

RUCKUS One Online Help

(index.html)

Search



Creating an Open Network

You can create a network that allows users to join the network without going through any authentication process.

Complete the following steps to create an open network.

CAUTION: RUCKUS strongly advises against creating an open network. Wireless communication on an open network is not secure and information (including sensitive data, such as personal information, credit card information, and so on) that your users send over or through the network can easily be intercepted.

1. On the navigation bar, click Wi-Fi > (and then) Wi-Fi Networks > (and then) Wi-Fi Networks List.
The Networks page is displayed.
2. Click Add Wi-Fi Network. Alternatively, select a Open Network setting that you want to copy and click Clone at the top of the table.
The Create New Network page is displayed.
3. Complete the following settings on the Network Details page.
 - Network Name: Enter a name (up to 32 characters) that you want assign to the network.
 - Set different SSID: Use this option to configure the SSID different from the network name.
 - Description: Enter a description (up to 64 characters) to help you identify the network using.
 - Network Type: Click Open Network.

When the network type is selected, a structure diagram of a Open Network type is displayed.

4. Click Next.
The Open Settings page is displayed.
Open Network Settings

Wi-Fi / Wi-Fi Networks / Network List /

Create New Network

Open Settings

- OWE encryption ☒
- OWE Transition mode ☐
- MAC Authentication ☒
- ☐ MAC Registration List
- ☒ External MAC Auth
- MAC Address Format: AA-BB-CC-DD-EE-FF

Authentication Service

Authentication Server [Add Server](#)

Proxy Service ☐

Accounting Service

Identity Group [View Details](#) | [Add](#)

Use single identity association to all onboarded devices ☐

[Show more settings](#)

[Cancel](#) [Back](#) [Next](#)

Diagram: Local AAA Server, My network, Data: Local-Breakout

5. Toggle the OWE encryption switch to enable this feature and configure OWE Transition mode.

6. Toggle the OWE Transition mode switch to enable this feature.

The migration from an open Wi-Fi network to an enhanced open Wi-Fi network is completed step by step, while user devices are also gradually upgrading. For STAs that do not support OWE authentication, the OWE transition mode is available so that such STAs can access the network in open authentication mode. Meanwhile, the OWE transition mode allows OWE-capable STAs to access the network in OWE authentication mode. The OWE transition mode is implemented as follows:

- Two SSIDs are created on an AP, for example, SSID 1 for open authentication and SSID 2 for OWE authentication.
- SSID 1 is broadcast, and SSID 2 is hidden. Therefore, only SSID 1 is visible to STAs. SSID 1 carries an OWE Transition Mode element and SSID 2 information. When an OWE-capable STA connects to SSID 1, it is directly associated with SSID 2 in OWE transition mode.
 - Non OWE-capable device connects SSID1
 - OWE-capable device connect to SSID2 from SSID1

Note: The OWE transition WLAN allows you to broadcast the OWE SSID either on the 6 GHz radio band alone or across all the radio bands (2.4 GHz, 5 GHz, and 6 GHz) in a venue.

Enabling OWE Encryption

Wi-Fi / Wi-Fi Networks / Network List /

Create New Network

Open Settings

- ☒ Enable OWE encryption ?
- ☒ Enable OWE Transition mode ?
- ☐ MAC Authentication ?

My network

Data: Local-Breakout

Show more settings

Cancel Back Next

7. For the MAC Authentication option, toggle the switch to enable this feature and complete the following fields:

Enabling MAC Authentication

Wi-Fi / Wi-Fi Networks / Network List /

Create New Network

Open Settings

- ☒ Enable OWE encryption ?
- ☒ Enable OWE Transition mode ?
- ☒ MAC Authentication ?

- ☐ MAC Registration List
- ☒ External MAC Auth

Authentication Service

Authentication Server

Radius_10.223.71.191 Add Server

Primary Server

10.223.71.191:1812

Shared Secret

.....

Cancel Back Next

Note: MAC Authentication provides an additional level of security for corporate networks. Client MAC addresses are passed to the configured RADUIS servers for authentication and accounting. You cannot

modify previously configured MAC authentication settings. To accommodate any modifications, you must create a new MAC authentication settings.

Note: Regardless of whether MAC authentication is configured using MAC Registration List or External MAC Auth, the Dynamic VLAN setting will be automatically enabled. You will find the Dynamic VLAN option under the VLAN sub-tab when you click Show more settings.

Note: If you configured MAC Registration List, you will also have to configure a new Identity profile (refer to *Adding an Identity (GUID-12CB0293-3EB3-42D6-A099-1DBE817C0D34.html)*) and associate it with a client device (refer to *Adding a Device to an Identity (GUID-C5FC7A1E-37C8-433C-87E9-56181161B24D.html)*).

- Select one option from the following:
 - MAC Registration List: Complete the following fields:
 - MAC Registration List: Select the MAC registration from the drop down list or add a new MAC registration.
 - a. Click Add to add a new MAC registration. The Add MAC Registration List dialog box is displayed.
Add MAC Registration List Dialog Box

Add MAC Registration List

Name *

List Expiration *

☒ Never expires

☐ By date

☐ After...

Automatically clean expired entries

☒

Identity Group *

Select ... Add

Use Single Identity for all connections

☐

Adaptive Policy Set

Select ... Add

Apply Cancel

b. Complete the following fields:

- Name: Enter a name for the MAC registration list.
- List Expiration: Select one option from the following:
 - Never expires: This license do not have a expiry date.
 - Date: Select date, month, and year. This license expire after the selected date.
 - After: Select a number from the drop down list and select a duration of license expiration in Hours, Days, Weeks, Months, and Years. This license expire after the selected duration.
- Automatically clean expired entries: Toggle switch to ON to enable this feature.
- Access Policy Set: Select an access policy set from the drop down list or add a new access policy set.
 - 1) Click Add Access Policy Set to add a new access policy set. Refer to *Creating an Adaptive Policy*

(GUID-2B2C6C55-6C24-4EFE-8F2F-0C4B230D9C4A.html).

c. Click Apply.

- External MAC Auth: Select the external MAC authentication and complete the following fields:
 - Authentication Service: Select a RADIUS authentication server from the drop down list or add a new RADIUS authentication server.
 - a. Click Add Server to add a new RADIUS authentication server. Refer to *Creating a Radius Server Profile* (GUID-F0DFD674-D2E0-42F8-AA09-CBCBE9E419BF.html).

- Proxy Service: Toggle switch to ON to enable the proxy service.

Note: Use the controller as proxy in 802.1X networks. A proxy AAA server is used when APs send authentication/accounting messages to the controller and the controller forwards these messages to an external AAA server.

- Accounting Service: Toggle switch to ON to enable the accounting service. Select a RADIUS accounting server from the drop down list or add a new RADIUS accounting server.
 - a. Click Add Server to add a new RADIUS authentication server. Refer to *Creating a Radius Server Profile* (GUID-F0DFD674-D2E0-42F8-AA09-CBCBE9E419BF.html).

- Identity Group:

Note:

- When an identity group is selected, all devices joining the network will automatically become an identity within that group, as displayed on the Identity Group page.
 - Users have the option to either select an existing identity group from the list or create a new one.
 - Upon selecting an identity group, users can enable the Use single identity association to all onboarded devices option and subsequently choose a specific identity for association.
 - If a single identity is associated, all devices joining the network will be linked to that designated identity within the selected identity group.
 - During network editing, the initially selected identity group cannot be removed; however, it can be changed to a different identity group.
 - The identity configuration section is not applicable to the MAC Registration List when MAC Authentication is enabled.
- a. Select an identity group from the drop-down or click Add to add an identity group. Refer to *Adding an Identity Group* (GUID-60E97713-D793-4659-86BF-94F8BF209EA6.html) for instructions on how to add an identity group.
 - b. To view details about the identity group, click View Details. The Identity Group sidebar is displayed.
 - c. (Optional) Click the toggle to enable the Use single identity association to all onboarded devices option. The Identity section is displayed. If this option is selected, all devices that connect to this

network are associated with this identity. If this option is not enabled, an identity for each connected device is created under the identity group.

Configuring an Identity Group for Open Network

- d. Click Associate Identity to access the Associate Identity sidebar and select an identity to associate with the identity group, and then click Add.
- e. (Optional) Click Add Identity to access the Create Identity sidebar to add an identity. Refer to *Adding an Identity (GUID-12CB0293-3EB3-42D6-A099-1DBE817C0D34.html)* for instructions on how to add an identity. Click Change to access the Associate Identity sidebar and select another identity.

8. Click Show more settings.

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 *Configuring Additional Settings for a Wi-Fi Network (GUID-8AE1D265-5C9B-4B71-9A5C-A57C3CFA586A.html)* to configure each of the available 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/Jm3S4CCwJXZ22N8E9qAZdJ>)

9. Click Next.

The Venues page is displayed.









10. Complete the following steps to configure a venue:

a. Select the venues in which you want to activate this network:

- To activate the network in all of your venues, select the check box beside Venue at the top of the table and click Activate.
- To activate the network in a specific venue, locate the venue from the list, and set the switch to ON in the Activated column.

The APs, Radio, and Scheduling of the selected venue is displayed in the table.

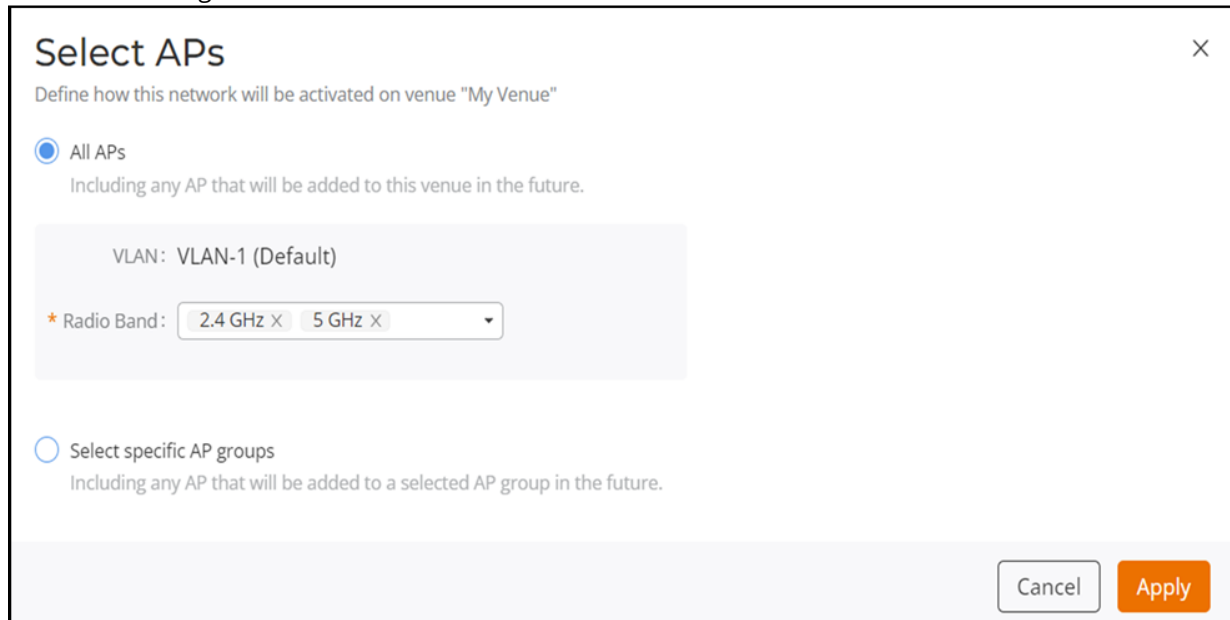
Selecting Venues

Venues								
Select venues to activate this network								
2 selected  Activate Deactivate								
 Venue	City	Country	Networks	Wi-Fi APs	Activated	APs	Radios	Scheduling
 1.space MM ^&*&MM	Sunnyvale, California	United States		0		All APs	2.4 GHz, 5 GHz	24/7 
 111sample	Sunnyvale, California	United States	7	2		All APs	2.4 GHz, 5 GHz	24/7 

b. By default, this network configuration is applicable for all APs and with Radio Band of 2.4 and 5 GHz. To select specific AP groups and modify Radio Band, complete the following steps:

- 1) Click All APs in the APs column. The Select APs dialog box is displayed. To activate this network on all current and future APs at this venue. You can also choose a radio band of 2.4 GHz, 5 GHz, or both.

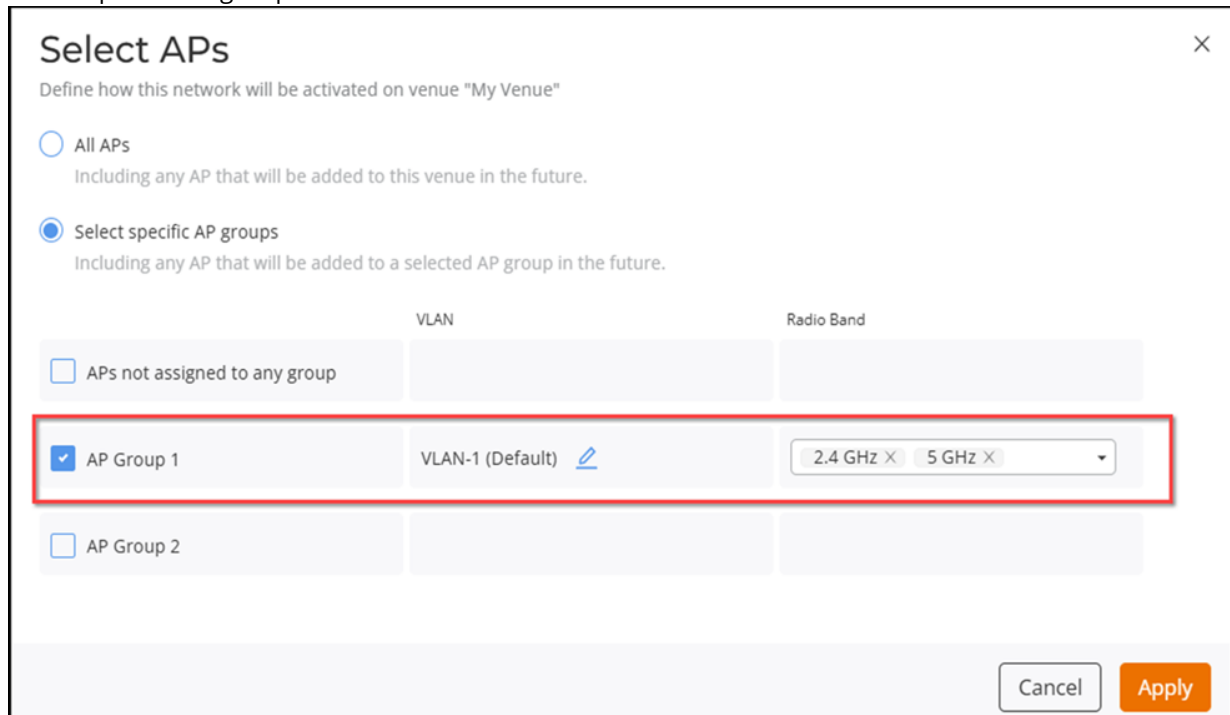
Select APs Dialog Box



The dialog box is titled "Select APs" with a close button (X) in the top right corner. Below the title is the instruction "Define how this network will be activated on venue 'My Venue'". There are two radio button options: "All APs" (selected) and "Select specific AP groups". The "All APs" option includes the text "Including any AP that will be added to this venue in the future." Below this, there is a light gray box containing the text "VLAN: VLAN-1 (Default)" and a "Radio Band" dropdown menu with "2.4 GHz" and "5 GHz" selected. The "Select specific AP groups" option includes the text "Including any AP that will be added to a selected AP group in the future." At the bottom right are "Cancel" and "Apply" buttons.

- 2) Click Select specific AP groups to activate this network on specific AP groups including any AP that is added to selected AP groups in the future. The APs not assigned to any group option is displayed. After APs not assigned to any group is selected, VLAN and Radio Band options are displayed:

Select specific AP groups



The dialog box is titled "Select APs" with a close button (X) in the top right corner. Below the title is the instruction "Define how this network will be activated on venue 'My Venue'". There are two radio button options: "All APs" and "Select specific AP groups" (selected). The "Select specific AP groups" option includes the text "Including any AP that will be added to a selected AP group in the future." Below this, there is a table with three columns: "AP Group", "VLAN", and "Radio Band". The first row is "APs not assigned to any group" with empty "VLAN" and "Radio Band" fields. The second row is "AP Group 1" (selected with a checkmark) with "VLAN-1 (Default)" and a pencil icon in the "VLAN" field, and a "Radio Band" dropdown menu with "2.4 GHz" and "5 GHz" selected. The third row is "AP Group 2" with empty "VLAN" and "Radio Band" fields. At the bottom right are "Cancel" and "Apply" buttons.

- 3) In the VLAN option, by default VLAN-1 is selected. Click Edit (pencil icon) icon and configure the VLAN or VLAN pool for the selected AP group.
- 4) In the Radio Band option, select 2.4 GHz, 5 GHz, or both 2.4 and 5 GHz from the drop down list for the selected AP group.
- 5) Click Apply.

h. By default, this network configuration is scheduled for 24/7. To configure the Scheduling, complete the following steps:

- 1) Click 24/7 in the Scheduling column. The Schedule for Network <network-name> in Venue <venue-name> dialog box is displayed. You can also choose a schedule of 24/7 or follow below steps to customize the schedule.

Schedule for Network Dialog Box

Schedule for Network "TEST-1" in Venue "1.space MM ^&*\$ MM"

Network availability

☐ 24/7

☒ Custom Schedule

Mark/ unmark areas to change network availability [See tips](#)

Venue time zone: UTC -07:00 (Pacific Daylight Time)

	Midnight	2 AM	4 AM	6 AM	8 AM	10 AM	Noon	2 PM	4 PM	6 PM	8 PM	10 PM	Midnight
<input checked="" type="checkbox"/> Mon													
<input checked="" type="checkbox"/> Tue													
<input checked="" type="checkbox"/> Wed													
<input checked="" type="checkbox"/> Thu													

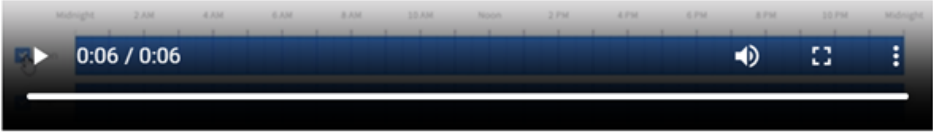
- 1) Click Custom Schedule.
- 2) Network schedule is customized as per the your requirement. You can configure the schedule for Monday through Sunday and from midnight to midnight (from 00:00 hours through 23.59 hours). For more information, click See tips. The Network Scheduler Tips dialog box is displayed.

Network Scheduler Tips

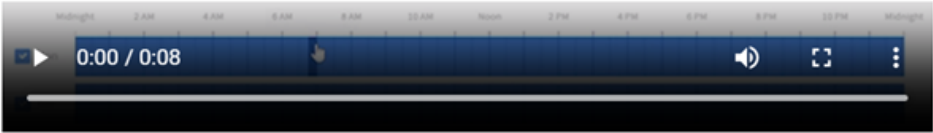
Network Scheduler Tips

You can set custom schedule using the following options:

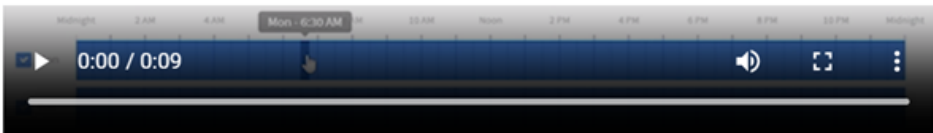
- Activate or deactivate the network for **entire day**
- Activate or deactivate the network for **any time-slot** by clicking on it
- Activate or deactivate the network for **multiple adjacent time-slots** by dragging your mouse over them



To set the network schedule for entire day use the checkbox next to it



To set the network schedule for any time-slot, click the time slot



- To set the network schedule for **multiple adjacent time-slots**, drag the mouse over them
- All the rectangles in the drag area will receive the same status – opposite the status of the rectangle where the drag started

OK

3) Click OK to close the Network Scheduler Tips dialog box.

4) Click Apply.

11. Click Next.

The Summary page is displayed.

12. Review the settings that you configured.

13. Click Finish.

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