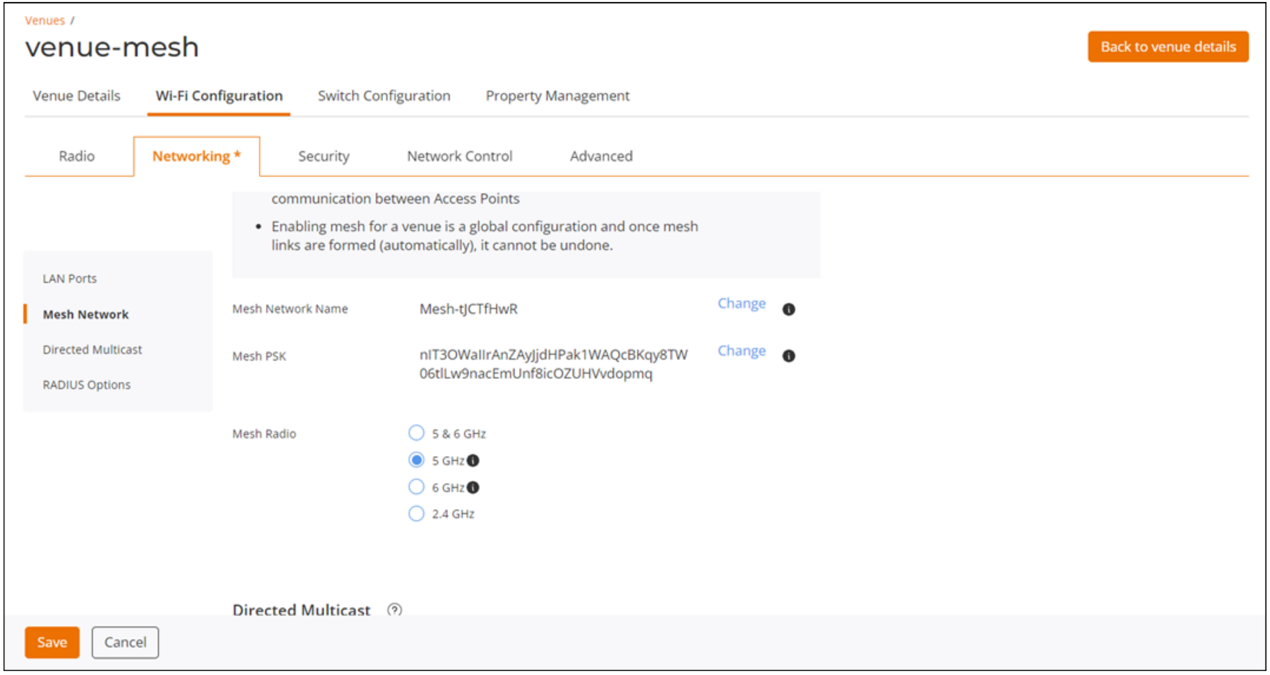
- (Optional) If you want to revert to the default port settings, click Reset to default. A confirmation message is displayed, click Continue. Modifications to the LAN port settings at the venue level are specific to each AP model, meaning any change or reset will only affect the selected AP model. Depending on the AP model, the following configurations will be reset to their default settings: PoE Operating Mode, Enable Port, Ethernet Port Profile, Enable SoftGRE Tunnel, and Client Isolation.

Configuring a Mesh Network

1. (Optional) Enable and configure Mesh networking. Go to the Mesh Network portion of the screen.
   Mesh networking adds resiliency to your venue network by ensuring that wired APs in your venue maintain a connection to the network if they lose their wired connection and allows APs to be added to a network even if it is physically prohibitive to cable them to the network.

   Note: Once enabled and Mesh-enabled APs are assigned to this venue, you cannot disable the Mesh Network option.

   Mesh Network Settings



Venues /

venue-mesh

communication between Access Points

- Enabling mesh for a venue is a global configuration and once mesh links are formed (automatically), it cannot be undone.

Mesh Network Name: Mesh-tJCTfHwR

Mesh PSK: nIT3OWaIIrAnZAyJjdHPak1WAQcBKqy8TW06tlLw9nacEmUnf8icOZUHVvdopmq

Mesh Radio: ○ 5 & 6 GHz ● 5 GHz ○ 6 GHz ○ 2.4 GHz

Directed Multicast

2. Toggle the Mesh Network switch to ON. The screen refreshes, displaying these settings: By

default, Mesh Network is set to OFF.

- Mesh Network Name: Auto-generated by RUCKUS One
- Mesh PSK: Auto-generated by RUCKUS One
- Mesh Radio: Defaults to 5 & 6 GHz

3. (Optional) Click Change to modify the Mesh Network Name or Mesh PSK and click Save to save the change.

   > Note: To prevent networking issues, you may change the Mesh Network Name and Mesh PSK only one time (and you must Save the change), but RUCKUS strongly recommends not changing them.

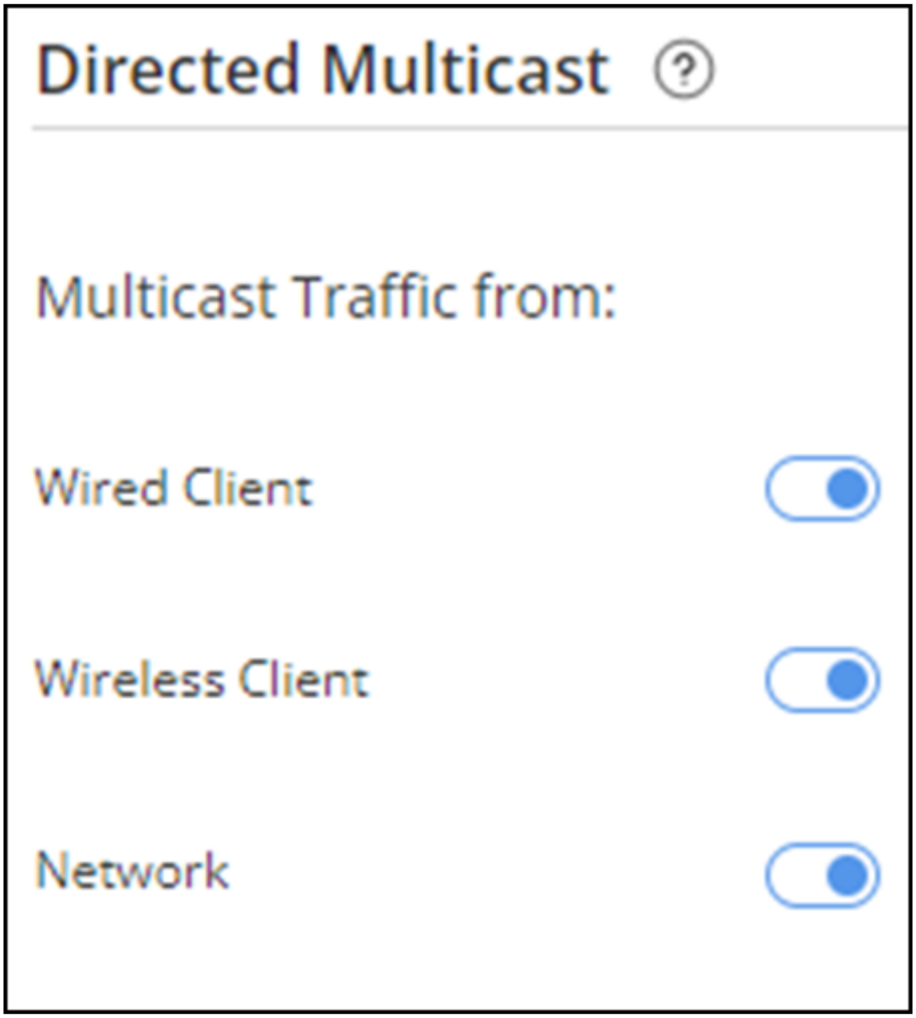
4. (Optional) Modify the Mesh Radio by selecting the 5 & 6 GHz (default) or 2.4 GHz option.

Configuring Directed Multicast

1. Configure handling of multicast traffic. Go to the Directed Multicast portion of the screen. Directed Multicast converts multicast traffic to unicast packets, thereby cutting down on multicast flooding and enhancing the performance in wireless networks.
   Enabled by default, the Directed Multicast feature can be disabled or re-enabled separately for Wired Client, Wireless Client, and Network traffic by toggling the switch OFF or ON, respectively.

2. Select one from the following options:
   - Wired Client: This option controls multicast-to-unicast conversion from wired clients on a non-trunk interface.
   - Wireless Client: This option controls multicast-to-unicast conversion from wireless clients.
   - Network: This option controls multicast-to-unicast conversion from wired clients on a trunk interface.

   Directed Multicast Settings



Directed Multicast

Multicast Traffic from:

Wired Client ●

Wireless Client ●

Network ●

When Directed Multicast is enabled, the AP inspects multicast traffic and monitors client IGMP/MLD subscriptions to determine packet handling. For multicast data that the wireless clients of the AP are subscribed to, the AP will convert packets to unicast. When no client is subscribed, the AP will drop the packets. Some well-known traffic types (Bonjour, uPnP, and so on) will bypass this logic altogether, and the multicast-to-unicast conversion will be determined by Directed Threshold in the WLAN advanced settings.

Configuring Cellular Options

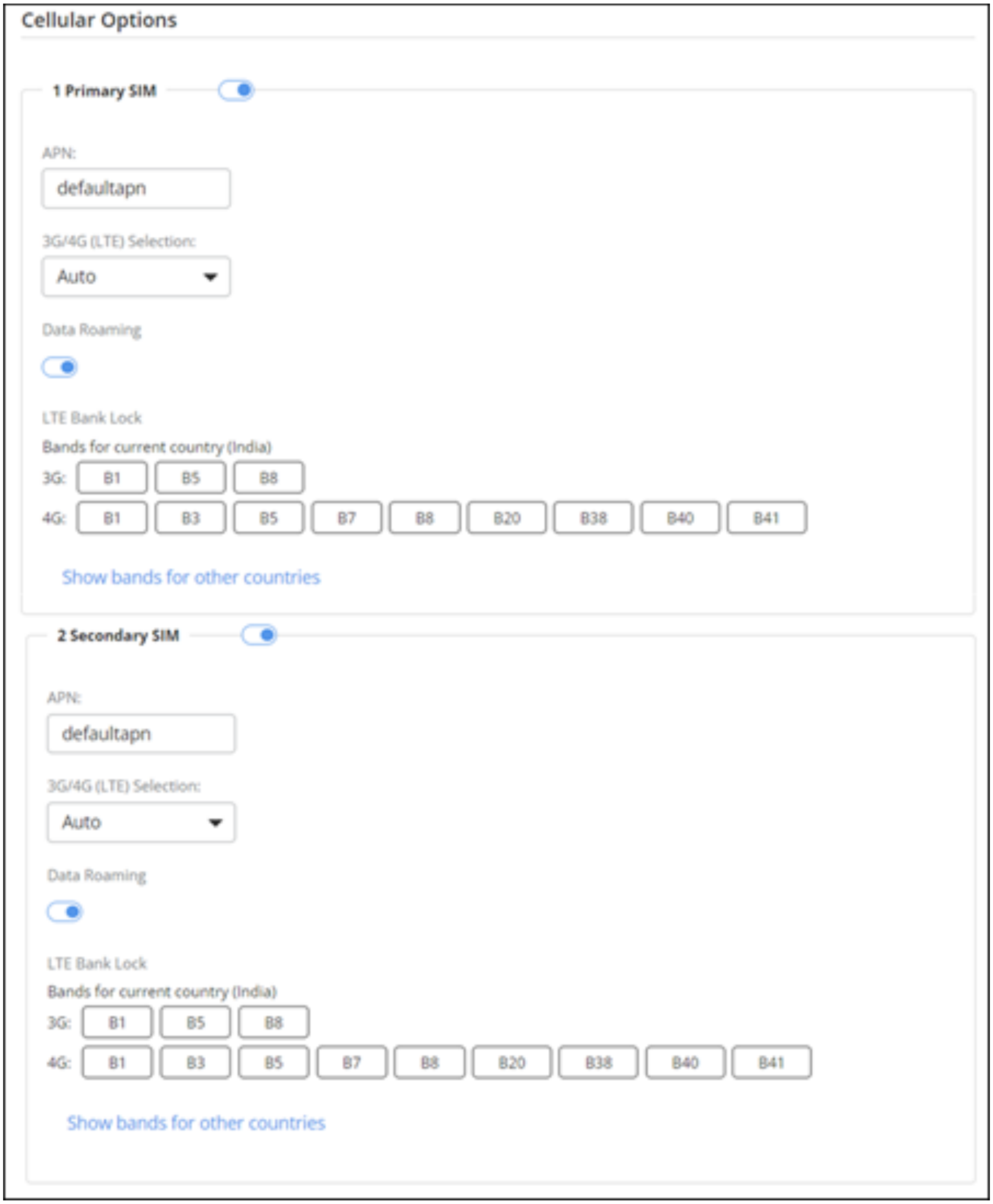
1. If your venue has an M510 AP, then you can access the Cellular Options sub-tab or scroll down to the Cellular Options section.

2. Configure the following settings (fields are identical for both the 1 Primary SIM and 2 Secondary SIM sections).

   By default, both 1 Primary SIM and 2 Secondary SIM are set to ON. Use the toggle button to set the SIMs to ON or OFF.

   Note: At least one SIM slot (Primary or Secondary) must be enabled.

   Cellular Options Settings



Cellular Options

1 Primary SIM

APN: defaultapn

3G/4G (LTE) Selection: Auto

Data Roaming

LTE Bank Lock

Bands for current country (India)

3G: B1 B5 B8

4G: B1 B3 B5 B7 B8 B20 B38 B40 B41

Show bands for other countries

2 Secondary SIM

APN: defaultapn

3G/4G (LTE) Selection: Auto

Data Roaming

LTE Bank Lock

Bands for current country (India)

3G: B1 B5 B8

4G: B1 B3 B5 B7 B8 B20 B38 B40 B41

Show bands for other countries

Configure the following settings (fields are identical for both the 1 Primary SIM and 2 Secondary SIM sections).

- APN: Enter the APN name.
- 3G/4G (LTE) Selection: By default, Auto is configured. You can select either 4G (LTE) only, or 3G only, or Auto.
- Data Roaming: By default, data roaming is set to ON. To disable data roaming, toggle the Data Roaming option to OFF.
- LTE Band Lock: Select the bands for 3G and 4G for your current country. Click Show band for other countries to view the available bands for other Domain 1 and Domain 2 countries, and Japan.

- Select the WAN Connection.
  - Ethernet (Primary) with cellular failover
  - Cellular (Primary) with Ethernet failover
  - Ethernet Only
  - Cellular Only
- Set the Primary WAN Recovery Timer. The default value is 60 seconds. The valid value is from 10 through 300 seconds.

Configuring Smart Monitor

1. Manage Smart Monitor settings at the venue level. Go to the Smart Monitor portion of the screen.
2. Toggle the switch to ON for all the APs in the Venue. By default, Smart Monitor is set to OFF.
3. Configure the settings:
   a. Heartbeat Interval: Indicates the time interval at which an AP sends a heartbeat (arping) to confirm its reachability to the default gateway. Valid values are 5 through 60 seconds, default is 10 seconds.
   b. Max Retries: Indicates the maximum number of failed connection attempts after which the gateway is considered unreachable. Valid values are 1 through 10, default is 3 retries.

Configuring RADIUS Options

1. Manage RADIUS options at the venue level. Go to the RADIUS Options portion of the screen. The Override the settings in active networks setting is disabled by default.
2. Toggle the switch to ON to enable the venue-level override.
3. Configure the settings:
   - NAS ID: Defines the ID sent to the RADIUS server, which will identify the AP. Select the appropriate option from the menu; options include WLAN BSSID (default selection), Venue Name, AP MAC, and User-defined. Note that selecting User-defined prompts you to define a Custom NAS ID.
   - MAC Delimiter: Select either Dash or Colon for the MAC Delimiter. This option appears for the NAS ID types WLAN BSSID and AP MAC.

- NAS Request Timeout: Indicates the duration after which an expected RADIUS Response message is considered to have failed. Valid values are 2 through 20 seconds, default is 2 seconds.
- NAS Max Retries: Indicates the maximum number of failed connection attempts after which the controller will failover to the backup RADIUS server. Valid values are 2 through 10 retries, default is 2 retries.
- NAS Reconnect Primary: Indicates the time interval after which the controller will recheck if the primary RADIUS server is available when the controller has failed over to the backup RADIUS server. Valid values are 1 through 300 minutes, default is 5 minutes.
- Called Station ID: Indicates the format for the called station ID, which is sent to the RADIUS server as an attribute, and can be used in policy decisions. Select the appropriate option from the menu; options include WLAN BSSID (default selection), AP MAC, AP Group, and None.
- Single Session ID Accounting: Enable this feature to allow the APs to maintain one accounting session (including statistics) for a user roaming between APs. Disabled by default. Toggle the switch to ON to enable the feature.

800-73730-001 Rev E 29 May 2025