

# RUCKUS Edge Configuration Guide, 2.1.0

**Supporting RUCKUS Edge 2.1.0 Release**

© 2024 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

## Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

*These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.*

## Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

## Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

## Trademarks

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see <https://www.commscope.com/trademarks>. All product names, trademarks, and registered trademarks are the property of their respective owners.

## Patent Marking Notice

For applicable patents, see [www.cs-pat.com](http://www.cs-pat.com).

# Contents

---

<b>Contact Information, Resources, and Conventions.....</b>	<b>5</b>
Contacting RUCKUS Customer Services and Support.....	5
What Support Do I Need?.....	5
Open a Case.....	5
Self-Service Resources.....	6
Document Feedback.....	6
RUCKUS Product Documentation Resources.....	6
Online Training Resources.....	6
Document Conventions.....	7
Notes, Cautions, and Safety Warnings.....	7
Command Syntax Conventions.....	7
<b>About This Guide.....</b>	<b>9</b>
Introduction.....	9
<b>Software Defined Local Area Network (SD-LAN).....</b>	<b>11</b>
Software Defined Local Area Network.....	11
Overview.....	11
Requirements.....	11
Limitations.....	12
Best Practices.....	12
Prerequisites.....	12
Configuring the SD-LAN Service.....	12
Viewing the SD-LAN Service.....	17
Viewing SD-LAN Statistics.....	19
Editing an SD-LAN Service.....	20
Removing the SD-LAN Service from a RUCKUS Edge Device.....	21
Deleting an SD-LAN Service.....	22
Multiple Venue Support for an SD-LAN Service.....	23
Feature Overview.....	23
Requirements.....	24
Considerations.....	24
Best Practices.....	24
Prerequisites.....	24
Viewing Networks Configured for a Venue.....	25
<b>High Availability.....</b>	<b>29</b>
High Availability.....	29
Overview.....	29
Requirements.....	29
Considerations.....	29
Best Practices.....	29
Prerequisites.....	29
Onboarding a Dual-Node Cluster for High Availability.....	30
Configuring a Dual-Node Cluster for High Availability with a LAG Interface.....	32
Link Aggregation Group (LAG), Port and Virtual IP Settings.....	35
Cluster Interface Settings.....	43
Configuring a Cluster for Active Standby High Availability deployment without a LAG interface.....	43

Link Aggregation Group (LAG), Port and Virtual IP Settings.....	45
Cluster Interface Settings.....	49
Onboarding a Single-Node Cluster.....	50
Editing a Cluster and Nodes.....	51
<b>Link Aggregation Group.....</b>	<b>53</b>
Link Aggregation Group.....	53
Overview.....	53
Requirements.....	53
Considerations.....	53
Best Practices.....	53
Limitations.....	54
Prerequisites.....	54
Configuring a RUCKUS Edge Link Aggregation Group.....	54
Editing a LAG.....	58
Deleting a LAG.....	59
Configuring a RUCKUS Edge Link Aggregation Group through Command Line Interface.....	61
<b>Tunnel Profile.....</b>	<b>67</b>
Tunnel Profile.....	67
Creating a Tunnel Profile.....	68
Editing or Deleting the Tunnel Profile.....	70
<b>Appendix.....</b>	<b>73</b>
Supported AP Models.....	73
Incompatible AP Firmware.....	73

# Contact Information, Resources, and Conventions

---

- [Contacting RUCKUS Customer Services and Support](#)..... 5
- [Document Feedback](#)..... 6
- [RUCKUS Product Documentation Resources](#)..... 6
- [Online Training Resources](#)..... 6
- [Document Conventions](#)..... 7
- [Command Syntax Conventions](#)..... 7

## Contacting RUCKUS Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and to customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using <https://support.ruckuswireless.com>, or go to <https://www.ruckusnetworks.com> and select **Support**.

### What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Submit a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Submit a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Click the **CONTACT** tab at the top of the page and explore the **Self-Service Online Help** options.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Click the **CONTACT** tab at the top of the page and explore the **Self-Service Online Help** options.

### Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at <https://support.ruckuswireless.com/contact-us> and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

## Self-Service Resources

The RUCKUS Support Portal at <https://support.ruckuswireless.com> offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—<https://support.ruckuswireless.com/documents>
- Community Forums—<https://community.ruckuswireless.com>
- Knowledge Base Articles—<https://support.ruckuswireless.com/answers>
- Software Downloads and Release Notes—[https://support.ruckuswireless.com/#products\\_grid](https://support.ruckuswireless.com/#products_grid)
- Security Bulletins—<https://support.ruckuswireless.com/security>

Using these resources will help you to resolve some issues, and will provide the Technical Assistance Center (TAC) with additional data from your troubleshooting analysis if you still require assistance through a support case or Return Merchandise Authorization (RMA). If you still require help, open and manage your case at [https://support.ruckuswireless.com/case\\_management](https://support.ruckuswireless.com/case_management).

## Document Feedback

RUCKUS is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to RUCKUS at [#Ruckus-Docs@commscope.com](mailto:#Ruckus-Docs@commscope.com).

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

## RUCKUS Product Documentation Resources

Visit the RUCKUS website to locate related documentation for your product and additional RUCKUS resources.

Release Notes and other user documentation are available at <https://support.ruckuswireless.com/documents>. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

White papers, data sheets, and other product documentation are available at <https://www.ruckusnetworks.com>.

## Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at <https://commscopeuniversity.myabsorb.com/>. The registration is a two-step process described in this [video](#). Create a CommScope account and then register for, and request access for, CommScope University.

# Document Conventions

The following table lists the text conventions that are used throughout this guide.

**TABLE 1** Text Conventions

Convention	Description	Example
monospace	Identifies command syntax examples	<code>device(config)# interface ethernet 1/1/6</code>
<b>bold</b>	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the <b>Start</b> menu, click <b>All Programs</b> .
<i>italics</i>	Publication titles	Refer to the <i>RUCKUS Small Cell Release Notes</i> for more information.

## Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

### NOTE

A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

### ATTENTION

An ATTENTION statement indicates some information that you must read before continuing with the current action or task.



### CAUTION

A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.



### DANGER

A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

## Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
<b>bold text</b>	Identifies command names, keywords, and command options.
<i>italic text</i>	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{x  y  z}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member[member...]</i> .
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.





# About This Guide

---

- Introduction..... 9

## Introduction

This *RUCKUS Edge Configuration Guide* provides information and guidance for managing the configurable application features and services that are used to configure the Edge device. You can download the installation guide from RUCKUS support website:

<https://support.ruckuswireless.com/documents>

Before deploying RUCKUS Edge, refer to the latest software and the release documentation.

- Release Notes and other user documentation is available at: <https://support.ruckuswireless.com/documents>.
- Software upgrades are available at: <https://support.ruckuswireless.com/software>.
- Software license and limited warranty information are available at: <https://support.ruckuswireless.com/warranty>.



# Software Defined Local Area Network (SD-LAN)

---

• Software Defined Local Area Network.....	11
• Configuring the SD-LAN Service.....	12
• Viewing the SD-LAN Service.....	17
• Viewing SD-LAN Statistics.....	19
• Editing an SD-LAN Service.....	20
• Removing the SD-LAN Service from a RUCKUS Edge Device.....	21
• Deleting an SD-LAN Service.....	22
• Multiple Venue Support for an SD-LAN Service.....	23

## Software Defined Local Area Network

Software Defined Local Area Network (SD-LAN) is a service provided on RUCKUS One that is implemented on Edge.

### Overview

The SD-LAN service provides centralized forwarding for RUCKUS access points, enabling the access points to tunnel User Equipment (UE) traffic to an Edge device. All intermediate network hops are hidden from the end user's traffic.

The SD-LAN service works as follows:

- A Generic Protocol Extension for Virtual Extensible LAN (VxLAN-GPE) tunnel is established between the access point (AP) and the Edge device to facilitate the forwarding of User Equipment (UE) traffic.
- The AP associates the VLAN with the corresponding Virtual Network Identifier (VNI) (both having the same ID). For example, VLAN 10 maps to VNI 10, and vice-versa.
- Layer 2 (L2) bridging allows user equipment (UE) traffic to be forwarded into the core network.

SD-LAN also provides the capability to forward Captive Portal guest WLAN traffic between a Data Center (DC) Edge and an Edge device located in the DMZ network. In the context of Wi-Fi networks, the DMZ is a logical network that adds an extra layer of security for the Local Area Network (LAN) by providing a safe zone, separating the LAN from untrusted networks (such as public internet).

### Requirements

The SD-LAN service requires the following:

- An onboarded Edge device with a LAN port enabled and configured as a core port.
- A configured venue with associated APs and a Wi-Fi network.
- An Edge cluster configured and associated with the venue.
- APs with 7.x or later firmware version.
- A Tunnel profile, for more information on creating a tunnel profile, refer to **Policies > Creating a Tunnel Profile** in the RUCKUS One online help.

## Software Defined Local Area Network (SD-LAN)

### Configuring the SD-LAN Service

#### NOTE

When configuring a VxLAN-GPE tunnel profile between a Data Center Edge device and a DMZ Edge device, the Gateway Path MTU mode should be configured as Manual (because automatic path MTU Discovery (PMTUD) is not supported between two Edge devices) and the maximum transmission unit (MTU) defined (select from 68 to 1450 bytes).

When configuring a VxLAN-GPE tunnel profile between an Access Point and a Data Center Edge device, the Gateway Path MTU mode can be configured as Auto or Manual.

## Limitations

The SD-LAN service has the following limitations:

- Network types supported:
  - Traffic tunneling between an AP and a Data Center Edge device: Supports all types of WLANs.
  - Traffic tunneling between a Data Center Edge device and a DMZ Edge device: Supports Captive Portal WLANs only.
- Captive Portal WLAN support:
  - Captive portal terminating to Data Center Edge support: Supports SSID-VLAN and VLAN pooling.
  - Captive portal terminating to DMZ Edge support (Redirected through Data Center Edge): Supports only SSID-VLAN.
- Path MTU Discovery (PMTUD) is not supported for tunnels between two Edge devices. PMTU should be manually configured for these tunnels.
- SD-LAN does not support VLAN 1. Regardless of the method used (VLAN pooling, dynamic VLAN assignment, SSID VLAN, or OS policy), VLAN 1 cannot be assigned to User Equipment (UE).
- SD-LAN supports only IPv4 traffic from the UE. It does not support IPv6 traffic from UE.

## Best Practices

This feature has no special recommendations for feature enablement or usage.

## Prerequisites

Ensure your RUCKUS One tenant account has the following configurations prior to starting this procedure:

- A configured venue with associated APs and a Wi-Fi network
- A configured Edge Cluster associated with the venue
- The LAN port must be configured as the core port on the Edges that are associated with the cluster participating in the SD-LAN service.

## Configuring the SD-LAN Service

You can configure an SD-LAN service to manage how end-user traffic is tunneled in a Wi-Fi network that includes RUCKUS Edge devices.

To add an SD-LAN service, follow these steps.

1. On the RUCKUS One navigation bar, hover over **Network Control** and click **My Services** or **Service Catalog**.

This displays the **My Services** or **Service Catalog** menu, respectively.

2. Access the **Add SD-LAN Service** page using one of the following methods:
  - On the **My Services** page: Click the **SD-LAN** tile, then click the **Add SD-LAN Service** button.
  - On the **Service Catalog** page: Click the **Add** button in the **SD-LAN** tile.This displays the **Add SD-LAN Service** page.

## Software Defined Local Area Network (SD-LAN)

### Configuring the SD-LAN Service

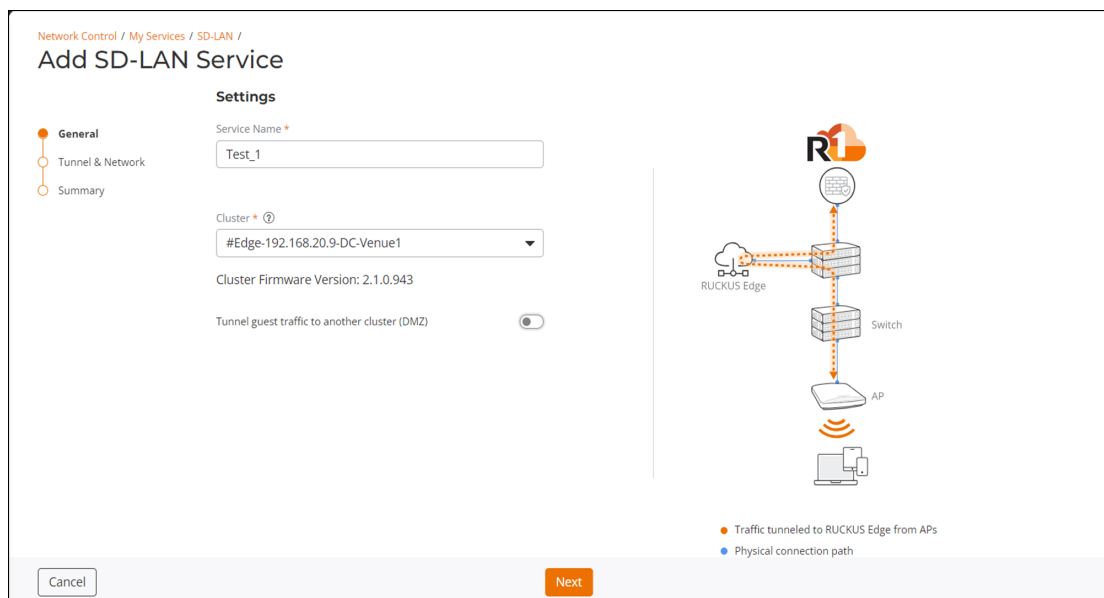
3. In the **Add SD-LAN Service** page, configure the following:

a) **Settings:** In this section, enter the following details:

- **Service Name:** Enter a meaningful name for the SD-LAN service.
- **Cluster:** Select the cluster to which all traffic is tunneled in the specified venue. Ensure the Data Center (DC) Edge device to which this service is associated already has a LAN port configured as a core port.
- **Tunnel guest traffic to another cluster (DMZ):** In a Wi-Fi network architecture, the demilitarized zone (DMZ) is a subnetwork that adds an extra layer of security by separating the LAN from untrusted networks (such as public networks). A toggle switch allows you to enable and disable this option.

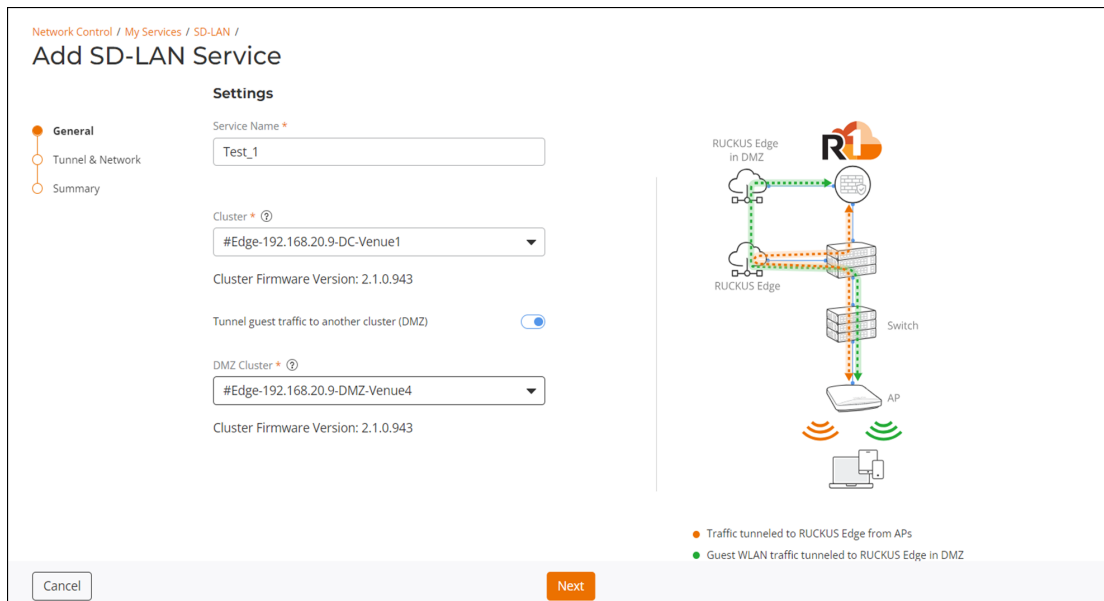
**Disable:** This is the default setting. Guest traffic is not sent to the DMZ RUCKUS Edge. The SD-LAN service is configured between the AP and the Data Center RUCKUS Edge device, with traffic tunneled only to the Data Center RUCKUS Edge device.

**FIGURE 1** Tunnel Guest Traffic to Another Cluster (DMZ) Disabled



**Enable:** Guest traffic is sent to the DMZ RUCKUS Edge. The SD-LAN service is configured between the Data Center and the DMZ RUCKUS Edge devices.

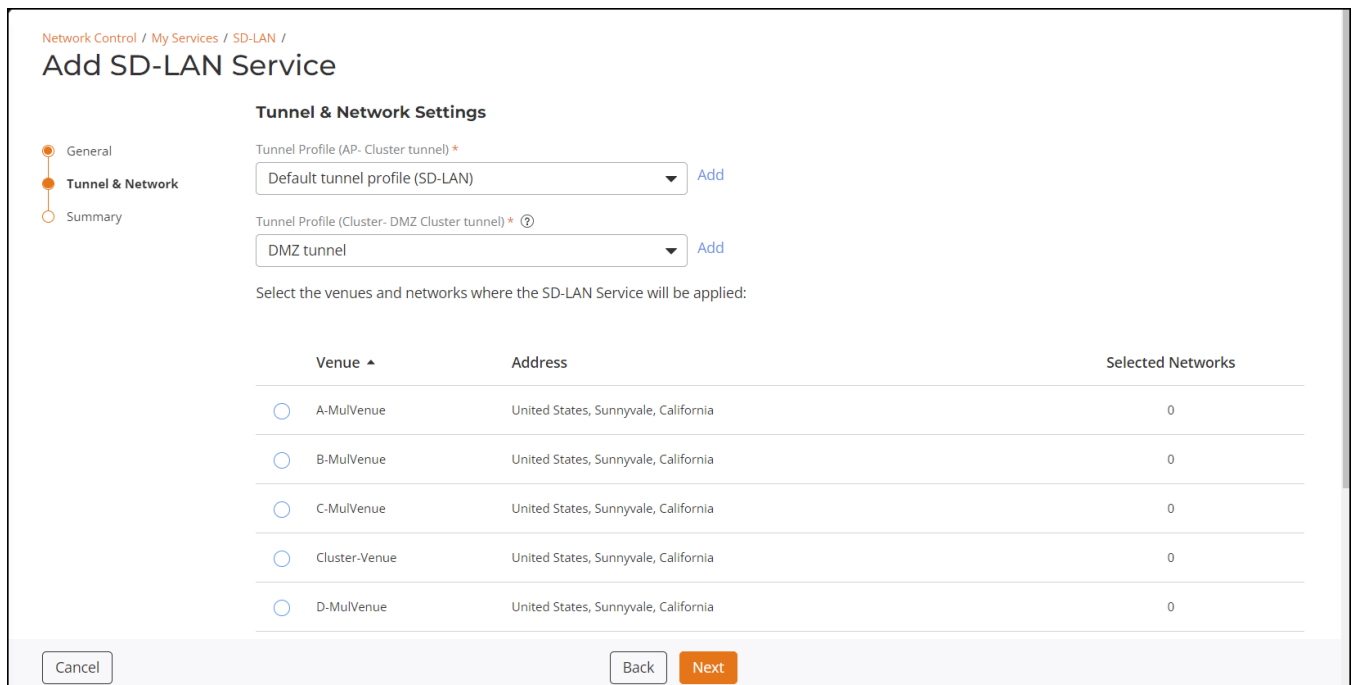
FIGURE 2 Tunnel Guest Traffic to Another Cluster (DMZ) Enabled



- **DMZ Cluster:** Select the cluster from the drop-down list to which the guest traffic is directed in the DMZ. This field appears only when **Tunnel Guest Traffic to another Cluster (DMZ)** is enabled.

After entering all the details, click **Next**. The **Tunnel & Network Settings** configuration is displayed.

FIGURE 3 Tunnel and Network Settings



## Software Defined Local Area Network (SD-LAN)

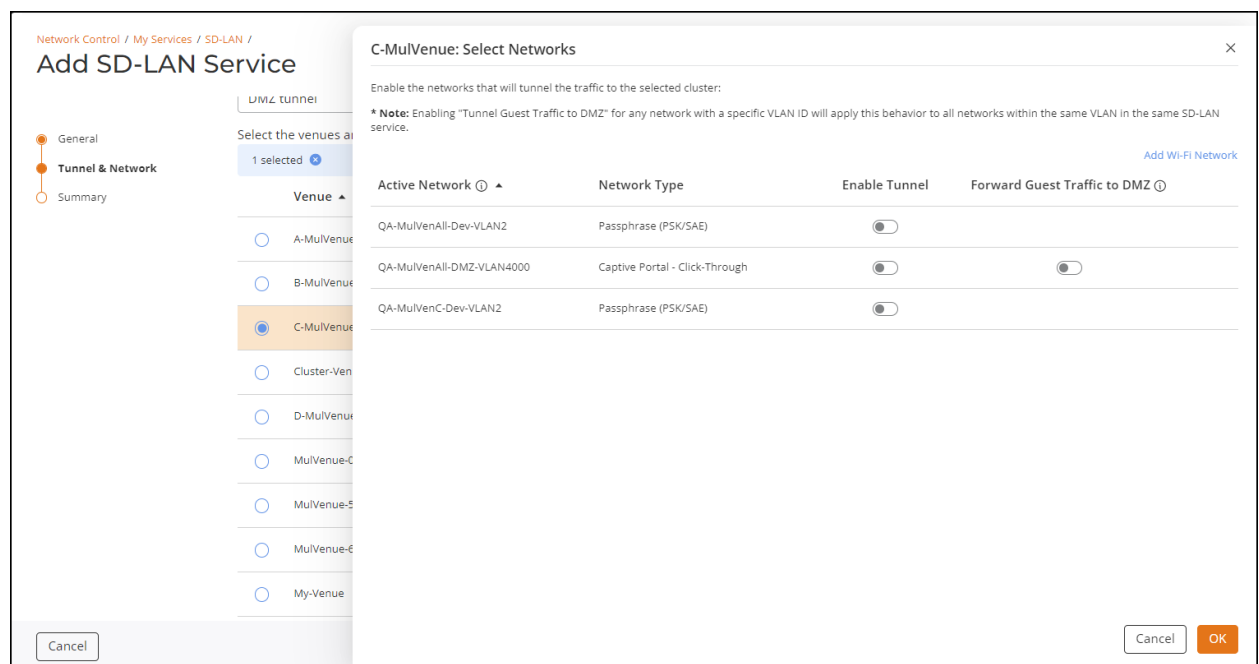
### Configuring the SD-LAN Service

b) **Tunnel & Network Settings:** In this section, enter the following details:

- **Tunnel Profile (AP-Cluster tunnel):** Select the tunnel profile from the drop-down list that is to be used between the AP and the Data Center RUCKUS Edge. Click **Add** if you want to create a new tunnel profile. Refer to [Creating a Tunnel Profile](#) on page 68 for more information.
- **Tunnel Profile (Cluster - DMZ Cluster tunnel):** Select the tunnel profile from the drop-down list that is that is to be used between the Data Center and the DMZ RUCKUS Edge devices. Click **Add** if you want to create a new tunnel profile. Refer to [Creating a Tunnel Profile](#) on page 68 for more information.
- Select the venues and networks where the SD-LAN Service will be applied. Click the radio button alongside a venue that you want to include, then click the **Select Networks** option.

The **Venue Select Networks** sidebar is displayed.

**FIGURE 4** Select Networks



- In the resulting sidebar, you can click the **Enable Tunnel** toggle switch and the **Forward Guest Traffic to DMZ** toggle switch (applicable for captive portal networks) for each Wi-Fi network, as desired, then click **OK** to close the sidebar. Repeat this for each venue to which you want this SD-LAN service applied.

#### NOTE

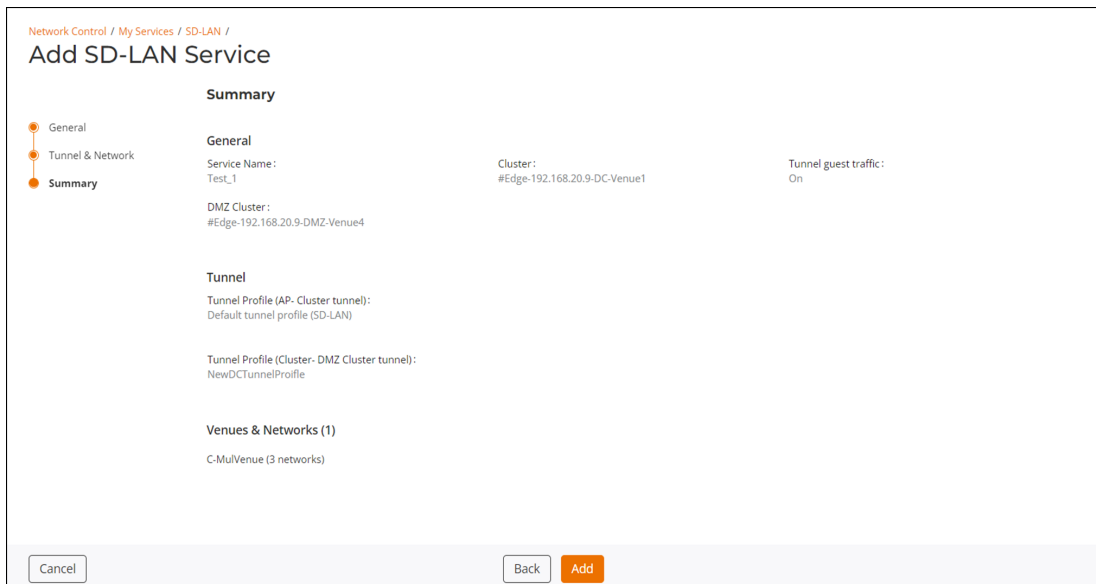
When creating or editing an SD-LAN service profile used for a Captive Portal network activated in multiple venues, the **Forward Guest Traffic to DMZ** option must be set the same (either enabled or disabled) across all venues using that same Captive Portal network and SD-LAN profile.

After entering all the fields, click **Next**.

- c) **Summary:** View and verify the configuration details of the SD-LAN service. To modify any of the configuration settings, click **Back**. To apply the new SD-LAN service configuration, click **Add**.



FIGURE 5 SD-LAN Summary



## Viewing the SD-LAN Service

You can view information pertaining to a configured SD-LAN service from the perspective of the service itself, the RUCKUS Edge cluster, or the venue.

Each navigation option results in slight variations on the service details provided, so choose one or more methods that best suit your needs.

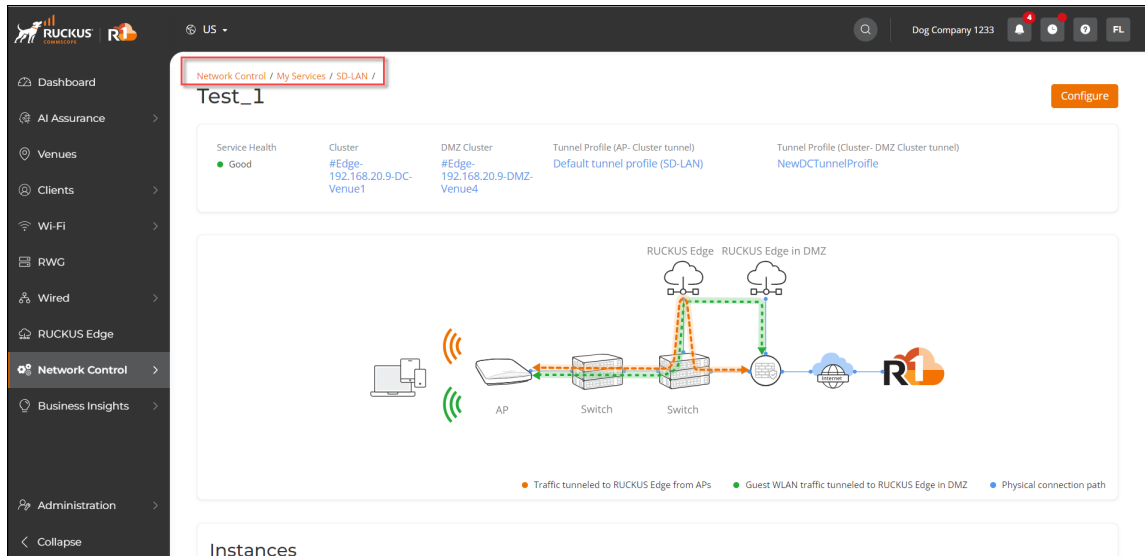
Perform one or more of the steps as follows:


1. View the SD-LAN Service through **Network Control**.
  - a. Click on the **Network Control > My Services** menu option, then click the **SD-LAN** tile.
  - b. In the list of SD-LAN services, click on the name of a specific SD-LAN service. The service details appear, reflecting the associated venue, cluster, and tunnel profile, as well as an end-to-end system architecture map and information regarding the related networks and RUCKUS Edge devices.

## Software Defined Local Area Network (SD-LAN)

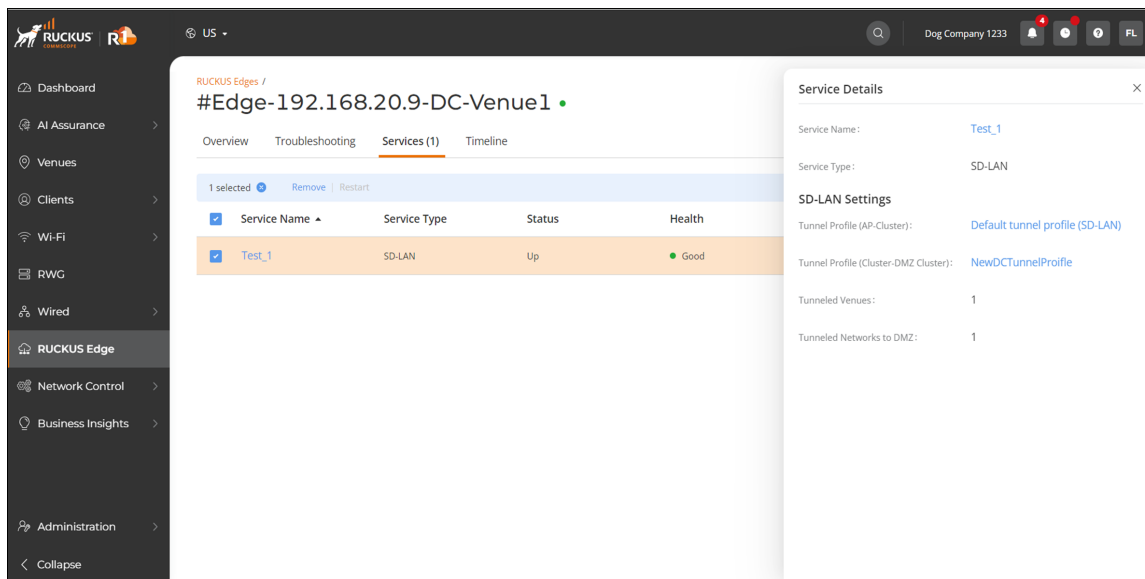
### Viewing the SD-LAN Service

**FIGURE 6** Viewing an SD-LAN Service via Network Control



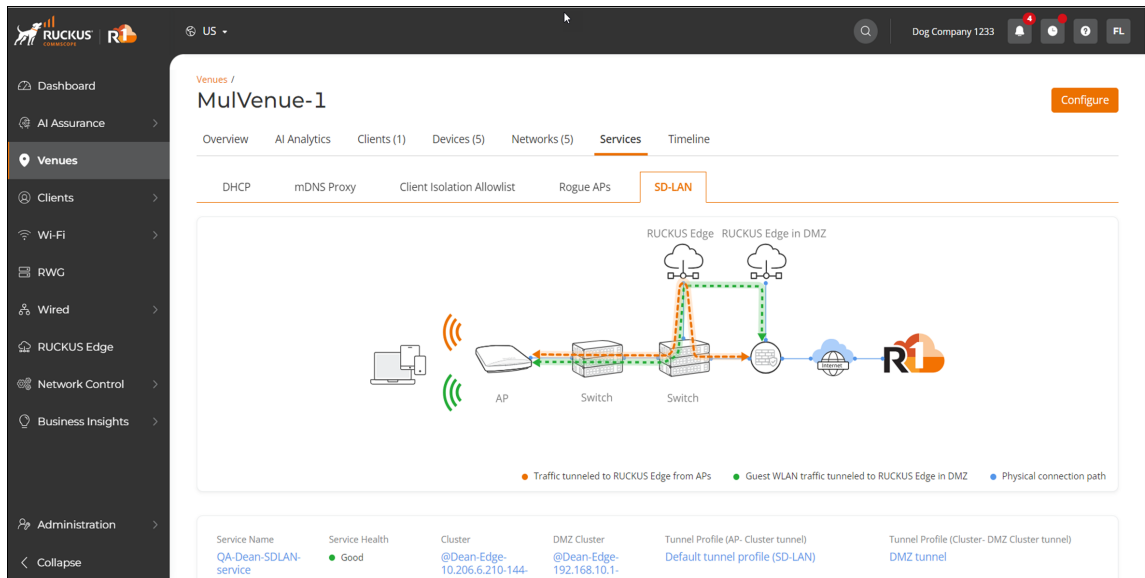
2. View the SD-LAN Service through **RUCKUS Edge**.
  - a. Click on the **RUCKUS Edge** menu option.
  - b. In the list of Edge devices, click the  icon to expand the cluster sublist.
  - c. Click on an Edge device in the sublist. The device **Overview** tab appears.
  - d. Click the **Services** tab. The SD-LAN service appears in the table, reflecting basic information such as status, health, service version, and whether an update is available.
  - e. Click on the name of the SD-LAN service to view the **Service Details** sidebar containing additional information.

**FIGURE 7** Viewing an SD-LAN Service via RUCKUS Edge



3. View the SD-LAN Service through **Venues**.
  - a. Click on the **Venues** menu option, then click the name of the venue you want to view. The venue **Overview** tab appears.
  - b. Click the **Services** tab. The **DHCP** sub-tab appears.
  - c. Click the **SD-LAN** sub-tab. The service details appear, reflecting the end-to-end system architecture map, the service name, service health, cluster, and tunnel profile, as well as networks that will tunnel the traffic to the cluster.

**FIGURE 8** View an SD-LAN Service via Venues



## Viewing SD-LAN Statistics

You can check the count of active VxLAN-GPE tunnels and number of VLANs tunneled for RUCKUS Edge devices running an SD-LAN service. To view these statistics, follow these steps:

1. On the navigation bar, click **Network Control > My Services**, then click the **SD-LAN** tile and click on a specific SD-LAN service name.
2. Navigate to the **Instances** section and click the **RUCKUS Edges** tab. This displays the number of tunnels, number of active APs, and number of tunneled VLANs for the configured clusters.

### NOTE

The SD-LAN tunnel statistics are updated every 5 minutes.

## Software Defined Local Area Network (SD-LAN) Editing an SD-LAN Service

FIGURE 9 SD-LAN Statistics

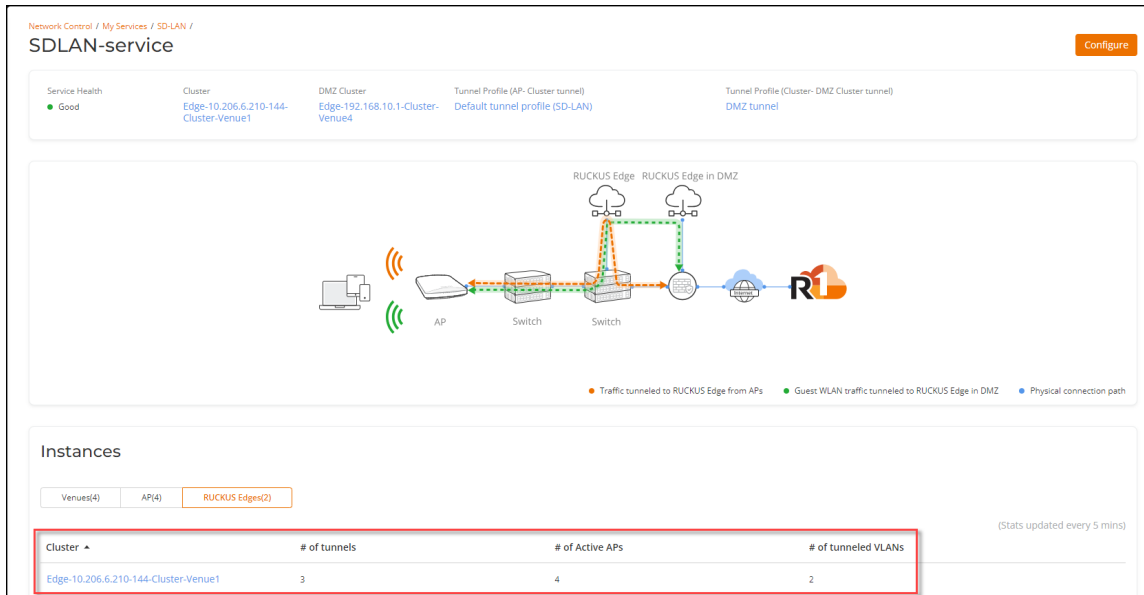
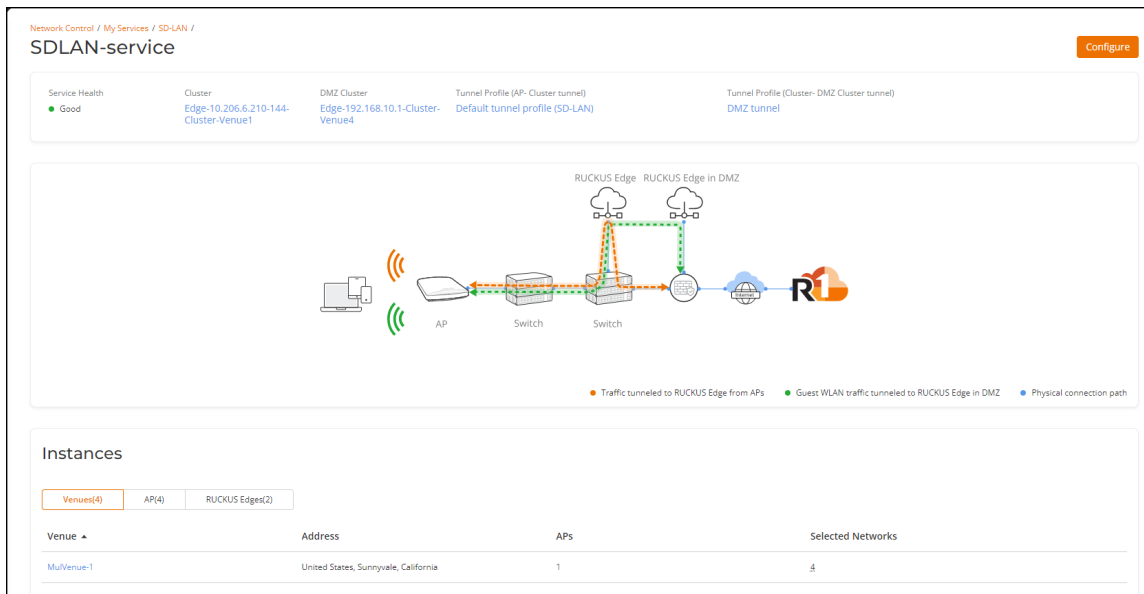


FIGURE 10 SD-LAN Statistics for Multi-Venue Support



## Editing an SD-LAN Service

To edit a SD-LAN service, follow these steps:

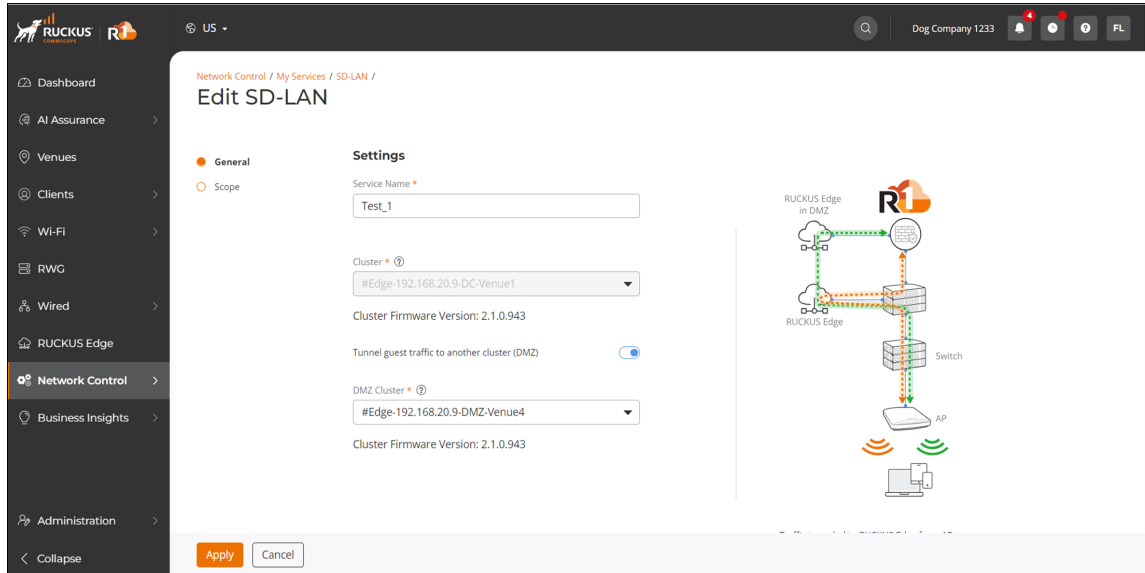
1. On the navigation bar, click **Network Control**, select **My Services > SD-LAN**. This displays the list of SD-LAN services.

2. Click on the SD-LAN service name, then click **Configure** on the resulting details page. Alternatively, select the checkbox adjacent to the service name, then click the **Edit** option. This displays the **Edit SD-LAN** page.
3. Modify the details in the **Settings** page and **Tunnel & Network** options in the **Scope** page as required. Click **Apply** to save the changes.

**NOTE**

Grayed-out fields cannot be changed.

**FIGURE 11** Edit SD-LAN



**NOTE**

If the **Tunnel Guest Traffic to another Cluster (DMZ)** option is disabled, the VXLAN-GPE tunnels connecting the access points (APs) to the Data Center are still communicating. However, the data traffic is disabled between the Data Center and the DMZ as this SD-LAN service is deleted from DMZ RUCKUS Edge device.

## Removing the SD-LAN Service from a RUCKUS Edge Device

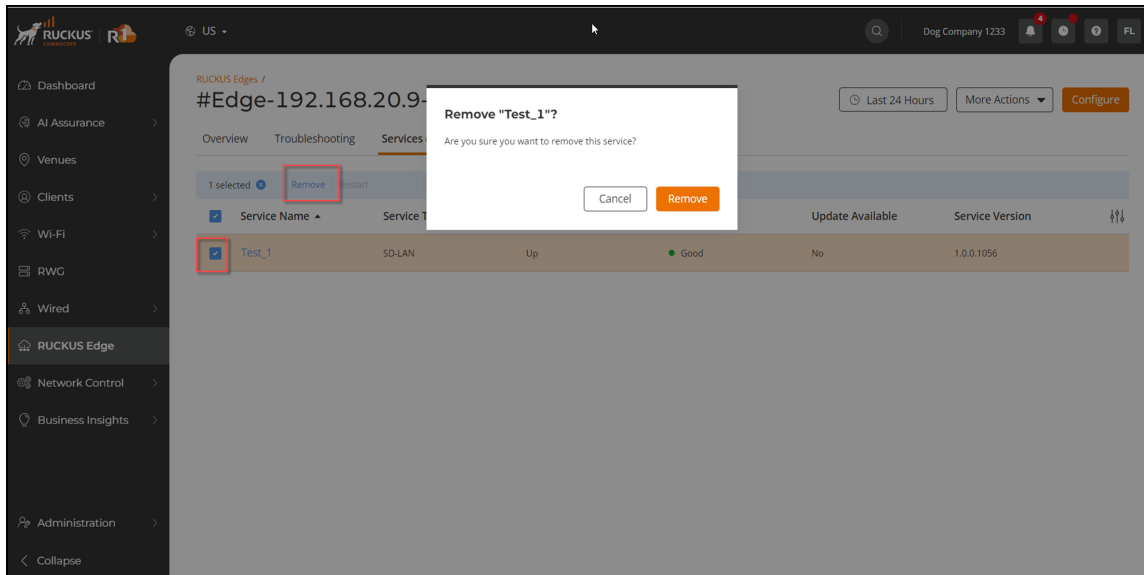
The SD-LAN service can be removed from an operational RUCKUS Edge device that is part of a multi-node Cluster with a **Ready** cluster status. The service will continue to exist in the RUCKUS One account. To remove the SD-LAN service from a RUCKUS Edge device, follow these steps:

1. Navigate to **RUCKUS Edge** and click the **+** icon to expand the cluster. This displays the Edge devices associated with the cluster.
2. Click on the Edge device name. This displays the device details in the **Overview** tab.
3. Click the **Services** tab.
4. Select the check box adjacent to the SD-LAN service name. The **Remove** option appears.
5. Click the **Remove** option. This displays the remove confirmation dialog box. Click the **Remove** button to confirm removal of the service from this Edge device.

## Software Defined Local Area Network (SD-LAN)

### Deleting an SD-LAN Service

**FIGURE 12** Remove SD-LAN Service from RUCKUS Edge



#### NOTE

After deleting the SD-LAN service from Data Center to DMZ, the VxLAN-GPE tunnels connecting the APs to the Data Center and from the Data Center to the DMZ are also removed.

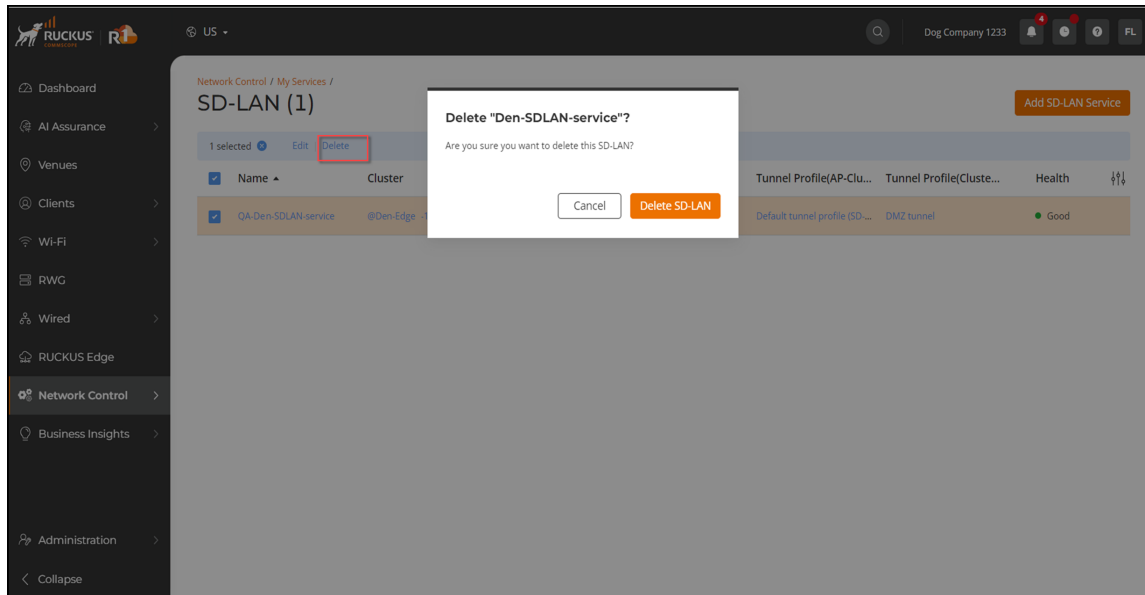
## Deleting an SD-LAN Service

Deleting an SD-LAN service not only removes it from the RUCKUS Edge device and venue to which it is associated, but also completely deletes the service from the RUCKUS One account.

To delete an SD-LAN service, follow these steps:

1. On the navigation bar, click **Network Control**, select **My Services > SD-LAN**. This displays the list of SD-LAN services for the Edge device.
2. Select the checkbox adjacent to the name of the service you wish to delete and click the **Delete** option. This displays a delete confirmation dialog box. Click the **Delete SD-LAN** button to confirm the deletion.

FIGURE 13 Delete SD-LAN Service



## Multiple Venue Support for an SD-LAN Service

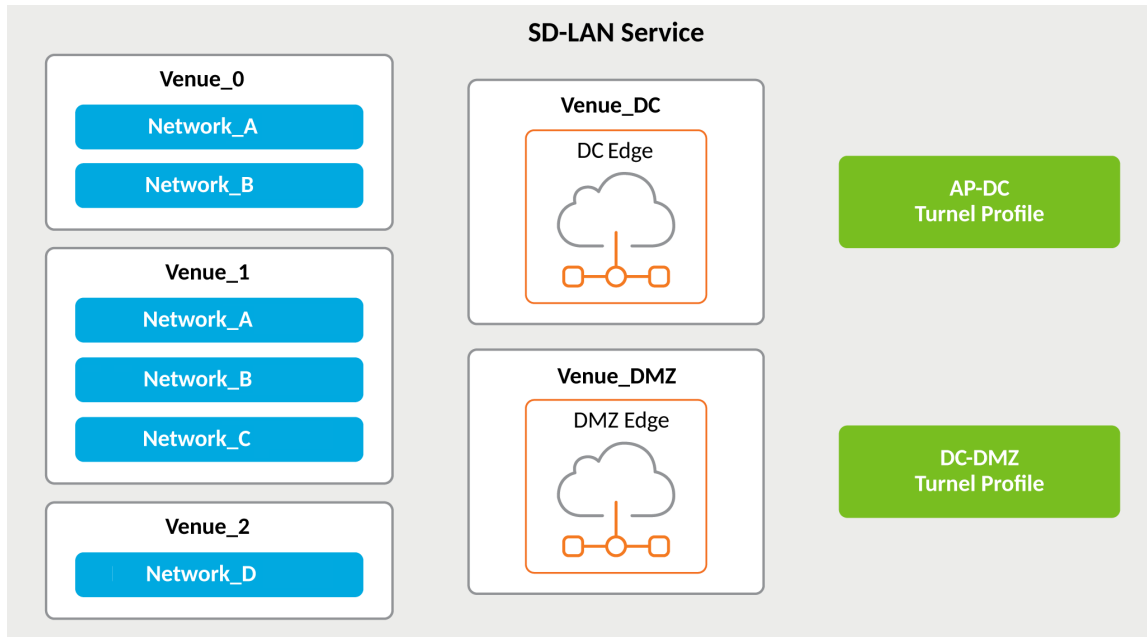
The Multiple Venue Support for an SD-LAN service feature offers a scalable and efficient way to manage multiple venues within an SD-LAN.

### Feature Overview

The Multiple Venue Support for an SD-LAN service feature enables network administrators to oversee, configure, and monitor various venues from a single centralized location, enhancing network efficiency and minimizing administrative workload. Networks from various venues can be integrated into a single SD-LAN service and a single Tunnel Profile.

The Data Center (DC) RUCKUS Edge and the DMZ RUCKUS Edge within the SD-LAN service do not need to be situated in the same venue. A venue hosting the DC RUCKUS Edge or DMZ RUCKUS Edge can support multiple SD-LAN services, each with different DC or DMZ RUCKUS Edge cluster.

FIGURE 14 Multiple Venue Support for an SD-LAN Service



## Requirements

The Multiple Venue support for an SD-LAN service feature supports APs with Wi-Fi 6, Wi-Fi 6E, and Wi-Fi 7 capabilities. This feature applies to both hardware and virtual Edge devices.

## Considerations

When creating or editing an SD-LAN service profile used for a Captive Portal network activated in multiple venues, the **Forward Guest Traffic to DMZ** option must be set the same (either enabled or disabled) across all venues using that same Captive Portal network and SD-LAN profile.

If the guest network at a specific venue routes traffic to the DMZ RUCKUS Edge, other venues using tunnels in the same network must route the traffic similarly.

## Best Practices

This feature has no special recommendations for feature enablement or usage.

## Prerequisites

Each SD-LAN venue must have at least one network tunnel.

The Tunnel Profile must be linked to the SD-LAN service to ensure that all venues, including DC and DMZ, can utilize the same Tunnel Profile. However, DC and DMZ can use different Tunnel Profiles if needed, and the DMZ is optional for an SD-LAN setup.



## Viewing Networks Configured for a Venue

You can view the details of networks that are configured for a venue.

Complete the following steps to view details about networks.

1. On the navigation bar, click **Venues**.

The **Venues** page is displayed.

**Software Defined Local Area Network (SD-LAN)**  
Multiple Venue Support for an SD-LAN Service

- Click on a specific venue name, then click the **Networks** tab.

The **Networks** tab for the venue displays the following information about each network that is assigned to the venue:

**FIGURE 15** Configured Networks in Venues

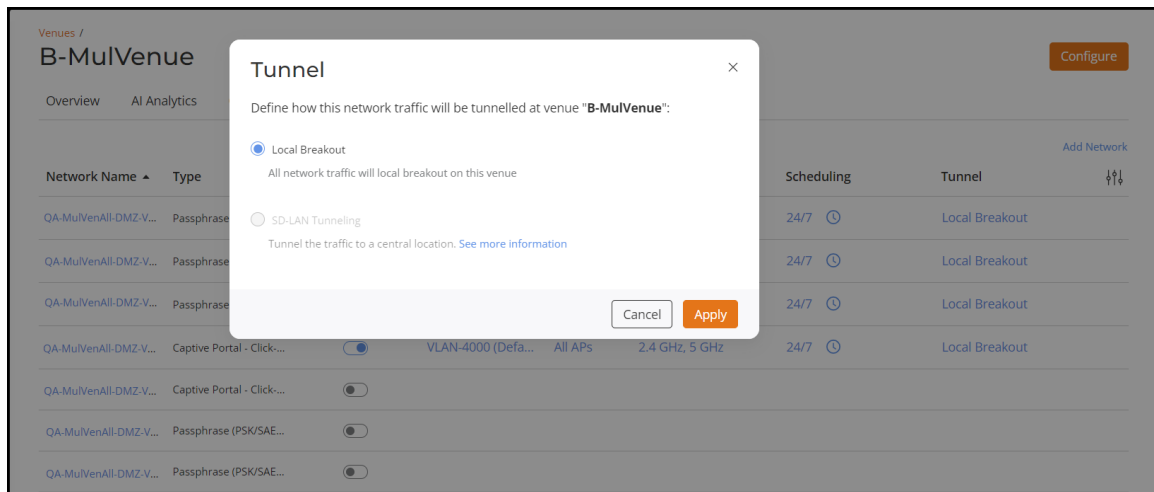
Network Name	Type	Activated	VLAN	APs	Radios	Scheduling	Tunnel
QA-MulVenAll-Dev-VLAN2	Passphrase (PSK/S...	<input checked="" type="checkbox"/>	VLAN-2 (Default)	All APs	2.4 GHz, 5 GHz	24/7	Tunneled (@Dean-Edge-1...
QA-MulVenAll-DMZ-VLAN4000	Captive Portal - Cli...	<input checked="" type="checkbox"/>	VLAN-10 (Defa...	All APs	2.4 GHz, 5 GHz	24/7	Tunneled (@Dean-Edge-1...
QA-MulVenC-Dev-VLAN2	Passphrase (PSK/S...	<input checked="" type="checkbox"/>	VLAN-2 (Default)	All APs	2.4 GHz, 5 GHz	24/7	Tunneled (@Dean-Edge-1...
QA-MulVenAll-DMZ-VLAN4000	Captive Portal - Cli...	<input checked="" type="checkbox"/>	VLAN-4000 (De...	All APs	2.4 GHz, 5 GHz	24/7	Local Breakout
QA-MulVenMulVen0-Dev-VLAN2	Passphrase (PSK/S...	<input type="checkbox"/>					
QA-MulVenMulVen0-DMZ-VLAN10	Captive Portal - Cli...	<input type="checkbox"/>					
QA-MulVenMulVen1-2nd-VLAN2	Passphrase (PSK/S...	<input type="checkbox"/>					
QA-MulVenMulVen2-Dev-VLAN2	Passphrase (PSK/S...	<input type="checkbox"/>					

- **Network Name:** The name of the network. To view more information about this network, click the network name.
- **Type:** One of the following types of network representing the network security:
  - Pre-Shared Key (PSK)
  - Dynamic Pre-Shared Key (DPSK)
  - Enterprise AAA
  - Captive Portal: Click-Through
  - Captive Portal: Self Sign In
  - Captive Portal: Cloudpath
  - Captive Portal: Host Approval
  - Captive Portal: Guest Pass
  - Captive Portal: 3rd Party (WISPr)
  - Open Network
- **Activated:** Shows ON or OFF to display whether the network is activated.
- **VLAN:** Shows the VLAN ID that is assigned to the network.
- **APs:** Displays if the network is active on all the APs or on specific AP Groups in the venue. Click the link to open a dialog box with the Radios option to configure the APs or AP Groups that are advertising this network.  
Click the information icon to view the AP and Wi-Fi feature compatibility information.
- **Radios:** Shows whether this network is available on the 2.4 GHz or 5 GHz bandwidth, or both. Click the link to open a dialog box with the APs/AP Group selection to configure the radio bandwidth.

- **Scheduling:** Shows network availability. Click the clock icon to open a window to set either 24/7 availability or customize the network availability down to 30-minute time periods for an individual day. Click **Save** to save your changes.
- **Tunnel:** Shows if the selected venue is associated to an SD-LAN service. When the Tunnel column for venue networks is blank, it indicates that they are not using SD-LAN or Local Breakout tunneling. No tunneling method is being employed for those networks.
  - **Local Breakout :** This option is automatically chosen when the venue is not linked to any SD-LAN service. The tunnel traffic will bypass the central location.

Click the **See more information** link, to view information on Configuring an SD-LAN service.

**FIGURE 16** Local Breakout



- **SD-LAN Tunneling**

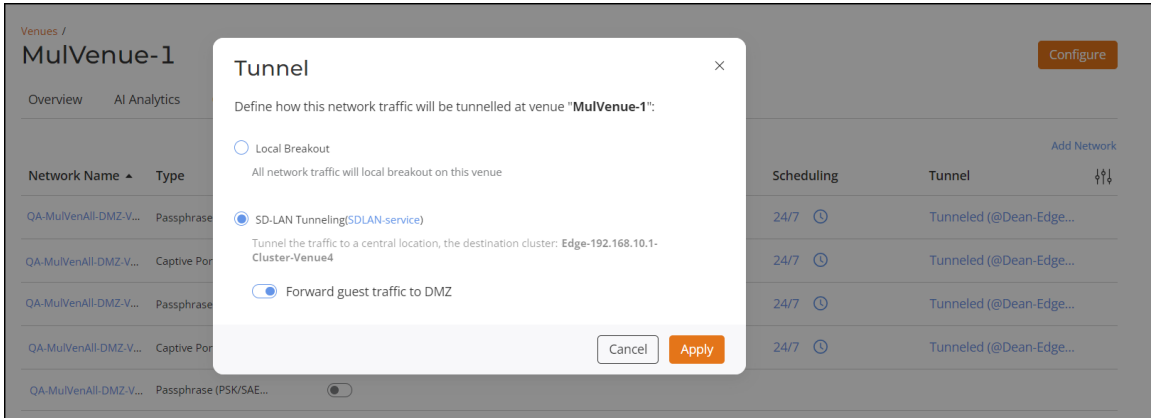
- › When the venue is linked to an SD-LAN service but does not enable tunneling guest traffic to another cluster in the DMZ.
- › When the venue is linked to an SD-LAN service but does not enable tunneling guest traffic to another cluster in the DMZ, where the network type is Captive portal. Enable the **Forward guest traffic to DMZ** option.

**NOTE**

If the venue is linked to an SD-LAN service, you can configure the DMZ or DC tunnel settings from this window. To configure, select the required option and click **Apply**.

**Software Defined Local Area Network (SD-LAN)**  
Multiple Venue Support for an SD-LAN Service

**FIGURE 17** Tunneling Options



# High Availability

---

- High Availability..... 29
- Onboarding a Dual-Node Cluster for High Availability..... 30
- Configuring a Dual-Node Cluster for High Availability with a LAG Interface..... 32
- Configuring a Cluster for Active Standby High Availability deployment without a LAG interface..... 43
- Onboarding a Single-Node Cluster..... 50
- Editing a Cluster and Nodes.....51

## High Availability

The High Availability (HA) for RUCKUS Edge enables the network to operate continuously without failing.

### Overview

High Availability (HA) refers to the ability of a network to remain operational despite an outage in the system, such as a link or node failure, by ensuring fast and reliable failover from the failed device to a redundant device.

### Requirements

The Cluster Interface is essential for enabling clustering in RUCKUS Edge. To configure it, a distinct physical interface must be provided within the RUCKUS Edge. This interface facilitates the exchange of cluster information, cluster formation, and node health maintenance. For each node in the dual-node cluster, this interface should be connected to the same Layer 2 network, separate from the LAN network.

The port or LAG connecting to the core switch from the RUCKUS Edge device should be configured as an IEEE 802.1w (RSTP) edge port or LAG. This configuration ensures faster transitions of the port or LAG to the RSTP forwarding state, which is crucial for correct VRRP role selection convergence.

### Considerations

In the RUCKUS Edge-deployed networks, active and standby nodes maintain communication and in the event of a failover, the below scenario is established:

- If the active node does not respond, the standby node becomes the active node.
- After the failed active node is operational and rejoins the cluster, it becomes the new standby node.

### Best Practices

This feature has no special recommendations for feature enablement or usage.

### Prerequisites

This section lists all the prerequisites to support High Availability on RUCKUS Edge.

- Install two RUCKUS Edge devices as there should be two nodes for the cluster to operate.
- Create a venue and associate the RUCKUS Edge cluster.

## High Availability

### Onboarding a Dual-Node Cluster for High Availability

# Onboarding a Dual-Node Cluster for High Availability

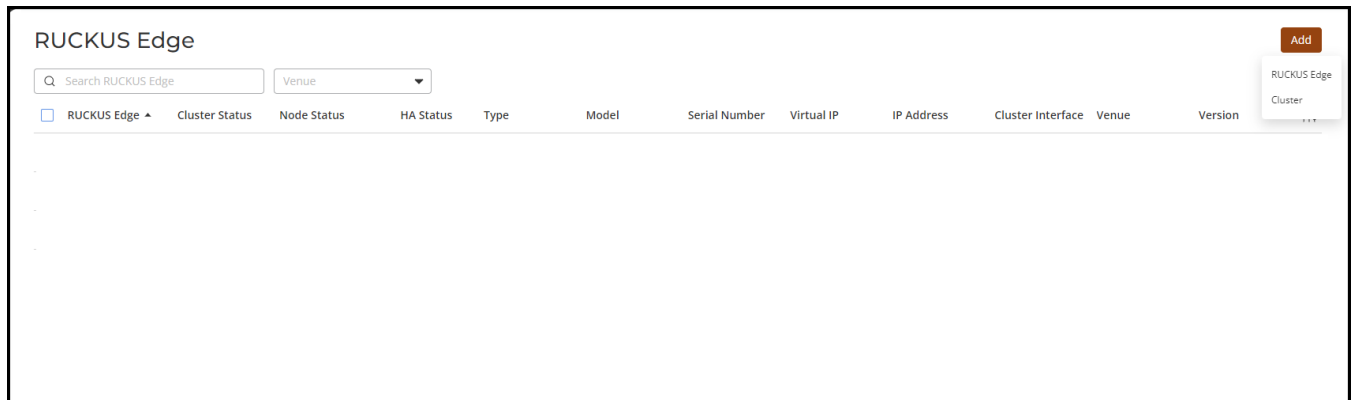
This task describes creating a two-node, high-availability RUCKUS Edge cluster in RUCKUS One.

Prior to performing this procedure, you must have already configured the Venue with which this cluster will be associated. You must also have two RUCKUS Edge devices installed and ready for onboarding to RUCKUS One.

Create a dual-node Edge cluster as follows:

1. Log in to the RUCKUS One web user interface with your credentials.
2. On the RUCKUS One navigation bar, click **RUCKUS Edge**.  
This displays the **RUCKUS Edge** page.
3. In the **RUCKUS Edge** page, click **Add** and select **Cluster**. This displays the **Add Cluster** page.

**FIGURE 18** Add Cluster



4. In the **Add Cluster** page, enter the following details:
  - **Venue:** Click the drop-down arrow to select a site for the new cluster.
  - **Cluster Name:** Enter a meaningful name for the cluster profile.
  - **Description:** Enter a purposeful statement for the device.

5. In the **RUCKUS Edges** section, define two Edge devices as two nodes are required to establish a complete cluster. Enter the name and serial number of the first Edge device in the available fields. Add a second Edge device in the same manner by clicking the **Add another RUCKUS Edge** option.
- RUCKUS Edge Name: Enter a meaningful name for the nodes.
  - Serial Number: Enter the serial number of the Edge device. You can obtain the serial number by logging in to the Edge CLI or by looking at the label on the physical Edge device.
  - Model: After the serial number is entered, the model name is displayed automatically.
- To delete a RUCKUS Edge device, click on the **Delete** icon adjacent to the RUCKUS Edge entry.

FIGURE 19 Adding a Dual Node Cluster

RUCKUS Edges /  
**Add Cluster**

Venue \*  
Document-Venue  
Venue firmware version for RUCKUS Edge: 2.1.0.943

Cluster Name \*  
Document-Cluster

Description  
Creating a new cluster profile for documentation

RUCKUS Edges (0)

The cluster function will operate when there are at least two nodes present. Please add more nodes to establish a complete cluster.

RUCKUS Edge Name *	Serial Number *	Model
Document-node1	965A6946097AE211EFB8E5000C2927AA64	vEdge
Document-node2	965A5D2A357AE211EFBA32000C298BC70A	vEdge

The one-time-password (OTP) will be automatically sent to your email address or via SMS for verification when you add a virtual RUCKUS Edge node. The password will expire in 10 minutes and you must complete the authentication process before using it.

Add Cancel

**NOTE**

The one-time-password (OTP) is automatically sent to your email address or through the SMS for verification when you add a virtual Edge node (each Edge added as part of the **Add Cluster** receives an OTP for verification). The password expires in 10 minutes, and you must complete the authentication process before the OTP expires; otherwise you have to request a new OTP.

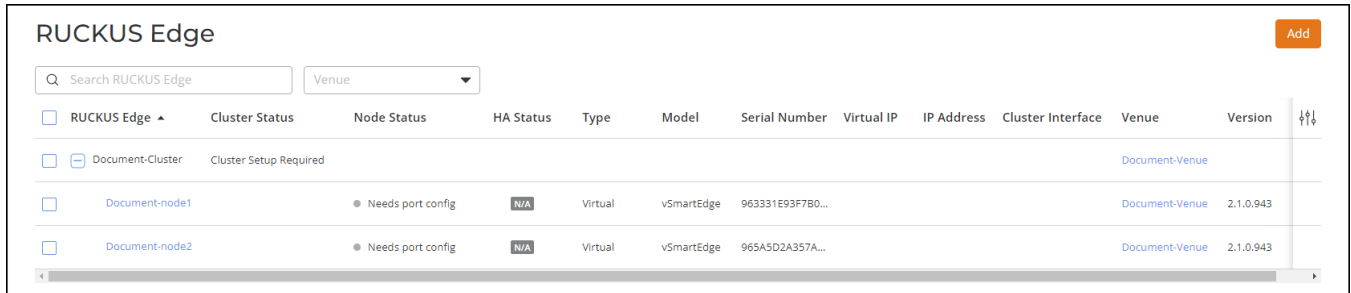
## High Availability

### Configuring a Dual-Node Cluster for High Availability with a LAG Interface

6. Click **Add**.

This displays the newly added **Cluster** and **Nodes** in the **RUCKUS Edge** screen.

**FIGURE 20** Node Status



<input type="checkbox"/> RUCKUS Edge ▲	Cluster Status	Node Status	HA Status	Type	Model	Serial Number	Virtual IP	IP Address	Cluster Interface	Venue	Version	⌵
<input type="checkbox"/> Document-Cluster	Cluster Setup Required									Document-Venue		
<input type="checkbox"/> Document-node1		● Needs port config	N/A	Virtual	vSmartEdge	963331E93F7B0...				Document-Venue	2.1.0.943	
<input type="checkbox"/> Document-node2		● Needs port config	N/A	Virtual	vSmartEdge	965A5D2A357A...				Document-Venue	2.1.0.943	

#### NOTE

After the nodes are added to the venue and onboarded, the **Node Status** is **Needs port config**.

## Configuring a Dual-Node Cluster for High Availability with a LAG Interface

This task describes configuring a two-node, high-availability RUCKUS Edge cluster in RUCKUS One.

Prior to performing this procedure, you must have already added the Edge cluster in RUCKUS One.

Configure a dual-node RUCKUS Edge cluster as follows:

1. Log in to the RUCKUS One web user interface with your credentials.
2. On the RUCKUS One navigation bar, click **RUCKUS Edge**.

This displays the **RUCKUS Edge** page.

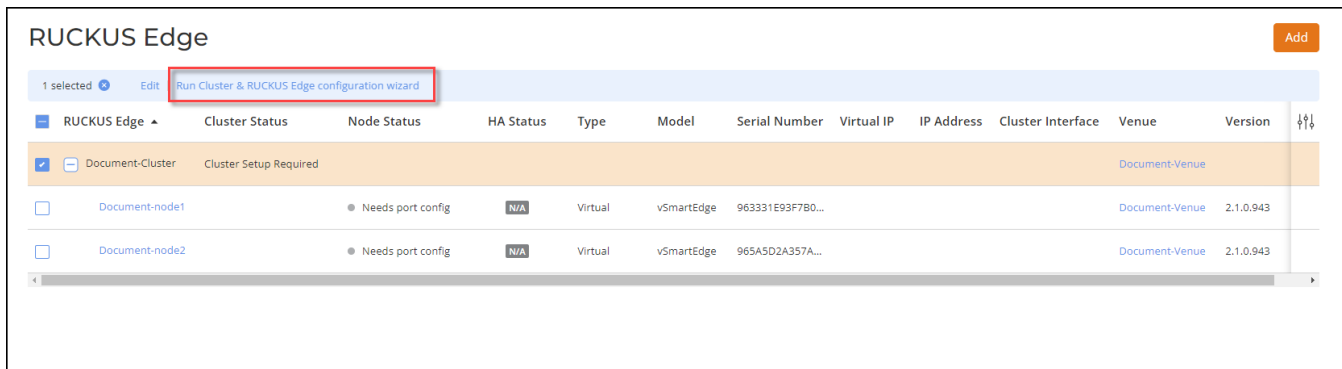


3. Select the checkbox adjacent to the RUCKUS Edge cluster. This highlights the **Edit** and **Run Cluster & RUCKUS Edge configuration wizard** options.

**NOTE**

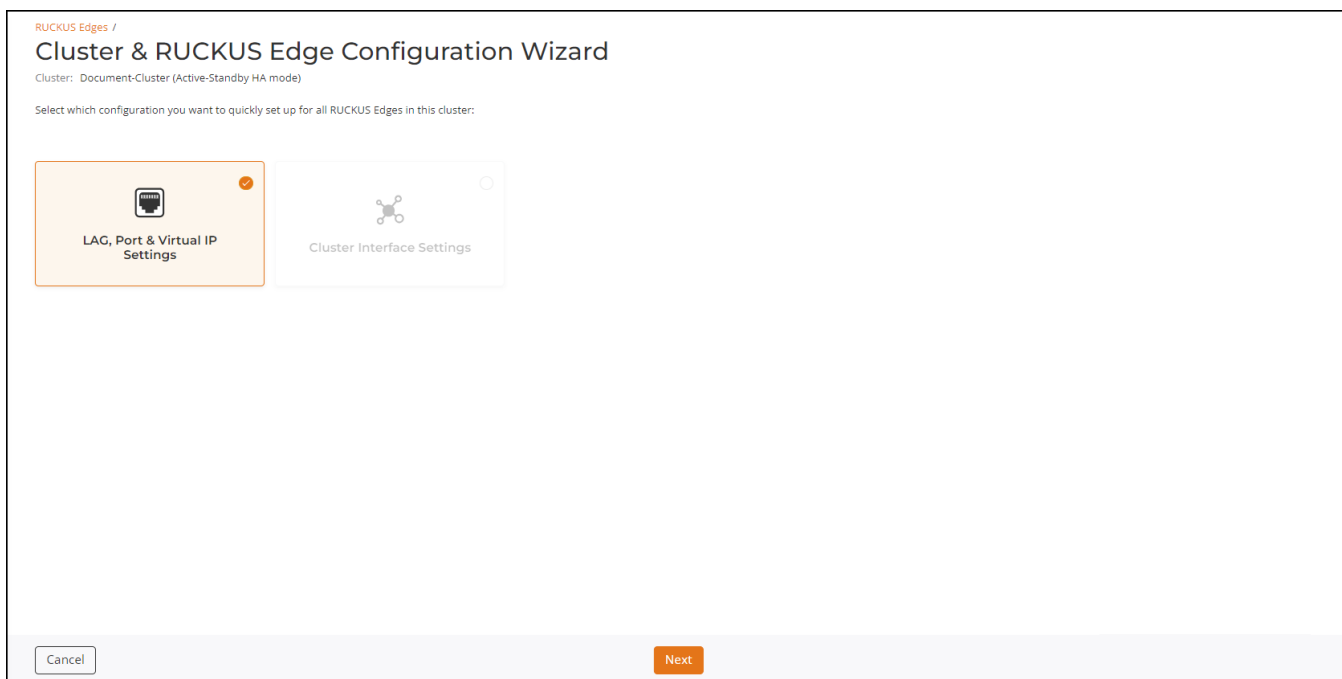
The **Node Status** is **Need port config**.

**FIGURE 21** Run Cluster and RUCKUS Edge Configuration Wizard



4. Click the **Run Cluster & RUCKUS Edge configuration wizard** option.  
This displays the **Cluster & RUCKUS Edge Configuration Wizard** screen of the selected RUCKUS Edge cluster with the two options.
  - **LAG, Port & Virtual IP Setting**
  - **Cluster Interface Settings**
5. Select the **LAG, Port & Virtual IP Setting** checkbox and click **Next** to start the configuration.

**FIGURE 22** Cluster and RUCKUS Edge Configuration Wizard



## High Availability

### Configuring a Dual-Node Cluster for High Availability with a LAG Interface

6. Proceed to section [Link Aggregation Group \(LAG\), Port and Virtual IP Settings](#) on page 35 for configuration details.

## Link Aggregation Group (LAG), Port and Virtual IP Settings

This section describes configuring LAG, Port, and Virtual IP Settings for a Edge cluster. The **LAG, Port & Virtual IP Settings** wizard begins on the **LAG Settings** screen.

1. **LAG Settings:** Click the **Add LAG** option.

**FIGURE 23** Add LAG Settings

RUCKUS Edges / Cluster & RUCKUS Edge Configuration Wizard  
Cluster: Document-Cluster (Active-Standby HA mode)

**LAG Settings**  
Create and configure the LAG for all RUCKUS Edges in this cluster if needed, or click 'Next' to skip:

Document-node1 Document-node2

[Add LAG](#)

LAG Name	Description	LAG Type	LAG Members	Port Type	IP Type	IP Address	Subnet Mask	Admin Status
No Data								

Nodes Compatibility Check: ● Pass

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

## High Availability

Configuring a Dual-Node Cluster for High Availability with a LAG Interface

FIGURE 24 Add LAG

The screenshot shows a configuration window titled "Add LAG" with a close button (X) in the top right corner. The window contains the following fields and controls:

- LAG Name:** A dropdown menu showing "LAG 1".
- Description:** A text input field containing "Configuring LAG for node-1".
- LAG Type:** A dropdown menu showing "LACP (Dynamic)".
- Mode:** A dropdown menu showing "Active".
- Timeout:** A dropdown menu showing "Short".
- Select LAG members:** A section with two checkboxes: "Port1" (checked) and "Port2" (unchecked). To the right of "Port1" is a "Port Enabled" toggle switch, which is currently turned on.
- Port Type:** A dropdown menu showing "LAN".
- Use this LAG as Core LAG:** A checked checkbox with a help icon.
- LAG Enabled:** A toggle switch, which is currently turned on.
- IP Settings:**
  - IP Assignment:** Radio buttons for "DHCP" (unselected) and "Static/Manual" (selected).
  - IP Address:** A text input field containing "192.168.101.1".
  - Subnet Mask:** A text input field containing "255.255.0.0".
  - Gateway:** A text input field containing "192.168.101.1".

At the bottom of the window are two buttons: "Cancel" and "Add".

2. On the **Add LAG** interactive sidebar, complete the fields and click **Add**.

**NOTE**

Refer to Configuring Link Aggregation Group for descriptions of the fields in the Add LAG sidebar.

## High Availability

### Configuring a Dual-Node Cluster for High Availability with a LAG Interface

- Repeat [Step 1](#) and [Step 2](#) for the second node. When the compatibility check successfully passes, click Next to proceed to the next page of the wizard.

RUCKUS One performs a compatibility check of the configurations on each node. If a mismatch is detected, it displays a warning message labeled **Mismatch**. You can click on the **See Details** option to view the root cause and specifics of the mismatch to quickly identify the discrepancies.

You can Edit or Delete the offending LAG by selecting the checkbox adjacent to the LAG. After the mismatches are resolved, the compatibility check result changes to **Pass**.

**FIGURE 25** LAG Nodes Compatibility Check with Mismatch

The screenshot shows the 'Cluster & RUCKUS Edge Configuration Wizard' for a 'Document-Cluster (Active-Standby HA mode)'. The 'LAG Settings' section is active, showing configuration for 'Document-node1' and 'Document-node2'. A table lists LAG configurations, with 'LAG 0' selected. A 'Nodes Compatibility Check' bar at the bottom indicates a 'Mismatch' with a red circle icon and a 'See details' link. A 'Compatibility Check' modal is open on the right, showing the root cause: 'The nodes' configurations are not in sync on the number and port type.' The modal lists details for 'Document-node1' (1 LAG, 1 Core Port, LAN Port Types) and 'Document-node2' (1 LAG, 1 Core Port, CLUSTER Port Types). Navigation buttons include 'Cancel', 'Next', and 'OK'.

LAG Name	Description	LAG Type	LAG Members	Port Type	IP Type
LAG 0		LACP (Active)	0	CLUSTER	Static IP

FIGURE 26 LAG Nodes Compatibility Check with Pass Result

The screenshot shows the 'Cluster & RUCKUS Edge Configuration Wizard' interface. The breadcrumb path is 'RUCKUS Edges /'. The cluster is named 'Document-Cluster (Active-Standby HA mode)'. The current step is 'LAG Settings', which includes a sidebar with 'LAG' selected and other options like 'Port General', 'Cluster Virtual IP', and 'Summary'. The main area shows 'LAG Settings' for 'Document-node2'. A table lists one LAG configuration: 'LAG 0' with 'LACP (Active)' type, 0 members, LAN port type, Static IP, IP address 192.168.201.1, Subnet Mask 255.255.255.0, and Admin Status 'Enabled'. At the bottom, a green bar indicates 'Nodes Compatibility Check' with a 'Pass' result, highlighted by a red box. 'Cancel' and 'Next' buttons are also visible.

RUCKUS Edges /  
Cluster: Document-Cluster (Active-Standby HA mode)

### LAG Settings

Create and configure the LAG for all RUCKUS Edges in this cluster if needed, or click 'Next' to skip:

Document-node1 | **Document-node2**

1 selected | Edit | Delete | Add LAG

LAG Name	Description	LAG Type	LAG Members	Port Type	IP Type	IP Address	Subnet Mask	Admin Status
LAG 0		LACP (Active)	0	LAN	Static IP	192.168.201.1	255.255.255.0	Enabled

Nodes Compatibility Check: **Pass**

Cancel | Next

## High Availability

### Configuring a Dual-Node Cluster for High Availability with a LAG Interface

#### 4. **Ports General Settings:** Configure the port general settings for all Edge devices.

- Description: Enter a meaningful description for the port settings.
- Port Type: Select a port type from the drop-down menu.

#### **NOTE**

As you have configured LAG as a LAN port, for **Port Type**, select **Cluster** and enable the **Port Enabled** option.

- IP Settings: Configure the IP settings for the cluster port:
  - IP Assignment: Select **DHCP** or **Static/Manual**. If static/manual IP is selected, then enter the **IP Address** and **Subnet Mask** of the port.
- Select the other node and configure the appropriate port.

**FIGURE 27** RUCKUS Edge LAG, Port, and Virtual IP Settings: Port Settings

The screenshot displays the 'Cluster & RUCKUS Edge Configuration Wizard' interface. The breadcrumb trail shows 'RUCKUS Edges / Cluster & RUCKUS Edge Configuration Wizard'. The current step is 'Port General Settings', which is highlighted in the left-hand navigation menu. The wizard is for a 'Document-Cluster (Active-Standby HA mode)'. The main content area is titled 'Port General Settings' and includes the instruction: 'Configure the port general settings for all RUCKUS Edges in this cluster:'. Below this, there are two tabs: 'Document-node1' (selected) and 'Document-node2'. A red warning message states: 'At least one port must be enabled and configured to WAN or core port to form a cluster.' There are two port selection buttons: 'Port1' and 'Port2', with 'Port2' being the active selection. The IP Address is '192.168.30.97/24' and the MAC Address is '00:0c:29:27:aa:6e'. The Description field contains 'Configuring ports for node1'. The Port Type dropdown menu is set to 'Cluster'. The Port Enabled toggle switch is turned on. Under the 'IP Settings' section, the IP Assignment radio buttons are set to 'Static/Manual'. The IP Address field contains '192.168.30.97'. At the bottom, a green bar indicates 'Nodes Compatibility Check: Pass'. Navigation buttons include 'Cancel', 'Back', and 'Next'.

Click **Next**.



5. **Cluster Virtual IP:** Virtual IP Address of a Cluster is similar to any other IP address except it does not have a specific host or node to resolve.
  - Virtual IP: In this section, click **Select Interface** link. This displays the **Select Interfaces** sidebar. In the **Select Interfaces** window, select the **Ports** for node 1 and 2 and click **Ok**. The Node Name, Interface and IP address details are displayed in the **Virtual IP** section.
  - Virtual IP Address: Enter the VRRP IP address for switches to connect to Edge.
  - Failover Settings: Drag the **HA Timeout** timeline bar to adjust the amount of time allowed to elapse before triggering a failover.

**NOTE**

An HA failover time of 6 seconds or longer is recommended for Edge use-cases. A timer set to less than this is very aggressive and could potentially cause VRRP issues in some networks. HA timeout refers to the time period within which a node must receive a periodic heartbeat signal from the active node. If the timer expires prior to receiving a heartbeat signal, then the system initiates the failover process to select the next active node and maintain system functionality.

**FIGURE 28** RUCKUS Edge LAG, Port, and Virtual IP Settings: Virtual IP and Failover

The screenshot displays the 'Cluster & RUCKUS Edge Configuration Wizard' for a 'Document-Cluster (Active-Standby HA mode)'. The 'Cluster Virtual IP' section is active, showing a table of interfaces for two nodes and a virtual IP address field. The 'Failover Settings' section includes an HA Timeout slider set to 6 seconds. A 'Nodes Compatibility Check' bar at the bottom indicates 'Pass'. A 'Select Interfaces: #1 Virtual IP' sidebar is open on the right, showing 'Lag0' selected for both nodes.

**Cluster Virtual IP**

Please select the interfaces for RUCKUS Edges and assign virtual IPs for seamless failover:

**#1 Virtual IP**

Interfaces \*

Node Name	Interface	IP Subnet
Document-node1	Lag0	192.168.201.10/16
Document-node2	Lag0	192.168.201.1/16

Virtual IP Address \*

192.168.0.1

Suggested range: 192.168.0.0/16

**Failover Settings**

HA Timeout ⓘ

3 seconds — 6 seconds — 15 seconds

Nodes Compatibility Check: ● Pass

Cancel Back Next Cancel OK

Click **Next**.

## High Availability

### Configuring a Dual-Node Cluster for High Availability with a LAG Interface

6. **Summary:** This displays the configuration settings on the cluster. View and verify the configuration details and click **Apply & Continue** to proceed to the **Cluster Interface Settings** configuration, or **Apply & Finish** to complete the **LAG, Port and Virtual IP Settings** configuration without proceeding to the **Cluster Interface Settings** configuration.

**FIGURE 29** RUCKUS Edge LAG, Port, and Virtual IP Settings: Summary

RUCKUS Edges / Cluster & RUCKUS Edge Configuration Wizard  
Cluster: Document-Cluster (Active-Standby HA mode)

Summary

LAG

RUCKUS Edge	LAG Name	LAG Type	LAG Members	Port Type	IP Type	IP Address	Admin Status
Document-node1	Lag0	LACP (Active)	1	LAN	Static IP	192.168.201.10	Enabled
Document-node2	Lag0	LACP (Active)	1	LAN	Static IP	192.168.201.1	Enabled

Port General

RUCKUS Edge	Port	Admin Status	Port Type	IP Type	IP Address
Document-node2	port2	Disabled	CLUSTER	Static IP	192.168.30.91
Document-node1	port2	Enabled	CLUSTER	Static IP	192.168.30.97

Cluster Virtual IP

#1 Virtual IP

Interfaces	Virtual IP Address
Document-node1 - Lag0 Document-node2 - Lag0	192.168.0.1

HA Timeout  
6 seconds

Nodes Compatibility Check: ● Pass

Cancel Back Apply & Continue Apply & Finish

#### NOTE

After the nodes are configured, the **Node Status** changes from **Needs Port Config** to **Operational**, **Cluster Status** is **Ready 2/2** and **HA Status** is node 1 is **Active** and node 2 status is **Standby**.

FIGURE 30 Nodes Status is Operational

RUCKUS Edge												Add
Search RUCKUS Edge												Venue
<input type="checkbox"/> RUCKUS Edge	Cluster Status	Node Status	HA Status	Type	Model	Serial Number	Virtual IP	IP Address	Cluster Interf...	Venue	Version	
<input type="checkbox"/> Document-Cluster	Ready (2/2)						192.168.10.13			Document/Venue		
<input type="checkbox"/> Document-node1		Operational	Active	Virtual	vSmartEdge	9667EFA7D5641...		192.168.10.91/24	port2	Document/Venue	2.1.0.943	
<input type="checkbox"/> Document-node2		Operational	Standby	Virtual	vSmartEdge	9669C3AB31641...		192.168.10.68/24	port2	Document/Venue	2.1.0.943	

7. Proceed to section [Cluster Interface Settings](#) on page 43 for configuration details

## Cluster Interface Settings

The cluster interface is used as a communication channel between the RUCKUS Edge devices.

This section describes configuring Cluster Interface Settings.

After configuring the [LAG, Port and Virtual IP Settings](#) and clicking **Apply & Continue** (as described in [Link Aggregation Group \(LAG\), Port and Virtual IP Settings](#) on page 35), select the **Cluster Interface** checkbox and click **Next**. This displays **Cluster Interface** page containing a tab for each Edge device in the cluster.

1. On the first device tab, configure these settings:
  - **Set cluster interface on:** Use the drop-down menu to select the port that want to serve as the cluster interface to the other Edge device.
  - Enter the **IP Address** and **Subnet Mask** address of cluster interface port.
2. Repeat [Step 1](#) on the second device tab.
3. Click **Apply & Finish**.

## Configuring a Cluster for Active Standby High Availability deployment without a LAG interface

This section describes configuring a cluster for high availability without a LAG interface in RUCKUS Edge.

You can choose to configure a cluster without a LAG when the cluster for HA ensure redundancy and failover capabilities including link failures.

Configure a dual-node RUCKUS Edge cluster without LAG as follows:

1. Log in to the RUCKUS One web user interface with your credentials.

## High Availability

Configuring a Cluster for Active Standby High Availability deployment without a LAG interface

2. On the RUCKUS One navigation bar, click **RUCKUS Edge**.

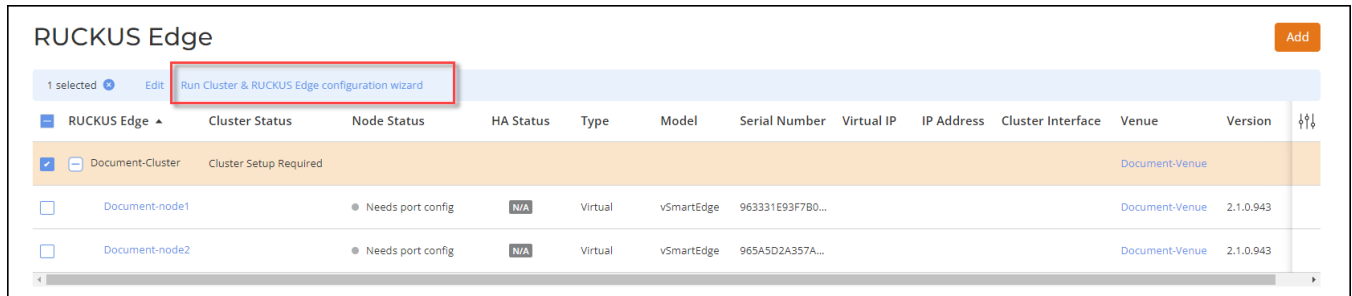
This displays the **RUCKUS Edge** page.

3. Select the checkbox adjacent to the RUCKUS Edge cluster name. This highlights the **Edit** and **Run Cluster & RUCKUS Edge configuration wizard** options.

### NOTE

The **Node Status** is **Need port config**.

**FIGURE 31** Run Cluster and RUCKUS Edge Configuration Wizard



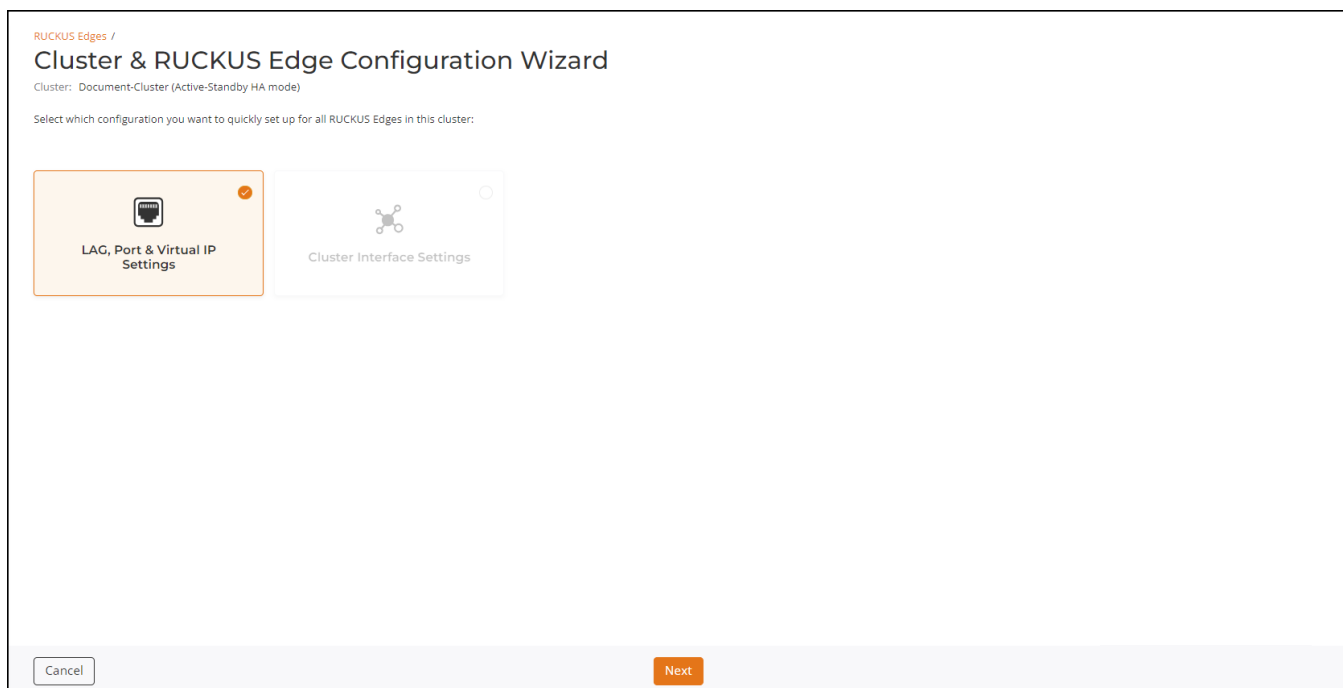
4. Click the **Run Cluster & RUCKUS Edge configuration wizard** option.

This displays the **Cluster & RUCKUS Edge Configuration Wizard** screen of the selected RUCKUS Edge device with the two options.

- **LAG, Port and Virtual IP Setting**
- **Cluster Interface Settings**

5. Select the **LAG, Port & Virtual IP Settings** checkbox and click **Next** to start the configuration.

**FIGURE 32** Cluster and RUCKUS Edge Configuration Wizard



## Link Aggregation Group (LAG), Port and Virtual IP Settings

This section describes configuring LAG, Port and Virtual IP Settings.

1. **LAG Settings:** To configure a cluster without a LAG interface, click **Next**.

## High Availability

### Configuring a Cluster for Active Standby High Availability deployment without a LAG interface

2. **Ports General Settings:** Configure the port general settings for all RUCKUS Edge devices.
  - Description: Enter a meaningful description for the port settings.
  - Port Type: Select a port type from the drop-down menu. If a LAG is not configured, it is necessary to configure at least one port to function as a LAN port or core port in order to form a cluster. To configure one port as core port, follow these steps:
    - a. In the sub-tab for one RUCKUS Edge device (node), select the **Port1** sub-tab and enter the description.
    - b. In the **Port Type** drop-down menu, select **LAN** and select the check box **Use this port as Core Port**. By default, the **Port Enabled** option is enabled.
    - c. Remain in the same device (node) sub-tab, then select the **Port2** sub-tab and enter the description.
    - d. In the **Port Type** drop-down menu, select **Cluster**. By default, the **Port Enabled** option is enabled.

**FIGURE 33** Configuring Ports Without a LAG - 1

The screenshot displays the 'Cluster & RUCKUS Edge Configuration Wizard' interface. The main heading is 'Port General Settings' with a sub-heading 'Configure the port general settings for all RUCKUS Edges in this cluster:'. The wizard is currently on the 'Document-node1' tab. The 'Port Type' dropdown menu is set to 'LAN', and the 'Use this port as Core Port' checkbox is checked. The 'Port Enabled' checkbox is also checked. The 'IP Settings' section is visible, showing 'IP Assignment' set to 'Static/Manual', 'IP Address' as '192.168.10.64', 'Subnet Mask' as '255.255.255.0', and 'Gateway' as '192.168.10.254'. A 'Model Compatibility Check' at the bottom indicates 'Pass'. Navigation buttons for 'Cancel', 'Back', and 'Next' are present at the bottom of the form.

FIGURE 34 Configuring Ports Without a LAG - 2

RUCKUS Edge / Cluster & RUCKUS Edge Configuration Wizard  
Cluster: Document-Cluster (Active-Standby HA mode) Back to Cards

LAG  
**Port General**  
 Cluster-Virtual IP  
 Summary

Port General Settings  
 Configure the port general settings for all RUCKUS Edges in this cluster:

Document-node1 Document-node2

Port1 Port2

IP Address: 192.168.30.97/24 | MAC Address: 00:0c:29:27:aa:5e

Description

Port Type \*  
 Cluster

Port Enabled

IP Settings  
 IP Assignment \*  
 DHCP  
 Static/Manual

IP Address \*  
 192.168.30.97

Subnet Mask \*  
 255.255.255.0

Nodes Compatibility Check: ● Pass

Cancel Back Next

- e. Repeat steps 2.1 through 2.4 to configure ports for the second RUCKUS Edge device (node) in the cluster, then click **Next**.

**NOTE**

**Use this port as Core Port** is utilized for the SD-LAN service, the core port on this RUCKUS Edge establishes tunnels for directing data traffic effectively.

- IP Settings: Configure the IP settings for the cluster ports:
  - IP Assignment: Select **DHCP** or **Static/Manual**. If static/manual IP is selected, then enter the **IP Address**, **Subnet Mask** and **Gateway** of the port.

**NOTE**

The **Gateway** field is available only when the **Port Type** is set to **LAN**.

- Click **Next**.

## High Availability

Configuring a Cluster for Active Standby High Availability deployment without a LAG interface

3. **Cluster Virtual IP:** This section displays the configured **Node Name**, **Interface** and **IP Subnet Mask**. Enter the **Virtual IP Address**.

To edit/delete the configuration, click **Change** or **Clear**.

- Virtual IP Address: Enter the VRRP IP address for switches to connect to RUCKUS Edge.
- Failover Settings: Drag the **HA Timeout** timeline bar to adjust the amount of time allowed to elapse before triggering a failover.

### NOTE

An HA failover time of 6 seconds or longer is recommended for RUCKUS Edge use-cases. A timer set to less than this is very aggressive and could potentially cause VRRP issues in some networks. HA timeout refers to the time period within which a node must receive a periodic heartbeat signal from the active node. If the timer expires prior to receiving a heartbeat signal, then the system initiates the failover process to select the next active node and maintain system functionality.

**FIGURE 35** Cluster Virtual IP

The screenshot shows the 'Cluster & RUCKUS Edge Configuration Wizard' interface. The main heading is 'Cluster Virtual IP' with the instruction: 'Please select the interfaces for RUCKUS Edges and assign virtual IPs for seamless failover:'. On the left, a sidebar shows the configuration steps: LAG, Port: General, Cluster Virtual IP (selected), and Summary. The main content area is divided into two sections: '#1 Virtual IP' and 'Failover Settings'. The '#1 Virtual IP' section contains a table with columns for Node Name, Interface, and IP Subnet, and a 'Virtual IP Address' input field. The 'Failover Settings' section features an 'HA Timeout' slider ranging from 3 seconds to 15 seconds. At the bottom, a green bar indicates 'Nodes Compatibility Check: Pass' and navigation buttons for 'Cancel', 'Back', and 'Next' are visible.

Node Name	Interface	IP Subnet
Document-node1	Port1	192.168.10.64/ 24
Document-node2	Port1	192.168.10.212/ 24

Virtual IP Address: 192.168.10.100  
Suggested range: 192.168.10.0/ 24

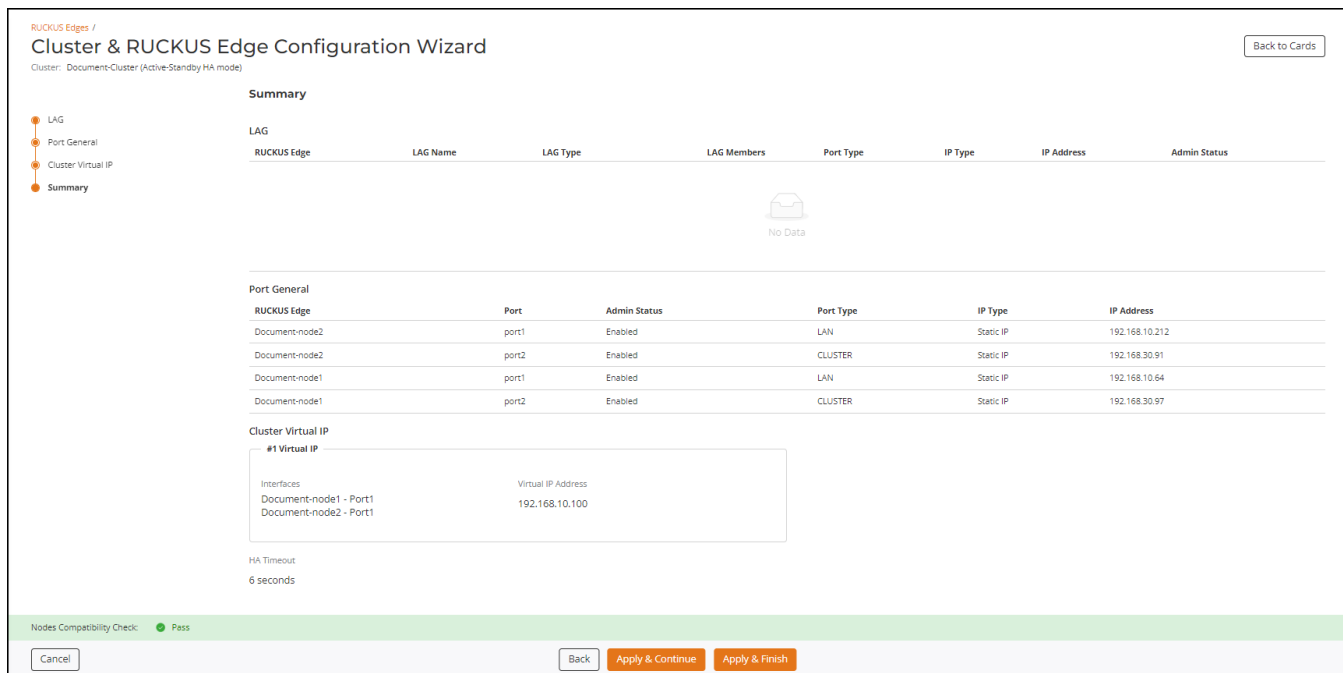
HA Timeout: 3 seconds to 15 seconds

Click **Next**.



4. **Summary:** This displays the configuration settings on the cluster. View and verify the configuration details and click **Apply & Continue** to proceed to the **Cluster Interface Settings** configuration, or **Apply & Finish** to complete the **LAG, Port and Virtual IP Settings** configuration without proceeding to the **Cluster Interface Settings** configuration.

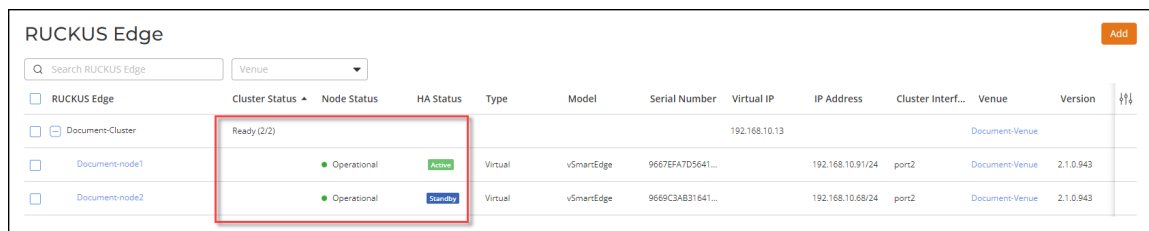
**FIGURE 36** Summary of the Cluster Configuration without a LAG



**NOTE**

After the nodes are configured, the **Node Status** changes from **Needs Port Config** to **Operational**, **Cluster Status** is **Ready 2/2**, and **HA Status** reflects node 1 is **Active** and node 2 is **Standby**.

**FIGURE 37** Nodes Status is Operational



## Cluster Interface Settings

The cluster interface is used as a communication channel between the RUCKUS Edge devices.

This section describes configuring Cluster Interface Settings.

## High Availability

### Onboarding a Single-Node Cluster

After configuring the **LAG, Port and Virtual IP Settings** and clicking **Apply & Continue** (as described in [Link Aggregation Group \(LAG\), Port and Virtual IP Settings](#) on page 35), select the **Cluster Interface** checkbox and click **Next**. This displays **Cluster Interface** page containing a tab for each RUCKUS Edge device in the cluster.

1. On the first device tab, configure these settings:
  - **Set cluster interface on:** Use the drop-down menu to select the port that want to serve as the cluster interface to the other RUCKUS Edge device.
  - Enter the **IP Address** and **Subnet Mask** address of cluster interface port.
2. Repeat [Step 1](#) on page 43 on the second device tab.
3. Click **Apply & Finish**.

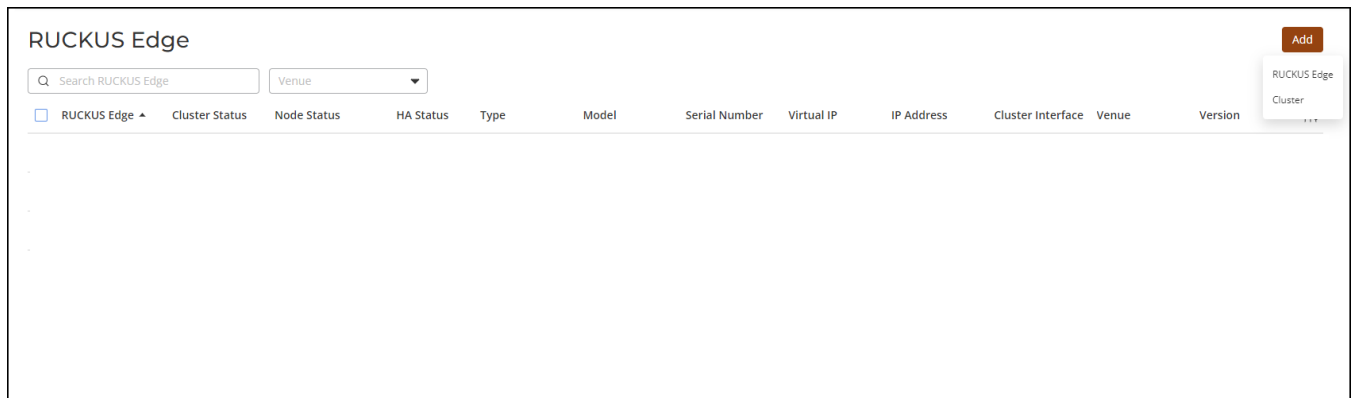
## Onboarding a Single-Node Cluster

A single-node cluster runs on a standalone RUCKUS Edge device and does not provide redundancy. If the node goes down, the data is lost.

This section describes onboarding a RUCKUS Edge single-node cluster.

1. Log in to the RUCKUS One web user interface with your credentials.
2. On the navigation bar, click **RUCKUS Edge**.  
This displays the **RUCKUS Edge** page.
3. In the **RUCKUS Edge** page, click **Add** and select **Cluster**. This displays the **Add Cluster** page.

**FIGURE 38** Add Cluster



4. In the **Add Cluster** page, enter the following details:
  - **Venue:** Click the drop-down arrow to select a site for the new cluster.
  - **Cluster Name:** Enter a meaningful name for the cluster profile.
  - **Description:** Enter a purposeful statement for the device.

5. In the **RUCKUS Edges** section, enter the following details:

- RUCKUS Edge Name: Enter a meaningful name for the node.
- Serial Number: Enter the serial number of the RUCKUS Edge device. You can obtain the serial number by logging in to the RUCKUS Edge CLI or by looking at the label on the physical RUCKUS Edge device.
- Model: After the serial number is entered, the model name is displayed automatically.

**IMPORTANT**

In a single-node setup, the absence of redundancy eliminates the need for Virtual Router Redundancy Protocol (VRRP) addresses and any cluster-related configuration.

To delete a RUCKUS Edge device, click on the **Delete** icon adjacent to the RUCKUS Edge entry.

**FIGURE 39** Adding a Single-Node Cluster

RUCKUS Edges /  
Add Cluster

Venue \*  
Document-Venue

Venue firmware version for RUCKUS Edge: 2.1.0.943

Cluster Name \*  
Document-Cluster

Description  
Creating a new cluster profile for documentation

RUCKUS Edges (0)

The cluster function will operate when there are at least two nodes present. Please add more nodes to establish a complete cluster.

RUCKUS Edge Name \*  
Document-node1

Serial Number \*  
965A6946097AE211EFB8E500C2927AA64

Model  
vEdge

Add another RUCKUS Edge

The one-time-password (OTP) will be automatically sent to your email address or via SMS for verification when you add a virtual RUCKUS Edge node. The password will expire in 10 minutes and you must complete the authentication process before using it.

Add Cancel

**NOTE**

The one-time-password (OTP) is automatically sent to your email address or through the SMS for verification when you add a virtual RUCKUS Edge node. The password expires in 10 minutes and you must complete the authentication process before the OTP expires; otherwise you will have to request a new OTP.

## Editing a Cluster and Nodes

You can make changes to the cluster profile and individual nodes comprising a cluster. This section describes editing a cluster profile and nodes.

1. Log in to the RUCKUS One web user interface with your credentials.
2. On the RUCKUS One navigation bar, click **RUCKUS Edge**.

This displays the list of RUCKUS Edge devices.

## High Availability

### Editing a Cluster and Nodes

3. Select the checkbox adjacent to the RUCKUS Edge cluster or device. This highlights the **Edit** and **Run Cluster & RUCKUS Edge configuration wizard** options.

4. Click the **Edit** option.

This displays the **Configure <Cluster Name>** page of the selected cluster with details.

5. In the **Configure <Cluster Name>** page, click on a tab and edit the details.

- **Cluster Details:** Displays general information of the cluster.
- **Virtual IP:** Displays virtual IP address of the nodes.
- **Cluster Interface:** Displays cluster interface details. To modify a specific node, select the **Node Name** and click **Edit**. This displays cluster interface details of the node.

**FIGURE 40** Configure <Cluster Name>

RUCKUS Edges /

## Configure Document-Cluster

Cluster Details Virtual IP Cluster Interface

Venue \*

Document-Venue

Venue firmware version for RUCKUS Edge: 2.1.0.943

Cluster Name \*

Document-Cluster

Description

RUCKUS Edges (2)

The cluster function will operate when there are at least two nodes present. Please add more nodes to establish a complete cluster.

RUCKUS Edge Name *	Serial Number *	Model
Document-node1	963331E93F7B0911EF8389000C2927AA64	vSmartEdge
RUCKUS Edge Name *	Serial Number *	Model
Document-node2	965A5D2A357AE211EFBA32000C298BC70A	vSmartEdge

Apply Cancel

6. After entering the values, click **Apply**.

# Link Aggregation Group

---

- [Link Aggregation Group.....](#) 53
- [Configuring a RUCKUS Edge Link Aggregation Group.....](#) 54
- [Configuring a RUCKUS Edge Link Aggregation Group through Command Line Interface.....](#) 61

## Link Aggregation Group

Link aggregation is a mechanism to bundle or aggregate one or more physical ports into a single logical port.

### Overview

A Link Aggregation Group (LAG) port can be created by combining two or more physical ports on the same node into one logical port. Each physical interface is called a member interface. Link aggregation increases the bandwidth by load balancing the traffic across the member interfaces. It also provides redundancy; if one interface fails, the traffic is distributed among the remaining links.

There are two types of Link Aggregation Group:

- **Static LAG:** These types of LAGs are manually configured by the administrators. All ports that are operationally **Up** are considered active members of the LAG.
- **Dynamic LAG:** These types of LAGs automatically bundle multiple physical ports by exchanging Link Aggregation Control Protocol (LACP) Protocol Data Units (PDU) between the connected devices.

RUCKUS Edge software load balances traffic across all operational member ports of a LAG using a hash derived from packet headers. These packet headers include Source IP, Destination IP address, and Layer 4 (TCP/UDP) ports.

### Requirements

A Link Aggregation Group requires the following:

- Each LAG interface requires at least one physical interface as a member link.
- For a dynamic LAG, all member interfaces should be of the same speed.

### Considerations

When configuring a Link Aggregation Group, keep the following considerations in mind:

- Non-PCI passthrough interfaces should not be configured as LAG member ports and are not a supported configuration. LAG is not supported with VMware® ESXi™ NIC teaming.
- A LAG port is considered operationally **Up** when at least one of its member ports is up. Similarly, it is marked as operationally **Down** when all the member ports are down.
- A physical port can be part of only one LAG at any point of time.
- All the member interfaces of a LAG should be of the same speed.

### Best Practices

This feature has no special recommendations for feature enablement or usage.

## Link Aggregation Group

### Configuring a RUCKUS Edge Link Aggregation Group

## Limitations

The LAG port has the following limitations:

1. Only Dynamic LAGs (LACP - as defined in IEEE Standard 802.3ad) are supported. RUCKUS Edge does not support Static LAGs.
2. The interfaces should be in the **unconfigured state**; it is recommended that the interfaces which are going to be part of the LAG should not have any prior configurations.
3. Modifying the LACP mode and timeout for an existing LAG can trigger LACP negotiation, potentially leading to traffic disruption.
4. When a LAG interface is created, it uses the MAC address of the first physical port as its interface MAC. If that port is later removed (which serves as the MAC provider for the LAG), the next member port's MAC address will be selected as the LAG's MAC address. This transition may cause a brief traffic disruption. It is strongly recommended to avoid removing the port for which the MAC address is currently being used by the LAG. Configuring the LAG's MAC address is not supported.

### NOTE

If the ports within a LAG is of different speeds after auto-negotiation, there is no check for the operational speed mismatch.


## Prerequisites

This feature has no prerequisites for feature enablement or usage.

# Configuring a RUCKUS Edge Link Aggregation Group

To configure a Link Aggregation Group (LAG), follow these steps:

A RUCKUS Edge device or cluster of devices must already be onboarded and in operational state.

1. On the RUCKUS One navigation bar, click on **RUCKUS Edge**.  
This displays the RUCKUS Edge devices.
2. Select a device and click the  icon to expand and view the associated devices.
3. Click on the device name. This displays the **Overview** page.

4. In the **Overview** page, click the **Configure** button on upper-right hand corner and click the **LAGs** sub-tab. Alternatively, you can directly click the **LAGs** tab on the **Overview** page and click **Configure LAG Settings**.

This displays LAG details page.

FIGURE 41 LAG Configuration

The screenshot shows the RUCKUS Edge configuration interface for a device named E144\_852\_971\_1. The interface includes a top navigation bar with 'Overview', 'Troubleshooting', 'Services (0)', and 'Timeline' tabs. A 'Configure' button is visible in the top right corner. Below the navigation bar, there are several status indicators: 'No active alarms', 'Ports: 8', 'Storage Usage: 27.3 GB (7%)', 'Memory Usage: 5.86 GB (13%)', and 'CPU Usage: 18%'. A 'More Details' link is also present. The 'LAGs' tab is highlighted in the navigation bar, and a 'Configure LAG Settings' button is visible in the top right corner of the LAGs section. Below the navigation bar, there is a table with the following columns: LAG Name, Description, LAG Type, Status, Admin Status, LAG Members, Port Type, Interface MAC, IP Address, and IP Type. The table contains one entry for LAG2.

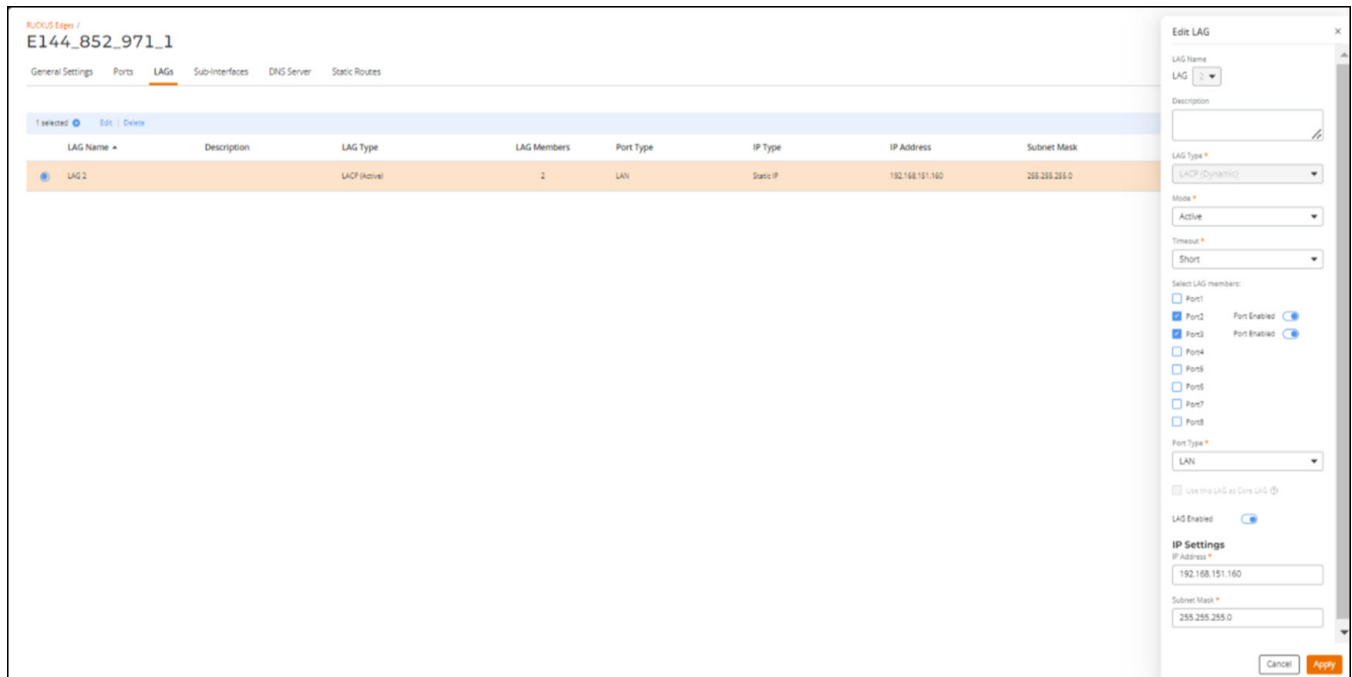
LAG Name	Description	LAG Type	Status	Admin Status	LAG Members	Port Type	Interface MAC	IP Address	IP Type
LAG2		LACP	Up	Enabled	2	LAN	80:bc:37:22:7b:c1	192.168.151.160/24	Static IP

## Link Aggregation Group

### Configuring a RUCKUS Edge Link Aggregation Group

5. In the **LAGs** page, click **Add LAG**.  
This displays the **Add LAG** sidebar.

**FIGURE 42** Add LAG



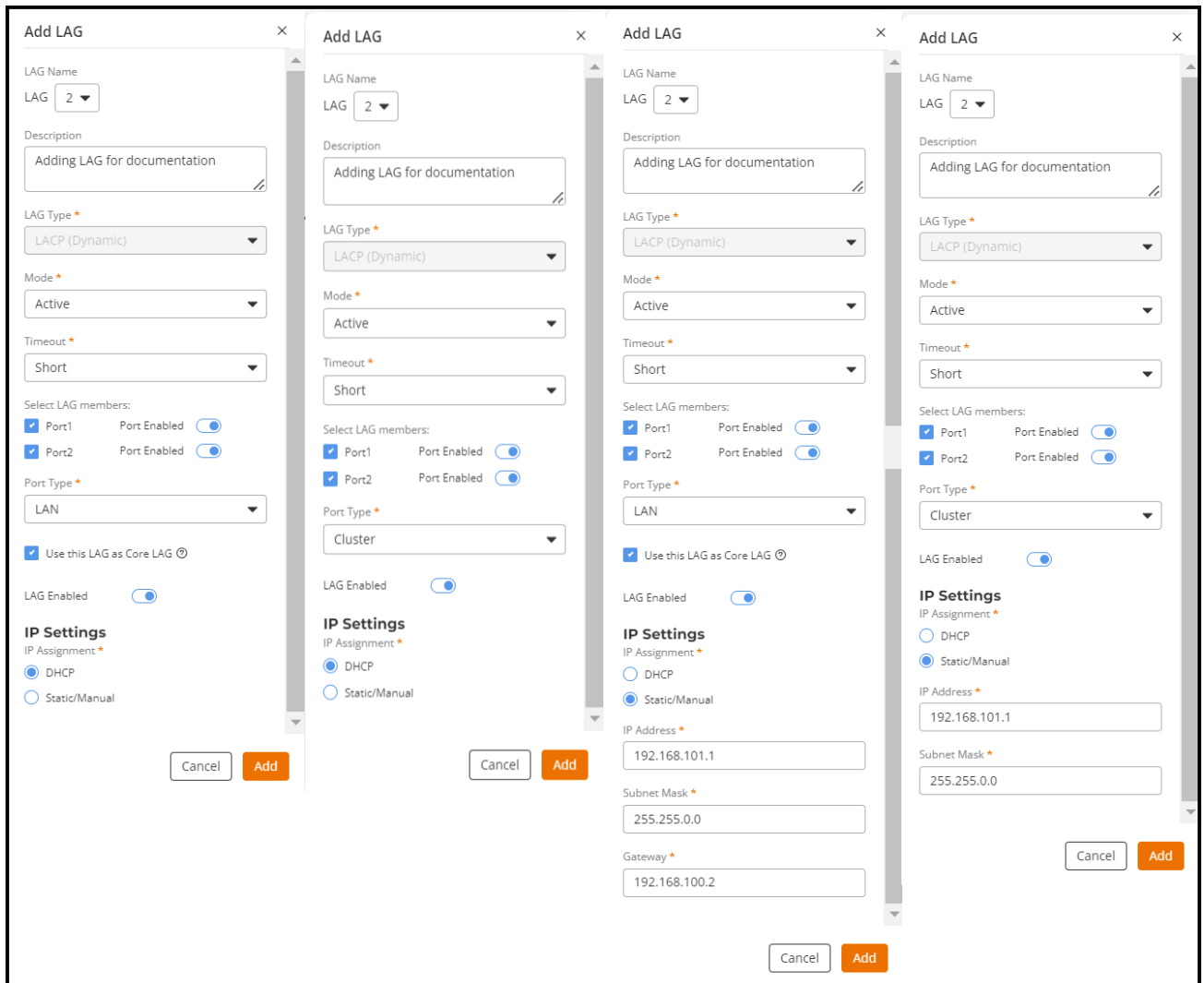
Enter the following details to add a LAG to the RUCKUS Edge device.

- **LAG Name:** Select name of the LAG from the drop-down list. The LAG name is a numeric value between 0 to 3. After the LAG is created, you cannot edit the LAG name.
- **Description:** Enter a meaningful short description about the LAG.
- **LAG Type:** The default type is **LACP (Dynamic)** as RUCKUS Edge does not support static LAG.
- **Mode:** Click the drop-down list and select the mode of the LAG. There are two types of modes:
  - **Active :** Always initiates Link Aggregation Control Protocol (LACP) and Protocol Data Unit (PDU) to the peer. This is the default mode for RUCKUS Edge LACP LAG.
  - **Passive :** Never initiates any LACP exchange on its own. It responds only after receiving LACP and PDU messages from the peer/partner device. Hence, both peers cannot be in passive mode. At least one of the peers should be configured in active mode.
- **Timeout:** Time interval indicates how long the LACP should wait before declaring the partner as down. This interval also defines the rate at which LACP hello packets are exchanged among the peers. There are two types of timeout.
  - **Long/Slow Timeout:** The value of this timeout is 90 seconds. Hello packets are transmitted every 30 seconds. After 3 misses ( $3 * 30s = 90$  seconds), the peer information is flushed and LACP state is declared as down.
  - **Short/Fast Timeout:** The value of this timeout is 3 seconds. Hello packets are transmitted every 1 second. After 3 misses ( $3 * 1s = 3$  seconds), the peer information is flushed. This is the default timeout for RUCKUS Edge LACP LAG.
- **Select LAG Members:** A physical port associated with a LAG interface is a LAG member. To associate LAG members, select the ports which need to be a member of a LAG and enter the following details:
  - **Port Type -** Select the type of port from the drop-down list.
    - › **LAN:** If **LAN** is selected as the port type, **Use this LAG as Core LAG** is activated for SD-LAN service.



- › Cluster: Select **Cluster** to connect two RUCKUS Edge devices for clustering in a High Availability (HA) deployment.
- **IP Settings:** Select one of the following for **IP Assignment**.
  - DHCP - Dynamic Host Configuration Protocol (DHCP) is a client or server protocol that automatically provides and Internet Protocol (IP) with its host IP address.
  - Static/Manual - Enter the IP address, Subnet Mask, and Gateway Protocol manually.

**FIGURE 43** Add LAG - Examples of IP Settings Options



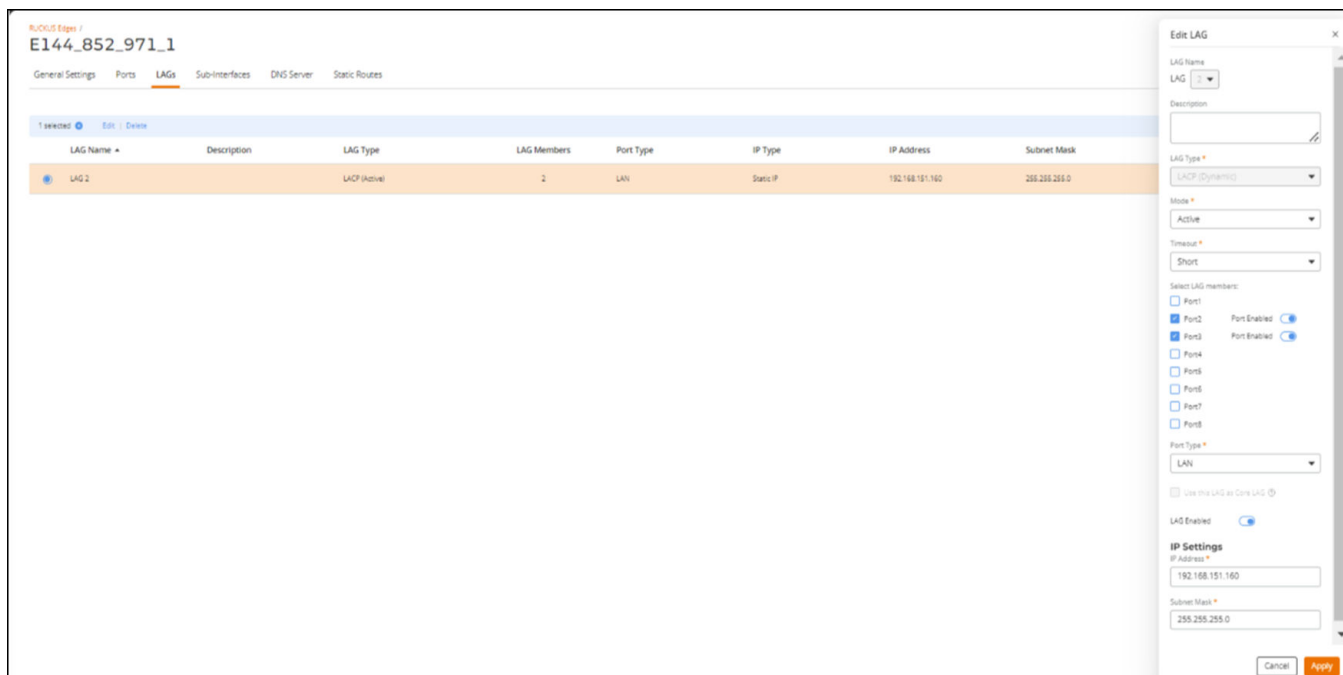
## Link Aggregation Group

### Configuring a RUCKUS Edge Link Aggregation Group

6. After entering all the details, click **Add**.

The newly created LAG port is displayed in the RUCKUS Edge page under **LAGs** tab. You can also view the LAG information in the RUCKUS Edge **Overview** page.

**FIGURE 44** New LAG with Port Information



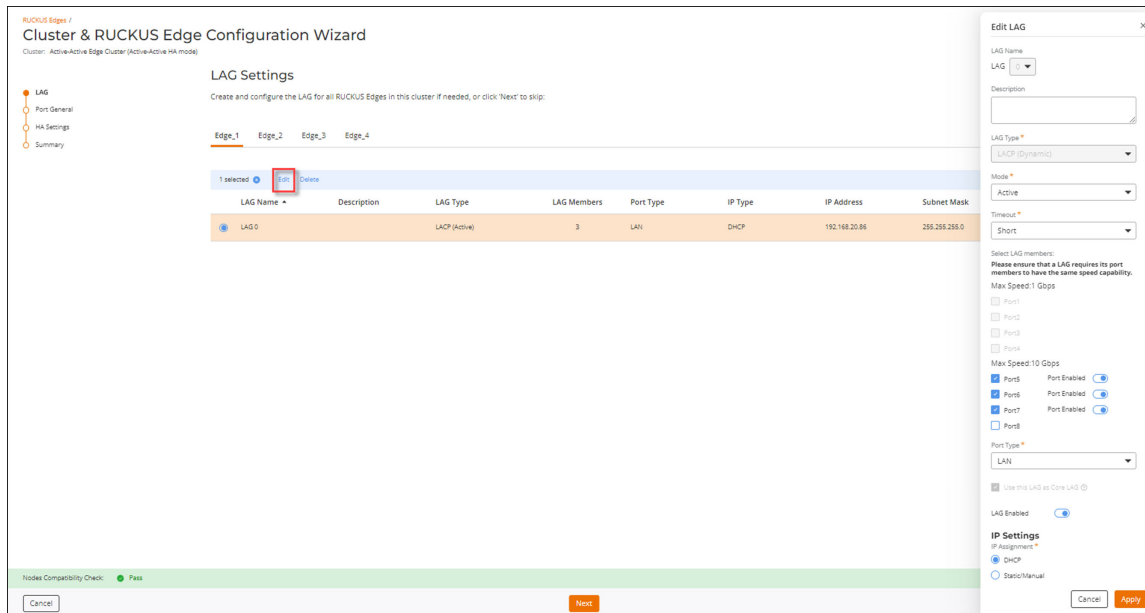
## Editing a LAG

To edit a LAG port, follow these steps:

1. On the navigation bar, click **RUCKUS Edge**.  
This displays the **RUCKUS Edge** page.
2. Select a Edge device from the list and click on the name.  
This displays the RUCKUS Edge details page.
3. Click the **Configure** button in the upper-right corner of the page.  
This displays the **General Settings** page.
4. In the **General Settings** page, click the **LAGs** tab.  
This displays the **LAGs** page.

5. In the **LAGs** page, select a **LAG** from the list. This highlights the **Edit** and **Delete** links, click **Edit**. This displays the **Edit LAG** sidebar. Modify the details and click **Apply**.

FIGURE 45 Edit LAG



## Deleting a LAG

To delete a LAG port, follow these steps:

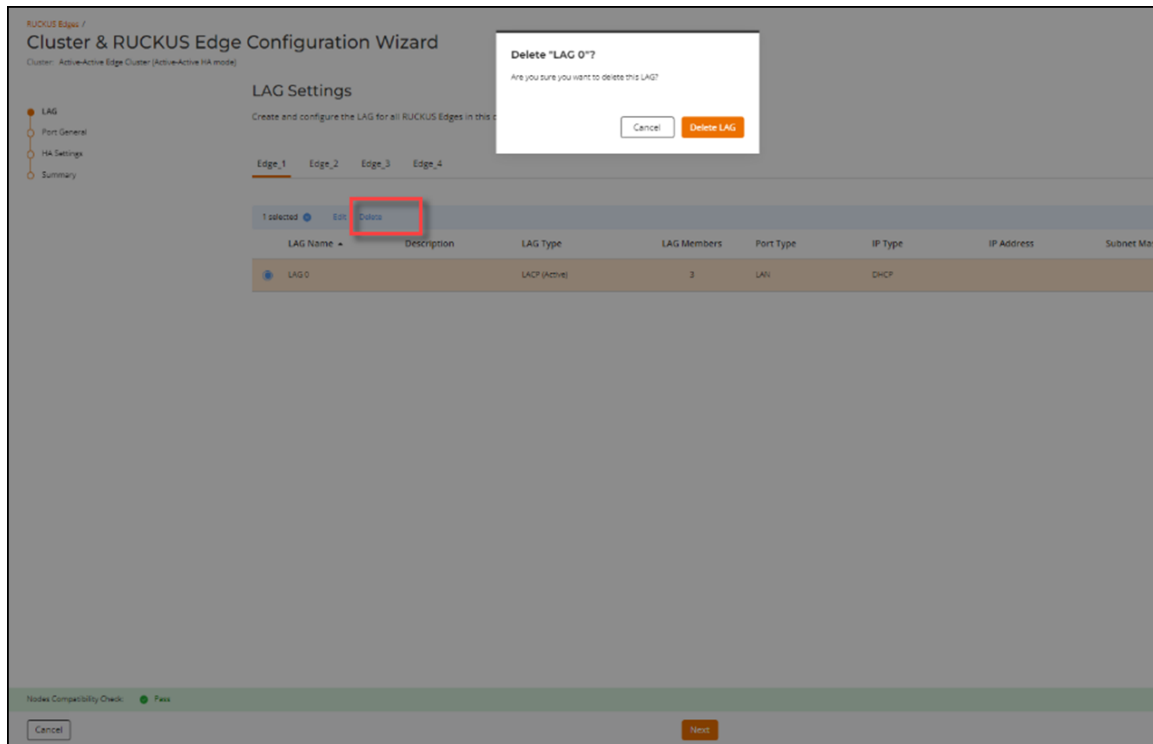
1. On the navigation bar, click **RUCKUS Edge**.  
This displays the **RUCKUS Edge** page.
2. Select a Edge device from the list and click on the name.  
This displays the RUCKUS Edge details page.
3. Click the **Configure** button in the upper-right corner of the page.  
This displays the **General Settings** page.
4. In the **General Settings** page, click the **LAGs** tab.  
This displays the **LAGs** page.

## Link Aggregation Group

### Configuring a RUCKUS Edge Link Aggregation Group

5. In the **LAGs** page, select a **LAG** from the list. This highlights the **Edit** and **Delete** links, click **Delete**. This displays the confirm pop-up window. Click **Delete LAG**.

**FIGURE 46** Delete LAG



# Configuring a RUCKUS Edge Link Aggregation Group through Command Line Interface

This procedure describes configuring a LAG using the command line interface (CLI). Using CLI enables quick execution of commands and allows more precise control over the system.

## NOTE

Before onboarding the RUCKUS Edge to RUCKUS One, you can use CLI commands to create a LAG port.

1. Log in with your administrator credentials to establish an SSH connection to the Edge device.

This displays the device information screen.

FIGURE 47 Device Details

```
#####
#   Welcome to SmartEdge   #
#####
login: admin
Password:
Last login: Fri Jan 19 00:09:02 on tty1
Device has not been enrolled.
Device Serial: 967901200704570418704010-40054055670

..... Waiting for user to add the serial number in Ruckus One
..... You would get an Email/SMS with OTP
Please use the command 'enroll-device <OTP>' to enroll the device with Ruckus One
SmartEdge>
```

2. Enter the **enable** command to enter advanced CLI mode. Enter your password again when prompted.

## Link Aggregation Group

### Configuring a RUCKUS Edge Link Aggregation Group through Command Line Interface

3. Enter the **network** command to access the network configuration mode.

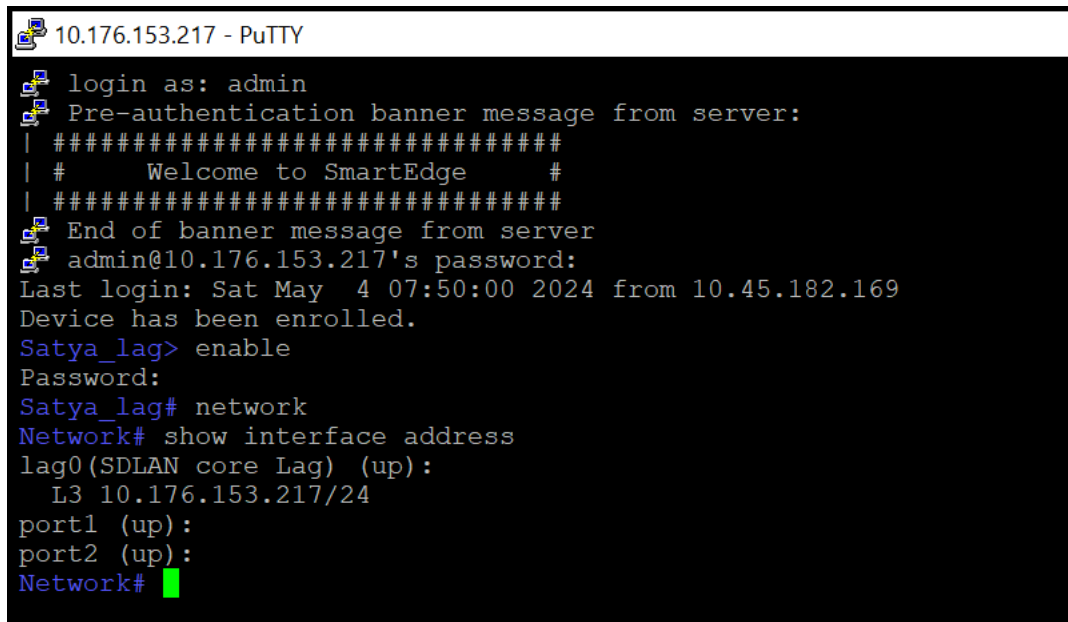
FIGURE 48 enable and network Commands

```
#####
#   Welcome to SmartEdge   #
#####
966b1102716511001a2110051055670 login: admin
Password:
Last login: Fri Jan 19 00:09:02 on tty1
Device has not been enrolled.
Device Serial: 966b1102716511001a2110051055670

#####
..... Waiting for user to add the serial number in Ruckus One
..... You would get an Email/SMS with OTP
Please use the command 'enroll-device <OTP>' to enroll the device with Ruckus One
SmartEdge> enable
Password:
SmartEdge# network
Network# _
```

- To view the IP addresses and operational status of all interfaces, enter the **show interface address** command. This displays the interfaces available on the switch.

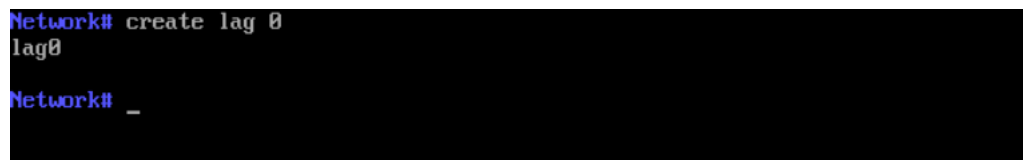
**FIGURE 49** show interface address Command



```
10.176.153.217 - PuTTY
login as: admin
Pre-authentication banner message from server:
| #####
| #      Welcome to SmartEdge      #
| #####
End of banner message from server
admin@10.176.153.217's password:
Last login: Sat May  4 07:50:00 2024 from 10.45.182.169
Device has been enrolled.
Satya_lag> enable
Password:
Satya_lag# network
Network# show interface address
lag0 (SDLAN core Lag) (up):
  L3 10.176.153.217/24
port1 (up):
port2 (up):
Network# █
```

- To create a Dynamic LAG using LACP with a specific identifier, enter the **create lag** command. The *lag\_id* must be specified as a number and serves as the LAG interface name. RUCKUS Edge supports LAG IDs in the range of 0 through 3. In the example below, a dynamic LAG is created using LAG ID 0.

**FIGURE 50** Creating a LAG



```
Network# create lag 0
lag0
Network# _
```

## Link Aggregation Group

### Configuring a RUCKUS Edge Link Aggregation Group through Command Line Interface

- After creating a LAG, add a port to the LAG. To add a port, enter the **lag add** command and specify the LAG ID (created during the previous step) and the port number.

#### NOTE

The **lag add** command is used to add one port at a time. To add multiple ports, run this command for each member of the port.

To remove a LAG port, enter the **lag remove** command.

FIGURE 51 Adding a LAG Port

```
Network# lag add 0 port1
set dhcp client: dhcp client not enabled on port1

set dhcp client: dhcp client already enabled on lag0
Network# _
```

The LACP LAG configuration is now complete. Subsequent steps describe viewing LACP LAG information using the command line interface.

- (OPTIONAL) To view the LAG configuration, enter the **show lag** command.

This displays the interface name, the automatically assigned software interface index identifier, the mode, the network layers for which traffic is being load balanced, the number of active members (ports), and the total number of members (ports) associated with the LAG.

FIGURE 52 show lag Command

```
Network# show lag
interface name  sw_if_index  mode      load balance  active members  members
lag0            6                lacp      134           1                1
Network#
```

- (OPTIONAL) To view the LAG details, enter the **show lag details** command.

FIGURE 53 show lag details Command

```
Network# show lag details
lag0
  mode: lacp
  load balance: 134
  number of active members: 1
    port1
  number of members: 1
    port1
  device instance: 0
  interface id: 0
  sw_if_index: 6
  hw_if_index: 6
Network# _
```



9. (OPTIONAL) To view the LACP details, enter the **show lacp details** command.

**FIGURE 54** show lacp details Command

```

Network# show lacp details
Number of interfaces: 2
port1
  Good LACP PDUs received: 2308
  Bad LACP PDUs received: 0
  LACP PDUs sent: 92
  last LACP PDU received: .19 seconds ago
  last LACP PDU sent: 9.63 seconds ago
  Good Marker PDUs received: 0
  Bad Marker PDUs received: 0
  debug: 0
  loopback port: 0
  port_enabled: 1
  port moved: 0
  ready_n: 1
  ready: 1
  long timer: 0
  Actor
    system: 08:35:71:13:69:02
    system priority: 65535
    key: 7
    port priority: 255
    port number: 1
    state: 0x3f
      LACP_STATE_LACP_ACTIVITY (0)
      LACP_STATE_LACP_TIMEOUT (1)
      LACP_STATE_AGGREGATION (2)
      LACP_STATE_SYNCHRONIZATION (3)
      LACP_STATE_COLLECTING (4)
      LACP_STATE_DISTRIBUTING (5)
  Partner
    system: fc1b1:cd:20:26:6a
    system priority: 1
    key: 20001
    port priority: 1
    port number: 31
    state: 0x3d
      LACP_STATE_LACP_ACTIVITY (0)
      LACP_STATE_AGGREGATION (2)
      LACP_STATE_SYNCHRONIZATION (3)
      LACP_STATE_COLLECTING (4)
      LACP_STATE_DISTRIBUTING (5)
    wait while timer: not running
    current while timer: 2.80 seconds
    periodic timer: 20.37 seconds
  RX-state: CURRENT
  TX-state: TRANSMIT
  MUX-state: COLLECTING_DISTRIBUTING
  PTX-state: PERIODIC_TX

port2
  Good LACP PDUs received: 1957
  Bad LACP PDUs received: 0
  LACP PDUs sent: 71
  last LACP PDU received: .89 seconds ago
  last LACP PDU sent: 9.63 seconds ago
  Good Marker PDUs received: 0
  Bad Marker PDUs received: 0
  debug: 0
  loopback port: 0
  port_enabled: 1
  port moved: 0
  ready_n: 1
  ready: 1
  long timer: 0
  Actor
    system: 08:35:71:13:69:02
    system priority: 65535
    key: 7
    port priority: 255
    port number: 2
    state: 0x3f
      LACP_STATE_LACP_ACTIVITY (0)
      LACP_STATE_LACP_TIMEOUT (1)
      LACP_STATE_AGGREGATION (2)
      LACP_STATE_SYNCHRONIZATION (3)
      LACP_STATE_COLLECTING (4)
      LACP_STATE_DISTRIBUTING (5)
  Partner
    system: fc1b1:cd:20:26:6a
    system priority: 1
    key: 20001
    port priority: 1
    port number: 32
    state: 0x3d
      LACP_STATE_LACP_ACTIVITY (0)
      LACP_STATE_AGGREGATION (2)
      LACP_STATE_SYNCHRONIZATION (3)
      LACP_STATE_COLLECTING (4)
      LACP_STATE_DISTRIBUTING (5)
    wait while timer: not running
    current while timer: 2.10 seconds
    periodic timer: 20.37 seconds
  RX-state: CURRENT
  TX-state: TRANSMIT
  MUX-state: COLLECTING_DISTRIBUTING
  PTX-state: PERIODIC_TX
Network#

```

## Link Aggregation Group

### Configuring a RUCKUS Edge Link Aggregation Group through Command Line Interface

10. (OPTIONAL) To view the interface details, enter the **show interface address** command.

**FIGURE 55** show interface address Command

```
Network# show interface address
lag0 (up):
  L3 192.168.20.3/24
port1 (up):
port2 (up):
Network# _
```

This displays the L3 IP address assigned to LAG 0.

11. (OPTIONAL) To delete a LAG, enter the **delete lag** command, including the LAG ID.

The LAG is deleted.

**FIGURE 56** delete lag Command

```
Network# delete lag 0
Network# show lag
interface name  sw_if_index  mode                load balance  active members  members

Network# show lag details
Network# show interface address
port1 (up):
port2 (up):
Network# _
```

# Tunnel Profile

- Tunnel Profile..... 67
- Creating a Tunnel Profile..... 68
- Editing or Deleting the Tunnel Profile..... 70

## Tunnel Profile

Tunnel mode enables wireless clients to roam across different APs on different subnets. For example, a Wi-Fi network may tunnel end-user traffic by utilizing an SD-LAN service configured with a tunnel profile that supports VLAN to VNI mapping. If the WLAN has clients that require uninterrupted wireless connection (for example, VoIP devices), RUCKUS recommends enabling tunnel mode.

### NOTE

When tunnel mode is enabled on a WLAN, multicast video packets are blocked on that WLAN. Multicast voice packets, however, are allowed.

Complete the following steps to view the Tunnel Profile details:

1. From the navigation bar, select **Network Control > Policies & Profiles**.

The **Policies & Profiles** page is displayed.

2. In the **Policies & Profiles** page, click the **Tunnel Profile** tile.

The **Tunnel Profile** page is displayed. The Tunnel profiles are displayed in the table. The **Name** column displays the Tunnel profile names, **Gateway Path MTU Mode** displays the status, **Force Fragmentation** displays the status, **SD-LAN** displays the total number of SD-LAN services configured to use this tunnel profile, and **Networks** displays the total number of network instances that use the Tunnel profile.

**FIGURE 57** Tunnel Profile Page

The screenshot shows the 'Tunnel Profile (5)' page. At the top right is an 'Add Tunnel Profile' button. Below the title are search and filter fields: 'Search Name', 'SD-LAN', and 'Networks'. The main content is a table with the following data:

<input type="checkbox"/>	Name ▲	Network Segment Type	Gateway Path MTU Mode	Force Fragmentation	SD-LAN	Networks
<input type="checkbox"/>	DMZ Tunnel Profile	VLAN to VNI map	Manual (1450)	OFF	0	0
<input type="checkbox"/>	Default tunnel profile (SD-LAN)	VLAN to VNI map	Auto	OFF	1	7
<input type="checkbox"/>	Manual-Mode-1200-FF-Profile	VLAN to VNI map	Manual (1200)	ON	0	0
<input type="checkbox"/>	sri-1200	VLAN to VNI map	Manual (1200)	OFF	1	5
<input type="checkbox"/>	sri-tun-profile	VLAN to VNI map	Auto	OFF	0	0

## Tunnel Profile

### Creating a Tunnel Profile

3. In the **Name** column, click on a specific tunnel profile name.

Detailed information is displayed for the selected tunnel profile, including the tunnel configuration settings and the network instances with which the tunnel profile is associated.

**FIGURE 58** Details Page for a Tunnel Profile

The screenshot shows the details page for a tunnel profile named 'sri-1200'. The breadcrumb navigation is 'Network Control / Policies & Profiles / Tunnel Profile / sri-1200'. A 'Configure' button is in the top right. The configuration settings are as follows:

Network Segment Type	Gateway Path MTU Mode	PMTU Timeout	PMTU Retries	Force Fragmentation	Tunnel Idle Timeout
VLAN to VNI map	Manual (1200)		retries	OFF	20 minutes
Keep Alive Interval	Keep Alive Retries				
2 seconds	5 retries				

Below the settings is a section titled 'Instances (5)' with a table:

Network	Type	Venues
guest-1	Captive Portal - Captive Portal	1

## Creating a Tunnel Profile

A tunnel profile is essential for managing and optimizing the behavior of tunnels between Access Points (APs) and the RUCKUS Edge device. You can apply the same Tunnel Profile to multiple venues, but each venue can have only one Tunnel Profile applied.

APs use tunnel keepalive request messages to verify the reachability of the RUCKUS Edge device before establishing AP data tunnel and broadcasting WLANs enabled with an SD-LAN service. Once the tunnel is established, APs continue to send periodic keepalive request messages to monitor the reachability of the Edge device. If the AP does not receive responses for the maximum number of consecutive keepalive requests, it assumes the Edge is unreachable, brings down the tunnel, and stops broadcasting the WLANs. The AP continues to send periodic keepalive requests and will re-establish the tunnel and resume broadcasting WLANs upon receiving responses.

Complete the following steps to create a Tunnel Profile:

1. From the navigation bar, select **Network Control > Policies & Profiles**.

The **Policies & Profiles** page is displayed.

2. In the **Policies & Profiles** page, click **Tunnel Profile** tile and click the **Add Tunnel Profile**. Alternatively, in the **Policies & Profiles** page, click the **Add Policy or Profile** then select the **Tunnel Profile** tile, and click **Next**.

The **Add Tunnel Profile** page is displayed.

**FIGURE 59** Add Tunnel Profile Page

Network Control / Policies & Profiles / Tunnel Profile /

### Add Tunnel Profile

Profile Name \*

Network Segment Type ⓘ

VLAN to VNI map

Gateway Path MTU Mode ⓘ

Auto

Manual

Path MTU Request Timeout ⓘ

   Seconds

Path MTU Request Retries ⓘ

   retries

Force Fragmentation ⓘ

Tunnel Idle Timeout ⓘ

   Minute(s)

Tunnel Keep Alive Interval ⓘ

   seconds

Tunnel Keep Alive Retries ⓘ

   retries

## Tunnel Profile

### Editing or Deleting the Tunnel Profile

- Complete the following fields:
  - Profile Name:** Enter the name for the tunnel policy.
  - Network Segmentation Type:** The **VLAN to VNI map** option is selected by default. The **SD-LAN** service maps the VLAN ID to the VNI for tunneling.
  - Gateway Path MTU Mode:** Select one of following options:
    - Auto**
    - Manual:** Enter the value in bytes (allowed values are 68 to 1450). The value must be lesser than the Ethernet MTU on the AP.

#### NOTE

Check the Ethernet MTU on the AP; Tunnel MTU gets applied only if it is less than the Ethernet MTU.

- Path MTU Request Timeout:** The maximum wait time for a response to a path MTU request. Range: 10 milliseconds to 10 seconds; default is 2 seconds.
  - Path MTU Request Retries:** The maximum number of Path MTU requests sent to test one MTU value. Range: 3 through 64; default is 5 retries.
  - Force Fragmentation:** When enabled, the AP or Edge device will automatically fragment packets, ignoring the Don't Fragment (DF) bit in the IP header of the packets. Forced packet fragmentation can reduce congestion and improve network throughout, but it may lead to fragment loss, packet reassembly issues, and memory exhaustion. This option is disabled by default. Toggle the switch to **ON** to enable.
  - Tunnel Idle Timeout:** The amount of time a tunnel is allowed to remain active without any traffic. Select **Minutes**, **Days**, or **Weeks** from the drop-down list and then enter the duration or use the up/down arrows to set the value. Range: 5 through 10080 minutes, 1 through 7 days, or 1 week; default is 20 minutes.
  - Tunnel Keep Alive Interval:** Defines the interval between two consecutive keepalive request messages. Range: 1 through 5 seconds, with a default value of 2 seconds.
  - Tunnel Keep Alive Retries:** Defines the maximum number of consecutive keepalive requests that can fail before the AP determines the Edge device is unreachable. Range: 3 through 10 retries, with a default value of 5.
- Click **Add**.

The Tunnel Profile is created and is displayed in the **Tunnel Profile** page.

## Editing or Deleting the Tunnel Profile

As your network evolves, you may edit or delete Tunnel Profiles, as necessary.

Complete the following steps to edit or delete a Tunnel Profile:

- From the navigation bar, select **Network Control > Policies & Profiles**.  
The **Policies & Profiles** page is displayed.
- In the **Policies & Profiles** page, click the **Tunnel Profile** tile.  
The **Tunnel Profile** page is displayed.

- Select the checkbox next to the profile that you want to edit and click **Edit**. Alternatively, click on the profile **Name**, and click **Configure**.

**FIGURE 60** Tunnel Profile Page

Network Control / Policies & Profiles / Tunnel Profile (5) Add Tunnel Profile

1 selected Edit Delete

<input type="checkbox"/>	Name ▲	Network Segment Type	Gateway Path MTU Mode	Force Fragmentation	SD-LAN	Networks
<input type="checkbox"/>	DMZ Tunnel Profile	VLAN to VNI map	Manual (1450)	OFF	0	0
<input type="checkbox"/>	Default tunnel profile (SD-LAN)	VLAN to VNI map	Auto	OFF	1	7
<input type="checkbox"/>	Manual-Mode-1200-FF-Profile	VLAN to VNI map	Manual (1200)	ON	0	0
<input checked="" type="checkbox"/>	sri-1200	VLAN to VNI map	Manual (1200)	OFF	1	5
<input type="checkbox"/>	sri-tun-profile	VLAN to VNI map	Auto	OFF	0	0

The **Edit Tunnel Profile Settings** page is displayed.

**FIGURE 61** Edit Tunnel Profile

Network Control / Policies & Profiles / Tunnel Profile / Edit Tunnel Profile

Profile Name \*

Network Segment Type ⓘ  
 VLAN to VNI map

Gateway Path MTU Mode ⓘ  
 Auto  
 Manual  bytes

ⓘ Please check Ethernet MTU on AP, Tunnel MTU gets applied only if its less than Ethernet MTU

Force Fragmentation ⓘ

Tunnel Idle Timeout ⓘ  
 Minute(s)

Tunnel Keep Alive Interval ⓘ  
 seconds

Tunnel Keep Alive Retries ⓘ  
 retries

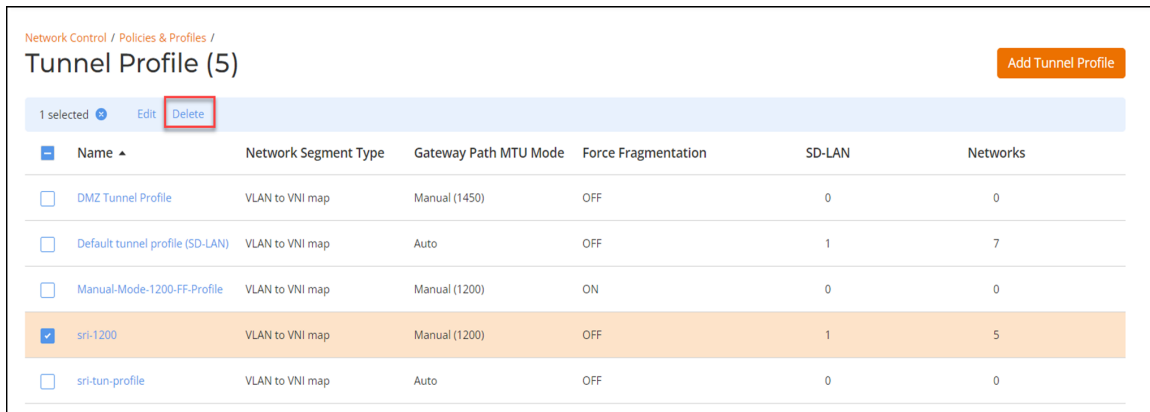
Apply Cancel

## Tunnel Profile

### Editing or Deleting the Tunnel Profile

4. Update the **Profile Name**, **Gateway Path MTU Mode**, **Force Fragmentation**, **Tunnel Idle Timeout**, **Tunnel Keep Alive Interval**, or **Tunnel Keep Alive Retries** options, as necessary, and click **Apply**.
5. Complete the following steps to delete a tunnel profile:
  - a) Proceed with [Step 1](#) and [Step 2](#).
  - b) Select the checkbox next to the profile that you want to delete and click **Delete**.

**FIGURE 62** Delete a Tunnel Profile



The screenshot shows the 'Tunnel Profile (5)' management page. At the top right is an 'Add Tunnel Profile' button. Below the title is a toolbar with '1 selected', 'Edit', and 'Delete' buttons. The 'Delete' button is highlighted with a red box. Below the toolbar is a table with the following columns: Name, Network Segment Type, Gateway Path MTU Mode, Force Fragmentation, SD-LAN, and Networks. The 'sri-1200' profile is selected, and its row is highlighted in orange.

Name	Network Segment Type	Gateway Path MTU Mode	Force Fragmentation	SD-LAN	Networks
<input type="checkbox"/> DMZ Tunnel Profile	VLAN to VNI map	Manual (1450)	OFF	0	0
<input type="checkbox"/> Default tunnel profile (SD-LAN)	VLAN to VNI map	Auto	OFF	1	7
<input type="checkbox"/> Manual-Mode-1200-FF-Profile	VLAN to VNI map	Manual (1200)	ON	0	0
<input checked="" type="checkbox"/> sri-1200	VLAN to VNI map	Manual (1200)	OFF	1	5
<input type="checkbox"/> sri-tun-profile	VLAN to VNI map	Auto	OFF	0	0

The **Delete** dialog box is displayed.

- c) Click **Delete Policy**.

A message confirming successful deletion is displayed.



# Appendix

- Supported AP Models..... 73

## Supported AP Models

Table 2 provides a list of APs that are supported by RUCKUS Edge release 2.1.0.

**TABLE 2** Supported AP Models for Release 2.1.0

IEEE Standard	Profile ID	Image Type	Supported AP Models
802.11be	ap-arm-11beax	R770	R770
802.11ax	ap-arm-11ax	R730	R730, R750, R650, T750, T750SE, R850, R550, R760, R560
	ap-arm-cypress	H550	H550, T350C, T350D, T350SE, R350, H350
802.11ac Wave 2	ap-arm-dakota	R510	R320, M510, R510, H510, H320, E510, T310C, T310D, T310N, T310S
	ap-arm-qca	R710	R720, R710, R610, T710, T710s, T610, T610S
802.11ac Wave 1	ap-11n-scorpion	T300	R500, R600, R310, T300, T300E, T310N, T310S

## Incompatible AP Firmware

RUCKUS Edge version 2.1.0.971 supports APs with firmware version 7.0.0.200.6407 or later. Although APs with older versions are allowed in the venue, a VxLAN tunnel cannot be established. This triggers a warning message indicating the incompatibility of the AP firmware and recommending an upgrade. Only after upgrading the AP (such as through the RUCKUS One controller) a tunnel can be established between the AP and RUCKUS Edge.

To view the service impacted due to AP firmware incompatibility, navigate to the Venue in which the APs and Edges deployed and click the **Devices** tab (which automatically displays the **Wi-Fi** sub-tab). An error message is displayed on the top-right corner within the **Wi-Fi** sub-tab. Click **See details**, the **Incompatibility Details** widget is displayed, as shown in [Figure 63](#). The warning message displays the service impacted, minimum version required to support, supported AP model, and the number of APs incompatible. To upgrade the AP firmware, go to **Administration > Version Management > AP Firmware** and upgrade the firmware.

FIGURE 63 AP Firmware Incompatibility Warning Message

### Incompatibility Details ×

Some features are not enabled on specific access points in this venue due to firmware or device incompatibility. Please see the minimum firmware versions required below. Also note that not all features are available on all access points. You may upgrade your firmware from [Administration > Version Management > AP Firmware](#)

WI-FI    **RUCKUS Edge**

---

#### SD-LAN

Minimum required version  
7.0.0.200.6407

Supported AP Model Family  
Wi-Fi 6, Wi-Fi 6E, Wi-Fi 7

Incompatible Access Points (Currently)  
1 / 1

#### Tunnel Profile

Minimum required version  
7.0.0.200.6407

Supported AP Model Family  
Wi-Fi 6, Wi-Fi 6E, Wi-Fi 7

Incompatible Access Points (Currently)  
1 / 1



© 2024 CommScope, Inc. All rights reserved.  
350 West Java Dr., Sunnyvale, CA 94089 USA  
<https://www.commscope.com>