

RUCKUS One Online Help

(index.html)

Search



Creating a Network That Uses a Captive Portal with SAML Identity Provider (IdP)

You can create a captive portal network that allows users to join by entering an organization-based SAML Identity Provider (IdP) for secure Single Sign-On (SSO) using their credentials.

Complete the following steps to create a captive portal network that uses the SAML IdP option.

1. On the navigation bar, click Wi-Fi > (and then) Wi-Fi Networks > (and then) Wi-Fi Networks List.
The Wi-Fi Networks page is displayed.
2. Click Add Wi-Fi Network. Alternatively, select an existing Captive Portal Wi-Fi network with SAML IdP 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 (from 2 through 32 characters) that you want to assign to the network.
 - Set different SSID: Use this option to configure an 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 256 characters).
 - Network Type: Click Captive Portal.

A structure diagram of a Captive Portal network type is displayed.

4. Click Next.
The Portal Type page is displayed.
5. Click SAML Identity Provider (IdP).
The Captive Portal SAML Identity Provider (IdP) network type diagram is displayed.
Creating a SAML Identity Provider (IdP) Captive Portal Network Type

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

Create New Network

- Network Details
- Portal Type**
- Onboarding
- Portal Web Page
- 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
- ☒ SAML Identity Provider (IdP)
Users authenticate through the organization's SAML Identity Provider (IdP)

Cancel

Back Next

6. Click Next.

The Onboarding page is displayed.

7. Complete the following settings on the Onboarding page:

- Select Identity Provider (IdP) via SAML: Select a SAML IdP profile from the drop-down list or click Add to create a new SAML IdP profile (refer to *Adding and Managing a SAML Identity Provider Profile (GUID-B91F5A70-F9C8-4FF4-9AE8-3C6C0E895F4D.html)*). If you select an existing profile, you can click View Details to easily view the SAML IdP Details in a sidebar without leaving the network creation wizard.
- Identity Group: Select an identity group profile or click Add to create a new SAML Identity Group profile. Refer to *Adding an Identity Group (GUID-60E97713-D793-4659-86BF-94F8BF209EA6.html)* for more information.
- (Optional) 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: 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 six WLANs can be created per venue, per AP group.

- (Optional) Redirect users to: Select the Redirect users to checkbox and enter a valid URL. You can redirect users to your company website or another URL after they log in successfully. If the checkbox is not selected, users are sent to the page they originally requested.
- (Optional) Enable RUCKUS DHCP service: Select the Enable RUCKUS DHCP service checkbox 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. Refer to the DHCP Service of each Venue for more information.
- (Optional) Use Bypass Captive Network Assistant: Select the Use Bypass Captive Network Assistant checkbox to prevent the controller from using the mini browser on mobile devices. Instead, with CNA bypass enabled, a standard browser is opened for any unauthenticated page (HTTP) and redirected to the login portal. Bypass CNA is supported by iOS and Android devices.
- Walled Garden: Enter the network destinations (URLs or IP addresses) of the IdP server to allow communication between RUCKUS One and IdP. 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.

8. (Optional) 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: In the User Connection sub-tab, for Max number of devices per credentials, you can set the maximum number of devices that may use the same SAML IdP login credentials. The default is 1; the allowed values are 1 through 10.

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 Portal Web Page is displayed.

10. Under Guest Portal Service, select a Guest Portal Service from the drop-down list or click Add Guest Portal Service to add a new Guest Portal Service. The Guest Portal Service is where you define the look and feel of the webpage that the guest uses to join the captive portal network. For more information, refer to *Adding a Guest Portal Service (GUID-F27DC50B-9239-4A4F-B751-945FF9828F08.html)*.

11. Click Next.

The Venues page is displayed.

12. 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 checkbox 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 toggle on the switch in the Activated column.








The APs, Radios, Scheduling, and Network Tunneling columns of the selected venue are displayed in the table.

Select Venues to Activate a Captive Portal Network

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

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 ✕

5 GHz ✕

▼

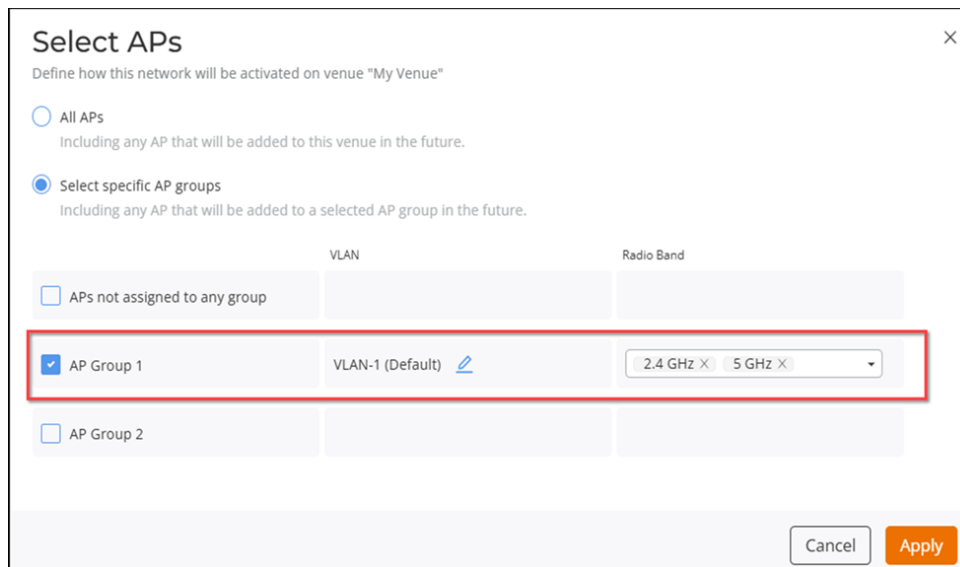
☐ Select specific AP groups
Including any AP that will be added to a selected AP group in the future.

Cancel

Apply

- 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




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) 	2.4 GHz X 5 GHz X
<input type="checkbox"/> AP Group 2		

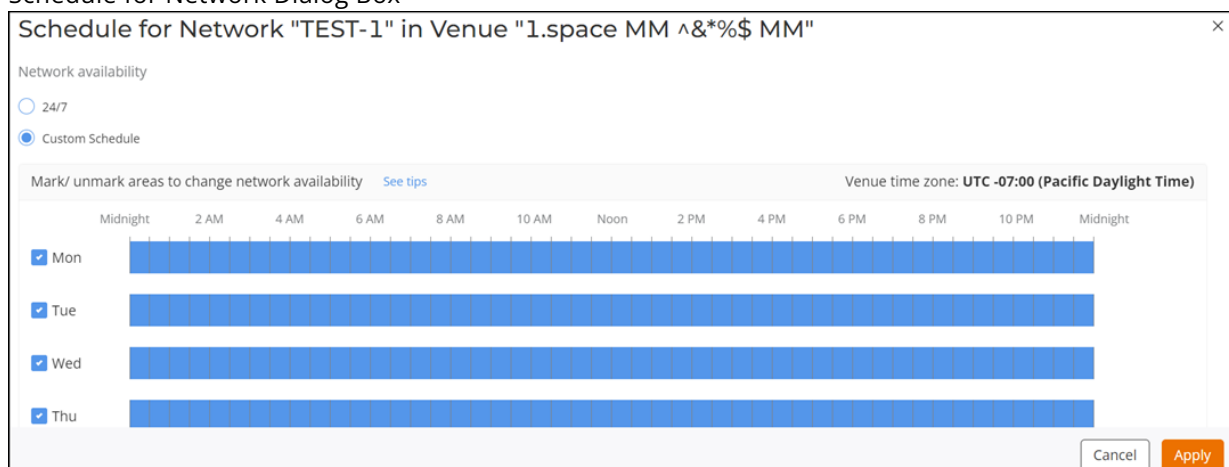
Cancel Apply

- 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 also choose a schedule of 24/7 or complete the following 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													

Cancel Apply

- 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 Network Tunneling column shows the tunneling service or profile associated with each active network. Click the toggle to enable tunneling and select a Network Topology tunnel type from the drop-down list and click Save to apply your changes.

13. Click Next.

Example: The Summary page is displayed.

14. Review the settings that you configured.

15. Click Add.

800-73730-001 Rev D 29 April 2025

© 2024 CommScope, Inc. All rights reserved.