

# RUCKUS One Online Help

## (index.html)

Search



---

## Creating a Network That Uses a Third-Party Captive Portal (WISPr Feature)

---

Learn how to create a network that allows users to access the network through a third-party captive portal, authenticated by a RADIUS server.

The login credentials used in the captive portal are validated using AAA on a RADIUS server.

**Note:** The licensing and subscription may vary from each 3rd-party WISPr provider. For more details, refer to individual partner documents. This is not included with the RUCKUS One subscription.

Complete the following steps to create a captive portal network that uses the third-party authentication option.

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 an existing Third-Party Captive Portal (WISPr Feature) Wi-Fi 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 settings on the Network Details page.
  - Name: Type 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 an optional description to help you identify the network using up to 64 characters.
  - Type: Click Captive Portal.

When the network type is selected, a structure diagram of a Captive Portal type of network displays.

4. Click Next.  
The Portal Type page is displayed.
5. Click 3rd Party Captive Portal (WISPr).

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

## Create New Network

**Portal Type**

Select the way users gain access to the network through the captive portal

- ☐ Click-Through  
Users just need to accept Terms and Conditions in order to access the network
- ☐ Self Sign In  
Users can sign in with their social media account or register their details in the portal and get personal password
- ☐ Cloudpath Captive Portal  
Users connect through an enhanced captive portal experience with Cloudpath
- ☐ Host Approval  
Users register their details in the portal including their host email - the host needs to approve the request
- ☐ Guest Pass  
Users sign in with personal password which they need to get in advance from the network administration staff
- ☒ 3rd Party Captive Portal (WISPr)  
Users connect through a 3rd party captive portal, authenticated by a AAA server
- ☐ Active Directory/ LDAP Server  
Users are required to enter an organizational username and password to gain access to the network

Diagram: 3rd Party Portal, Authentication Service (AAA), Captive Portal Provider (R1), Public network, Data: Local-Breakout

Buttons: Cancel, Back, Next

To access the network, users connect through a 3rd party captive portal, authenticated by a RADIUS server. The 3rd-Party Captive Portal type of network diagram appears.

6. Click Next.

The Settings page is displayed.

7. In the Portal Provider field, select a name of the provider from the drop-down list.

8. Based on Portal Provider selection, the Captive Portal URL or Region field is displayed.

- Captive Portal URL: Enter the vendor's complete URL for the above selected the Portal Provider. It is recommended to copy URL from the vendor's configuration.
- Region: Select a region for the above selected the Portal Provider from the drop-down list.

9. Select the Redirect Users to check box and enter a valid URL.

You can redirect users to your company website or another URL after they log in successfully. If the check box is not selected, users are sent to the page they originally requested.

10. In the Integration Key field, a password is displayed. Click Copy Key to copy this password to your vendor's configuration to allow it to connect to RUCKUS One.

11. For the Secure your network option, select one of the following options:

- None (default): No encryption method is used.
- Pre-Share Key (PSK): Select Pre-Share Key (PSK) and select a Security Protocol for the network.
  - WPA2 (Recommended) (default): Encrypts traffic using the WPA2 standard, which complies with the IEEE 802.11i security standard. Select WPA2 (Recommended) and enter a passphrase of at least eight characters in length in the Passphrase field.

- WPA3: The WPA3 standard has several security enhancements when compared to WPA2. Select WPA3 and enter a passphrase of at least eight characters in length in the SAE Passphrase field. The IEEE 802.11ax (Wi-Fi 6E) and IEEE 802.11be (Wi-Fi 7) APs support only WPA3. The 6 GHz radios are supported with WPA3 only.
- WPA2/WPA3 mixed mode: Allows mixed networks of WPA2- and WPA3-compliant devices ensuring compatibility. Select WPA2/WPA3 mixed mode and in the WPA2 Passphrase and WPA3 SAE Passphrase fields, enter a passphrase of at least eight characters each in length.
- WPA: It can be configured if you have older devices that do not support WPA2. These devices were manufactured before 2006. RUCKUS recommends that you upgrade or replace the older devices. 6 GHz radios are supported with WPA3 only.
- WEP (Unsafe): RUCKUS does not recommend using WEP to secure your wireless network because it might be insecure and could be exploited easily. RUCKUS One offers WEP to enable customers with old devices (that are difficult or expensive to replace) to continue using those devices to connect to the wireless network. If you must use WEP, do not use the devices using WEP to transmit sensitive information over the wireless network. 6 GHz radios are supported with WPA3 only.

Note: Due to security concerns, WEP will no longer be supported for users. However, this change will not impact existing networks that currently utilize WEP.

- OWE Encryption: Opportunistic Wireless Encryption (OWE) provides encrypted communications for open Wi-Fi networks without needing passwords. Select this option if you do not want users to authenticate with a password.
- OWE Transition mode: Enables a seamless transition from Open unencrypted WLANs to OWE WLANs without adversely impacting the end user experience. The OWE Transition mode setting is not visible unless OWE Encryption is enabled.

Note: The OWE transition mode allows STAs that do not support OWE authentication to access the network in open authentication mode, while OWE-capable STAs can use OWE authentication mode.

The migration to an enhanced open Wi-Fi network is done gradually, with user devices also upgrading over time. In OWE Transition mode, an AP creates two SSIDs: SSID1 (broadcast) for open authentication and SSID2 (hidden) for OWE authentication (read only). Non-OWE devices connect to SSID1, while OWE-capable devices initially connect to SSID1 but are then associated with SSID2 for secure access.

If SSID1 is deleted or OWE Transition mode is disabled, SSID2 will also be deleted. Cloning SSID1 creates two new WLANs.

Note: SSID1 and SSID2 co-exist as a pair and a maximum of 6 WLANs can be created per venue, per AP group.

12. Select the Enable MAC auth bypass check box to enable MAC base authentication method.

13. Check the Enable RUCKUS DHCP service check box to automatically create and assign a new DHCP-Guest Service and DHCP Pool for those Guest WLAN-related venues that do not have a specified DHCP Service. Please refer to the DHCP Service at each Venue for more information.

14. In the Walled Garden box, enter the network destinations (URLs or IP addresses) that users can access without going through authentication. A walled garden is a limited environment to which an unauthenticated user is given access for the purpose of setting up an account. After the account is established, the user is allowed out of the walled garden.

A walled garden is a limited environment to which an unauthenticated user is given access for the purpose of setting up an account. After the account is established, the user is allowed out of the walled garden.

Enter each destination in a new line. The following are the accepted formats for destinations:

- IP address (for example, 10.11.12.13)
- IP address range (for example, 10.11.12.13-10.11.12.15)
- CIDR (for example, 10.11.12.13/28)
- IP address and mask (for example, 10.11.12.13 255.255.255.0)
- Website FQDN (for example, www.ruckus.com)
- Website FQDN with a wildcard (for example, \*.amazon.com;\*.com)

15. In the Authentication Service section automatically the selected Portal Provider primary and secondary servers are filled.

16. Check the Accept All Connections option to enable the Accept All Connections feature.

By default, the Accept All Connections feature is disabled. You must disable Enable MAC auth bypass to enable the Accept All Connections feature.

17. In the Accounting Service section automatically the selected Portal Provider primary and secondary servers are filled.

18. 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/Jm3S4CCwJX2Z2N8E9qAZdJ>)*

19. Click Next.

The Venues page is displayed.






20. 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, Radios, Scheduling, and Tunnel of the selected venue is displayed in the table.

#### Select Venues

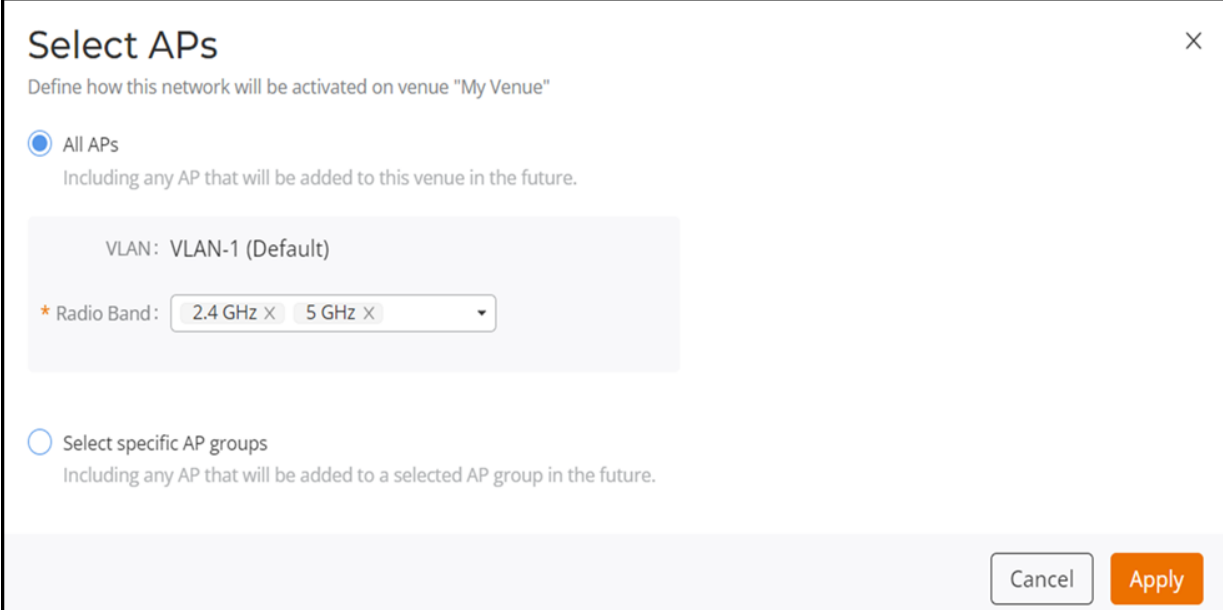
Venues								
Select venues to activate this network								
2 selected  <a href="#">Activate</a>   <a href="#">Deactivate</a>								
<input type="checkbox"/> Venue	City	Country	Networks	Wi-Fi APs	Activated	APs	Radios	Scheduling
<input checked="" type="checkbox"/> 1.space MM ^&*&%\$ MM	Sunnyvale, California	United States		0		All APs	2.4 GHz, 5 GHz	24/7 
<input checked="" type="checkbox"/> 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 all radio bands supported by the APs. To select specific AP groups or modify the radio bands that will broadcast this network, complete one of 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 to remove or add any AP-supported radio bands in the Radio Band drop-down list giving you the flexibility of broadcasting this network only on the selected radio bands.

#### Select APs Dialog Box



**Select APs** ×

Define how this network will be activated on venue "My Venue"

☒ All APs  
Including any AP that will be added to this venue in the future.

VLAN: VLAN-1 (Default)

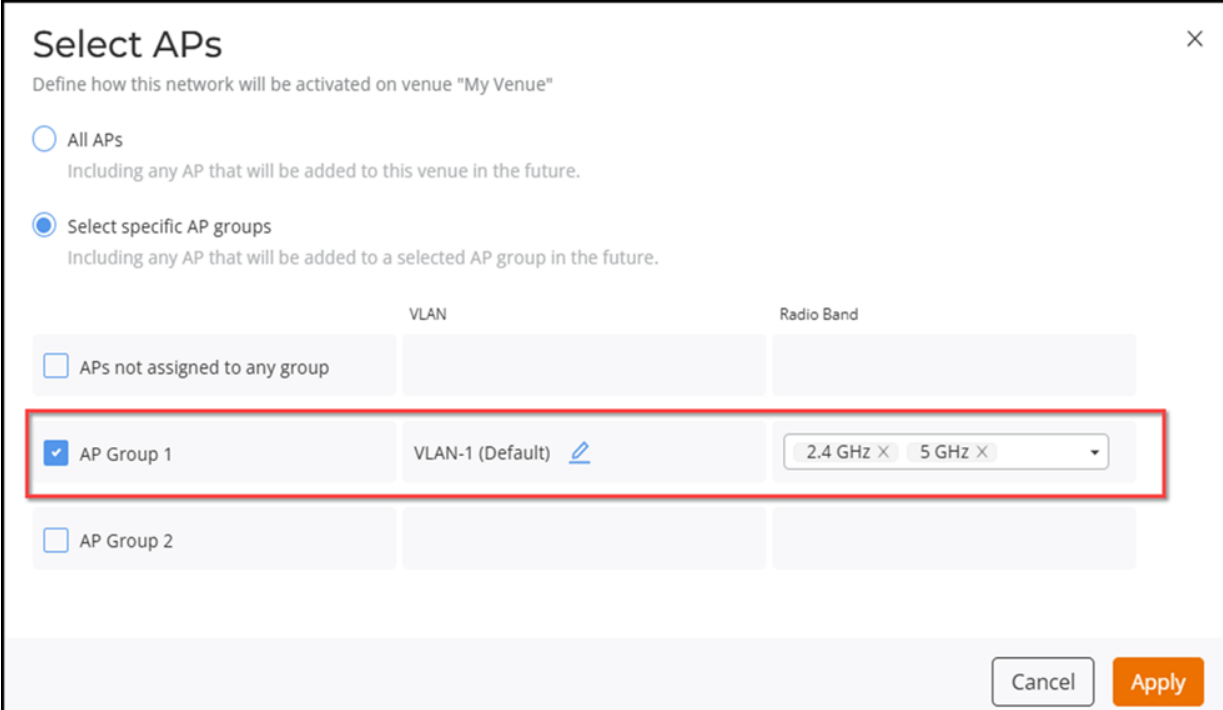
\* Radio Band: 2.4 GHz X 5 GHz X ▼

☐ Select specific AP groups  
Including any AP that will be added to a selected AP group in the future.

Cancel Apply

- 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




**Select APs** ×


Define how this network will be activated on venue "My Venue"

☐ All APs  
Including any AP that will be added to this venue in the future.

☒ Select specific AP groups  
Including any AP that will be added to a selected AP group in the future.

	VLAN	Radio Band
<input type="checkbox"/> APs not assigned to any group		
<input checked="" type="checkbox"/> AP Group 1	VLAN-1 (Default) 	<span>2.4 GHz X</span> <span>5 GHz X</span> ▼
<input type="checkbox"/> AP Group 2		

Cancel Apply

- 3) In the VLAN option, by default VLAN-1 is selected. Click the  icon and configure the VLAN or VLAN pool for the selected AP group.

4) In the Radio Band option, remove or add any AP-supported radio bands in 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	Available	Available	Available	Available	Available	Available	Available	Available	Available	Available	Available	Available	Available
<input checked="" type="checkbox"/> Tue	Available	Available	Available	Available	Available	Available	Available	Available	Available	Available	Available	Available	Available
<input checked="" type="checkbox"/> Wed	Available	Available	Available	Available	Available	Available	Available	Available	Available	Available	Available	Available	Available
<input checked="" type="checkbox"/> Thu	Available	Available	Available	Available	Available	Available	Available	Available	Available	Available	Available	Available	Available

Cancel Apply

2) Click Custom Schedule.

3) Network schedule is customized as per 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 opens, displaying different configuration tips in the form of animated GIFs.

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

5) Click Apply.

n. The Tunnel column shows the tunneling service or profile associated with each active network. By default, Tunnel is set to Local Breakout when the venue is not linked to any SD-LAN or SoftGRE tunneling service. The SD-LAN Tunneling option is available only in networks containing RUCKUS Edge devices.

21. Click Next.

The Summary page is displayed.

22. Review the settings that you configured.

23. Click Finish.

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