

RUCKUS One Online Help

(index.html)

Search



Creating a Network That Uses a Cloudpath Captive Portal

You can learn to create a network that allows users to connect through an enhanced captive portal experience with Cloudpath.

Complete the following steps to create a captive portal network that uses the Cloudpath 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 Cloudpath Captive Portal 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.
 - Network Name: Enter a name (up to 32 characters) that you want to assign to the network.
 - Set different SSID: Use this option to configure the SSID different from the network name. For SSID, enter an SSID name (from 2 through 32 characters and up to 32 bytes when using UTF-8 non-Latin characters).
 - Description: Enter an optional description (up to 64 characters).
 - Network Type: Click Captive Portal.
4. Click Next.
The Portal Type page is displayed.
5. Click Cloudpath Captive Portal.
The Captive Portal Cloudpath network type diagram is displayed.
Creating a Cloudpath Captive Portal Network Type

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

Create New Network

- Network Details
- Portal Type**
- Settings
- Venues
- Summary

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

6. Click Next.

The Settings page is displayed.

7. Complete the following steps on the Settings page:

- In the Enrollment Workflow URL field enter the URL. The user will be redirected to this URL to enroll in the system. It is recommended to copy the URL from the cloud path configuration.
- Secure your network: 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.
 - OWE Encryption: Opportunistic Wireless Encryption (OWE) provides encrypted communications for open Wi-Fi networks without needing passwords. Choose this option to allow users to access the network without needing to enter a password for authentication.
 - 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.s

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.

- Select the Use MAC authentication during reconnection check box to enable this option. This option authenticates clients by MAC address. Cloudpath uses the MAC address as the user login name and password.
- Select the Use Bypass Captive Network Assistant check box to enable this option. This option allows the device that is authenticated at the beginning to reconnect to the onboard network without authentication whenever the device is disconnected.
- In the Walled Garden section, 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 to set up an account. After the account is established, the user is allowed out of the walled garden.
- In the Authentication Service, select the existing RADIUS Server from the drop-down list or click Add Server and configure a new RADIUS Server. Refer to *Creating a Radius Server Profile (GUID-F0DFD674-D2E0-42F8-AA09-CBCBE9E419BF.html)* for more information.
- Toggle the Proxy Service switch to ON to enable the proxy service.

Note: Use the controller as a 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.

- In the Accounting Service toggle the switch to ON to enable this option and select the existing RADIUS Server from the drop-down list or click Add Server and configure a new RADIUS Server. Refer to *Creating a Radius Server Profile (GUID-F0DFD674-D2E0-42F8-AA09-CBCBE9E419BF.html)*.

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/Jm3S4CCwJX2Z2N8E9qAZdJ>)

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 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 columns of the selected venue are displayed in the table.

Select 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 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:

- Click All APs in the APs column. The Select APs dialog box is displayed. Select All APs 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

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 has a subtext: "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" section with a star icon, a dropdown menu showing "2.4 GHz X" and "5 GHz X", and a downward arrow. At the bottom right are "Cancel" and "Apply" buttons.

- 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, the VLAN and Radio Band options are displayed.

Selecting 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 has a subtext: "Including any AP that will be added to a selected AP group in the future." Below this is a table with three columns: "APs not assigned to any 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 blue checkmark), with "VLAN-1 (Default)" and a blue edit icon in the "VLAN" field, and a "Radio Band" dropdown menu showing "2.4 GHz X" and "5 GHz X". The third row is "AP Group 2" with empty "VLAN" and "Radio Band" fields. At the bottom right are "Cancel" and "Apply" buttons.

- 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.

- In the Radio Band option, remove or add any AP-supported radio bands in the drop-down list for the selected AP group.
- Click Apply.

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

- Click 24/7 in the Scheduling column. The Schedule for Network <network-name> in Venue <venue-name> dialog box is displayed. You can choose a schedule of 24/7 or 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													

- Click Custom Schedule. The network schedule is customized as per your requirements. 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.
- Click OK to close the Network Scheduler Tips dialog box.
- Click Apply.

d. 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.

11. Click Next.

Example: 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.