

RUCKUS One Online Help

(index.html)

Search



Configuring Additional Settings for a Wi-Fi Network

While creating a new network or modifying an existing network, you can configure a range of additional options that give you a high degree of control over the way the network functions.

These options include VLAN configuration, network access controls, radio throughput settings, networking configurations, and advanced quality or service settings. Note that options vary from network to network, for example, only Captive Portal networks include User Connection options.

Complete one of the following steps to configure the additional settings for a Wi-Fi network.

1. Configure additional options while adding a new wireless network.
 - a. Step through the Create New Network wizard until you reach the Settings or Onboarding page (page name is dependent on the network type).
 - b. Click on Show more settings to expand the list of additional settings.
2. Edit an existing network.
 - a. Navigate to Wi-Fi > (and then) Wi-Fi Networks > (and then) Wi-Fi Networks List.
 - b. Click the check box for the specific Wi-Fi network that you want to configure, then click Edit. The Edit Network page is displayed.
 - c. Click Next to advance through the wizard until you reach the More Settings page, or click More Settings in the wizard's navigation menu.

The following sub-tabs are accessible. By default, the VLAN sub-tab is displayed. Each sub-tab includes additional Wi-Fi configuration options to configure the settings of your preference. Refer to the following instructions to customize each of the available settings:

 - VLAN - Refer to *Configuring the VLAN Settings*
 - Hotspot 2.0 - Refer to *Configuring the Hotspot 2.0 Settings for a Wi-Fi Network*. The Hotspot 2.0 sub-tab is displayed only for the Hotspot 2.0 Access network type.
 - User Connection - Refer to *Configuring the User Connection Settings*. The User Connection sub-tab is displayed only for Captive Portal network types.

- Network Control - Refer to *Configuring the Network Control Settings*
- Radio - Refer to *Configuring the Wi-Fi Radio Settings*
- Networking - Refer to *Configuring the Networking Settings*
- Advanced - Refer to *Configuring the Advanced Settings*

Note:

Demonstration of Advanced Settings for a Wi-Fi Network. This video explains advanced settings for a Wi-Fi network and walks you through the process of configuring them.

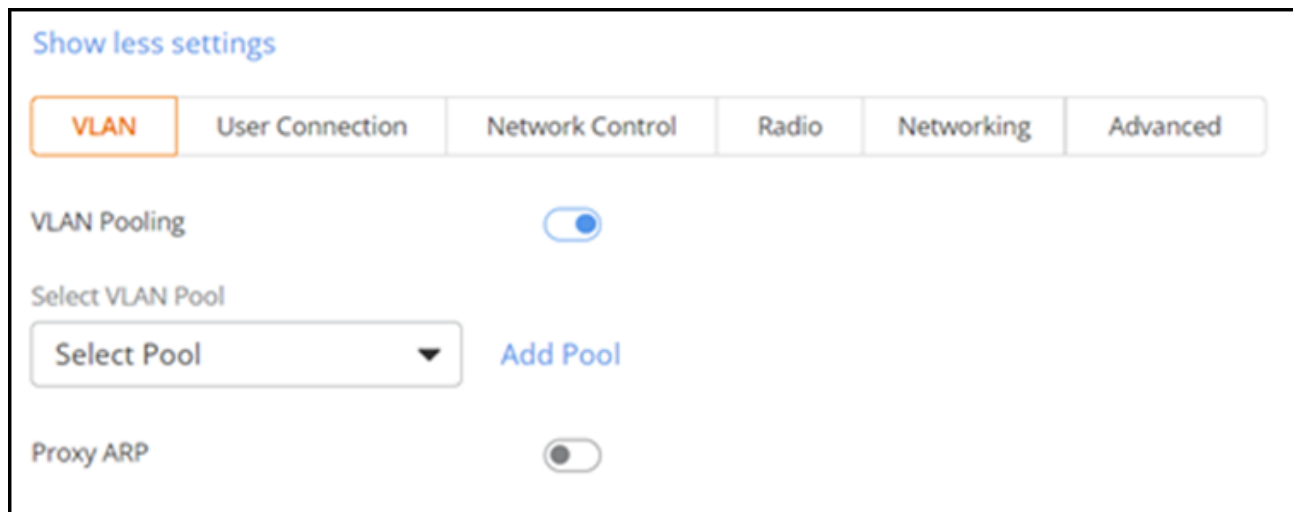
Click to play video in full screen mode. (<https://play.vidyard.com/Jm3S4CCwJX2Z2N8E9qAZdJ>)

Configuring the VLAN Settings for a Wi-Fi Network

Configure any or all of the settings in the VLAN sub-tab, as necessary, for your network needs. Note that required fields already have a default value assigned, which you may retain or modify.

1. You can either configure VLAN Pooling or assign a VLAN ID to this network. Toggle the VLAN sub-tab, toggle the VLAN Pooling switch to ON to assign a VLAN pooling policy to this WLAN. From the Select VLAN Pooling drop-down list, select a VLAN pool or click Add Pool to configure a new VLAN pool. A VLAN pool policy allows a single VLAN, multiple VLANs (separated by comma), or a VLAN range (from 2 through 4094). By default, VLAN Pooling is disabled. Refer to *Creating a VLAN Pool (GUID-6C4711A6-F69D-4CE5-AD00-803F0C410863.html)* for more information.

Configuring the VLAN Settings



Show less settings

VLAN User Connection Network Control Radio Networking Advanced

VLAN Pooling ☒

Select VLAN Pool

Select Pool ▼ Add Pool

Proxy ARP ☐

2. For VLAN ID, enter the VLAN ID number that you want to assign to this network.
The valid range is from 1 through 4094. The default value is 1. The VLAN ID option is not available if the VLAN Pooling or Enable RUCKUS DHCP service setting is enabled.
3. Dynamic VLAN is enabled by default when MAC Authentication is enabled. Dynamic VLAN automatically and dynamically assigns wireless clients to different VLANs based on their MAC addresses, using either a pre-registered MAC list or an external MAC authentication service.
Dynamic VLAN option is available only for Passphrase (PSK/SAE), DPSK, Enterprise AAA (802.1X), 3rd Party Captive Portal (WISPr) and Open network types.
4. For Proxy ARP, toggle the switch to ON to enable this network to respond to ARP requests. Proxy ARP is disabled by default.

Configuring the Hotspot 2.0 Settings for a Wi-Fi Network

Configure any or all of the Hotspot 2.0 settings, as necessary, for your Hotspot 2.0 network needs. Note that required fields already have a default value assigned, which you may retain or modify.

1. Select the Hotspot 2.0 sub-tab.
2. For Accounting Interim Updates, set the accounting update interval, ranging from 0 through 1440. Default value is 5 minutes.

Configuring the Hotspot 2.0 Settings

Hotspot 2.0 configuration page. The 'Hotspot 2.0' tab is selected. The 'Accounting Interim Updates' is set to 5 minutes. 'Internet Access' is enabled. 'Access Network Type' is set to Private. 'IPv4 Address' is set to Single NATed private address. The 'Connection Capabilities' table shows ICMP and FTP protocols.

Protocol	Protocol No.	Port	Status
ICMP	1 (ICMP)	0	Closed
FTP	6 (TCP)	20	Closed

- Internet Access is enabled by default, which allows devices to connect to the internet through the hotspot. If this option is disabled, any device attempting to connect to the Hotspot Wi-Fi network will be able to connect to the network but will not be able to access the internet.
- For Access Network Type, select the access network type from the list.
- For IPV4 Address, select the IPV4 address type for the network.
- For Protocol, select a preconfigured protocol from the Connection Capabilities table or click Add. In the Add Protocol sidebar, add a Protocol Name, Protocol Number, Port Number, Status, and click Save.

Configuring the User Connection Settings for a Wi-Fi Network

Configure any or all of the user connection settings, as necessary, for your Captive Portal network needs. Note that required fields already have a default value assigned, which you may retain or modify.

- Select the User Connection sub-tab.

Configuring the User Connection Settings

Show less settings

VLAN	User Connection	Network Control	Radio	Networking	Advanced
------	------------------------	-----------------	-------	------------	----------

Max number of devices per credentials * ?

1

User Connection Settings

Allow the user to stay connected for ?

1 Days

Do not redirect to the portal when reconnecting within

☒ 4 Hours since last redirection, or ?

60 Minutes since disconnection (Grace period) ?

2. For Max number of devices per credentials, use the arrows or enter a value ranging from 1 through 10. The default value is 1. Sets the maximum number of devices that the guest can connect using the Active Directory or LDAP credentials. This option is available for Active Directory or LDAP server captive portal network type.

3. For Allow the user to stay connected for, from the drop-down list, select the Minutes, Hours, or Days and then enter the duration of connection time after which the client is disconnected or use the arrows to select the duration in minutes, hours, or days. By default, the duration is set to 1 day. The maximum duration can be up to 10 days, 240 hours, or 14400 minutes.

Note: After exceeding the configured duration for the session, the client will be disconnected from the network and asked to re-authenticate with the portal.

4. In the Do not redirect to the portal when reconnecting within section, from the drop-down list, select Minutes, Hours, Days, or Weeks and then enter the duration or use the arrows to select the number of minutes, hours, days, or weeks. enter the duration of wait time after which the client is redirected to reconnect with the portal for or use the arrows to select the duration in Minutes, Hours, or Days, or Weeks.

- Minutes: The valid range is from 1 through 1440 minutes.
- Hours: The valid range is from 1 through 24 hours.
- Days: The valid range is from 1 through 30 days.
- Weeks: The valid range is from 1 through 7 weeks.

5. You can set the Grace Period, which determines the number of minutes during which previously authenticated clients can reconnect to the network without re-authentication. By default, the grace period is set to 60 minutes. However, the grace period cannot exceed the total connection time allotted to the user or 14,399 minutes (approximately 10 days).

Configuring the Network Control Settings for a Wi-Fi Network

Configure any or all of the network control settings, as necessary, for your network needs. Note that required fields already have a default value assigned, which you may retain or modify.

1. Select the Network Control sub-tab.

Configuring the Network Control Settings

[Show less settings](#)

VLAN	User Connection	Network Control	Radio	Networking	Advanced
------	-----------------	------------------------	-------	------------	----------

DNS Proxy

☐

Wi-Fi Calling

☐

Client Isolation

☐

Anti-spoofing

☐

Logging client data to external syslog

☐

Application Recognition & Control [?](#)

☒

DHCP

Force DHCP

☐

DHCP Option 82

☐

Access Control

[Select separate profiles](#)

Access Control

☐

Access Policy

Policy Details

Layer 2

--

Layer 3

--

Device & OS

--

Applications

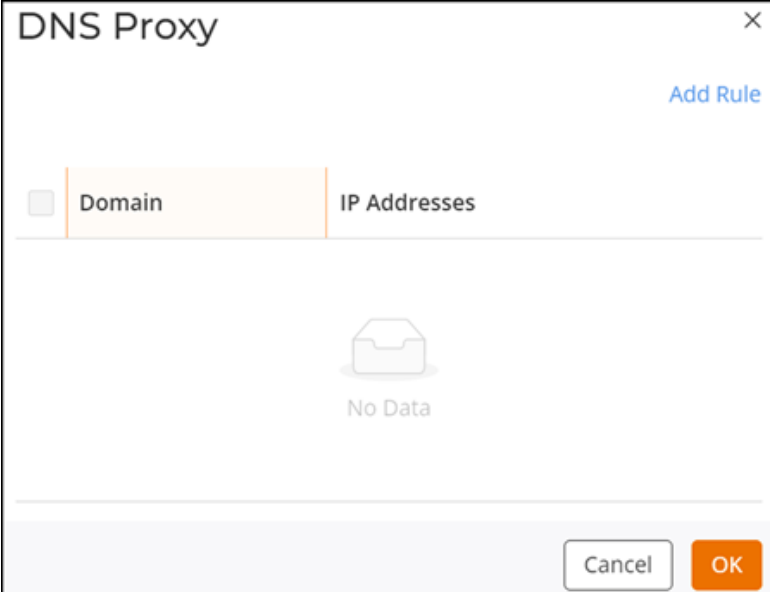
--

Client Rate Limit

--

2. (Optional) Toggle the DNS Proxy switch to ON. The DNS Proxy dialog box is displayed. DNS Proxy enables this network to respond to DNS requests. DNS Proxy is disabled by default.

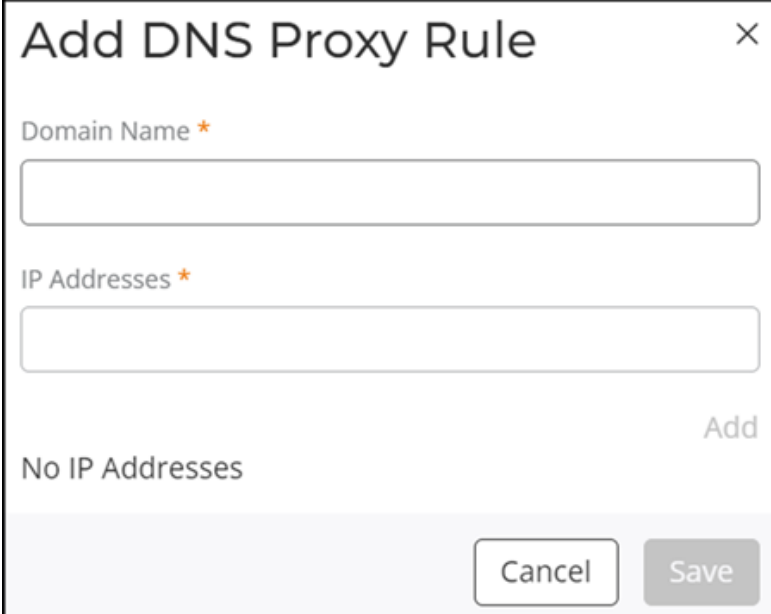
DNS Proxy Dialog Box



The screenshot shows a window titled "DNS Proxy" with a close button (X) in the top right corner. In the top right, there is a blue link labeled "Add Rule". Below this, there are two tabs: "Domain" (selected, highlighted in orange) and "IP Addresses". The main area of the window is empty, with a folder icon and the text "No Data" in the center. At the bottom, there are two buttons: "Cancel" and "OK".

- a. Click Add Rule to add a new DNS proxy rule. In the Add DNS Proxy Rule dialog box, configure the following settings:
- Domain Name: Enter a domain name for the DNS proxy rule.
 - IP Addresses: Enter an IP address.

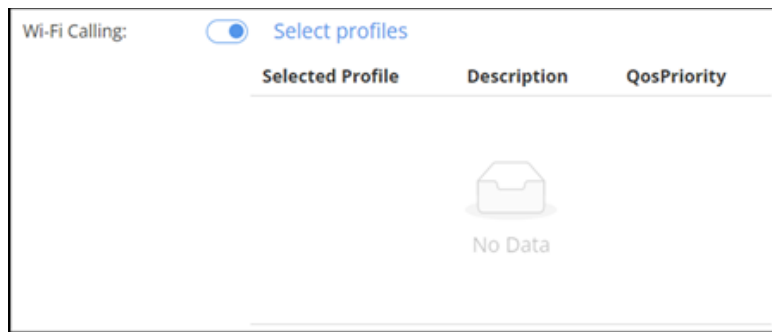
Adding a DNS Proxy Rule



The screenshot shows a dialog box titled "Add DNS Proxy Rule" with a close button (X) in the top right corner. It contains two input fields: "Domain Name" (marked with an orange asterisk) and "IP Addresses" (marked with an orange asterisk). Below the "IP Addresses" field, there is a button labeled "Add". At the bottom, there are two buttons: "Cancel" and "Save".

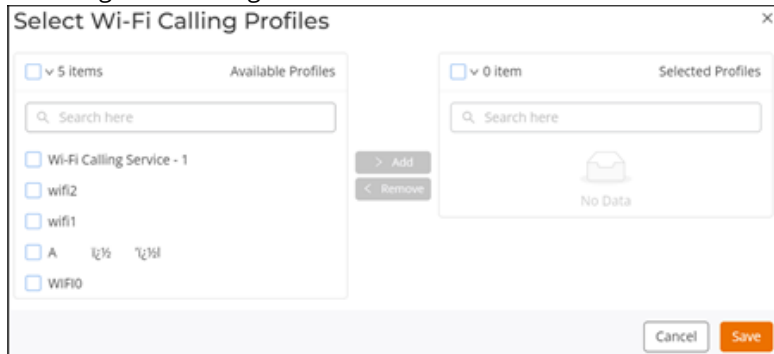
- b. Click Add to add the domain name and IP address to the table.
- c. Click Save.
- d. Click OK.
3. (Optional) Toggle the Wi-Fi Calling switch to ON to allow voice calls over a Wi-Fi network instead of a cellular network. Wi-Fi Calling is disabled by default.

Wi-Fi Calling Dialog Box



- a. Toggle the Select Profiles switch to ON. The Select Wi-Fi Calling Profiles dialog box is displayed.

Selecting Wi-Fi Calling Profiles



- b. Select the profiles in the Available Profiles table and click Add to move the selected profile to the Selected Profiles table. To remove the profiles from the Selected Profiles table, select the profiles in the Selected Profiles table and click Remove.

- c. Click Save.

4. (Optional) Toggle the Client Isolation switch to ON to prevent devices on the same network from communicating directly with each other, enhancing security. Client Isolation is disabled by default.

Client Isolation Setting


Client Isolation: ☒

Isolate Packets:

Unicast ▼

Automatic support for VRRP/HSRP: ☒

Client Isolation Allowlist by Venue: ☒

Venue	Isolation Allowlist
<div> No Data</div>	

- Isolation Packets: Select Unicast, Multicast/broadcast, or Unicast and Multicast/broadcast from the drop-down list.
- Automatic support for VRRP/HSRP: Set the switch to ON to enable the automatic support for VRRP/HSRP.
- Client Isolation Allowlist by Venue: Set the switch to ON to enable the client isolation allowlist by venue.

- (Optional) Toggle the Anti-spoofing switch to ON to verify the authenticity of devices and prevents IP address spoofing. Anti-spoofing is disabled by default.

Anti-Spoofing Setting

Anti-spoofing: ☒

☒ ARP request rate limit

15

^
v

 ppm

☒ DHCP request rate limit

15

^
v

 ppm

☐ Force DHCP

Complete the following fields:

- ARP request rate limit: Enter the ARP request rate limit.

- DHCP request rate limit: Enter the DHCP request rate limit.
6. (Optional) Toggle the Logging client data to external syslog switch to ON to send client activity logs to an external Syslog server for monitoring and analysis. Logging client data to external syslog is disabled by default.
 7. (Optional) Application Recognition & Control is enabled by default. Manages the usage and reporting of network guest application activities. You can see the applications usage of device clients from the RUCKUS One dashboard. Disabling this setting stops the monitoring and reporting of these activities.
 8. (Optional) Under DHCP, configure the following settings:
 - Force DHCP: Ensures that all devices on this network obtain their IP addresses through the DHCP server. Force DHCP is disabled by default. Toggle the Force DHCP switch to ON to enable this setting. If you enable the Anti-spoofing setting, then Force DHCP is disabled and greyed out.
 - DHCP Option 82: DHCP Option 82 allows a DHCP relay agent to insert circuit-specific information into a request that is being forwarded to a DHCP server. By default, this feature is disabled. Toggle the DHCP Option 82 switch to ON to enable this setting. This option works by setting two sub-options:
 - Agent Circuit ID (enabled by default): Select a circuit ID from the drop-down list.
 - Agent Remote ID (disabled by default): Select a remote ID from the drop-down list.
 - Sub-option 150 with VLAN ID
 - Sub-option 151
 - AP & Client MAC format delimiter

The insertion of DHCP Option 82 information is supported for wireless clients in RUCKUS One. The DHCP relay agent adds information such as the port number of the client or its own MAC address to the DHCP packet before forwarding it to the DHCP server.

Configuring DHCP Option 82

DHCP

Force DHCP ☐

DHCP Option 82 ☒

Sub-option 1 ☒ AP MAC

Sub-option 2 ☒ AP MAC-hex: ESSID

Sub-option 150 with VLAN ID ☒

Sub-option 151 ☒ ESSID

AP & Client MAC format delimiter
AA:BB:CC:DD:EE:FF

9. (Optional) Toggle the Access Control switch to ON.

Access Control Setting

Access Control [Select separate profiles](#)

Access Control ☒

Access Control Policy

1-migration-access-... ▼ [Add](#)

Access Policy	Policy Details
Layer 2	--
Layer 3	--
Device & OS	1-Migration-Access-control
Applications	--
Client Rate Limit	--

- Select a policy from the Access Control Policy drop-down list.
- Click Add to add an access control policy.
- Click Select Separate Profiles to select another access control policy. For more information, refer to *Creating an Access Control Policy (GUID-4973E975-83D3-409E-A047-AF70C969FAFF.html)*.
- Click Save as AC Policy to display the Add Access Control Policy dialog box and create a new access control policy.
- For Policy Name, enter a name.
- For Description, enter a short description for the policy.
- Configure Layer 2, Layer 3, Device & OS, Applications, and Client Rate Limit. For more information, refer to *Creating an Access Control Policy (GUID-4973E975-83D3-409E-A047-AF70C969FAFF.html)*.
- Click Save as AC Profile to create a new Access Control policy.
- If you want to cancel the Access Control Policy selection, click Select separate profiles to exit from the Select Access Control Profile.

Adding an Access Control Policy

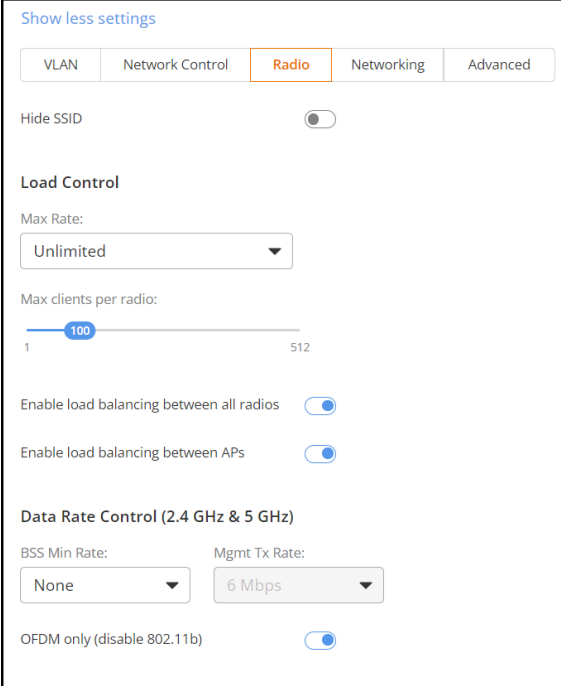
The screenshot shows the 'Add Access Control Policy' dialog box overlaid on the 'Create New Network' page. The dialog box has a title bar 'Add Access Control Policy' and a 'Settings' section. It contains two text input fields: 'Policy Name' (with a red asterisk indicating it is required) and 'Description'. Below these is a section titled 'Access Control Components' with five toggle switches: 'Layer 2', 'Layer 3', 'Device & OS', 'Applications', and 'Client Rate Limit'. At the bottom of the dialog are 'Add' and 'Cancel' buttons. The background page shows a sidebar with 'Settings' selected, and a main area with various network configuration options like 'Client Isolation', 'Anti-spoofing', 'Logging', 'DHCP', 'Force DHCP', 'DHCP Options', 'Access Control', 'Layer 2', 'Layer 3', 'Device & OS', 'Applications', and 'Client Rate Limit'. At the bottom of the main area are 'Cancel', 'Back', and 'Next' buttons.

Configuring the Wi-Fi Radio Settings for a Wi-Fi Network

Configure any or all of the radio settings, as necessary, for your network needs. Note that required fields already have a default value assigned, which you may retain or modify.

1. Select the Radio sub-tab.

Radio Settings



Show less settings

VLAN Network Control **Radio** Networking Advanced

Hide SSID ☐

Load Control

Max Rate:
Unlimited

Max clients per radio:
1 100 512

Enable load balancing between all radios ☒

Enable load balancing between APs ☒

Data Rate Control (2.4 GHz & 5 GHz)

BSS Min Rate: Mgmt Tx Rate:
None 6 Mbps

OFDM only (disable 802.11b) ☒

2. Toggle the Hide SSID switch to ON if you want to hide the network name from being broadcast. This setting is disabled by default.

3. Under Load Control, complete the following fields:

- Max Rate: Choose one of the following options from the drop-down list:
 - Unlimited (default): No limits on bandwidth allocation.
 - Per AP: The maximum bandwidth allocation limit of all connections to that specific network on the AP. If selected, two other options appear (enabled by default), Upload Limit and Download Limit. If either (or both) check boxes are selected, a sliding scale appears and you can drag your cursor along the line to choose the Mbps limits for each. The upload and download limit ranges from 1 through 500 Mbps.
- Max clients per radio: Limits the number of clients that can associate with this network per AP radio (default is 100). The value ranges from 1 through 512.
- Enable load balancing between all radios (enabled by default): Select this check box to enable load balancing for all radios. Load balancing helps improve network performance by helping to spread the client load between the radios on the AP.
- Enable load balancing between APs (enabled by default): Select this check box to spread the client load between nearby access points, so that one AP does not get overloaded while another AP sits idle.

4. Under Data Rate Control (2.4 GHz & 5 GHz), configure the following settings:

- BSS Min Rate: Select None, 1 Mbps, 2 Mbps, 5.5 Mbps, 12 Mbps, or 24 Mbps from the drop-down list. Use BSS Min Rate option to configure the minimum transmission rate that is supported by the network. If OFDM Only (Disables 802.11b) is enabled, the only valid options are 12 Mbps and 24 Mbps, with Mgmt Tx Rate fixed at 6 Mbps. This option can also be used to prevent 802.11b clients from connecting, and to allow greater client density with higher data rates.
- Mgmt Tx Rate: Select 1, 2, 5.5, 6, 9, 11, 12, or 18 Mbps from the drop-down list. This option is only available if both Enable OFDM only and BSS Min Rate are disabled. (Otherwise, the Mgmt Tx Rate is defined by those settings.) Use the Mgmt Tx Rate setting to configure the rate at which management frames are sent. The default

is 6 Mbps.

- OFDM only (Disables 802.11b): Toggle the switch to ON to enable this option. Enabling this option disables CCK rates of 1, 2, 5.5, and 11 Mbps, so no 802.11b-only clients can connect. Beacons and probe responses will be transmitted at 6 Mbps, and data frames at 6, 9, 18, 24, 36, 48, and 54 Mbps. Enforcing higher minimum data rates increases overall network throughput capacity but reduces the distance at which clients are able to remain connected.

Configuring the Networking Settings for a Wi-Fi Network

Configure any or all of the networking settings, as necessary, for your network needs. Note that required fields already have a default value assigned, which you may retain or modify.

1. Select the Networking sub-tab.

Configuring the Networking Settings

[Show less settings](#)

VLAN	Network Control	Radio	Networking	Advanced
Enable Agile Multiband (AMB) ? <input type="checkbox"/>				
Enable 802.11k neighbor reports <input checked="" type="checkbox"/>				
Enable 802.11d ? <input checked="" type="checkbox"/>				
Enable 802.11r Fast BSS Transition ? <input type="checkbox"/>				
Client Inactivity Timeout ?				
<input type="text" value="120"/> <input type="button" value="↑"/> <input type="button" value="↓"/> Seconds				
Directed MC/BC Threshold:				
<input type="text" value="5"/> <input type="button" value="↑"/> <input type="button" value="↓"/>				
Per radio client count at which an AP will stop converting group addressed data traffic to unicast				
Airtime Decongestion: <input type="checkbox"/>				

2. Toggle the Enable Agile Multiband (AMB) switch to ON to enable the feature. Disabled by default. Agile Multiband prioritizes roaming performance in indoor environments, supporting IEEE protocols 802.11k, 802.11v, 802.11u, and 802.11r. Agile Multiband is a collection of features designed to improve resource utilization, balance Wi-Fi load, increase capacity, and provide the best possible Wi-Fi experience. AMB configures WLANs to send IE Multi Band Operation information elements that include beacon reporting, channel non-preference, cellular capability, and association disallow.
3. The Enable 802.11k neighbor reports setting enhances roaming by providing a list of neighbor APs to the client device. Enabled by default.

4. The Enable 802.11d setting allows the AP to support multiple regulatory domains by the addition of a country information element to beacons, probe requests, and probe responses. Enabled by default.
5. Toggle the Enable 802.11r Fast BSS Transition switch to ON and set the value of Mobility Domain ID (allowed value is 1 through 65535). The Enable 802.11r Fast BSS Transition setting improves efficiency and speeds up handoff processes between access points within the same network, ensuring smoother transitions and continuous connectivity. IEEE 802.11r Fast BSS Transition roaming protocol reduces the number of frame exchanges required for roaming and allows the clients and APs to reuse the master keys obtained during a prior authentication exchange. Mobility Domain ID defines the network area for fast roaming in IEEE 802.11r, allowing shared master keys for seamless client transitions. Enable 802.11r Fast BSS Transition is disabled by default.
6. For Client Inactivity Timeout, set the time duration (in seconds) after which an inactive client remains connected before being disconnected. The valid range is from 60 through 86400 seconds.
7. For Directed MC/BC Threshold, set the threshold for converting multicast or broadcast traffic to unicast to improve network efficiency. The valid range is from 0 through 5.
8. The Airtime Decongestion setting optimizes airtime usage by ensuring that all devices connected to the Wi-Fi network get a fair share of the available bandwidth. Enabled by default.
9. For Join RSSI Threshold, disable Airtime Decongestion to enable Join RSSI Threshold setting. Toggle the Join RSSI Threshold switch to ON (default is -80 dBm) and set the minimum signal strength (must be between -90 and -60 dBm) required for a client to join the network. By default, Join RSSI Threshold is disabled.
10. Toggle the Transient Client Management switch to ON and configure the following parameters:
Transient Client Management manages clients that frequently connect and disconnect to maintain network stability. This setting is disabled by default.
 - Join Wait Time: Enter a value in seconds or use the arrows. Valid value ranges from 1 through 60 seconds. The default value is -1 second.
 - Join Expire Time: Enter a value in seconds or use the arrows. Valid value ranges from 1 through 300 seconds. The default value is -1 second.
 - Join Wait Threshold: Enter a value in seconds or use the arrows. Valid value ranges from 1 through 50 seconds. The default value is 10 seconds.
11. Toggle the Optimized Connectivity Experience (OCE) switch to ON and configure the following parameters:
Optimized Connectivity Experience (OCE) enhances client connectivity and roaming performance. This setting is disabled by default.
 - Broadcast Probe Response Delay: Valid value is from 8 through 120 ms. The default value is 15 ms.
 - RSSI-Based Association Rejection Threshold: Valid value is from -90 through -60 dBm. The default value is -75 dBm.
12. Toggle the AP Host Name Advertisement in Beacon switch to ON to advertise the hostname of an AP in beacon frames for easier identification. This setting is disabled by default.
13. The GTK Rekey setting allows periodic generation of a new group key for securing multicast or broadcast traffic. Enabled by default.
14. Toggle the Multicast Filter switch to ON to enable this feature. By default, Multicast Filter is disabled.

Multicast Filter filters multicast traffic to reduce unnecessary network load. When the Multicast Filter option is enabled on an AP, it will drop all IPv4 and IPv6 multicast and broadcast from associated wireless clients except for the below which forms into "multicast filter bypass" list. Note that the downstream multicast is unaffected.

- ARP request
- DHCPv4 request
- DHCPv6 request
- IPv6 NS
- IPv6 NA
- IPv6 RS
- IGMP
- MLD
- All unicast packets

15. Multicast Rate Limiting limits the rate of multicast traffic to prevent network congestion. Multicast Filter must be enabled to configure the Multicast Rate Limiting setting.

Multicast Filter and Multicast Rate Limiting are mutually exclusive features. From the RUCKUS One web interface, you cannot enable them at the same time. SSID rate limiting will always take precedence if Multicast rate limiting is also configured. Multicast downlink rate limiting should not be greater than 50% of BSS min rate.

Note: Enabling Directed Multicast in the Venue-level or AP-level settings (which converts multicast packets to unicast) will impact the functionality of Multicast Rate Limiting.

16. BSS Priority: Adjusts the priority of Basic Service Set (BSS) to manage traffic more effectively. Set the BSS Priority to Low or High

- Low: Reduces the priority of the WLAN by limiting the throughput to all clients connected to this WLAN.
- High: Has no throughput limits. By default, the WLAN priority is set to High.

17. Under Wi-Fi 7, configure the following settings:

- Enable Wi-Fi 6/ 7: Allows some legacy Wi-Fi 5 clients with out-of-date drivers to inter-operate with a Wi-Fi 6/7 AP. Toggle the Enable Wi-Fi 6/ 7 switch to ON. By default, Enable Wi-Fi 6/ 7 is enabled.
- Multi-Link operation (MLO): MLO allows Wi-Fi 7 devices to use multiple radio channels simultaneously (at least two) for better throughput and efficiency. For MLO to function, radios on APs must be active, and their usage is determined by AP configuration, which limits the number of supported 6 GHz networks. By default, MLO is disabled and greyed out. For the functioning of MLO, ensure that either the WPA3 or OWE encryption method is activated.

18. Under RADIUS Options, configure the following settings. This option is available for Enterprise AAA (802.1X), Hotspot 2.0 Access, Open Network with External MAC Authentication, and third-party captive portal network types.

- NAS ID: Identifies clients to a RADIUS server. Select an option from the list.
- MAC Delimiter: Select Dash or Colon.
- NAS Request Timeout: Enter the timeout period (in seconds) after which an expected RADIUS response message is considered to have failed.

- NAS Max Retries: Enter the number of failed connection attempts after which RUCKUS One will failover to the backup RADIUS server.
- NAS Reconnect Primary: Enter the number of minutes after which RUCKUS One will attempt to reconnect to the primary RADIUS server after failover to the backup server.
- Called Station ID: Allows NAS to send the ID, which is called by the user. Select an option from the list.
- Single Session ID Accounting: Allows 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.
This option is not visible unless one of the selected identity providers enable an accounting service. You can find the Accounting Service option in the AAA Settings page by navigating to Network Control > (and then) Policies & Profiles > (and then) Identity Provider > (and then) Add Identity Provider.

RADIUS Options

RADIUS Options

NAS ID ?

WLAN BSSID ▼

MAC Delimiter

☒ Dash ☐ Colon

NAS Request Timeout *

3 ^ v Seconds

NAS Max Retries *

2 ^ v Retries

NAS Reconnect Primary *

5 ^ v Minutes

Called Station ID

WLAN BSSID ▼

Single Session ID Accounting ? ☐

Configuring the Advanced Settings for a Wi-Fi Network

Configure any or all of the advanced settings, as necessary, for your network needs. Note that required fields already have a default value assigned, which you may retain or modify.

1. Select the Advanced sub-tab.

Configuring the Advanced Settings

Show less settings

VLAN Network Control Radio Networking **Advanced**

DTIM (Delivery Traffic Indication Message) Interval ?

1 Lower latency Longer client battery life

QoS

QoS Mirroring ? ☒

QoS Mirroring Scope


MSCS requests only

Mirroring for clients sending MSCS (Mirrored Stream Classification Service) requests

QoS Map Set ☐

Back Next

- For DTIM (Delivery Traffic Indication Message) Interval, set a value ranging from 1 (default) through 255. DTIM interval controls how often DTIM messages are transmitted and this affects the frequency of data transmissions per broadcast beacon. Setting the DTIM interval to a lower value results in more frequent DTIM messages, which can prevent mobile devices from going into power-save mode and thereby increasing battery consumption.
- QoS Mirroring, enables APs to learn User Priority (UP) from uplink traffic and mirror it in downlink traffic. This ensures proper traffic differentiation, prioritizing critical applications like voice and video to maintain QoS. By default, QoS Mirroring is enabled. Configure the QoS Mirroring Scope by selecting one of the following options from the drop-down list:
 - MSCS requests only (default): When selected, QoS Mirroring is enabled only for clients that send mirrored stream classification service (MSCS) requests.
 - All clients: When selected, QoS Mirroring is enabled for all clients.

Click the  icon next to QoS Mirroring to view the feature synopsis and the minimum required AP firmware version. Click See the compatibility requirements to view the minimum required AP firmware version and the supported AP model families (denoted by their applicable IEEE 802.11 standard).

Note: QoS Mirroring is supported only on APs that are running RUCKUS One AP firmware 7.0 and later versions.

- Toggle the QoS Map Set switch to ON. The QoS Map Set setting reprioritizes downlink packets based on the configured mappings. When an AP receives a downlink packet, it checks the existing DSCP (Layer 3 QoS) marking, compares it to this map set and then changes the user priority (Layer 2 QoS) values for transmission by the AP. By default, QoS Map Set is disabled.
If you want to edit a QoS map set, select a specific QoS map set from the table and click the Edit option that appears above the table. In the Edit QoS Map sidebar, edit the required fields and click Apply.

- Click Next to go the Venue page to activate this network on the venue.

For the Captive Portal network types (except Cloudpath and third-party), you will see an additional screen, Portal Web Page before navigating to the Venue screen to activate the network.

800-73730-001 Rev D 29 April 2025
© 2024 CommScope, Inc. All rights reserved.