CONFIGURATION GUIDE

RUCKUS Edge Configuration Guide, 2.2.0

Supporting RUCKUS Edge 2.2.0 Release

Part Number: 800-73696-001 Rev A
Publication Date: September 2024

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.

Contents

Contact Information, Resources, and Conventions

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
- 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.

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.

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	`device(config)# interface ethernet 1/1/6`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *RUCKUS Small Cell Release Notes* 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
bold text	Identifies command names, keywords, and command options.
italic text	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, *member*[*member*...].
\	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

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.

New In This Document

TABLE 2 Key Features and Enhancements in RUCKUS Edge 2.2.0 (December 2024)

Feature	Description	Reference
AA HA support for DMZ cluster	**Updated**: Ensures AA HA support for DMZ cluster.	Active-Active High Availability on page 39
Fallback schedule support at AP, DC (Active-Active HA)	**Updated**: Allows an AP to reconnect to the preferred primary RUCKUS Edge device according to the user-configured schedule.	RUCKUS Edge Fallback on page 41
Personal Identity Network (PIN) For Campus Housing (EA)	**New**: Personal Identity Networks (PIN) use VxLAN tunneling to extend Wi-Fi client and wired client via RUCKUS switch access to the RUCKUS Edge, creating seamless connectivity across the network domain. It enables Wi-Fi and wired clients to securely access their networks and connected devices while also establishing Personal Area Networks (PAN) for secure, individualized connectivity.	Personal Identity Network on page 109
DHCP for PIN (EA)	**New**: Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automatically assign IP addresses and other communications to the devices connected in the network.	Dynamic Host Configuration Protocol (DHCP) on page 171
Left side Menu orientation	**Updated**: RUCKUS Edge menu is moved under the Gateway menu.	Throughout the guide
Minor editorial changes		

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.

HA supports two modes:

- Active-Standby: One device is active while the other is on standby. If the active device fails, the standby device takes over.
- Active-Active: Multiple devices actively share the load. If one device fails, the other nodes in the cluster continue to handle the workload, ensuring continuous availability.

Active Standby High Availability Mode

The Active Standby High Availability mode is a configuration that ensures continuous network service by having two identical devices where one acts as the active unit and the other acts as a standby unit.

Overview

In the Active Standby High Availability mode, if the active unit fails, the standby unit seamlessly takes over, ensuring minimal disruption and maintaining network connectivity. This configuration is essential for critical systems where even brief downtime can have significant consequences.

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 Active-Standby 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 Active-Standby Deployment Model

High Availability supports the Active-Standby deployment model.

High Availability (HA) mode supports two-node cluster operation in the Active-Standby deployment model. The High Availability functionality in RUCKUS Edge is based on Virtual Router Redundancy Protocol (VRRP). VRRP allows multiple routers to form a virtual router group and provide redundancy for the default gateway of the network.

This Active-Standby mode uses VRRP to provide the Data Plane redundancy. The active node provides RUCKUS Edge services to APs while the standby node only monitors the active node. If the active node fails, the standby node switches to the active node role and starts providing the services.

NOTE
The member APs connected to the RUCKUS Edge device are unaware of the failover transition as they are connected to the RUCKUS Edge device using the VRRP IP Address (VIP).

Services Supported for High Availability Active-Standby Deployment Model

This section describes the services supported for High Availability.

- **SD-LAN**: Software-Defined Local Area Network (SD-LAN) leverages the principles of software-defined networking for LANs. By implementing SD-LAN, resources and bandwidth can be virtually controlled and managed.

Failure and Expected Behavior

In case of active node failure, the standby node takes ownership of the VRRP IP address and becomes the active node in the network. All the data traffic from the AP/Switch moves automatically to the new active node in the network.

TABLE 3 LAN, Node and Cluster Link Failure and Expected Behavior

Failure Type	Failure Behavior	Failure Recovery Behavior
LAN Failure	In this case, the standby node acts as the active node. If the network is divided, then it is normal to have two active nodes in the network.	After the network failure or link failure is rectified, the cluster is back to Active-Standby mode for operation.
Node Failure	In this case, the standby node takes over as the active node.	After the active node is initialized, it rejoins the cluster as a standby node.

TABLE 3 LAN, Node and Cluster Link Failure and Expected Behavior (continued)

Failure Type	Failure Behavior	Failure Recovery Behavior
Cluster Link Failure	In this case, the standby node stops all the services and expects the active node to connect. In the described state, the standby node periodically transitions from the **waiting for active node** state to verify the Data Plane status. If the Data Plane status is active, then the standby node changes the status to active. If the Data Plane status is standby and the cluster link remains down, the standby node reverts back to the **waiting for active** state.	After the cluster link becomes active, the standby node rejoins the cluster, and the Data Plane is then enabled to participate in High Availability (HA).

Onboarding a Cluster for an Active-Standby High Availability Deployment

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

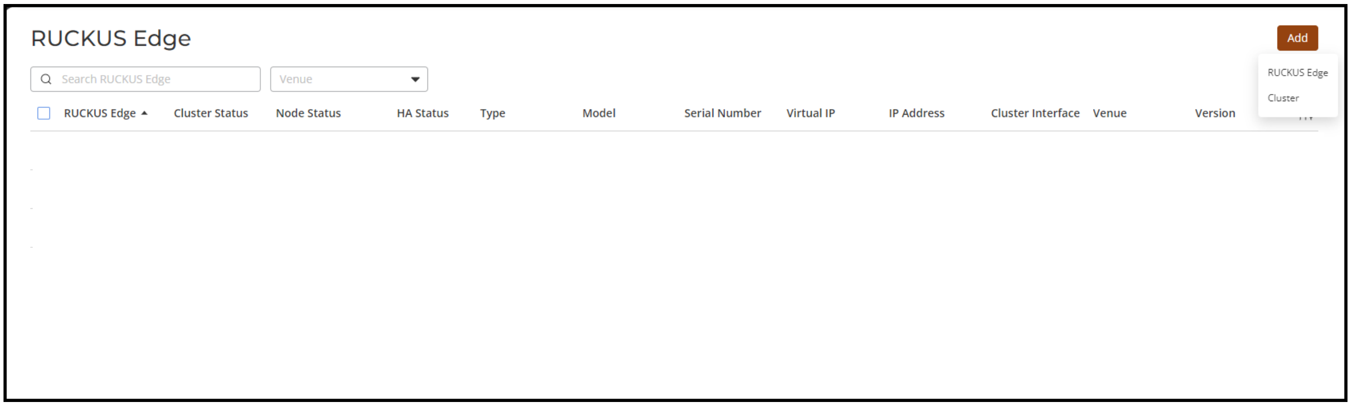
Prior to performing this procedure, you must have already configured the Venue with which this cluster will be associated. You must also have two RUCKUS Edge devices installed and ready for onboarding to RUCKUS One.

Create a dual-node active-standby Edge cluster as follows:

1. Log in to the RUCKUS One web user interface with your credentials.
2. Create the Venue for adding the device. Refer to #unique_22 for more information.
3. On the RUCKUS One navigation bar, click **Gateway** > **RUCKUS Edge**.

   This displays the **RUCKUS Edge** page.
4. In the **RUCKUS Edge** page, click **Add** and select **Cluster**. This displays the **Add Cluster** page.

   FIGURE 1 Add Cluster

   RUCKUS Edge

□	RUCKUS Edge ▲	Cluster Status	Node Status	HA Status	Type	Model	Serial Number	Virtual IP	IP Address	Cluster Interface	Venue	Version

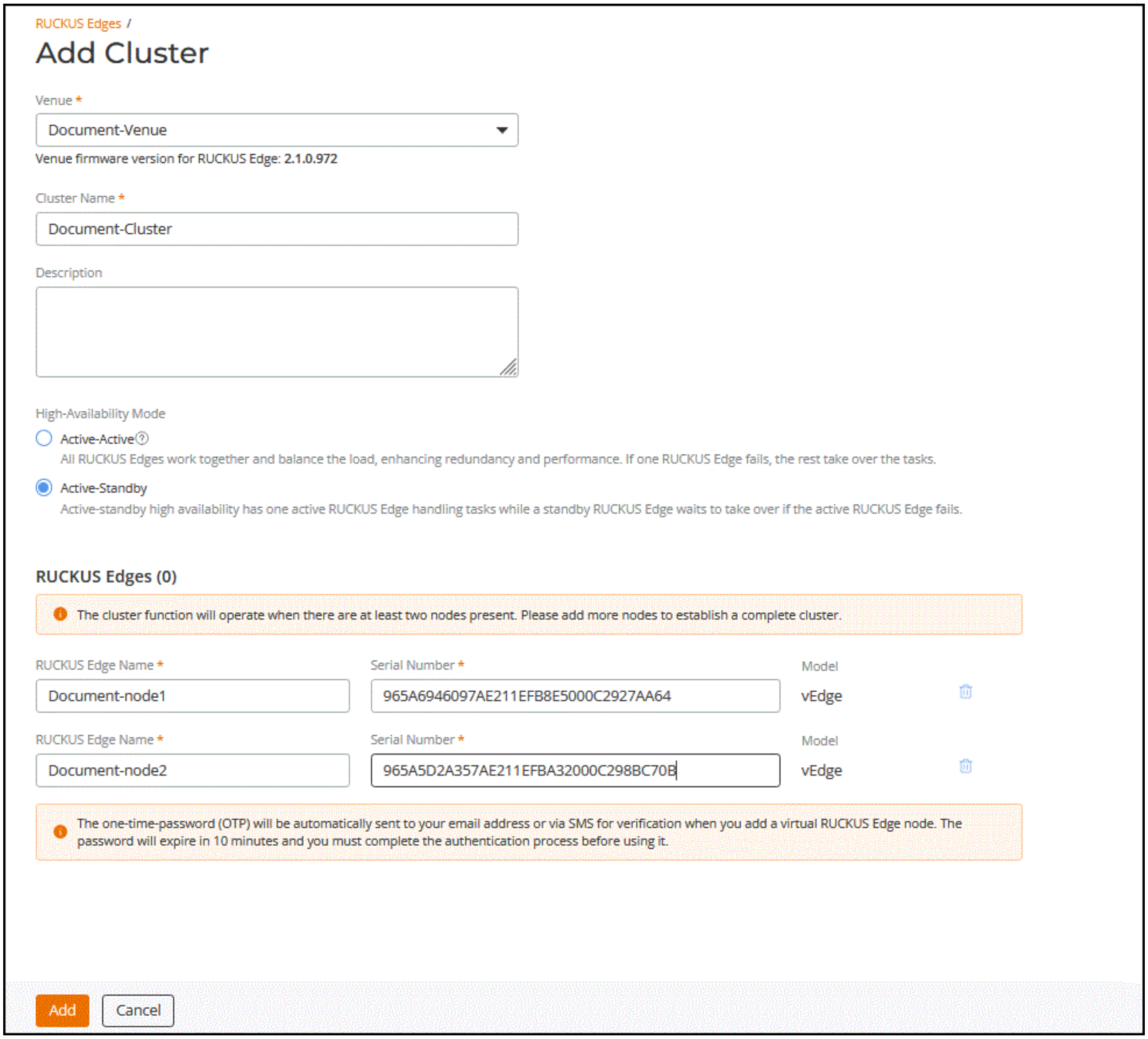
5. In the **Add Cluster** page, enter the following details:
   - **Venue**: Click the drop-down arrow to select a site for the new cluster.
   - **Cluster Name**: Enter a meaningful name for the cluster profile.
   - **Description**: Enter a purposeful statement for the device.
   - **High-Availability Mode**: Select the **Active-Standby** option.

6. 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 2 Adding a Dual Node Active Standby High Availability Cluster



Add Cluster

Venue *: Document-Venue

Venue firmware version for RUCKUS Edge: 2.1.0.972

Cluster Name *: Document-Cluster

Description:

High-Availability Mode

○ Active-Active

All RUCKUS Edges work together and balance the load, enhancing redundancy and performance. If one RUCKUS Edge fails, the rest take over the tasks.

● Active-Standby

Active-standby high availability has one active RUCKUS Edge handling tasks while a standby RUCKUS Edge waits to take over if the active RUCKUS Edge fails.

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	965A5D2A357AE211EFBA32000C298BC70B	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.

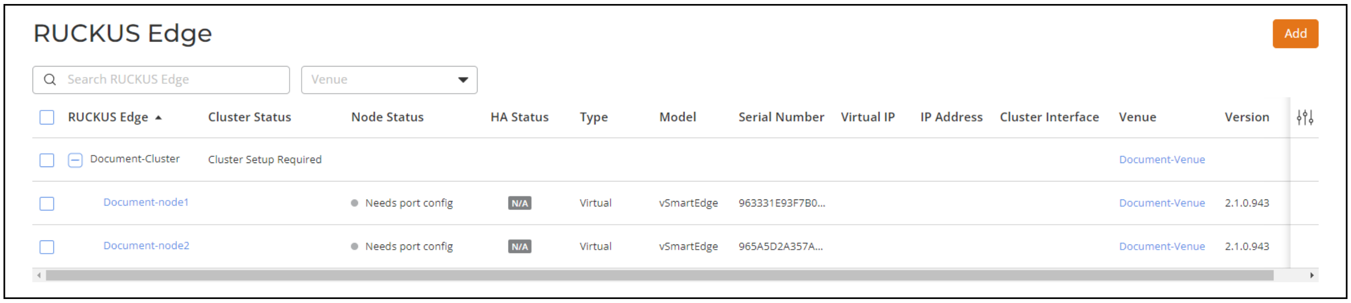
NOTE

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.

7. Click **Add**.

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

   FIGURE 3 Node Status



RUCKUS Edge

Add

Search RUCKUS Edge

Venue

□	RUCKUS Edge ▲	Cluster Status	Node Status	HA Status	Type	Model	Serial Number	Virtual IP	IP Address	Cluster Interface	Venue	Version
□	⊟ Document-Cluster	Cluster Setup Required									Document-Venue	
□	Document-node1		● Needs port config	N/A	Virtual	vSmartEdge	963331E93F7B0...				Document-Venue	2.1.0.943
□	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 Cluster for Active Standby High Availability Deployment with a LAG Interface

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

Prior to performing this procedure, you must have already added the Edge cluster (with HA mode as Active-Standby) in RUCKUS One.

Configure a dual-node active-standby High Availability RUCKUS Edge cluster as follows:

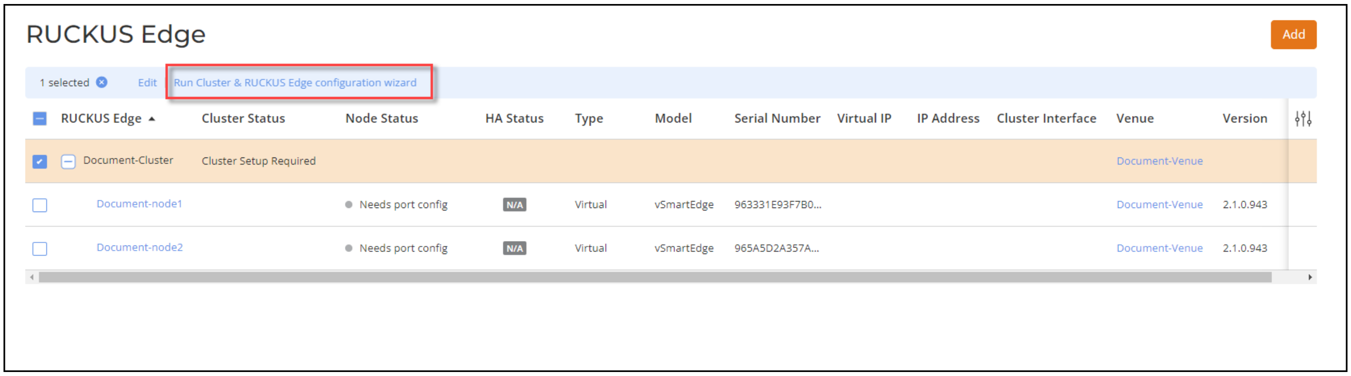
1. Log in to the RUCKUS One web user interface with your credentials.
2. On the RUCKUS One navigation bar, click **Gateway** > **RUCKUS Edge**.

   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 4 Run Cluster and RUCKUS Edge Configuration Wizard



RUCKUS Edge

☐	RUCKUS Edge ▲	Cluster Status	Node Status	HA Status	Type	Model	Serial Number	Virtual IP	IP Address	Cluster Interface	Venue	Version
☑	⊟ Document-Cluster	Cluster Setup Required									Document-Venue	
☐	Document-node1		● Needs port config	N/A	Virtual	vSmartEdge	963331E93F7B0...				Document-Venue	2.1.0.943
☐	Document-node2		● Needs port config	N/A	Virtual	vSmartEdge	965A5D2A357A...				Document-Venue	2.1.0.943

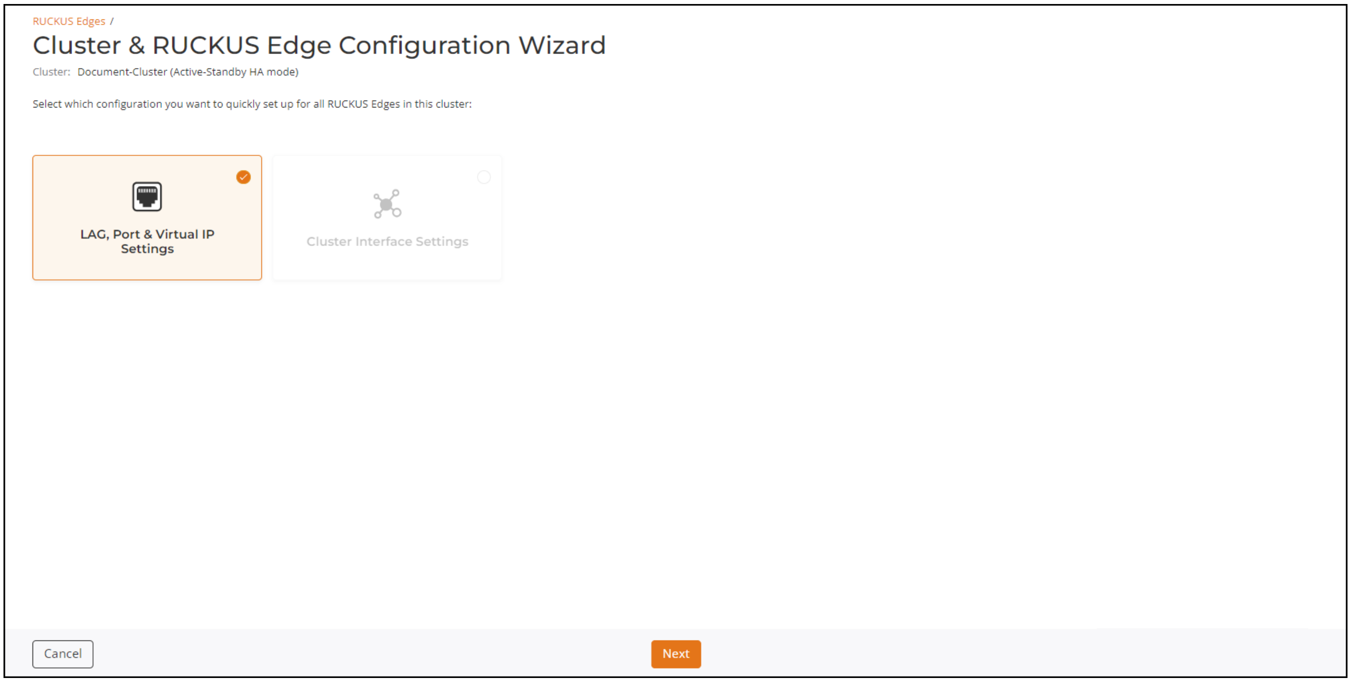
4. Click the **Run Cluster & RUCKUS Edge configuration wizard** option.

   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 5 Cluster and RUCKUS Edge Configuration Wizard



Cluster & RUCKUS Edge Configuration Wizard

Cluster: Document-Cluster (Active-Standby HA mode)

Select which configuration you want to quickly set up for all RUCKUS Edges in this cluster:

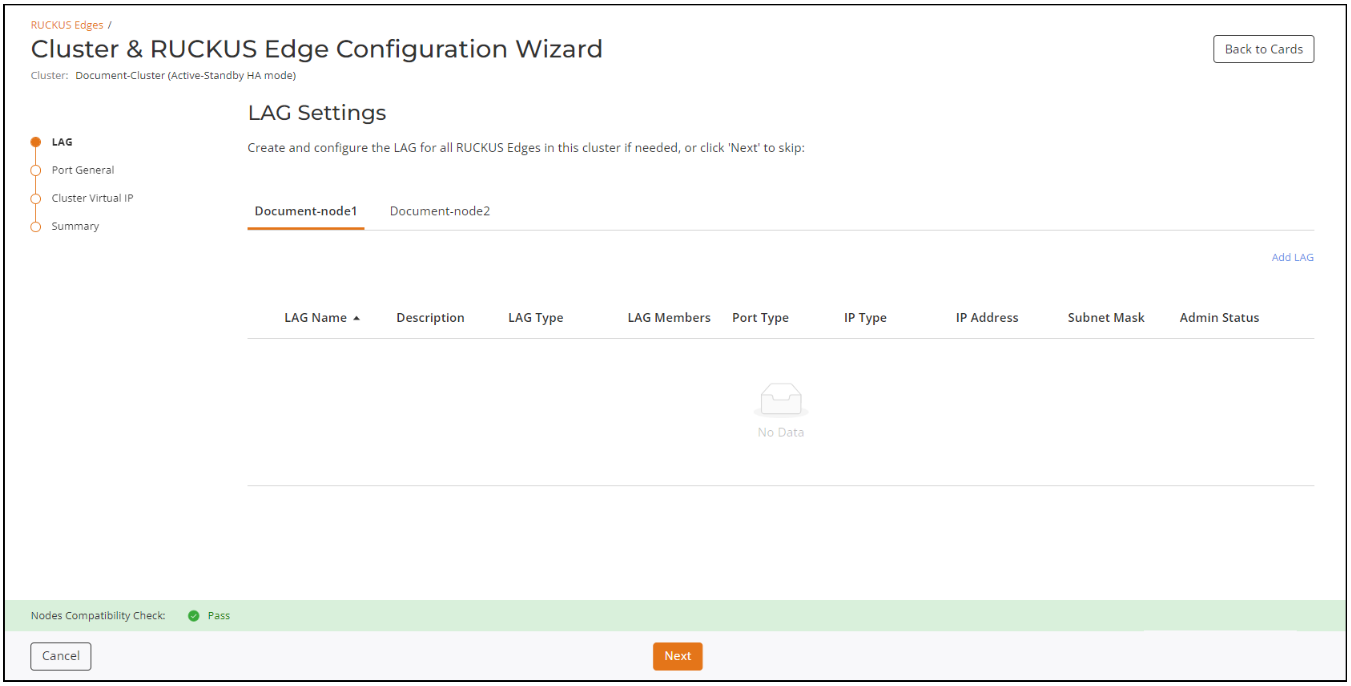
6. Proceed to section Link Aggregation Group (LAG), Port and Virtual IP Settings on page 20 for configuration details.

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 6 Add LAG Settings



RUCKUS Edges /

Cluster & RUCKUS Edge Configuration Wizard

Cluster: Document-Cluster (Active-Standby HA mode)

LAG Settings

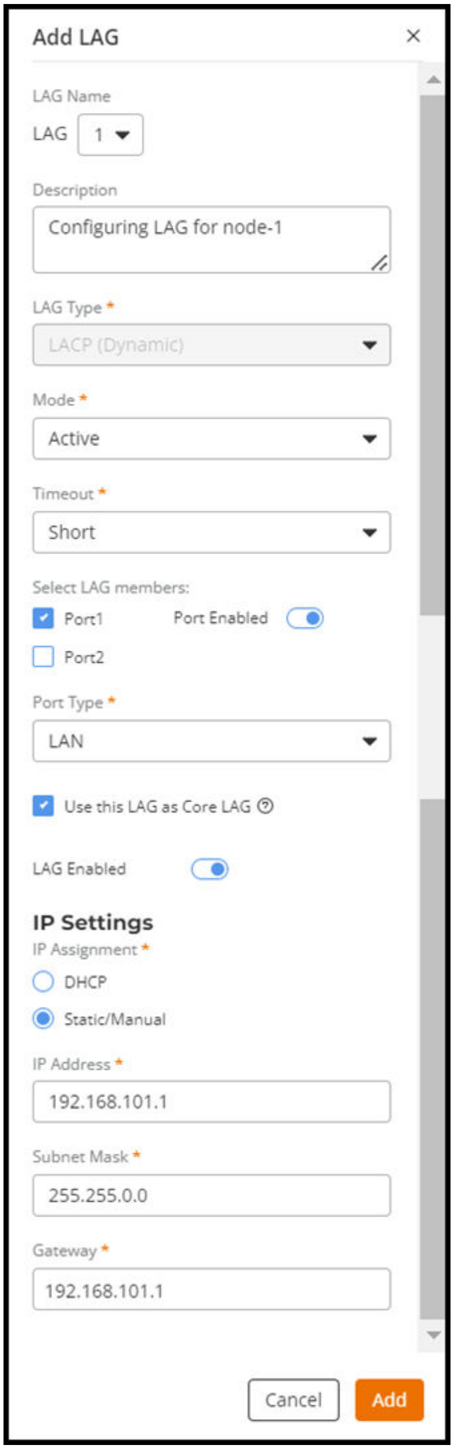
Create and configure the LAG for all RUCKUS Edges in this cluster if needed, or click 'Next' to skip:

LAG Name	Description	LAG Type	LAG Members	Port Type	IP Type	IP Address	Subnet Mask	Admin Status

No Data

Nodes Compatibility Check: Pass

FIGURE 7 Add LAG



Add LAG

LAG Name
LAG 1

Description
Configuring LAG for node-1

LAG Type *
LACP (Dynamic)

Mode *
Active

Timeout *
Short

Select LAG members:
☑ Port1 Port Enabled
□ Port2

Port Type *
LAN

☑ Use this LAG as Core LAG

LAG Enabled

IP Settings

IP Assignment *
○ DHCP
● Static/Manual

IP Address *
192.168.101.1

Subnet Mask *
255.255.0.0

Gateway *
192.168.101.1

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

   NOTE

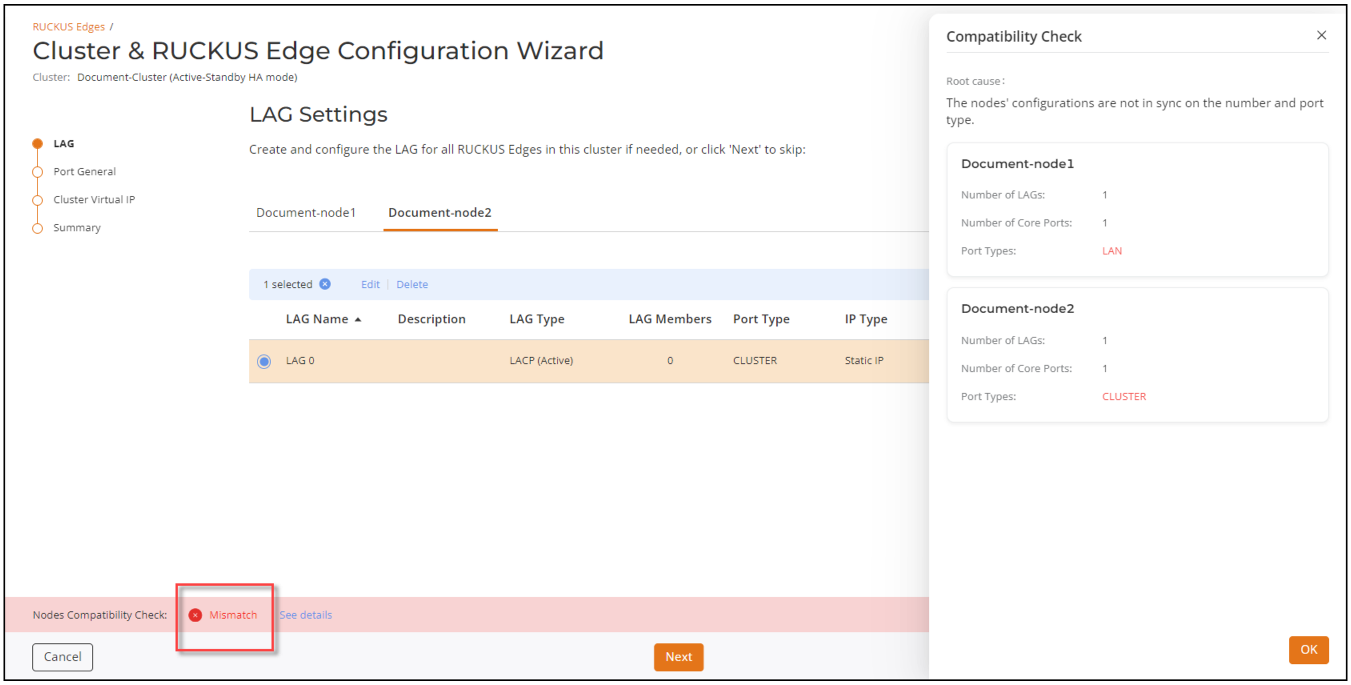
   Refer to Configuring Link Aggregation Group for descriptions of the fields in the Add LAG sidebar.

3. 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 8 LAG Nodes Compatibility Check with Mismatch



RUCKUS Edges /

Cluster & RUCKUS Edge Configuration Wizard

Cluster: Document-Cluster (Active-Standby HA mode)

- LAG
- Port General
- Cluster Virtual IP
- Summary

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

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

Nodes Compatibility Check: ⊗ Mismatch See details

Cancel | Next

Compatibility Check ×

Root cause:

The nodes' configurations are not in sync on the number and port type.

Document-node1

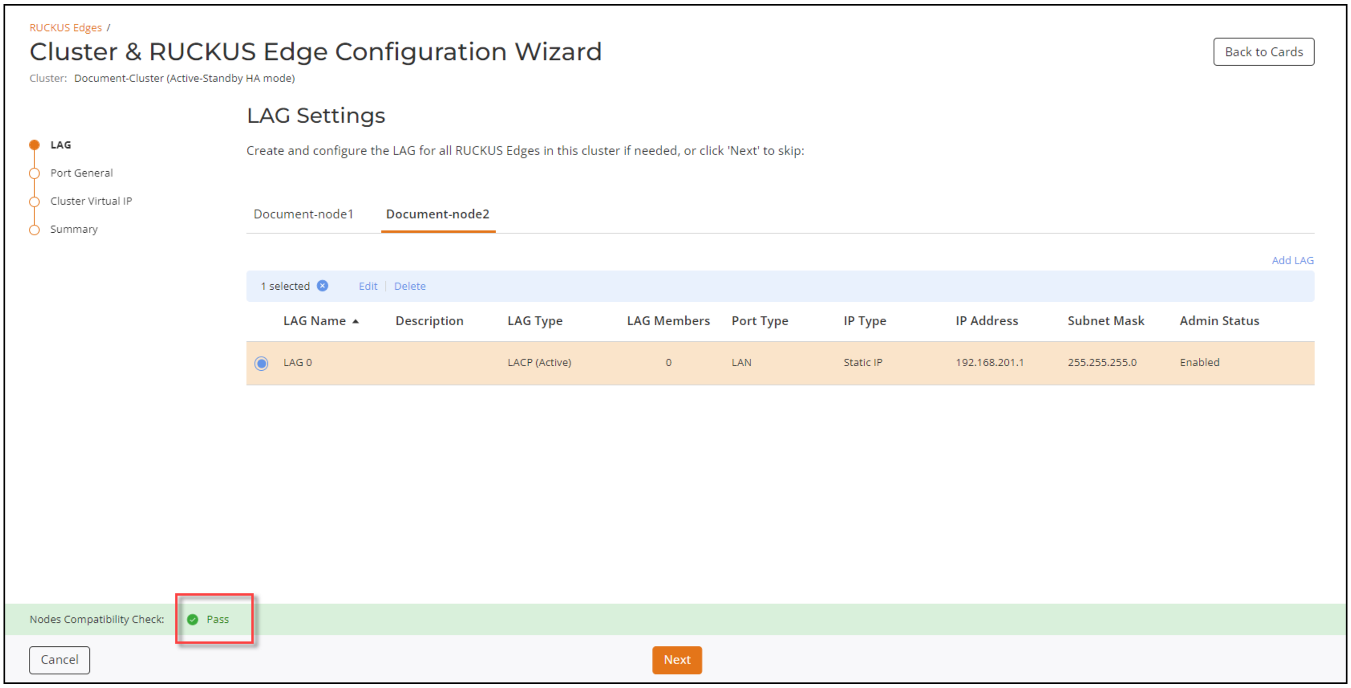
Number of LAGs: 1
Number of Core Ports: 1
Port Types: LAN

Document-node2

Number of LAGs: 1
Number of Core Ports: 1
Port Types: CLUSTER

OK

FIGURE 9 LAG Nodes Compatibility Check with Pass Result



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:

	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

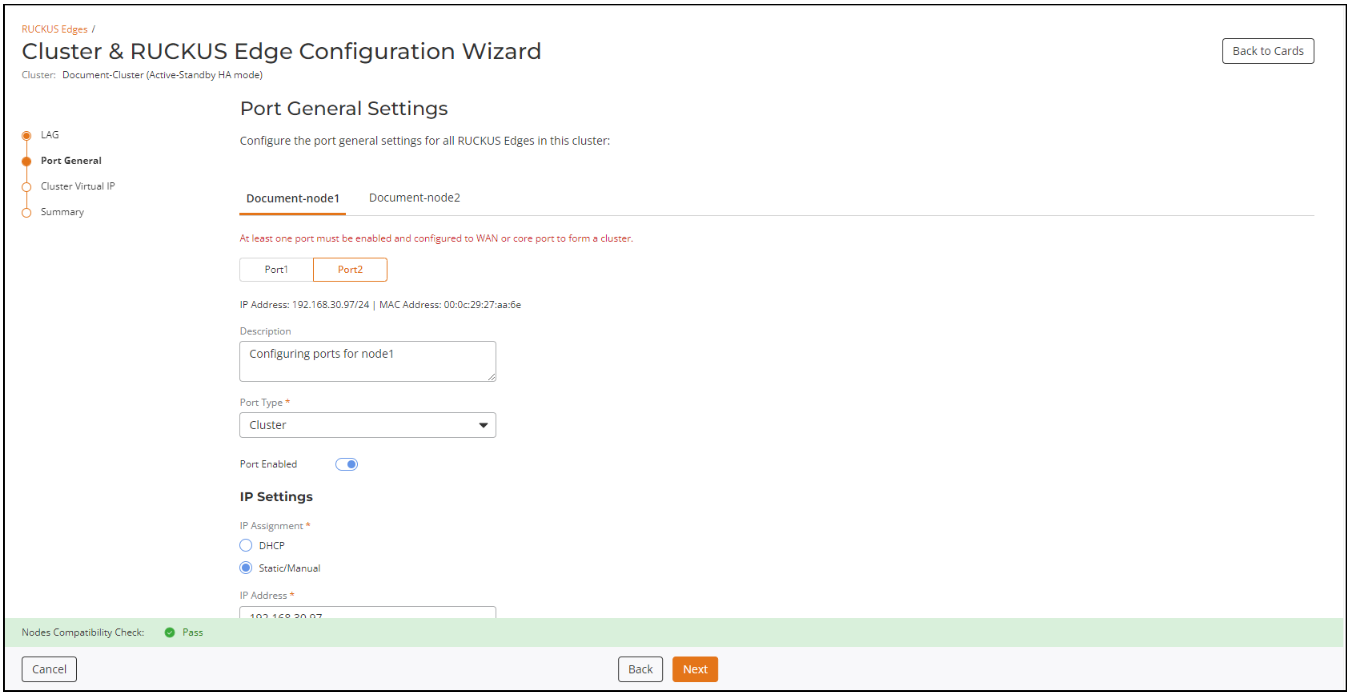
Nodes Compatibility Check: ✓ Pass

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 10 RUCKUS Edge LAG, Port, and Virtual IP Settings: Port Settings

   RUCKUS Edges /

   Cluster & RUCKUS Edge Configuration Wizard

   Cluster: Document-Cluster (Active-Standby HA mode)

   Port General Settings

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

   At least one port must be enabled and configured to WAN or core port to form a cluster.

   IP Address: 192.168.30.97/24 | MAC Address: 00:0c:29:27:aa:6e

   Description: Configuring ports for node1

   Port Type *: Cluster

   Port Enabled: ●

   IP Settings

   IP Assignment *
   ○ DHCP
   ● Static/Manual

   IP Address *: 192.168.30.97

   Nodes Compatibility Check: ✓ Pass

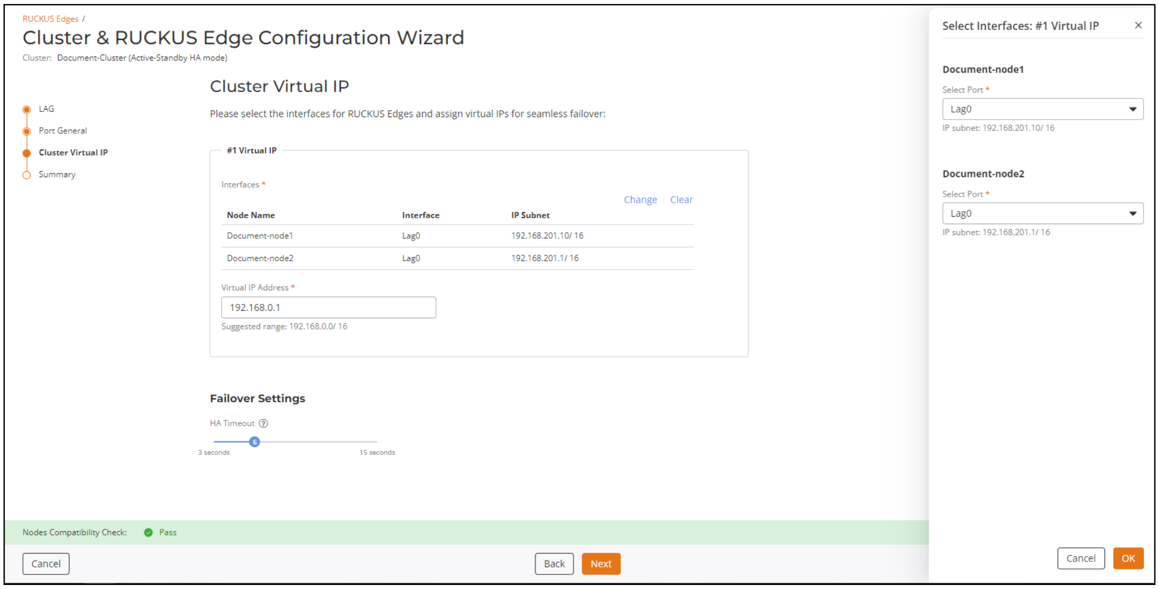
   Click **Next**.

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 11 RUCKUS Edge LAG, Port, and Virtual IP Settings: Virtual IP and Failover



RUCKUS Edges /

Cluster & RUCKUS Edge Configuration Wizard

Cluster: Document-Cluster (Active-Standby HA mode)

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: 6

Nodes Compatibility Check: Pass

Select Interfaces: #1 Virtual IP

Document-node1

Select Port *: Lag0

IP subnet: 192.168.201.10/ 16

Document-node2

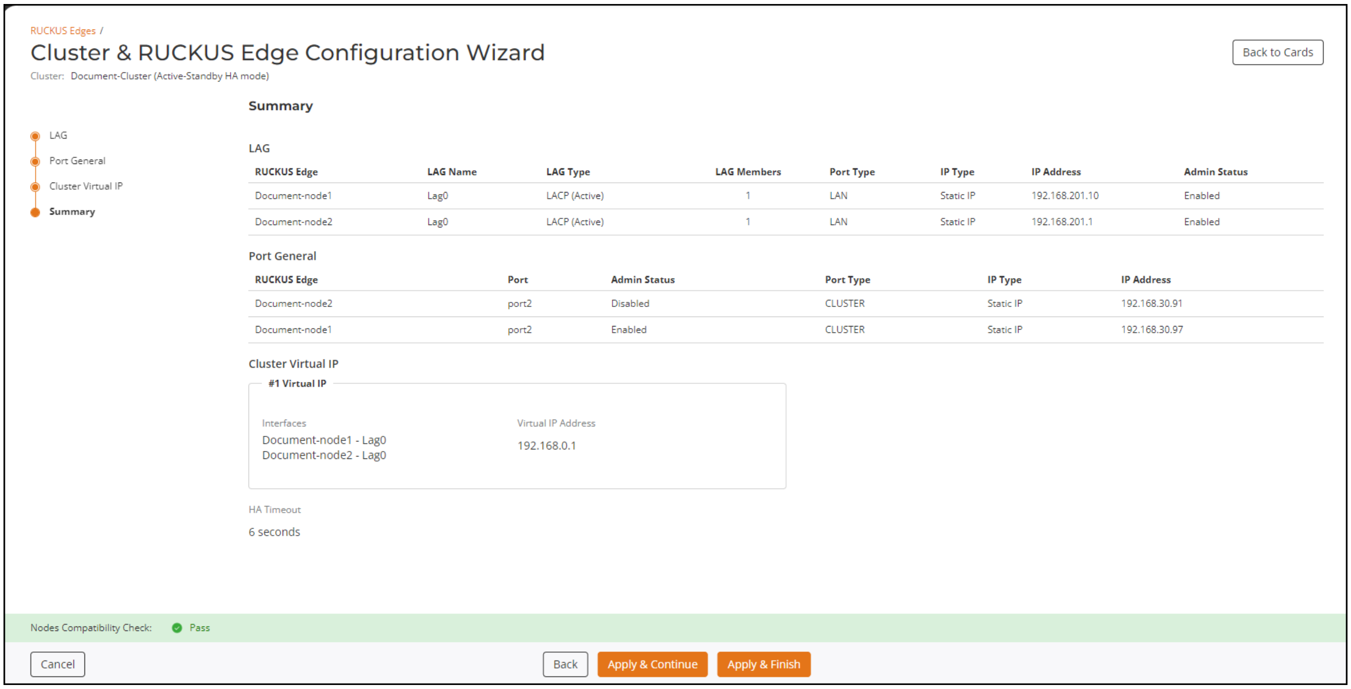
Select Port *: Lag0

IP subnet: 192.168.201.1/ 16

Click **Next**.

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 12 RUCKUS Edge LAG, Port, and Virtual IP Settings: Summary

   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: Document-node1 - Lag0, Document-node2 - Lag0

   Virtual IP Address: 192.168.0.1

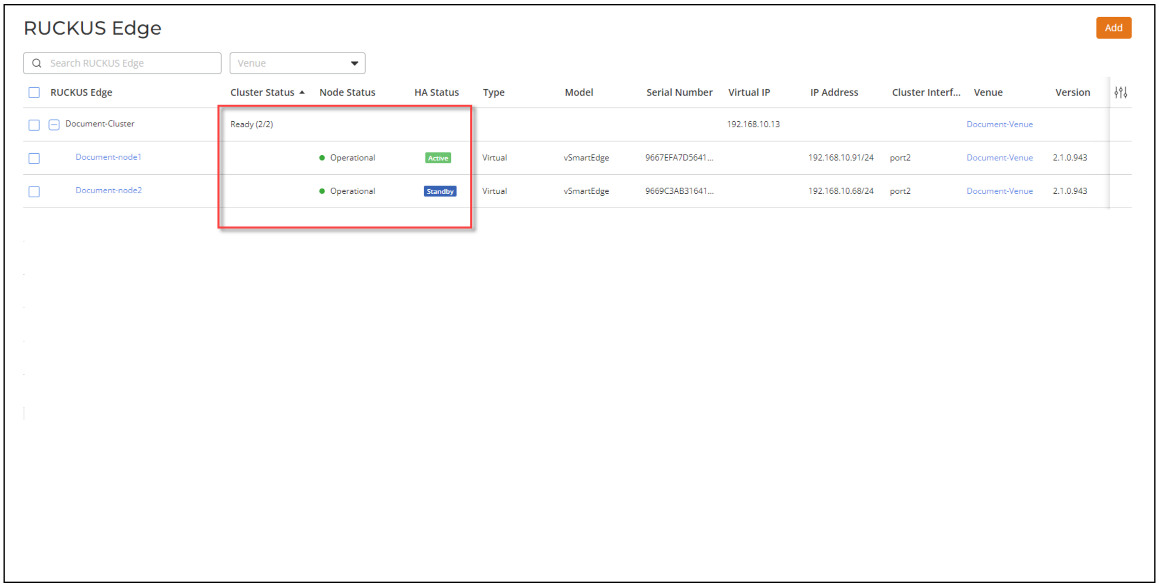
   HA Timeout: 6 seconds

   Nodes Compatibility Check: ● Pass

   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 13 Nodes Status is Operational



RUCKUS Edge

☐ RUCKUS Edge	Cluster Status ▲	Node Status	HA Status	Type	Model	Serial Number	Virtual IP	IP Address	Cluster Interf...	Venue	Version
☐ ⊟ Document-Cluster	Ready (2/2)						192.168.10.13			Document-Venue	
☐ Document-node1		● Operational	Active	Virtual	vSmartEdge	9667EFA7D5641...		192.168.10.91/24	port2	Document-Venue	2.1.0.943
☐ 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 28 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 20), 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**.

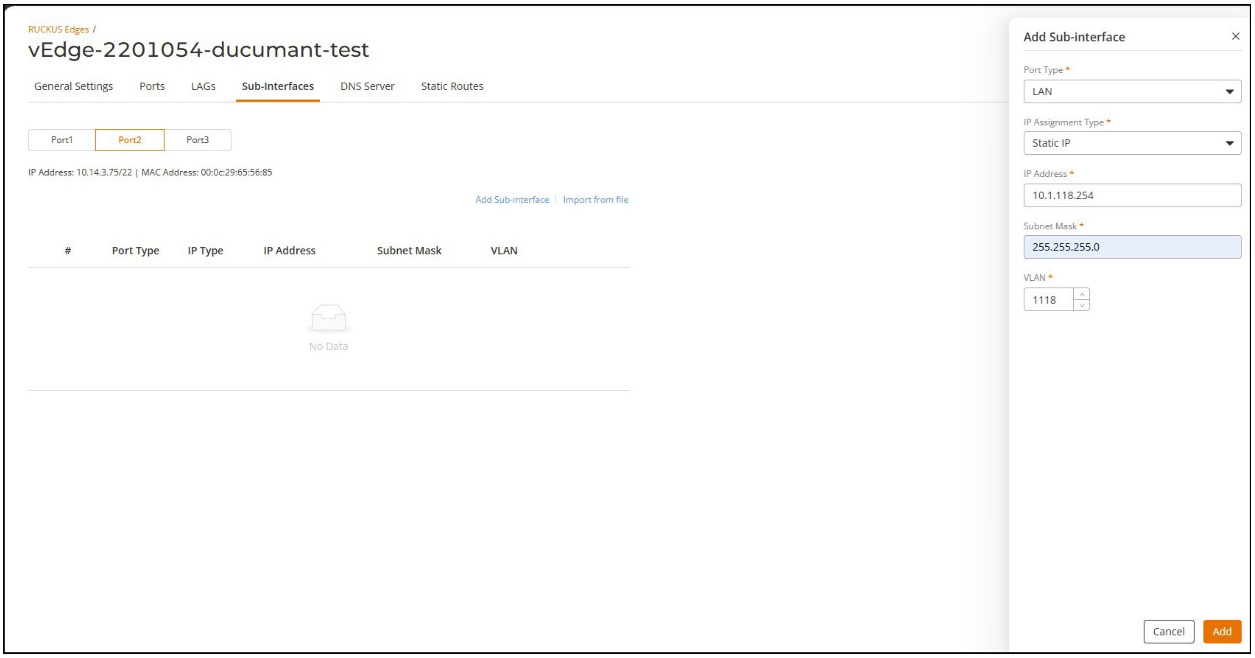
Sub-Interface

1. Click **Sub-Interface** tab and click **Add Sub-Interface**

   This displays **Add Sub-Interface** window.

2. In the **Add Sub-Interface** window, enter the following details:
   - **Port Type** - Select the port type from the drop-down list.
   - **IP Assignment Type** - By default, the IP assignment type is **DHCP**, however, to manually configure the ports, select **Static** from the drop-down list and enter the IP address.

   FIGURE 14 Sub-Interface Port Settings

   RUCKUS Edges /
   vEdge-2201054-ducumant-test

   IP Address: 10.14.3.75/22 | MAC Address: 00:0c:29:65:56:85

#	Port Type	IP Type	IP Address	Subnet Mask	VLAN

   No Data

   Add Sub-interface

   Port Type * LAN

   IP Assignment Type * Static IP

   IP Address * 10.1.118.254

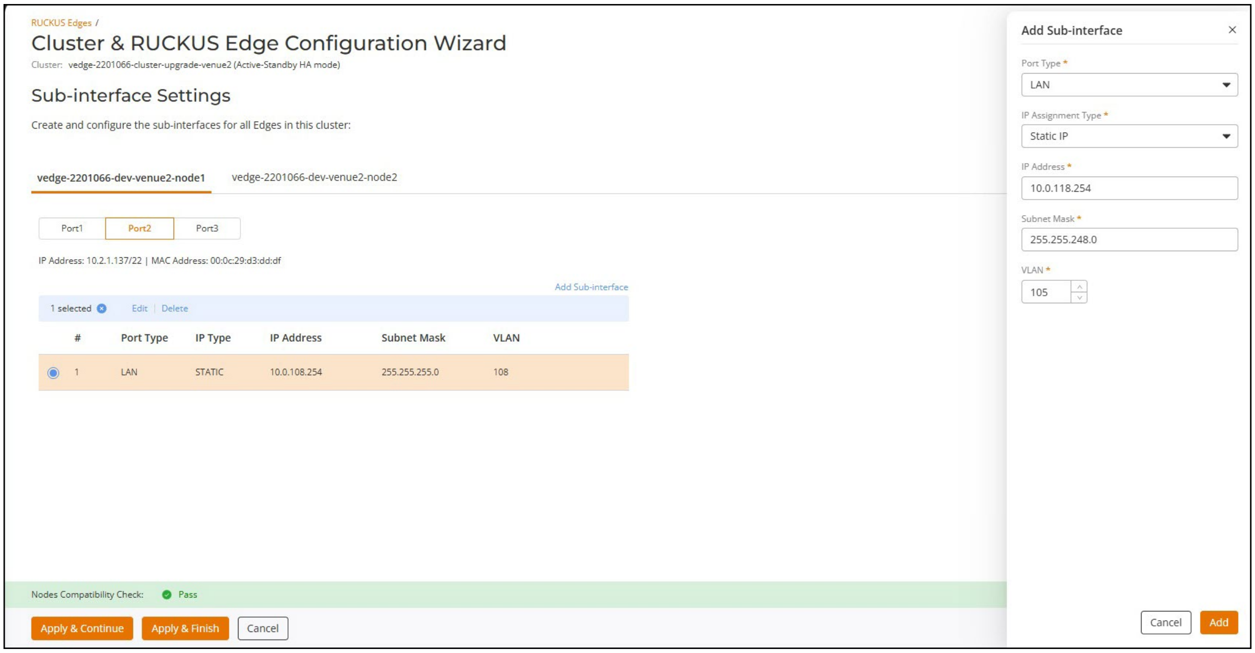
   Subnet Mask * 255.255.255.0

   VLAN * 1118

3. After entering all the details in the respective fields, click **Add**.

4. The sub-interface settings are displayed on the screen.

FIGURE 15 Sub-interface Settings



Cluster & RUCKUS Edge Configuration Wizard

Cluster: vedge-2201066-cluster-upgrade-venue2 (Active-Standby HA mode)

Sub-interface Settings

Create and configure the sub-interfaces for all Edges in this cluster:

vedge-2201066-dev-venue2-node1
vedge-2201066-dev-venue2-node2
Port1
Port2
Port3

IP Address: 10.2.1.137/22 | MAC Address: 00:0c:29:d3:dd:df

	#	Port Type	IP Type	IP Address	Subnet Mask	VLAN
●	1	LAN	STATIC	10.0.108.254	255.255.255.0	108

Nodes Compatibility Check: Pass

Add Sub-interface

Port Type *: LAN

IP Assignment Type *: Static IP

IP Address *: 10.0.118.254

Subnet Mask *: 255.255.248.0

VLAN *: 105

NOTE
Repeat the same steps to add interfaces to **Port 2** and **Port 3**.

5. User can also import file from the local system by clicking **Import from file**. Only .csv (Comma Separated Values) file type with file size not exceeding more than 5MB is allowed to be uploaded.

NOTE
User should have routes to reach the loopback of Distribution Switch from RUCKUS Edge and if the user is using external DHCP server then another route to reach the external DHCP server.

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

This section describes configuring a cluster for Active Standby 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:

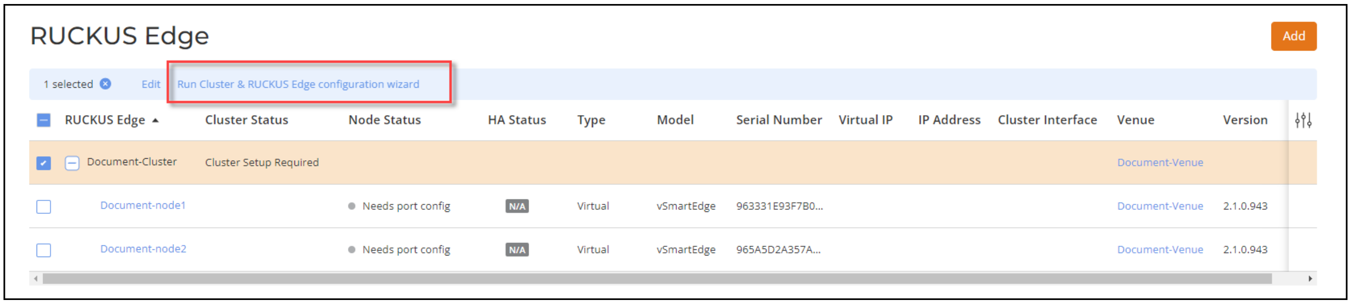
1. Log in to the RUCKUS One web user interface with your credentials.
2. On the RUCKUS One navigation bar, click **Gateway** > **RUCKUS Edge**.

   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 16 Run Cluster and RUCKUS Edge Configuration Wizard



RUCKUS Edge

	RUCKUS Edge	Cluster Status	Node Status	HA Status	Type	Model	Serial Number	Virtual IP	IP Address	Cluster Interface	Venue	Version
☑	Document-Cluster	Cluster Setup Required									Document-Venue	
□	Document-node1		● Needs port config	N/A	Virtual	vSmartEdge	963331E93F7B0...				Document-Venue	2.1.0.943
□	Document-node2		● Needs port config	N/A	Virtual	vSmartEdge	965A5D2A357A...				Document-Venue	2.1.0.943

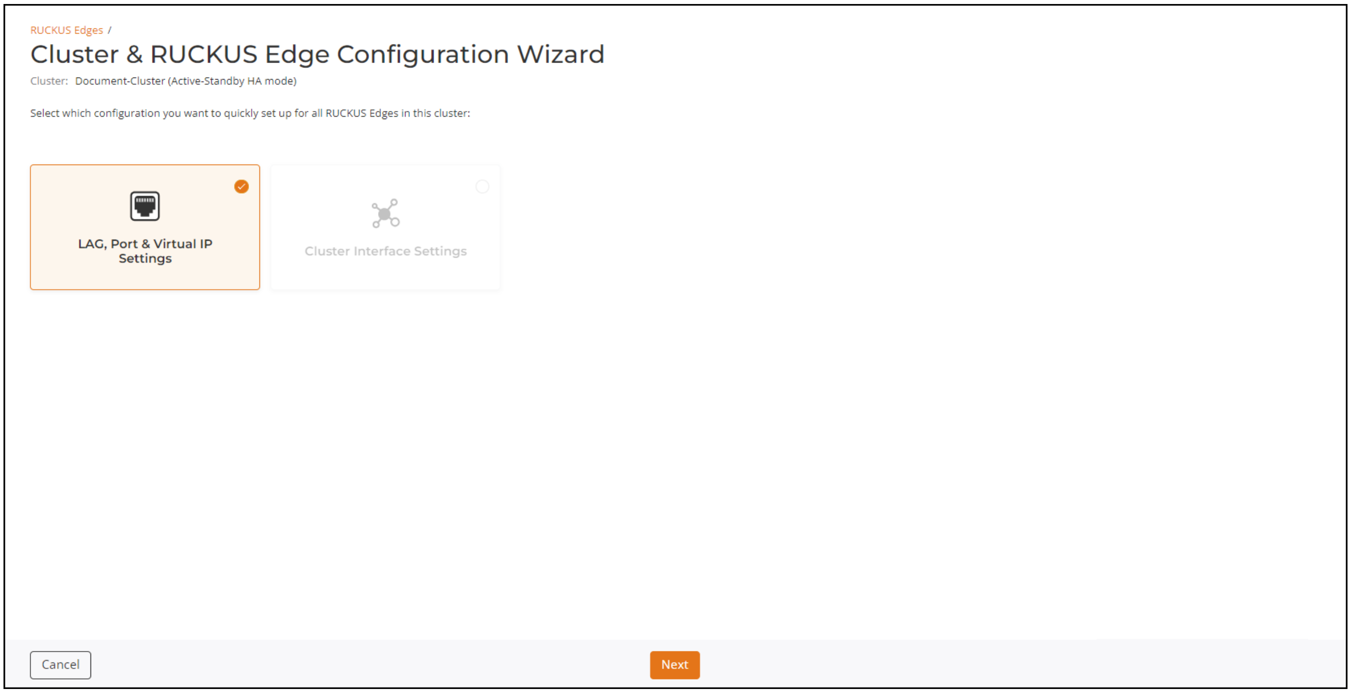
4. Click the **Run Cluster & RUCKUS Edge configuration wizard** option.

   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 17 Cluster and RUCKUS Edge Configuration Wizard



RUCKUS Edges /

Cluster & RUCKUS Edge Configuration Wizard

Cluster: Document-Cluster (Active-Standby HA mode)

Select which configuration you want to quickly set up for all RUCKUS Edges in this cluster:

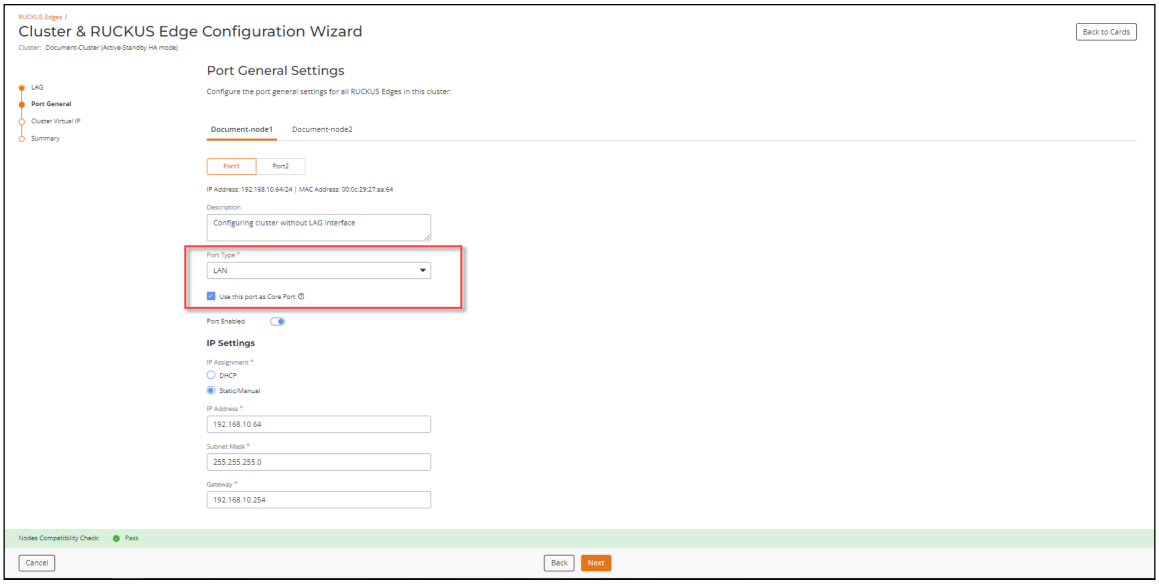
Link Aggregation Group (LAG), Port and Virtual IP Settings

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

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

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 18 Configuring Ports Without a LAG - 1



Cluster & RUCKUS Edge Configuration Wizard

Cluster: Document-Cluster (Active-Standby HA mode)

Port General Settings

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

IP Address: 192.168.10.64/24 | MAC Address: 00:0c:29:27:aa:64

Description: Configuring cluster without LAG interface

Port Type *: LAN

☑ Use this port as Core Port

Port Enabled: ●

IP Settings

IP Assignment *
○ DHCP
● Static/Manual

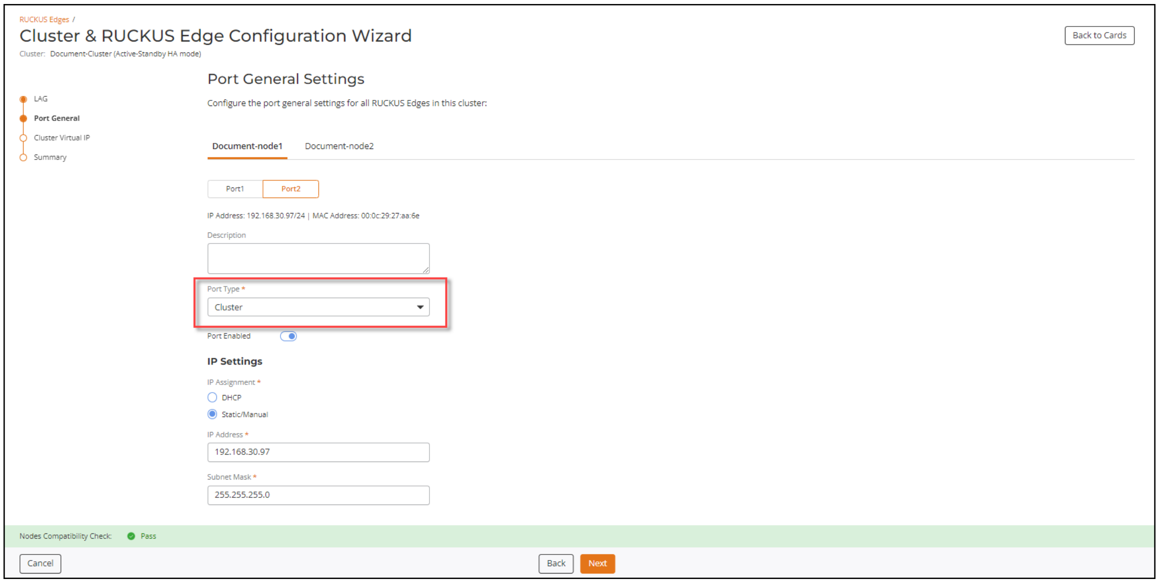
IP Address *: 192.168.10.64

Subnet Mask *: 255.255.255.0

Gateway *: 192.168.10.254

Nodes Compatibility Check: ✓ Pass

FIGURE 19 Configuring Ports Without a LAG - 2



RUCKUS Edges /

Cluster & RUCKUS Edge Configuration Wizard

Cluster: Document-Cluster (Active-Standby HA mode)

Port General Settings

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

IP Address: 192.168.30.97/24 | MAC Address: 00:0c:29:27:aa:6e

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

e. Repeat steps List item. through List item. 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**.

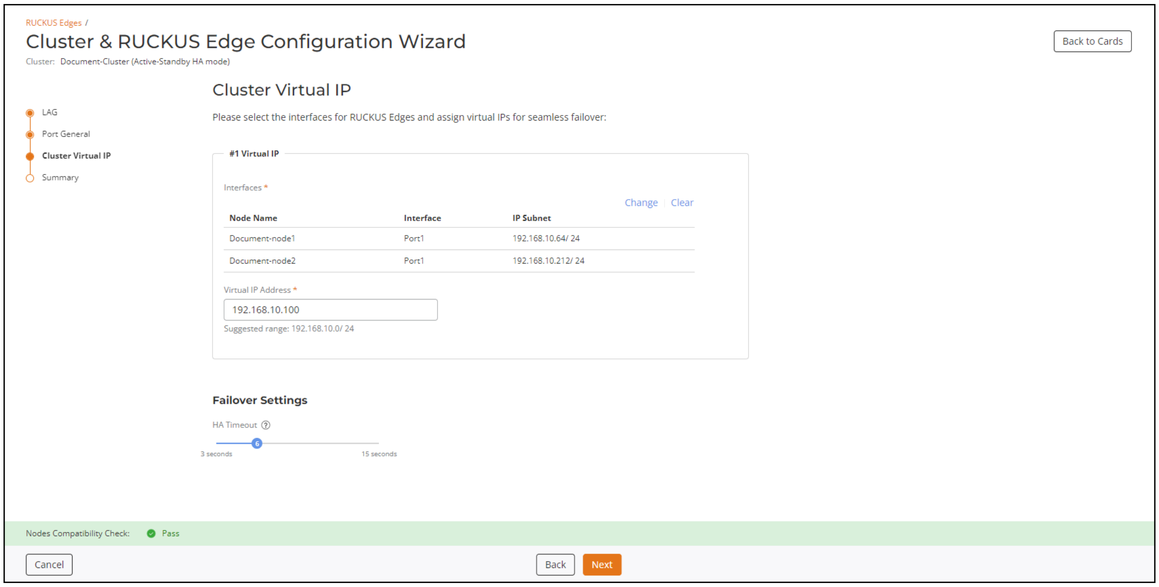
3. **Cluster Virtual IP**: This section displays the configured **Node Name**, **Interface** and **IP Subnet Mask**. Enter the **Virtual IP Address**.

   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 20 Cluster Virtual IP



RUCKUS Edges /

Cluster & RUCKUS Edge Configuration Wizard

Cluster: Document-Cluster (Active-Standby HA mode)

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	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

Failover Settings

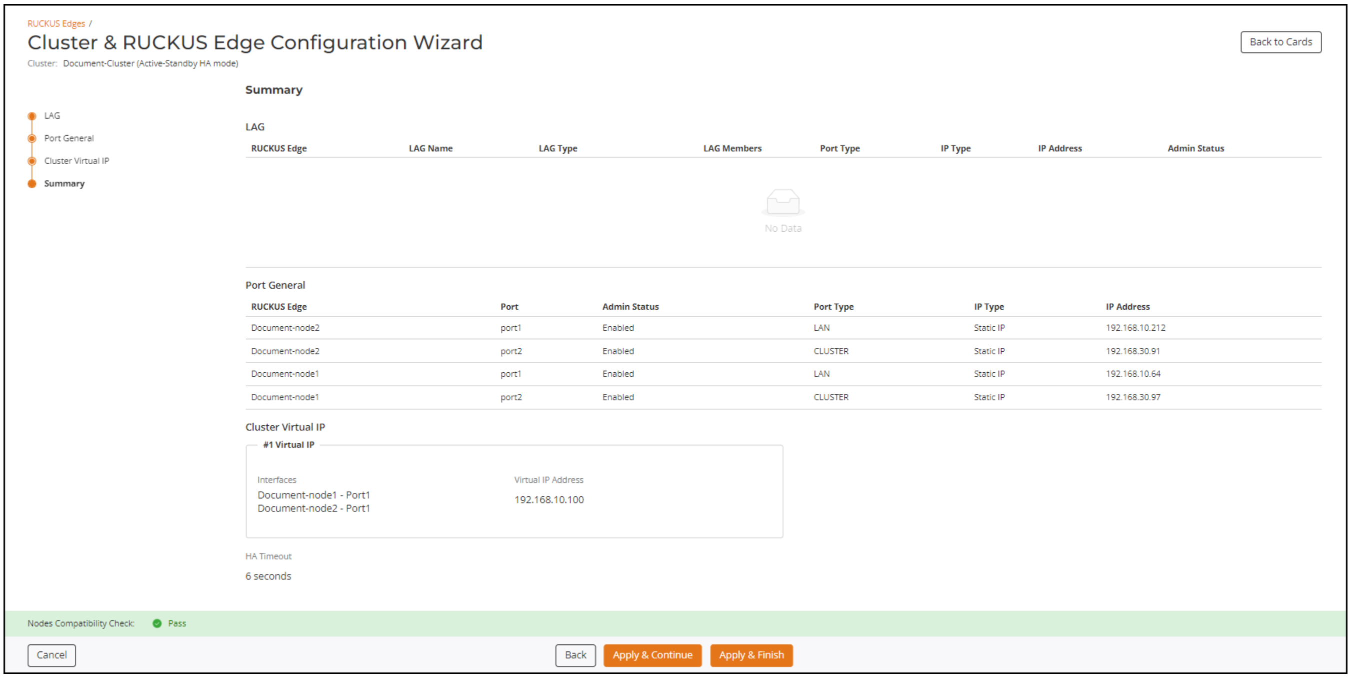
HA Timeout: 6

Nodes Compatibility Check: Pass

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 21 Summary of the Cluster Configuration without a LAG



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

No Data

Port General

RUCKUS Edge	Port	Admin Status	Port Type	IP Type	IP Address
Document-node2	port1	Enabled	LAN	Static IP	192.168.10.212
Document-node2	port2	Enabled	CLUSTER	Static IP	192.168.30.91
Document-node1	port1	Enabled	LAN	Static IP	192.168.10.64
Document-node1	port2	Enabled	CLUSTER	Static IP	192.168.30.97

Cluster Virtual IP

#1 Virtual IP

Interfaces
Document-node1 - Port1
Document-node2 - Port1

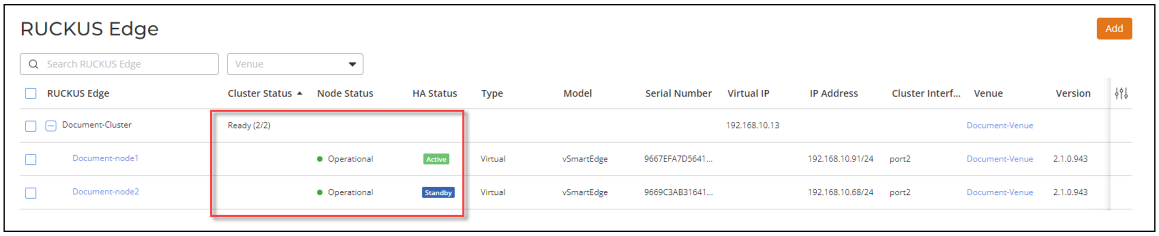
Virtual IP Address
192.168.10.100

HA Timeout
6 seconds

Nodes Compatibility Check: ● Pass

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 22 Nodes Status is Operational



RUCKUS Edge

RUCKUS Edge	Cluster Status ▲	Node Status	HA Status	Type	Model	Serial Number	Virtual IP	IP Address	Cluster Interf...	Venue	Version
Document-Cluster	Ready (2/2)						192.168.10.13			Document-Venue	
Document-node1		● Operational	Active	Virtual	vSmartEdge	9667EFA7D5641...		192.168.10.91/24	port2	Document-Venue	2.1.0.943
Document-node2		● Operational	Standby	Virtual	vSmartEdge	9669C3AB31641...		192.168.10.68/24	port2	Document-Venue	2.1.0.943

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 32), select the **Cluster Interface** checkbox and click **Next**. This displays **Cluster Interface** page containing a tab for each RUCKUS Edge device in the cluster for a non-LAG case as shown in Step 5 on page 31.

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 the second device tab.
3. Click **Apply & Finish**.

Editing an Active-Backup 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 **Gateway** > **RUCKUS Edge**.

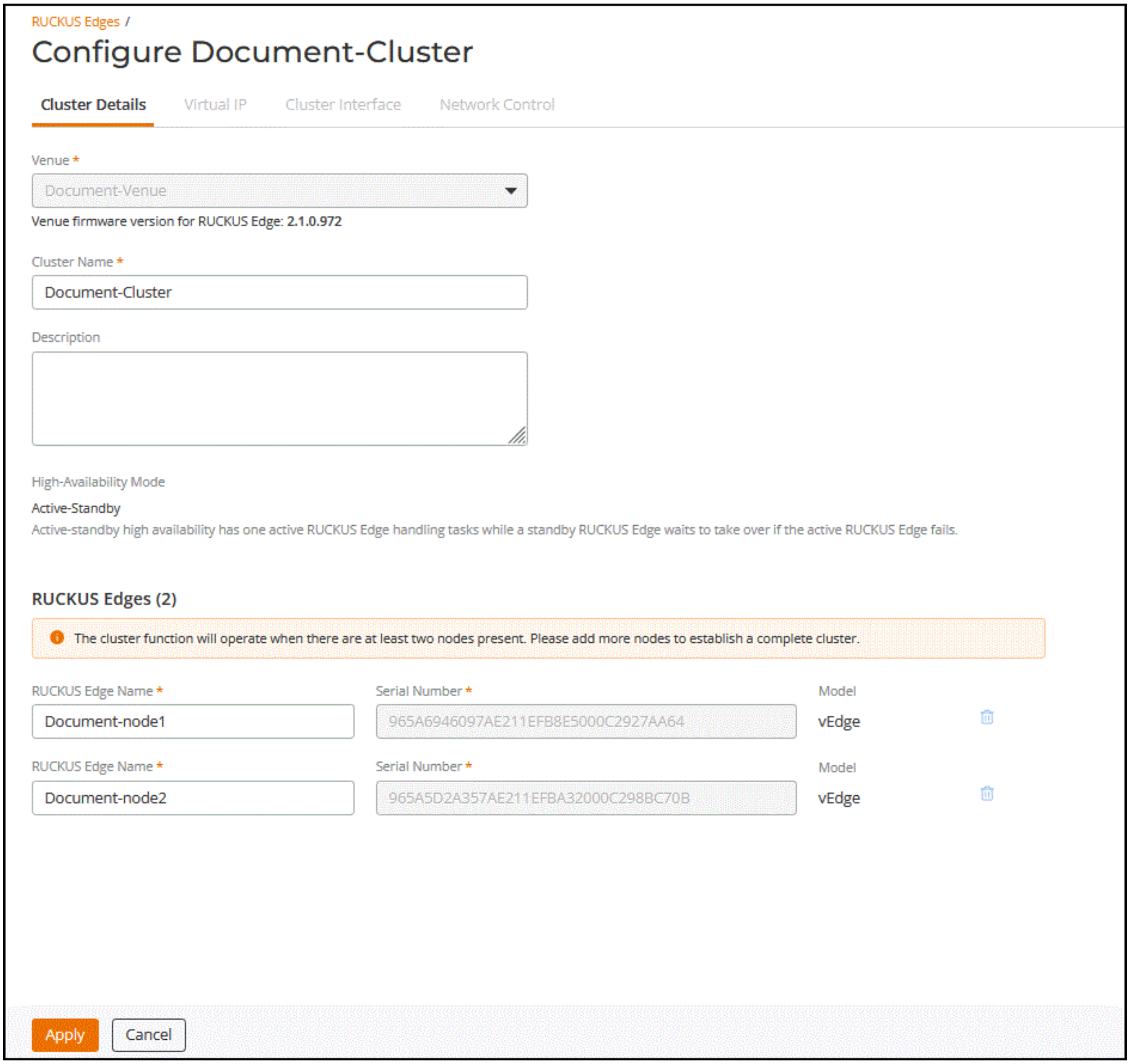
   This displays the list of RUCKUS Edge clusters.
3. Select the checkbox adjacent to the RUCKUS Edge cluster. This highlights the **Edit** and **Run Cluster & RUCKUS Edge configuration wizard** options.

   NOTE
   The High-Availability Mode of the cluster cannot be modified or edited.
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 23 Configure <Cluster Name>



Configure Document-Cluster

Venue * Document-Venue

Venue firmware version for RUCKUS Edge: 2.1.0.972

Cluster Name * Document-Cluster

Description

High-Availability Mode

Active-Standby

Active-standby high availability has one active RUCKUS Edge handling tasks while a standby RUCKUS Edge waits to take over if the active RUCKUS Edge fails.

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	965A6946097AE211EFB8E5000C2927AA64	vEdge
Document-node2	965A5D2A357AE211EFBA32000C298BC70B	vEdge

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

Active-Active High Availability

The Active-Active High Availability (AA HA) feature ensures that if one node in a cluster fails, the other nodes continue to manage the requests, providing continuous service without interruption.

Feature Overview

This feature requires a minimum of two nodes and supports a maximum of four nodes in a cluster. The Active-Active HA mode is designed to provide both redundancy and scalability. In this mode, all cluster nodes can simultaneously manage tunnels from APs.

If the SD-LAN service is enabled on the Edge cluster in Active-Active HA mode, RUCKUS One will provide APs with a list of Edge VXLAN Tunnel Endpoint (VTEP) IP addresses. This list includes the IP address of each node in the cluster.

To distribute the load of AP tunnels across all nodes in the Active-Active HA mode cluster, two load distribution methods are supported.

- Random distribution: Each AP randomizes the Edge VTEP IP address list using its serial number as a random seed. Each AP will then attempt to connect to the first Edge IP address in its randomized list, known as the Primary Edge. This approach directs the tunnels from APs to different nodes in the Active-Active HA cluster, effectively distributing the load.
- Per AP-group distribution: Each AP randomizes the Edge VTEP IP address list using the identifier of its AP Group. In this method, all APs in the same AP Group will derive the same randomized IP list. As each AP will attempt to connect to the first Edge IP address in its randomized list, all APs in same AP Group will tunnel to same Edge node. As long as a wireless client roams across APs in the same AP Group, there will not be any MAC movement for that wireless client's MAC address in the Edge uplink port switch network.

In a High Availability configuration, if an AP is unable to connect to the first Edge IP address in its randomized list, it will attempt to connect to the next IP address in the list and continue this process until a connection is established. If it cannot connect to the last IP address in the list, it will try the first IP address again. The AP will continue this process until it successfully connects to an Edge device. The Edge to which the AP connects is referred to as the Active Edge.

When an AP is connected to a RUCKUS Edge node, it will continuously send periodic keepalive traffic to ensure the Edge device is reachable. If the keepalive message to the Active Edge fails, the AP will attempt to connect to the next Edge node in the list. This process is known as AP tunnel failover to the next Edge node.

Requirements

The Cluster Interface is crucial for enabling clustering in RUCKUS Edge. To configure it, a dedicated physical interface must be provided within the RUCKUS Edge. facilitates cluster formation, the exchange of cluster information, 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.

Considerations

In RUCKUS Edge-deployed networks, all APs will have the IP addresses of all nodes in the active-active high availability cluster. Depending on the load distribution method, some APs will tunnel to node-1, while others will tunnel to node-2, and so on. Each AP will periodically send keepalive messages to the node it is tunneling to. In the event of a failure, the following scenario is established:

- If a node does not respond to the keepalive messages, APs that were tunneling to that node will now tunnel to other nodes in the cluster.
- After the failed node becomes operational and rejoins the cluster, the APs will resume tunneling to that node at a scheduled time.

Best Practices

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

Prerequisites

This feature requires the following prerequisites:

- Install two to four RUCKUS Edge devices based on the scale and redundancy needs.
- Use Edge nodes with comparable hardware capabilities to form a cluster.
- Configure all nodes in the Active-Active HA cluster to have their LAN ports within the same subnet..
- Create a venue and associate the RUCKUS Edge cluster.

High Availability Active-Active Deployment Model

High Availability supports the Active-Active deployment model.

This feature requires a minimum of two nodes and supports a maximum of four nodes in a cluster. The Active-Active HA mode is designed to provide both redundancy and scalability. In this mode, all cluster nodes can simultaneously manage tunnels from APs.

If the SDLAN service is enabled on the Edge cluster in Active-Active HA mode, RUCKUS One will provide APs with a list of Edge VXLAN Tunnel Endpoint (VTEP) IP addresses. This list includes the IP address of each node in the cluster.

To distribute the load of AP tunnels across all nodes in the Active-Active HA mode cluster, two load distribution methods are supported.

- **Random distribution**: Each AP randomizes the Edge VTEP IP address list using its serial number as a random seed. Each AP will then attempt to connect to the first Edge IP address in its randomized list, known as the Primary Edge. This approach directs the tunnels from APs to different nodes in the Active-Active HA cluster, effectively distributing the load.
- **Per AP-group distribution**: Each AP randomizes the Edge VTEP IP address list using the AP-group identifier. In this method, all APs in the same AP-group will derive same randomized IP list. As each AP will attempt to connect to the first Edge IP address in its randomized list, all APs in same AP-group tunnel to same Edge node. As long a wireless client roam across APs in same AP-group, there will not be any MAC movement for that wireless client MAC address in the Edge uplink port switch network.

In High Availability, if an AP is unable to connect to the first Edge IP address in its randomized list, it will attempt to connect to the next IP address in the list. If it cannot connect to the last IP address in the list, it will try the first IP address again. The AP will continue this process until it successfully connects to an Edge device. The Edge to which the AP connects is referred to as the Active Edge.

When an AP is connected to an Edge node, it will continuously send periodic keepalive traffic to ensure the Edge is reachable. If the keepalivemessage to the Active Edge fails, the AP will attempt to connect to the next Edge node in the list. This process is known as AP tunnel failover to the next Edge node.

Services Supported for High Availability Active-Active Deployment Model

This section describes the services supported for High Availability.

- **SD-LAN**: Software-Defined Local Area Network (SD-LAN) leverages the principles of software-defined networking for LANs. By implementing SD-LAN, resources and bandwidth can be virtually controlled and managed.

Failure and Expected Behavior

Whenever a node fails, all the APs which are tunneling to that node, will start tunneling to other available nodes in the cluster.

TABLE 4 LAN, Node, and Cluster Link Failure and Expected Behavior - AA HA

Failure Type	Failure Behavior	Failure Recovery Behavior
LAN Failure	In this case, APs which are tunneling to this node will start tunneling to other available nodes in the cluster.	After the network or link failure is rectified, the node rejoins the cluster.

TABLE 4 LAN, Node, and Cluster Link Failure and Expected Behavior - AA HA (continued)

Failure Type	Failure Behavior	Failure Recovery Behavior
Node Failure	In this case, APs which are tunneling to this node, will start tunneling to other available nodes in the cluster.	After the node initializes, it rejoins the cluster.

RUCKUS Edge Fallback

Active-active deployment ensures scalability and redundancy. In such deployments, each AP selects an ordered list of RUCKUS Edge IPs and begins tunneling to the first Edge device in the list. A keepalive probe continuously checks the liveness of this Edge device. If the response to the probe fails, the AP switches to the next Edge in the list. The first RUCKUS Edge device in the list is referred to as the Primary Edge.

Feature Overview

The RUCKUS Edge Fallback feature allows an AP to reconnect to the Primary Edge device according to the user-configured schedule. This helps balance the load of APs across RUCKUS Edge devices within the Data Center (DC) cluster. The AP will attempt to fall back to the primary RUCKUS Edge only if it is currently connected to a non-Primary Edge device. The fallback schedule offers the following three options for configuring the time interval:

- Daily: Sets the fallback schedule for the specified time each day.
- Weekly: Sets the fallback schedule for the chosen day at the specified time.
- By Interval: Sets the fallback schedule for the designated interval.

Requirements

This feature is disabled by default and can be enabled using the RUCKUS Edge Fallback option toggle switch on the HA Settings page for a specific cluster.

This feature has no special hardware or software requirements for feature enablement or usage.

Considerations

By default, the RUCKUS Edge Fallback feature is disabled. The default fallback schedule when enabled is set to 4 AM daily (local time zone of the venue to which the cluster is applied).

For DMZ tunnelling, fallback schedule configuration for DC cluster need to be configured under DMZ cluster HA setting.

Limitations

The Fallback scheduled time is not automatically adjusted for Daylight Saving Time. Therefore, when exiting Daylight Saving Time, the RUCKUS Edge device will trigger fallback an hour earlier than the scheduled time and while entering Daylight Saving Time, it will trigger fallback an hour later.

Best Practices

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

Prerequisites

You must have a RUCKUS Edge Active-Active High Availability cluster configured to use use this feature. This feature does not apply to standalone RUCKUS Edge devices.

Onboarding a Cluster for Active-Active High-Availability Deployment

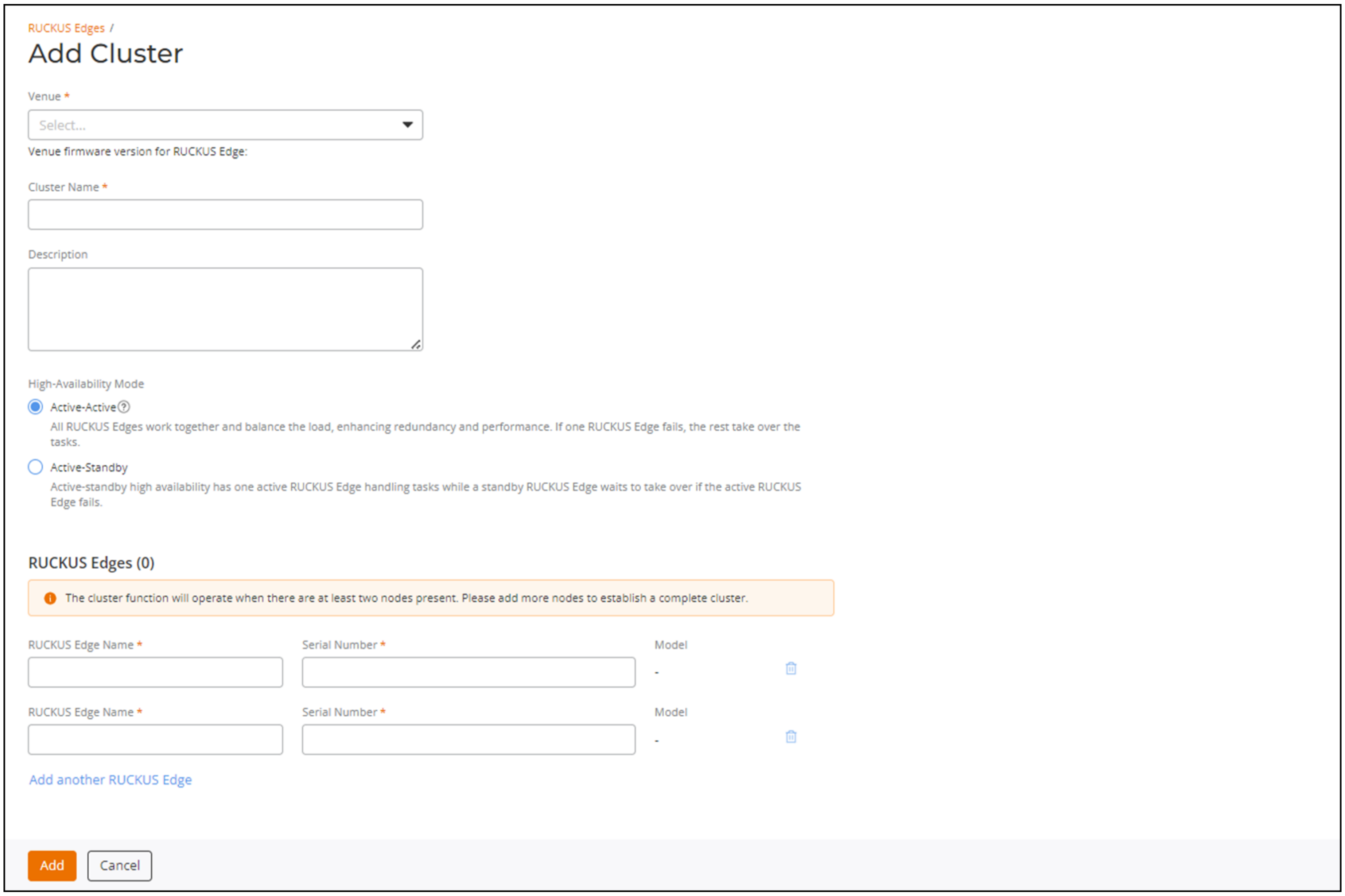
An active-active high-availability cluster must have a minimum of two nodes and a maximum of four nodes.

Create a cluster for active-active high-availability as follows:

1. Log in to the RUCKUS One web user interface with your credentials.
2. Create the Venue for adding the device. Refer to #unique_22 for more information.
3. On the RUCKUS One navigation bar, click **Gateway** > **RUCKUS Edge**.

   This displays the **RUCKUS Edge** page.
4. In the **RUCKUS Edge** page, click **Add** and select **Cluster**. This displays the **Add Cluster** page.

   FIGURE 24 Add Cluster

   RUCKUS Edges /

   Add Cluster

   Venue *

   Select...

   Venue firmware version for RUCKUS Edge:

   Cluster Name *

   Description

   High-Availability Mode

   ● Active-Active

   All RUCKUS Edges work together and balance the load, enhancing redundancy and performance. If one RUCKUS Edge fails, the rest take over the tasks.

   ○ Active-Standby

   Active-standby high availability has one active RUCKUS Edge handling tasks while a standby RUCKUS Edge waits to take over if the active RUCKUS Edge fails.

   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
		-
		-

   Add another RUCKUS Edge

   Add Cancel

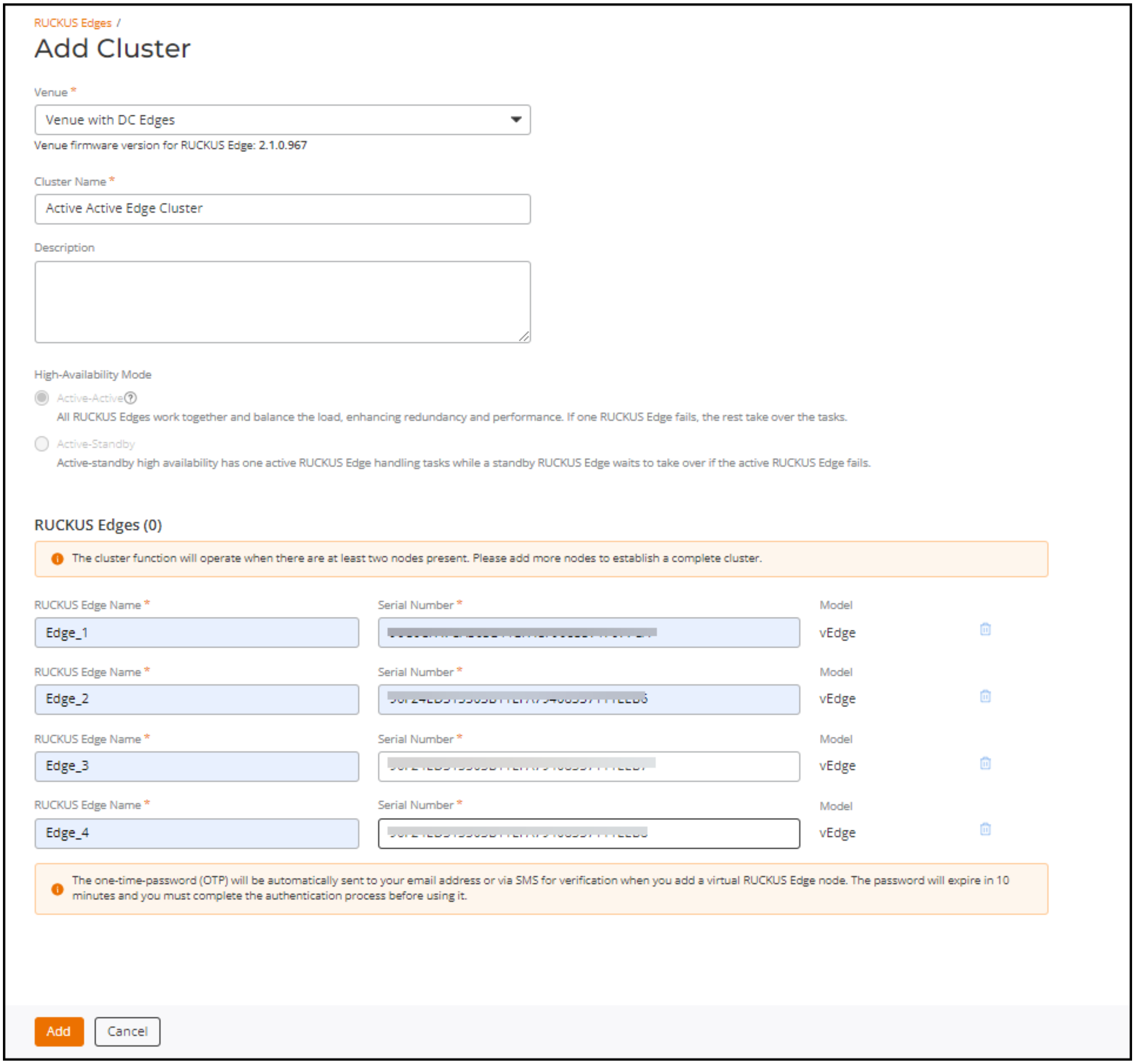
5. In the **Add Cluster** page, enter the following details:
   - **Venue**: Click the drop-down arrow to select a site for the new cluster.
   - **Cluster Name**: Enter a meaningful name for the cluster profile.
   - **Description**: Enter a purposeful statement for the device.
   - **High-Availability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

     All RUCKUS Edge nodes collaborate to balance the load, boosting both redundancy and performance. If one RUCKUS Edge node fails, the others seamlessly take over its tasks.

6. In the **RUCKUS Edges** section, define a minimum of two Edge devices as two nodes are required to establish a complete cluster. You can add a maximum of four nodes per cluster. Enter the **RUCKUS Edge Name** and **Serial Number** of the first Edge device in the available fields. To add more Edge devices to the cluster, click the **Add another RUCKUS Edge** option and enter the **RUCKUS Edge Name** and **Serial Number**.
   - **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 an Edge device, click on the **Delete** icon adjacent to the RUCKUS Edge entry.

FIGURE 25 Adding a Four-Node Cluster



RUCKUS Edges /

Add Cluster

Venue *

Venue with DC Edges

Venue firmware version for RUCKUS Edge: 2.1.0.967

Cluster Name *

Active Active Edge Cluster

Description

High-Availability Mode

● Active-Active

All RUCKUS Edges work together and balance the load, enhancing redundancy and performance. If one RUCKUS Edge fails, the rest take over the tasks.

○ Active-Standby

Active-standby high availability has one active RUCKUS Edge handling tasks while a standby RUCKUS Edge waits to take over if the active RUCKUS Edge fails.

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
Edge_1	[redacted]	vEdge
Edge_2	[redacted]	vEdge
Edge_3	[redacted]	vEdge
Edge_4	[redacted]	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.

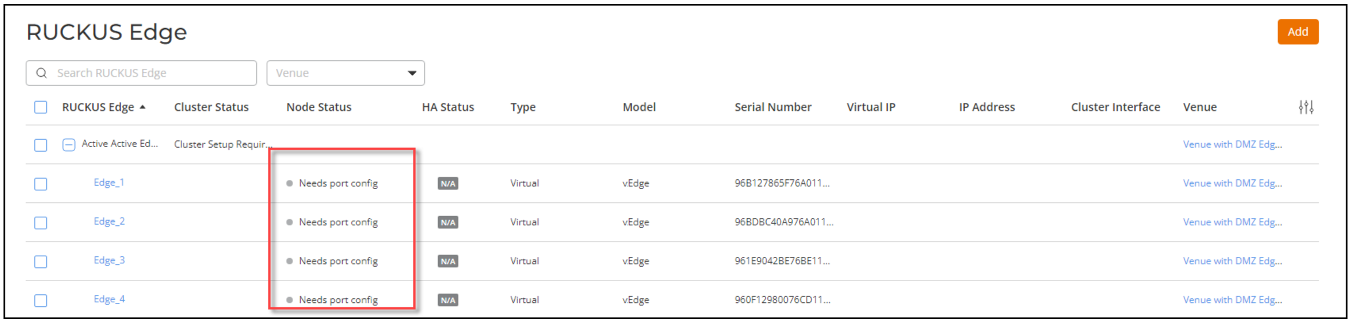
NOTE

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.

7. Click **Add**.

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

FIGURE 26 Node Status



RUCKUS Edge

□	RUCKUS Edge ▲	Cluster Status	Node Status	HA Status	Type	Model	Serial Number	Virtual IP	IP Address	Cluster Interface	Venue
□	⊟ Active Active Ed...	Cluster Setup Requir...									Venue with DMZ Edg...
□	Edge_1		● Needs port config	N/A	Virtual	vEdge	96B127865F76A011...				Venue with DMZ Edg...
□	Edge_2		● Needs port config	N/A	Virtual	vEdge	96BDBC40A976A011...				Venue with DMZ Edg...
□	Edge_3		● Needs port config	N/A	Virtual	vEdge	961E9042BE76BE11...				Venue with DMZ Edg...
□	Edge_4		● Needs port config	N/A	Virtual	vEdge	960F12980076CD11...				Venue with DMZ Edg...

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

Configuring a Cluster for Active-Active High Availability Deployment with a LAG Interface

This task describes configuring a multi-node, active-active high-availability RUCKUS Edge cluster, with a LAG interface, in RUCKUS One.

Prior to performing this procedure, you must have already added the Edge cluster (with HA mode as Active-Active) in RUCKUS One.

Configure a multi-node RUCKUS Edge cluster as follows:

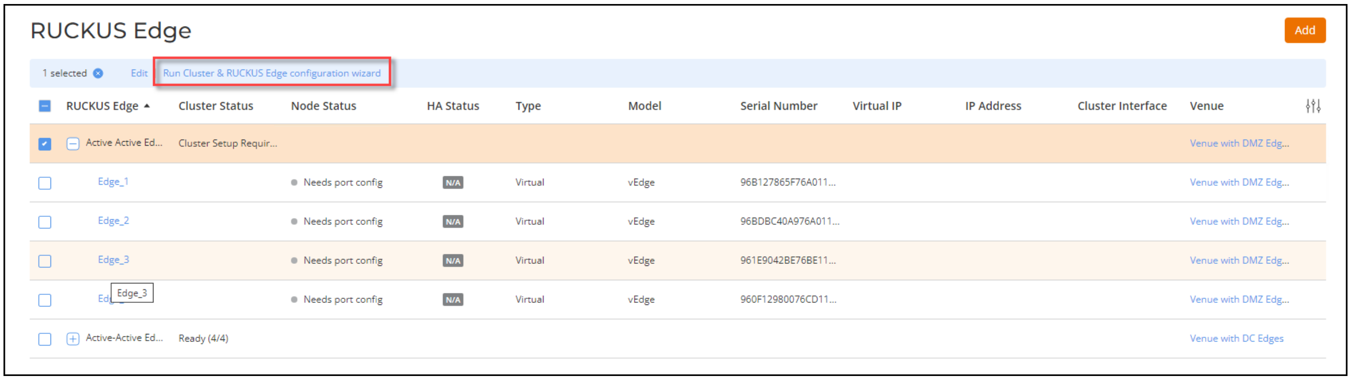
1. Log in to the RUCKUS One web user interface with your credentials.
2. On the RUCKUS One navigation bar, click **Gateway** > **RUCKUS Edge**.

   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 27 Run Cluster and RUCKUS Edge Configuration Wizard

   RUCKUS Edge

☐	RUCKUS Edge ▲	Cluster Status	Node Status	HA Status	Type	Model	Serial Number	Virtual IP	IP Address	Cluster Interface	Venue
☑	⊟ Active Active Ed...	Cluster Setup Requir...									Venue with DMZ Edg...
☐	Edge_1		● Needs port config	N/A	Virtual	vEdge	96B127865F76A011...				Venue with DMZ Edg...
☐	Edge_2		● Needs port config	N/A	Virtual	vEdge	96BDBC40A976A011...				Venue with DMZ Edg...
☐	Edge_3		● Needs port config	N/A	Virtual	vEdge	961E9042BE76BE11...				Venue with DMZ Edg...
☐	Ed Edge_3		● Needs port config	N/A	Virtual	vEdge	960F12980076CD11...				Venue with DMZ Edg...
☐	⊞ Active-Active Ed...	Ready (4/4)									Venue with DC Edges

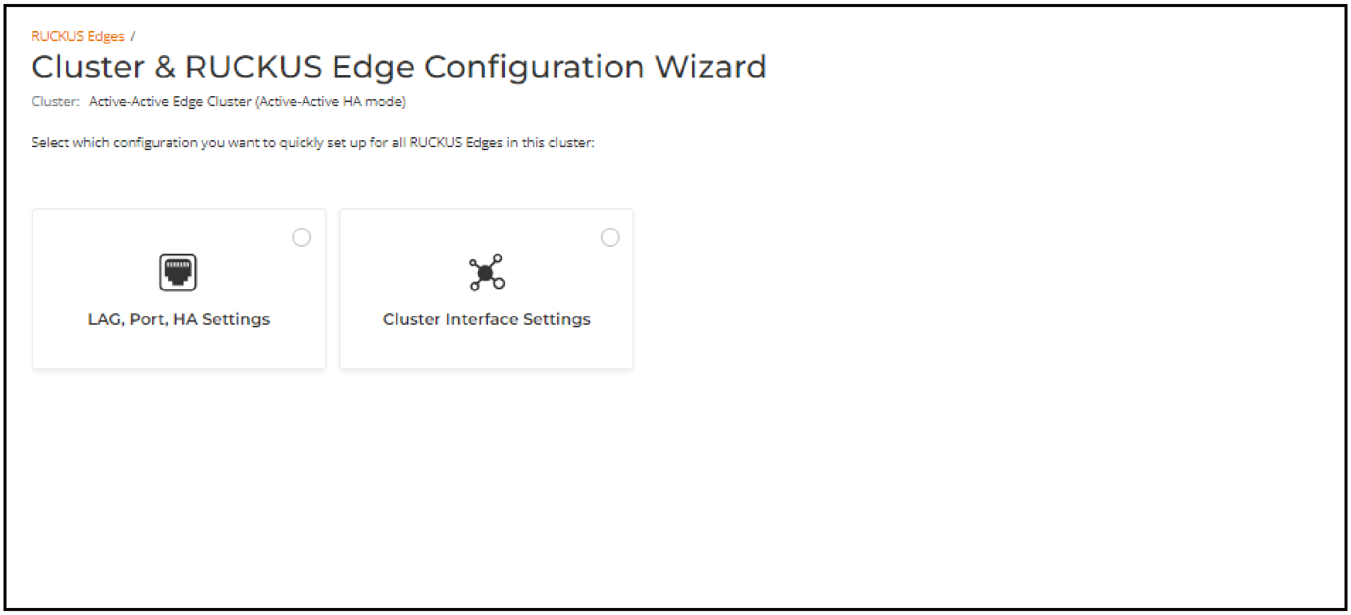
4. Click the **Run Cluster & RUCKUS Edge configuration wizard** option.

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

   - **LAG, Port, & HA Settings**
   - **Cluster Interface Settings**

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

   FIGURE 28 Cluster and RUCKUS Edge Configuration Wizard

   RUCKUS Edges /

   Cluster & RUCKUS Edge Configuration Wizard

   Cluster: Active-Active Edge Cluster (Active-Active HA mode)

   Select which configuration you want to quickly set up for all RUCKUS Edges in this cluster:

   ○ LAG, Port, HA Settings

   ○ Cluster Interface Settings

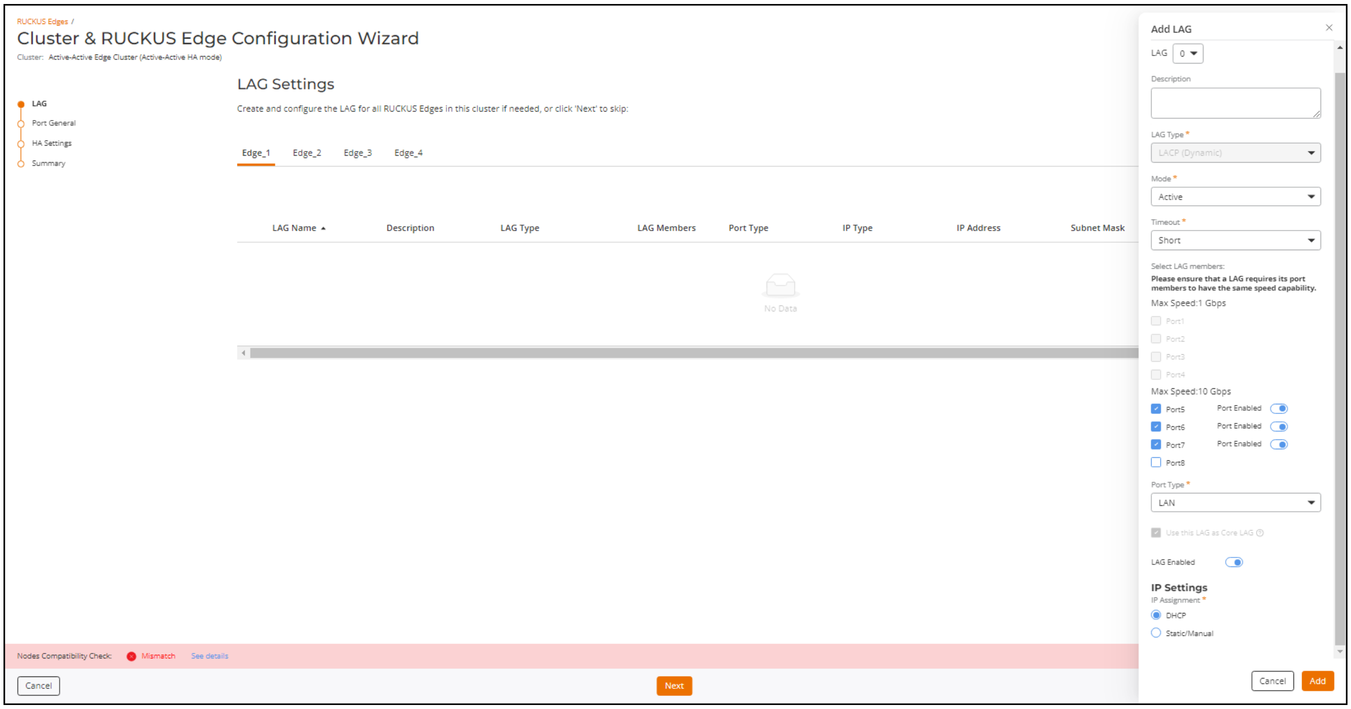
6. Proceed to section Configuring Link Aggregation Group (LAG), Port, and HA Settings on page 47 for configuration details.

Configuring Link Aggregation Group (LAG), Port, and HA Settings

This section describes configuring LAG, Port, and HA Settings for a RUCKUS Edge cluster. The **LAG, Port, & HA Settings** wizard begins on the **LAG Settings** screen, displaying the tab page for the first node in the cluster.

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

   FIGURE 29 Add LAG Settings



RUCKUS Edges /

Cluster & RUCKUS Edge Configuration Wizard

Cluster: Active-Active Edge Cluster (Active-Active HA mode)

LAG Settings

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

LAG Name ▲	Description	LAG Type	LAG Members	Port Type	IP Type	IP Address	Subnet Mask

No Data

Nodes Compatibility Check: ● Mismatch See details

Add LAG

LAG: 0

Description:

LAG Type *: LACP (Dynamic)

Mode *: Active

Timeout *: Short

Select LAG members:

Please ensure that a LAG requires its port members to have the same speed capability.

Max Speed:1 Gbps

□ Port1

□ Port2

□ Port3

□ Port4

Max Speed:10 Gbps

☑ Port5 Port Enabled

☑ Port6 Port Enabled

☑ Port7 Port Enabled

□ Port8

Port Type *: LAN

☑ Use this LAG as Core LAG

LAG Enabled

IP Settings

IP Assignment *

● DHCP

○ Static/Manual

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.

3. Repeat Step 1 on page 20 and Step 2 on page 22 for all other remaining nodes. 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.

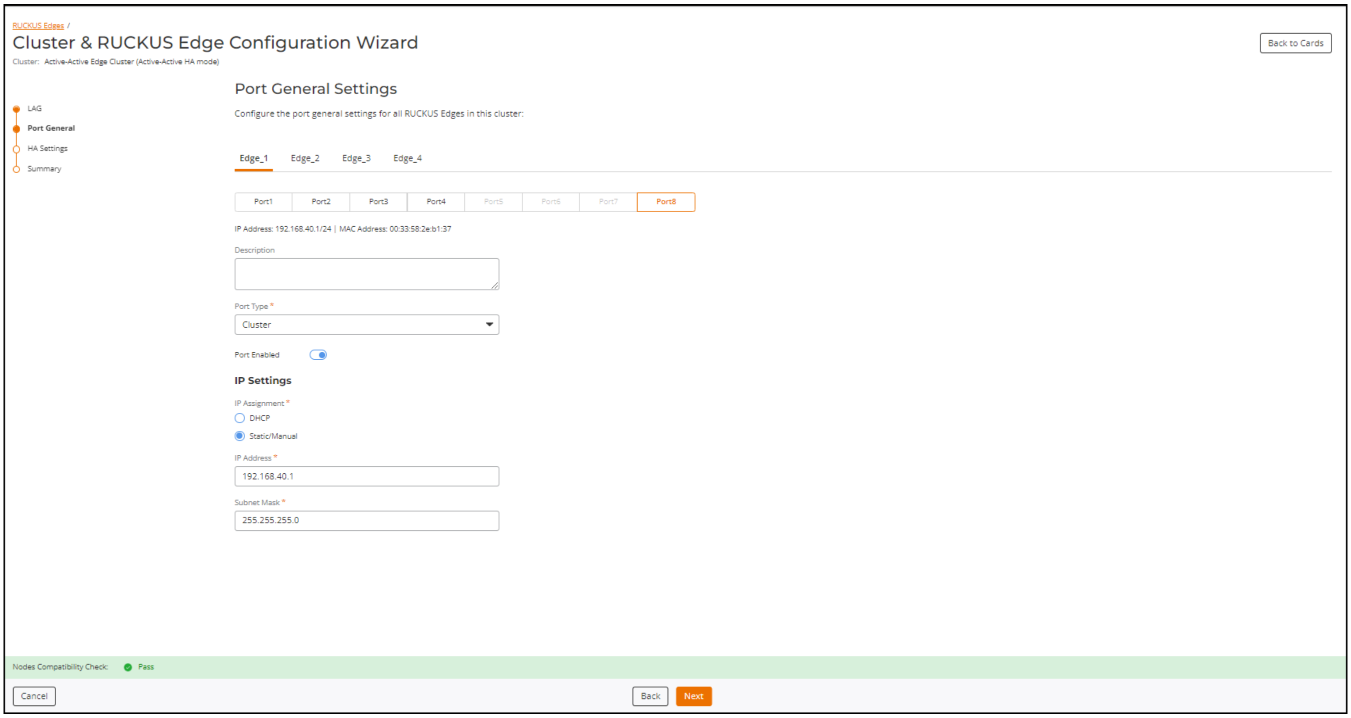
   You can Edit or Delete the offending LAG by selecting the checkbox adjacent to the LAG. After the mismatches are resolved, the compatibility check result changes to **Pass**.

4. **Port 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 each of the other node tabs and configure the appropriate port for each node.

FIGURE 30 RUCKUS Edge LAG, Port, and Virtual IP Settings: Port Settings



Cluster & RUCKUS Edge Configuration Wizard

Cluster: Active-Active Edge Cluster (Active-Active HA mode)

Port General Settings

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

IP Address: 192.168.40.1/24 | MAC Address: 00:33:58:2e:b1:37

Description

Port Type * Cluster

Port Enabled ●

IP Settings

IP Assignment *
○ DHCP
● Static/Manual

IP Address * 192.168.40.1

Subnet Mask * 255.255.255.0

Nodes Compatibility Check: Pass

5. After port settings have been configured for all nodes in the cluster, click **Next**. The **HA Settings** page is displayed.
6. (Optional) Toggle the **RUCKUS Edge Fallback** option off to enable the feature.

   NOTE
   For DMZ tunnelling, Fallback schedule configuration for DC cluster need to be configured under DMZ cluster HA setting.

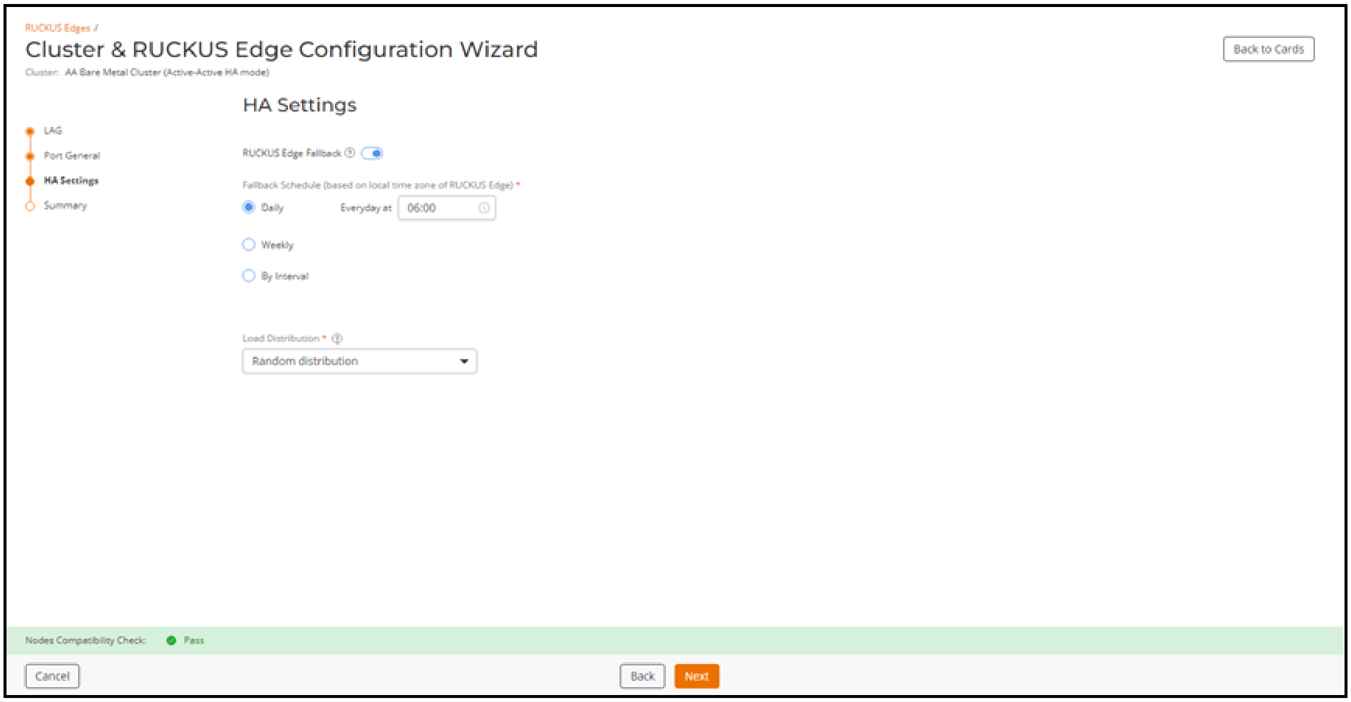
7. Choose one the following Fallback Schedule option.
   - **Daily**: Sets the fallback schedule for the specified time each day.
   - **Weekly**: Sets the fallback schedule for the chosen day at the specified time.
   - **By Interval**: Sets the fallback schedule for the designated interval.

     NOTE
     The scheduled fallback time will align with the local time zone of the venue, ensuring the fallback operations occur at the correct local time.

     NOTE
     Fallback scheduled time is not automatically adjusted for Daylight Saving Time. Therefore, when exiting Daylight Saving Time, the RUCKUS Edge device will trigger fallback an hour earlier than the scheduled time and while entering Daylight Saving Time, it will trigger fallback an hour later.

8. Select the **Load Distribution** required from the following drop-down options:
   - **Random distribution**: All the APs have a different random list for Edge IPs.
   - **Per AP group distribution**: All the APs in the same AP group will have the same random list of Edge IPs of the active-active cluster.

FIGURE 31 High Availability Settings



RUCKUS Edges /

Cluster & RUCKUS Edge Configuration Wizard

Cluster: AA Bare Metal Cluster (Active-Active HA mode)

HA Settings

RUCKUS Edge Fallback: on

Fallback Schedule (based on local time zone of RUCKUS Edge) *

● Daily Everyday at 06:00

○ Weekly

○ By Interval

Load Distribution *: Random distribution

Nodes Compatibility Check: Pass

9. Click **Next**.

   The configuration **Summary** page is displayed, reflecting configuration settings for the cluster.

10. View and verify the configuration details and click **Apply & Continue** proceed to the **Cluster Interface Settings** configuration, or click **Apply & Finish** to complete the **LAG**, **Port**, and **HA Settings** configuration without proceeding to the **Cluster Interface Settings** configuration.

    When the configuration settings are applied to all the Edge devices in the cluster, the **Node Status** changes from **Needs Port Config** to **Operational**, **Cluster Status** displays **Ready #/#** (reflecting how many nodes of the total number of nodes are Ready), and **HA Status** for each node is **Active**.

11. Proceed to section Configuring Cluster Interface Settings on page 50 for configuration details.

Configuring 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 HA Settings** and clicking **Apply & Continue** (as described in Configuring Link Aggregation Group (LAG), Port, and HA Settings on page 47), 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 you want to serve as the cluster interface to the other Edge devices.
   - Enter the **IP Address** and **Subnet Mask** address of cluster interface port.
2. Repeat Step 1 for all other nodes in the cluster.
3. Click **Apply & Finish**.

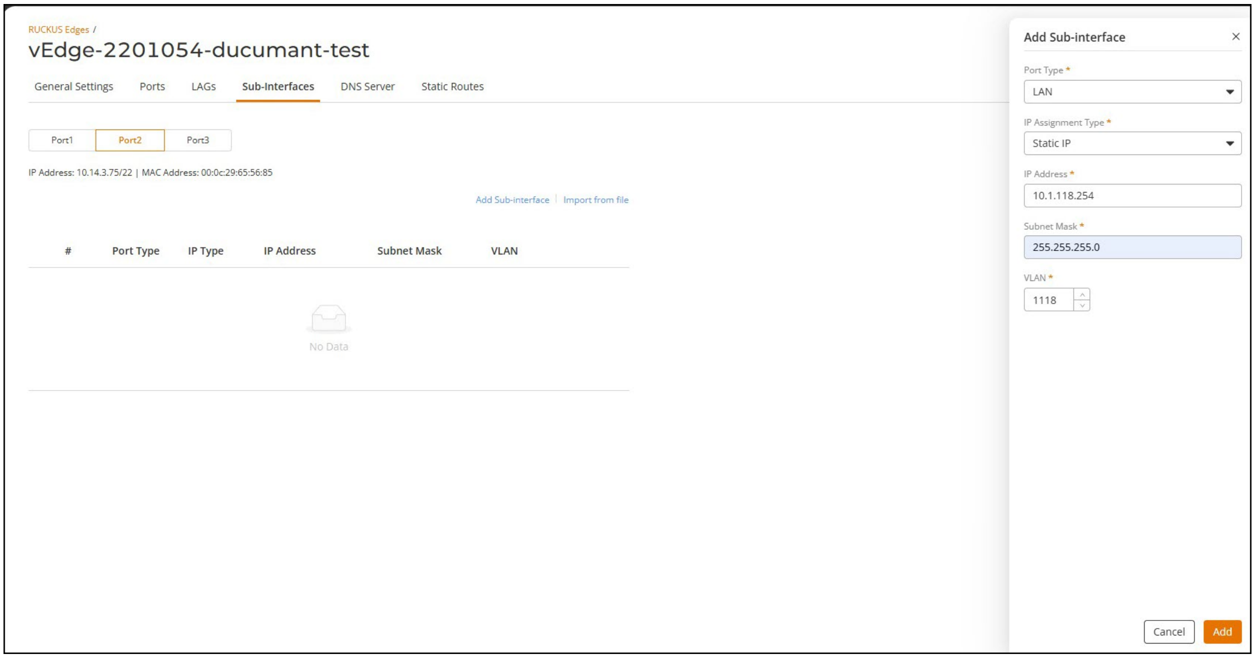
Sub-Interface

1. Click **Sub-Interface** tab and click **Add Sub-Interface**

   This displays **Add Sub-Interface** window.

2. In the **Add Sub-Interface** window, enter the following details:
   - **Port Type** - Select the port type from the drop-down list.
   - **IP Assignment Type** - By default, the IP assignment type is **DHCP**, however, to manually configure the ports, select **Static** from the drop-down list and enter the IP address.

   FIGURE 32 Sub-Interface Port Settings

   RUCKUS Edges /

   vEdge-2201054-ducumant-test

   IP Address: 10.14.3.75/22 | MAC Address: 00:0c:29:65:56:85

#	Port Type	IP Type	IP Address	Subnet Mask	VLAN

   No Data

   Add Sub-interface

   Port Type * LAN

   IP Assignment Type * Static IP

   IP Address * 10.1.118.254

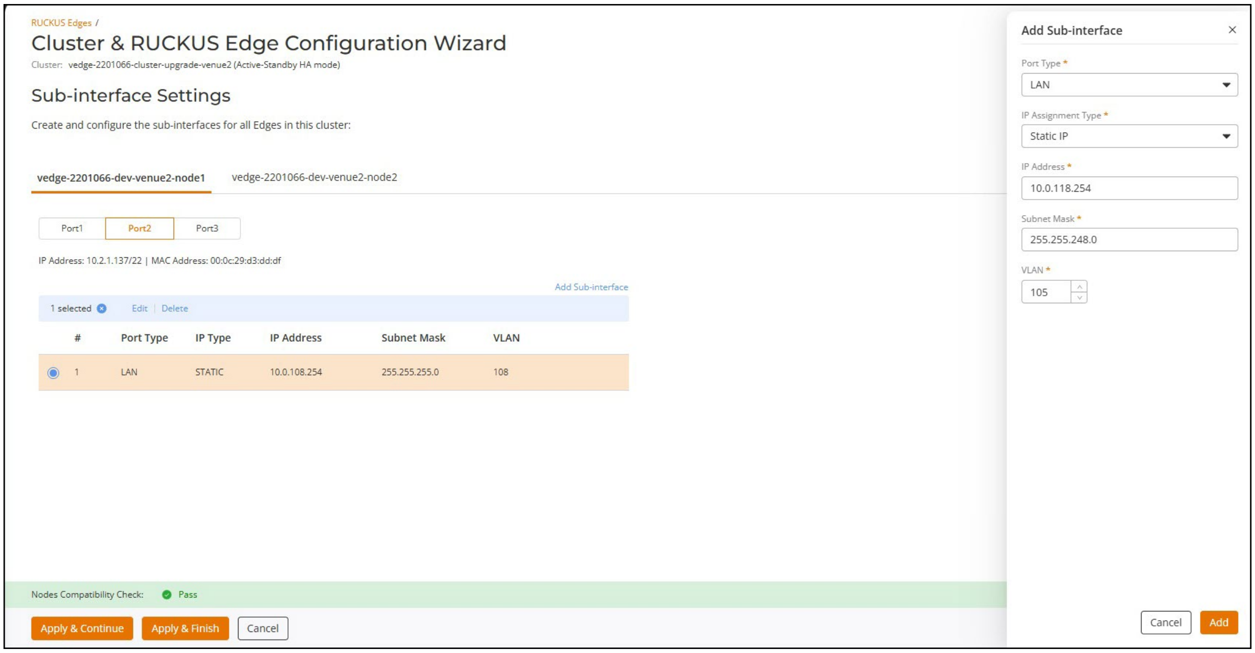
   Subnet Mask * 255.255.255.0

   VLAN * 1118

3. After entering all the details in the respective fields, click **Add**.

4. The sub-interface settings are displayed on the screen.

FIGURE 33 Sub-interface Settings



RUCKUS Edges /

Cluster & RUCKUS Edge Configuration Wizard

Cluster: vedge-2201066-cluster-upgrade-venue2 (Active-Standby HA mode)

Sub-interface Settings

Create and configure the sub-interfaces for all Edges in this cluster:

vedge-2201066-dev-venue2-node1
vedge-2201066-dev-venue2-node2
Port1
Port2
Port3

IP Address: 10.2.1.137/22 | MAC Address: 00:0c:29:d3:dd:df

Add Sub-interface
1 selected
Edit | Delete

	#	Port Type	IP Type	IP Address	Subnet Mask	VLAN
●	1	LAN	STATIC	10.0.108.254	255.255.255.0	108

Nodes Compatibility Check: Pass

Add Sub-interface

Port Type *: LAN

IP Assignment Type *: Static IP

IP Address *: 10.0.118.254

Subnet Mask *: 255.255.248.0

VLAN *: 105

NOTE
Repeat the same steps to add interfaces to **Port 2** and **Port 3**.

5. User can also import file from the local system by clicking **Import from file**. Only .csv (Comma Separated Values) file type with file size not exceeding more than 5MB is allowed to be uploaded.

   NOTE
   User should have routes to reach the loopback of Distribution Switch from RUCKUS Edge and if the user is using external DHCP server then another route to reach the external DHCP server.

Configuring a Cluster for Active-Active 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 multi-node RUCKUS Edge cluster without a LAG as follows:

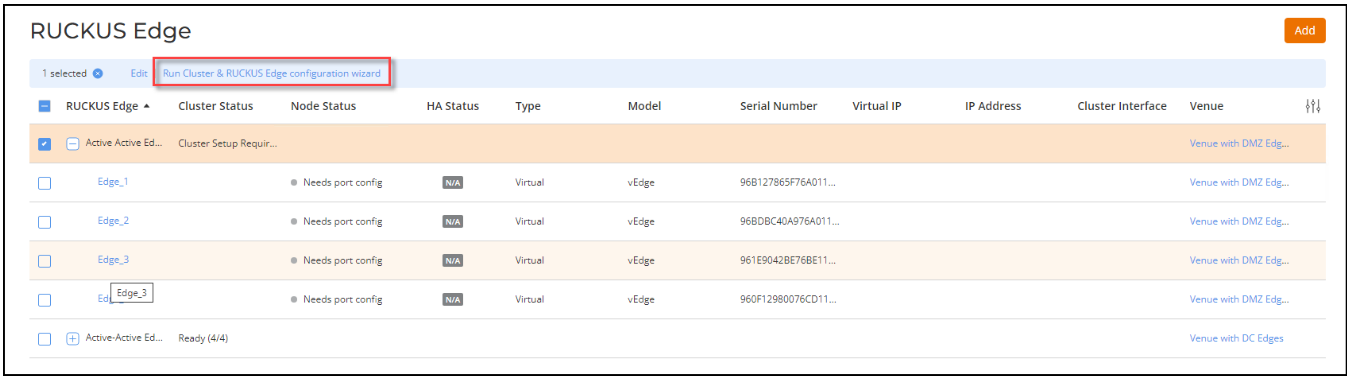
1. Log in to the RUCKUS One web user interface with your credentials.
2. On the RUCKUS One navigation bar, click **Gaeway** > **RUCKUS Edge**.

   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 34 Run Cluster and RUCKUS Edge Configuration Wizard



RUCKUS Edge

☐	RUCKUS Edge	Cluster Status	Node Status	HA Status	Type	Model	Serial Number	Virtual IP	IP Address	Cluster Interface	Venue
☑	Active Active Ed...	Cluster Setup Requir...									Venue with DMZ Edg...
☐	Edge_1		Needs port config	N/A	Virtual	vEdge	96B127865F76A011...				Venue with DMZ Edg...
☐	Edge_2		Needs port config	N/A	Virtual	vEdge	96BDBC40A976A011...				Venue with DMZ Edg...
☐	Edge_3		Needs port config	N/A	Virtual	vEdge	961E9042BE76BE11...				Venue with DMZ Edg...
☐	Ed Edge_3		Needs port config	N/A	Virtual	vEdge	960F12980076CD11...				Venue with DMZ Edg...
☐	Active-Active Ed...	Ready (4/4)									Venue with DC Edges

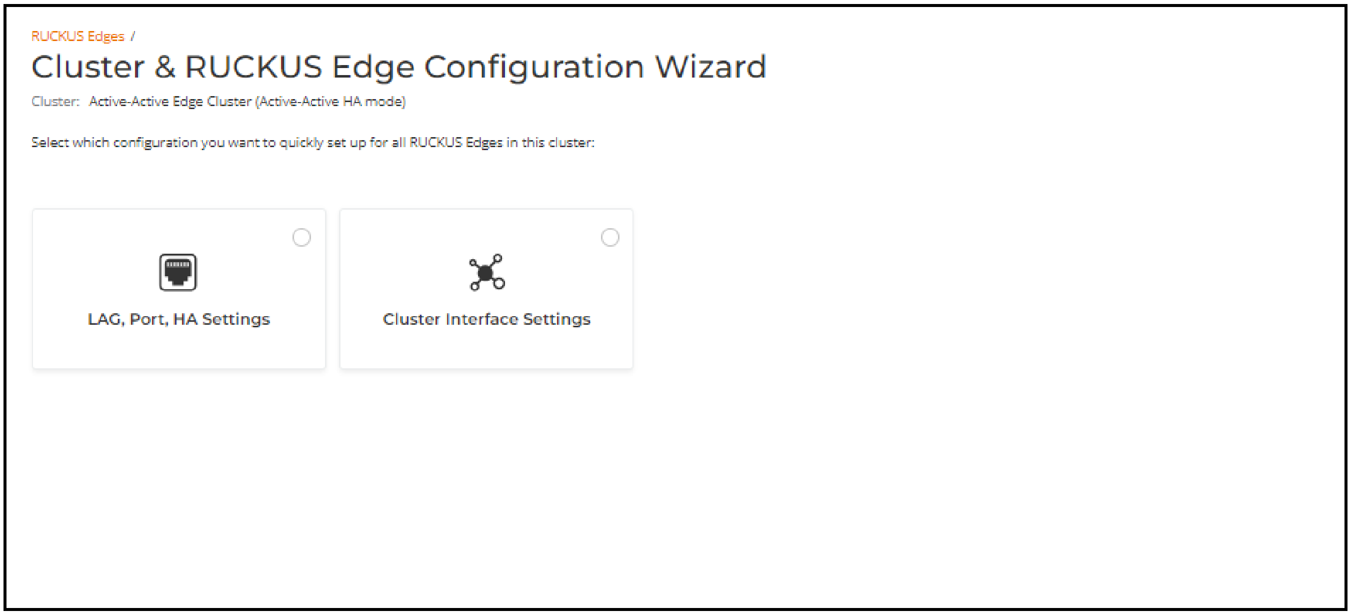
4. Click the **Run Cluster & RUCKUS Edge configuration wizard** option.

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

   - **LAG, Port, and HA Settings**
   - **Cluster Interface Settings**

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

FIGURE 35 Cluster and RUCKUS Edge Configuration Wizard



RUCKUS Edges /

Cluster & RUCKUS Edge Configuration Wizard

Cluster: Active-Active Edge Cluster (Active-Active HA mode)

Select which configuration you want to quickly set up for all RUCKUS Edges in this cluster:

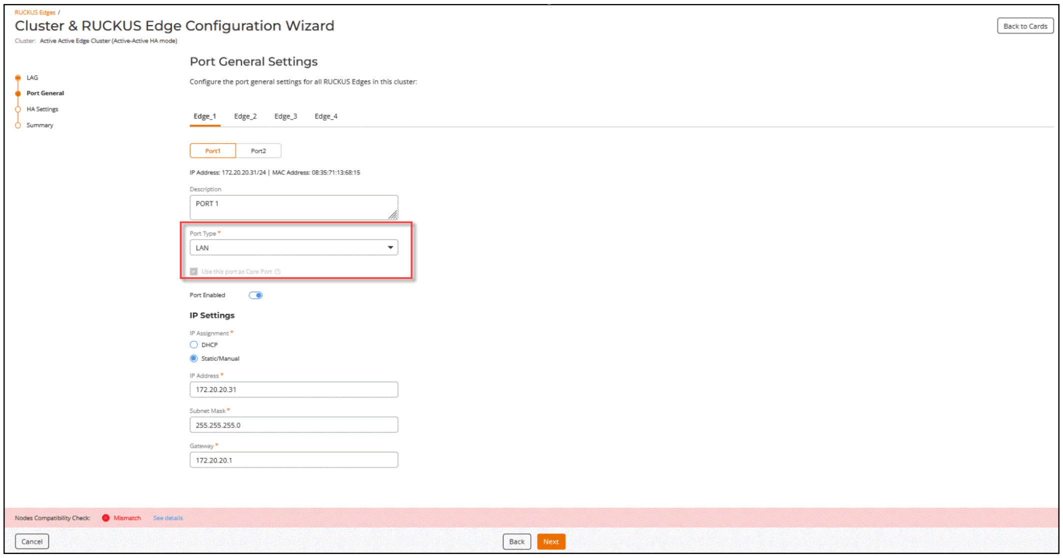
Link Aggregation Group (LAG), Port, and HA Settings

This section describes configuring LAG, Port, and HA Settings for a RUCKUS Edge cluster. The **LAG, Port, & HA Settings** wizard begins on the **LAG Settings** screen, displaying the tab page for the first node in the cluster.

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

2. **Port 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. Because 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 checkbox **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 36 Configuring Ports Without a LAG - Port1



Cluster & RUCKUS Edge Configuration Wizard

Cluster: Active Active Edge Cluster (Active-Active HA mode)

Port General Settings

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

IP Address: 172.20.20.31/24 | MAC Address: 08:35:71:13:68:15

Description: PORT 1

Port Type *: LAN

☑ Use this port as Core Port

Port Enabled: on

IP Settings

IP Assignment *
○ DHCP
● Static/Manual

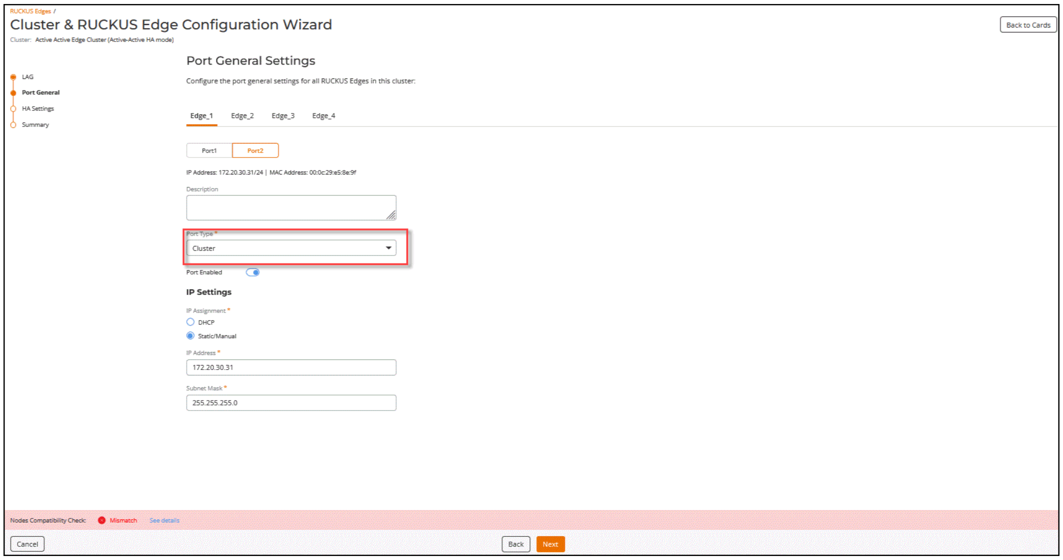
IP Address *: 172.20.20.31

Subnet Mask *: 255.255.255.0

Gateway *: 172.20.20.1

Nodes Compatibility Check: Mismatch See details

FIGURE 37 Configuring Ports Without a LAG - Port2



Cluster & RUCKUS Edge Configuration Wizard

Cluster: Active Active Edge Cluster (Active-Active HA mode)

Port General Settings

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

IP Address: 172.20.30.31/24 | MAC Address: 00:0c:29:e5:8e:9f

Description:

Port Type *: Cluster

Port Enabled: on

IP Settings

IP Assignment *
○ DHCP
● Static/Manual

IP Address *: 172.20.30.31

Subnet Mask *: 255.255.255.0

Nodes Compatibility Check: Mismatch See details

e. Repeat steps List item. through List item. to configure ports for the other RUCKUS Edge devices (nodes) in the cluster, then click **Next**.

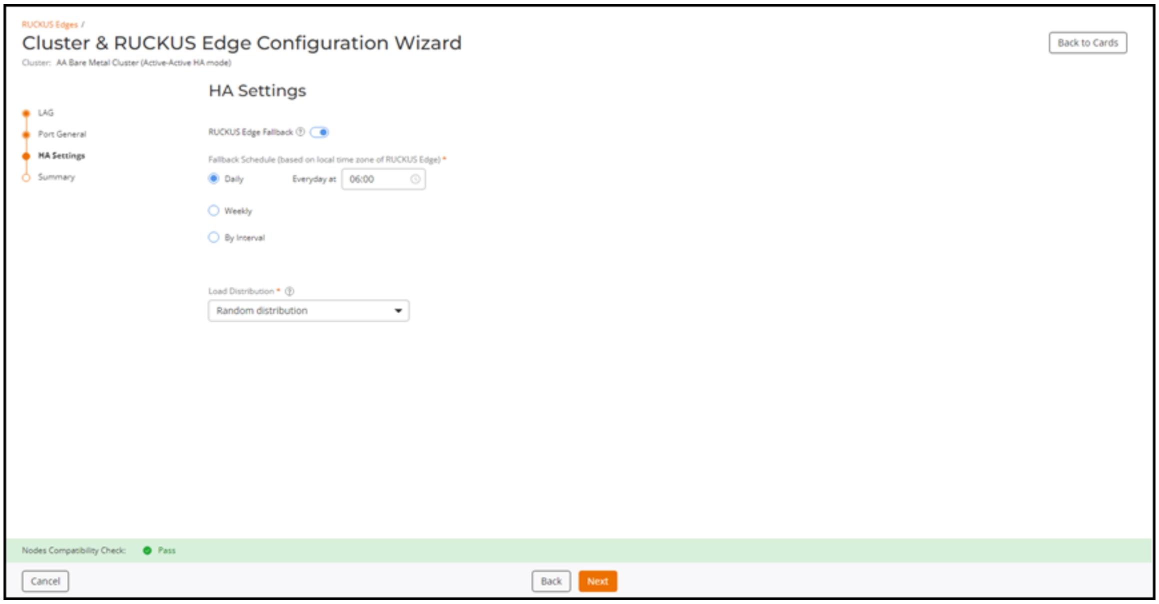
   NOTE
   Use this port as Core Port is utilized for the SD-LAN service, the core port on this RUCKUS Edge establishes tunnels for directing data traffic effectively.

- **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**.

3. After port settings have been configured for all nodes in the cluster, click **Next**. The **HA Settings** page is displayed.

FIGURE 38 HA Settings



RUCKUS Edges /

Cluster & RUCKUS Edge Configuration Wizard

Cluster: AA Bare Metal Cluster (Active-Active HA mode)

HA Settings

RUCKUS Edge Fallback ⓘ

Fallback Schedule (based on local time zone of RUCKUS Edge) *

● Daily Everyday at 06:00

○ Weekly

○ By Interval

Load Distribution * ⓘ

Random distribution

Nodes Compatibility Check: ● Pass

4. (Optional) Toggle the **RUCKUS Edge Fallback** option off to disable the feature.

   NOTE
   For DMZ tunnelling, Fallback schedule configuration for DC cluster need to be configured under DMZ cluster HA setting.

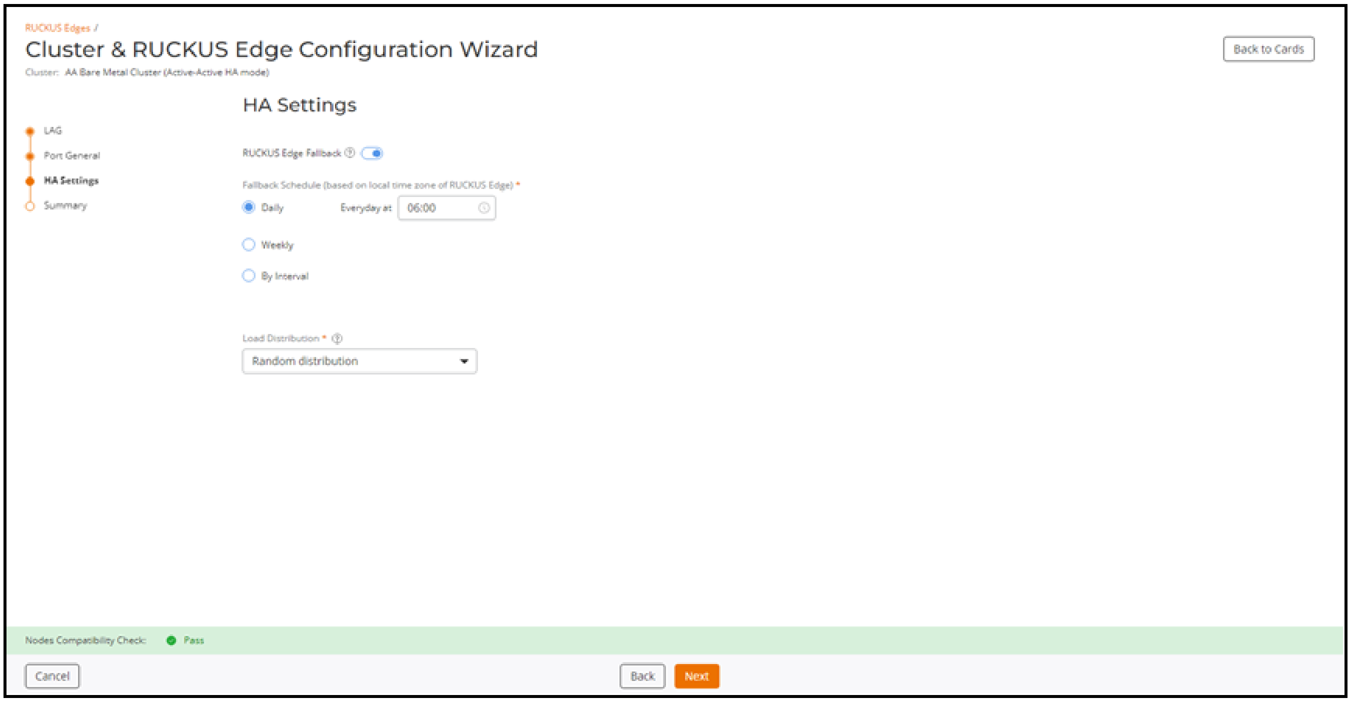
5. Choose one the following Fallback Schedule option.
   - **Daily**: Sets the fallback schedule for the specified time each day.
   - **Weekly**: Sets the fallback schedule for the chosen day at the specified time.
   - **By Interval**: Sets the fallback schedule for the designated interval.

   NOTE
   The scheduled fallback time will align with the local time zone of the venue, ensuring the fallback operations occur at the correct local time.

   NOTE
   Fallback scheduled time is not automatically adjusted for Daylight Saving Time. Therefore, when exiting Daylight Saving Time, the RUCKUS Edge device will trigger fallback an hour earlier than the scheduled time and while entering Daylight Saving Time, it will trigger fallback an hour later.

6. Select the **Load Distribution** required from the following drop-down options:
   - **Random distribution**: All the APs have a different random list for Edge IPs.
   - **Per AP group distribution**: All the APs in the same AP group will have the same random list of Edge IPs of the active-active cluster.

FIGURE 39 High Availability Settings



RUCKUS Edges /

Cluster & RUCKUS Edge Configuration Wizard

Cluster: AA Bare Metal Cluster (Active-Active HA mode)

HA Settings

RUCKUS Edge Fallback: on

Fallback Schedule (based on local time zone of RUCKUS Edge) *

● Daily   Everyday at 06:00

○ Weekly

○ By Interval

Load Distribution *: Random distribution

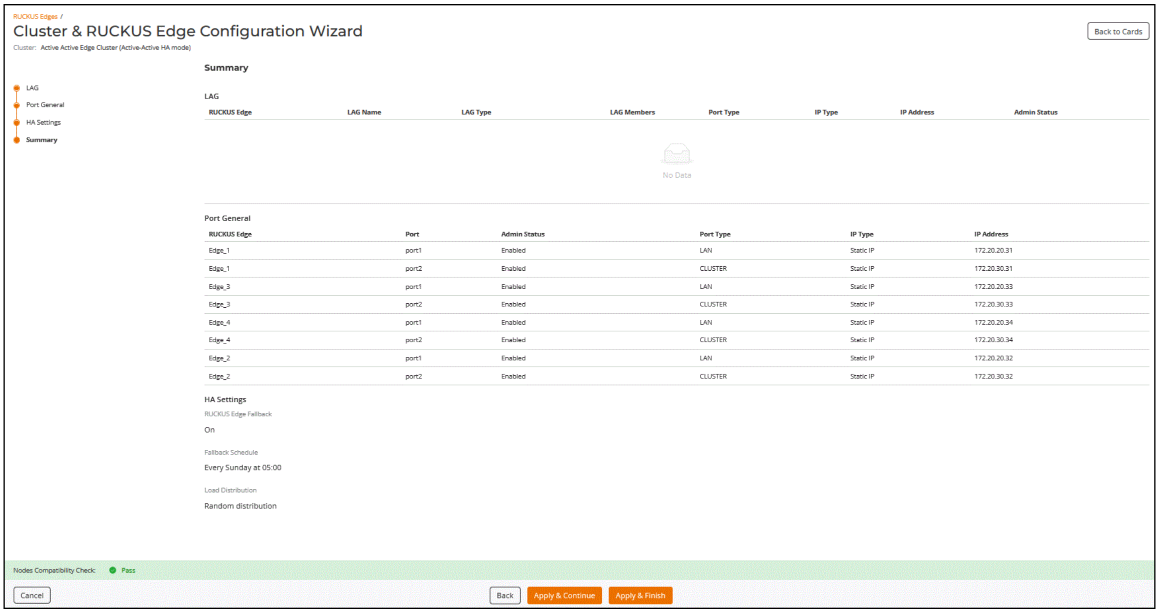
Nodes Compatibility Check: Pass

7. Click **Next**.

   The configuration **Summary** page is displayed, reflecting configuration settings for the cluster.

8. View and verify the configuration details and click **Apply & Continue** to proceed to the **Cluster Interface Settings** configuration, or click **Apply & Finish** to complete the **LAG, Port, and HA Settings** configuration without proceeding to the **Cluster Interface Settings** configuration.

FIGURE 40 Summary of the Cluster Configuration without a LAG



Cluster & RUCKUS Edge Configuration Wizard

Cluster: Active Active Edge Cluster (Active-Active HA mode)

Summary

LAG

RUCKUS Edge	LAG Name	LAG Type	LAG Members	Port Type	IP Type	IP Address	Admin Status

No Data

Port General

RUCKUS Edge	Port	Admin Status	Port Type	IP Type	IP Address
Edge_1	port1	Enabled	LAN	Static IP	172.20.20.31
Edge_1	port2	Enabled	CLUSTER	Static IP	172.20.30.31
Edge_3	port1	Enabled	LAN	Static IP	172.20.20.33
Edge_3	port2	Enabled	CLUSTER	Static IP	172.20.30.33
Edge_4	port1	Enabled	LAN	Static IP	172.20.20.34
Edge_4	port2	Enabled	CLUSTER	Static IP	172.20.30.34
Edge_2	port1	Enabled	LAN	Static IP	172.20.20.32
Edge_2	port2	Enabled	CLUSTER	Static IP	172.20.30.32

HA Settings

RUCKUS Edge Fallback: On

Fallback Schedule: Every Sunday at 05:00

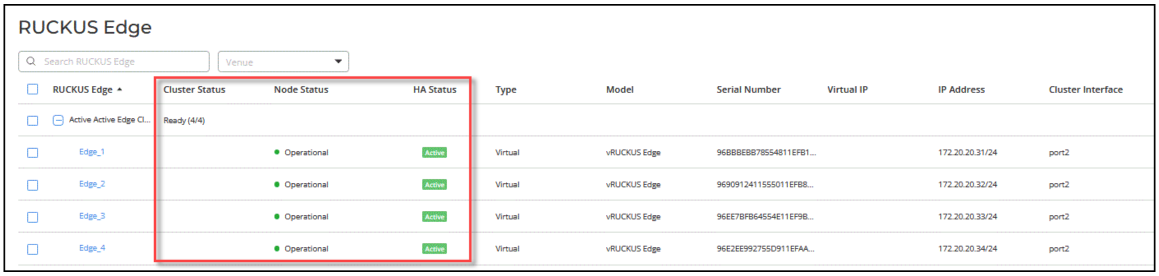
Load Distribution: Random distribution

Nodes Compatibility Check: ● Pass

NOTE

After the nodes are configured, the **Node Status** changes from **Needs Port Config** to **Operational**, **Cluster Status** displays **Ready #/#** (reflecting how many nodes of the total number of nodes are Ready), and **HA Status** for each node is Active.

FIGURE 41 Nodes Status is Operational



RUCKUS Edge	Cluster Status	Node Status	HA Status	Type	Model	Serial Number	Virtual IP	IP Address	Cluster Interface
Active Active Edge Cl...	Ready (4/4)								
Edge_1		● Operational	Active	Virtual	vRUCKUS Edge	96BBBEBB78554811EFB1...		172.20.20.31/24	port2
Edge_2		● Operational	Active	Virtual	vRUCKUS Edge	9690912411555011EFB8...		172.20.20.32/24	port2
Edge_3		● Operational	Active	Virtual	vRUCKUS Edge	96EE7BFB64554E11EF9B...		172.20.20.33/24	port2
Edge_4		● Operational	Active	Virtual	vRUCKUS Edge	96E2EE992755D911EFAA...		172.20.20.34/24	port2

Configuring 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 HA Settings** and clicking **Apply & Continue** (as described in Link Aggregation Group (LAG), Port, and HA Settings on page 54), 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 devices.
   - Enter the **IP Address** and **Subnet Mask** address of cluster interface port.
2. Repeat Step 1 for all other nodes in the cluster.
3. Click **Apply & Finish**.

Editing an Active-Active Cluster and Nodes

You can make changes to the cluster profile and individual nodes comprising a cluster.

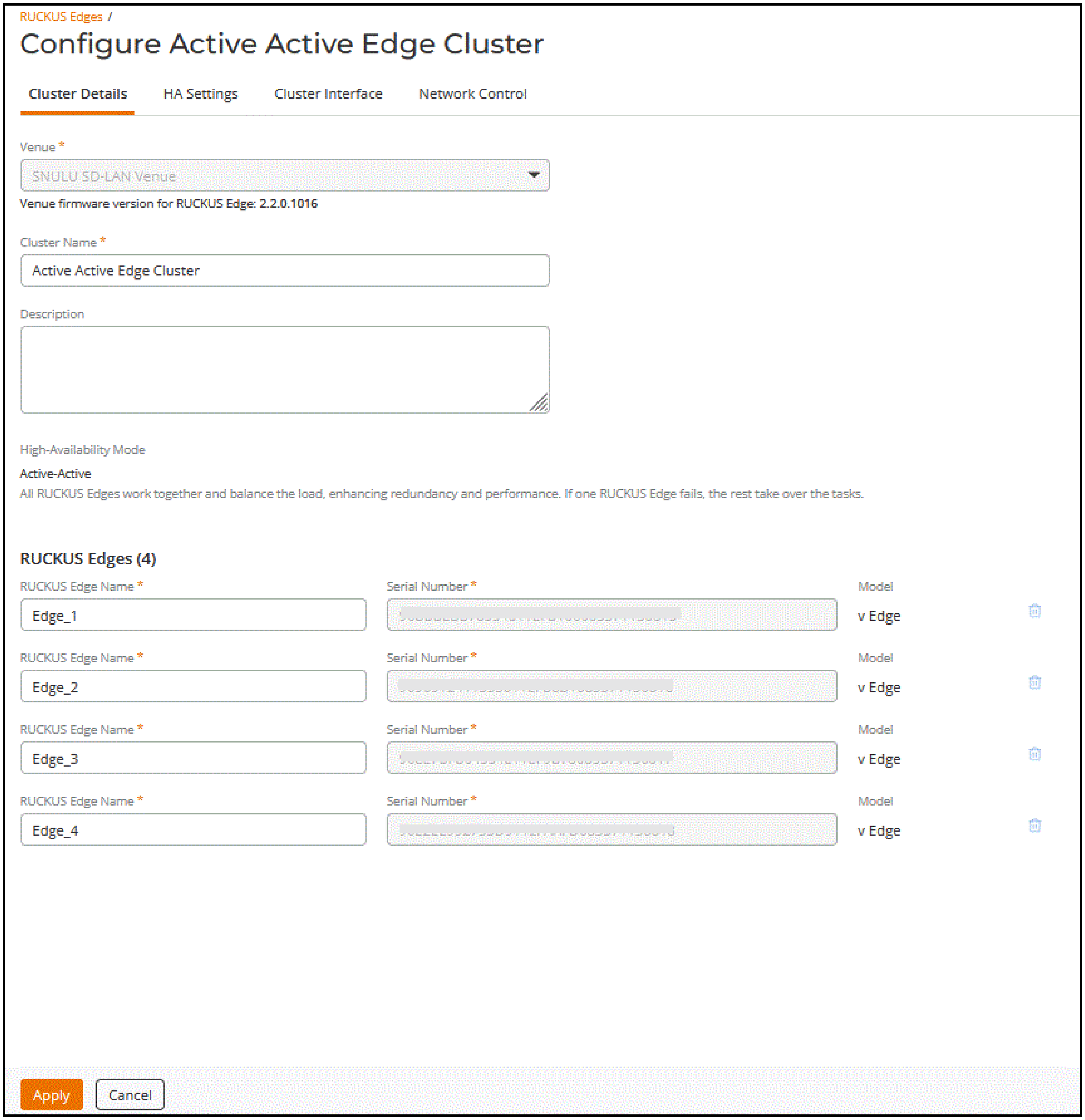
1. Log in to the RUCKUS One web user interface with your credentials.
2. On the RUCKUS One navigation bar, click **Gateway** > **RUCKUS Edge**.

   This displays the list of RUCKUS Edge clusters.
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 the necessary tab and edit the details.
   - **Cluster Details**: Displays general information of the cluster.
   - **HA Settings**: Displays the High Availability settings of the node.
   - **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 selected node.
   - **Network Control**: Displays network control details to configure DHCP Service.

FIGURE 42 Configure <Cluster Name>



RUCKUS Edges /

Configure Active Active Edge Cluster

Venue *
SNULU SD-LAN Venue

Venue firmware version for RUCKUS Edge: 2.2.0.1016

Cluster Name *
Active Active Edge Cluster

Description

High-Availability Mode
Active-Active
All RUCKUS Edges work together and balance the load, enhancing redundancy and performance. If one RUCKUS Edge fails, the rest take over the tasks.

RUCKUS Edges (4)

RUCKUS Edge Name *	Serial Number *	Model
Edge_1	[redacted]	v Edge
Edge_2	[redacted]	v Edge
Edge_3	[redacted]	v Edge
Edge_4	[redacted]	v Edge

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

Onboarding a Single-Node Cluster

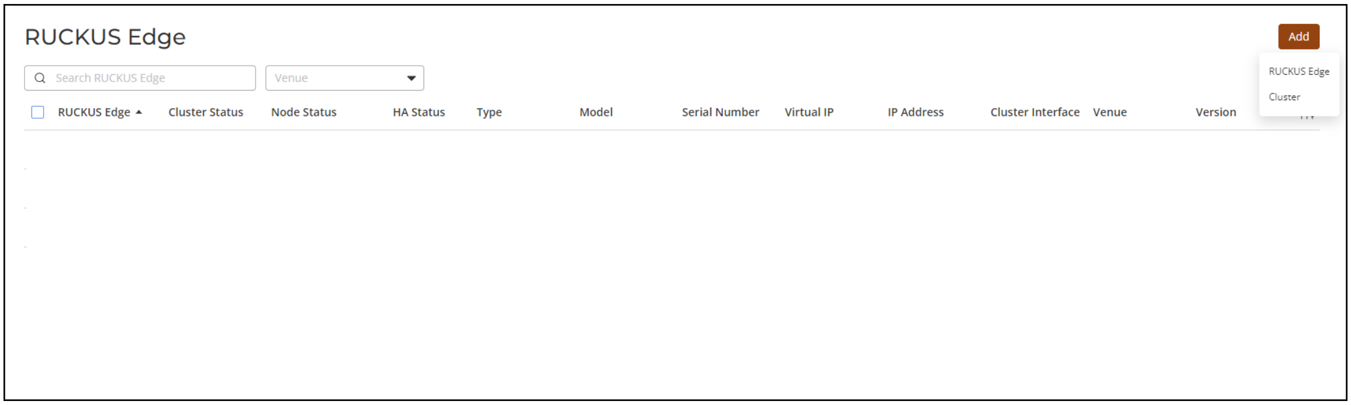
A single-node cluster runs on a standalone RUCKUS Edge device and does not provide redundancy. If the node goes down, the data is lost.

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 **Gateway** > **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 43 Add Cluster

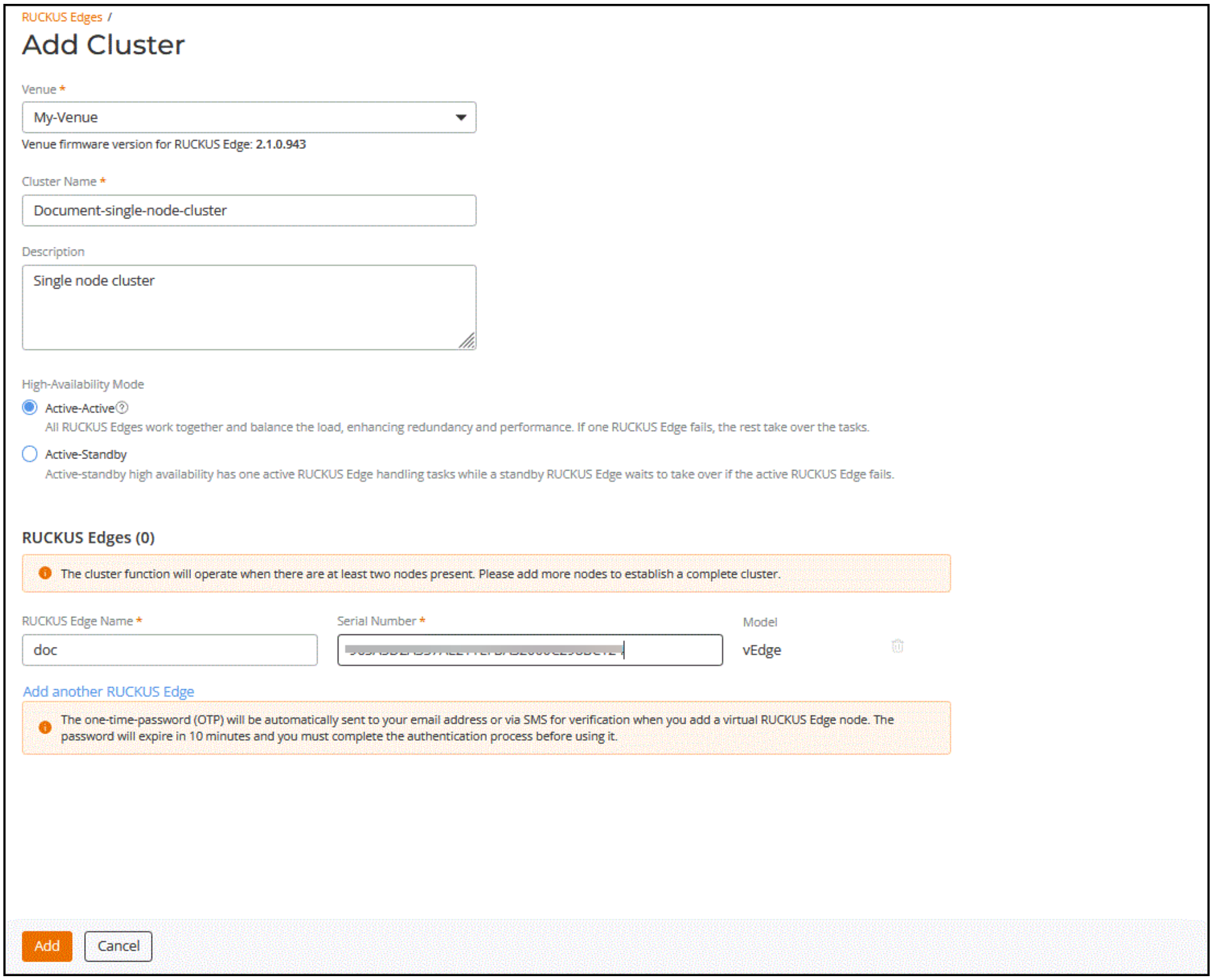
4. In the **Add Cluster** page, enter the following details:
   - **Venue**: Click the drop-down arrow to select a site for the new cluster.
   - **Cluster Name**: Enter a meaningful name for the cluster profile.
   - **Description**: Enter a purposeful statement for the device.
   - **High-Availability Mode**: Select either the **Active-Active** or the **Active-Standby** option. For a single node, HA mode is not significant. However, since the HA mode for the cluster cannot be changed, you may choose to set the HA mode for a single-node cluster, considering future requirements.

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 44 Adding a Single-Node Cluster



RUCKUS Edges /

Add Cluster

Venue * My-Venue

Venue firmware version for RUCKUS Edge: 2.1.0.943

Cluster Name * Document-single-node-cluster

Description Single node cluster

High-Availability Mode

● Active-Active
All RUCKUS Edges work together and balance the load, enhancing redundancy and performance. If one RUCKUS Edge fails, the rest take over the tasks.

○ Active-Standby
Active-standby high availability has one active RUCKUS Edge handling tasks while a standby RUCKUS Edge waits to take over if the active RUCKUS Edge fails.

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
doc	[redacted]	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.

   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.

Link Aggregation Group

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 interfaces 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.

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.

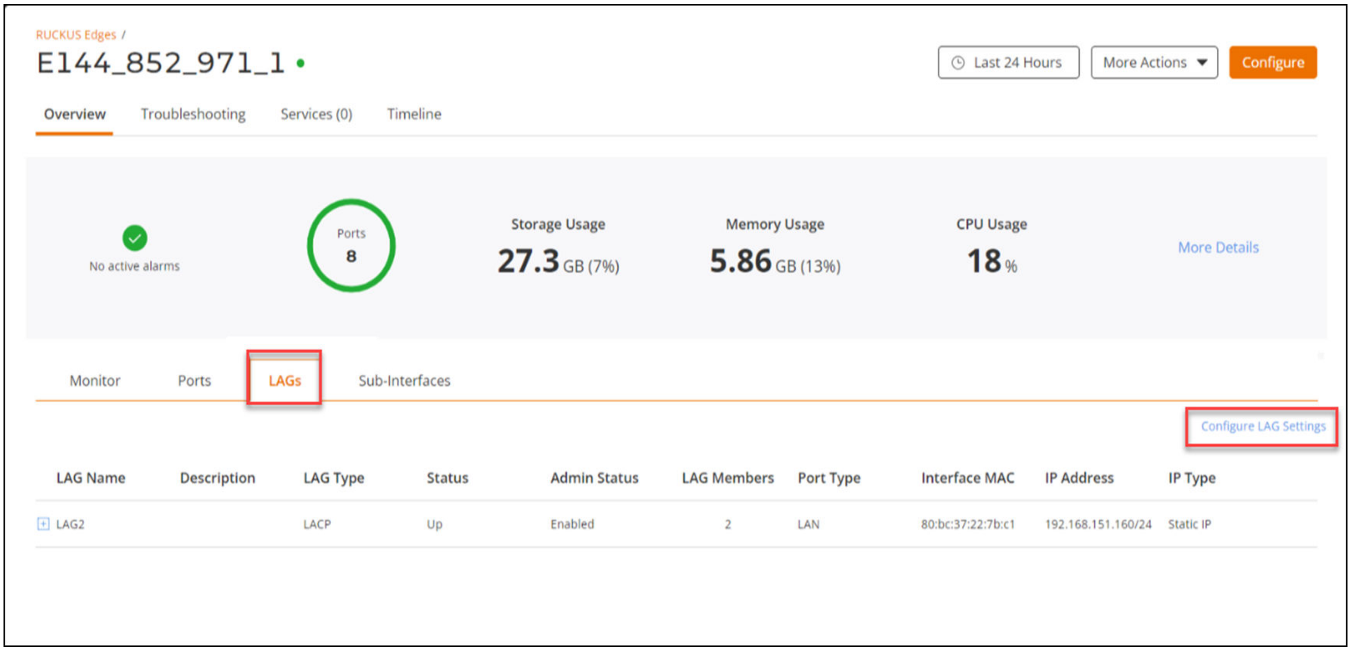
1. On the RUCKUS One navigation bar, click on **Gateway** > **RUCKUS Edge**.

   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 45 LAG Configuration

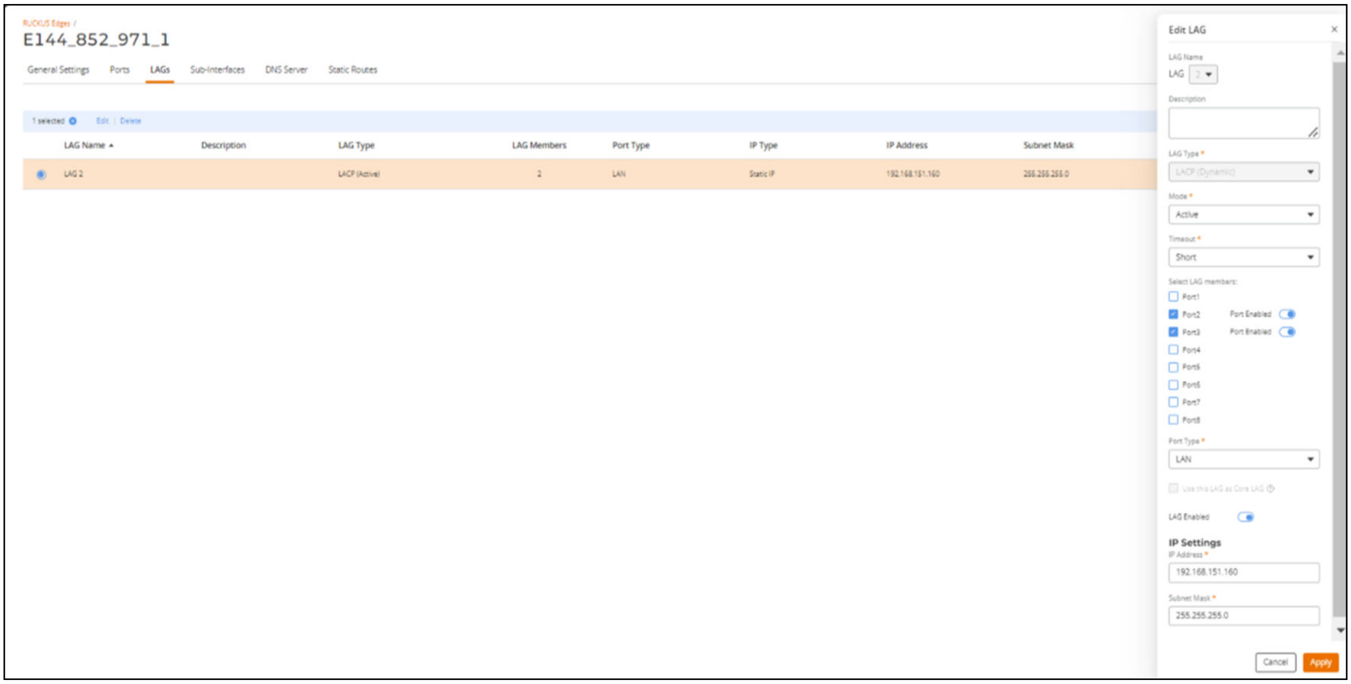


LAG Name	Description	LAG Type	Status	Admin Status	LAG Members	Port Type	Interface MAC	IP Address	IP Type
⊞ LAG2		LACP	Up	Enabled	2	LAN	80:bc:37:22:7b:c1	192.168.151.160/24	Static IP

5. In the **LAGs** page, click **Add LAG**.

   This displays the **Add LAG** sidebar.

   FIGURE 46 Add LAG



RUCKUS Edges /
E144_852_971_1

	LAG Name ▲	Description	LAG Type	LAG Members	Port Type	IP Type	IP Address	Subnet Mask
●	LAG 2		LACP (Active)	2	LAN	Static IP	192.168.151.160	255.255.255.0

Edit LAG

LAG Name: LAG 2

Description:

LAG Type *: LACP (Dynamic)

Mode *: Active

Timeout *: Short

Select LAG members:
- □ Port1
- ☑ Port2 Port Enabled
- ☑ Port3 Port Enabled
- □ Port4
- □ Port5
- □ Port6
- □ Port7
- □ Port8

Port Type *: LAN

□ Use this LAG as Core LAG

LAG Enabled

IP Settings

IP Address *: 192.168.151.160

Subnet Mask *: 255.255.255.0

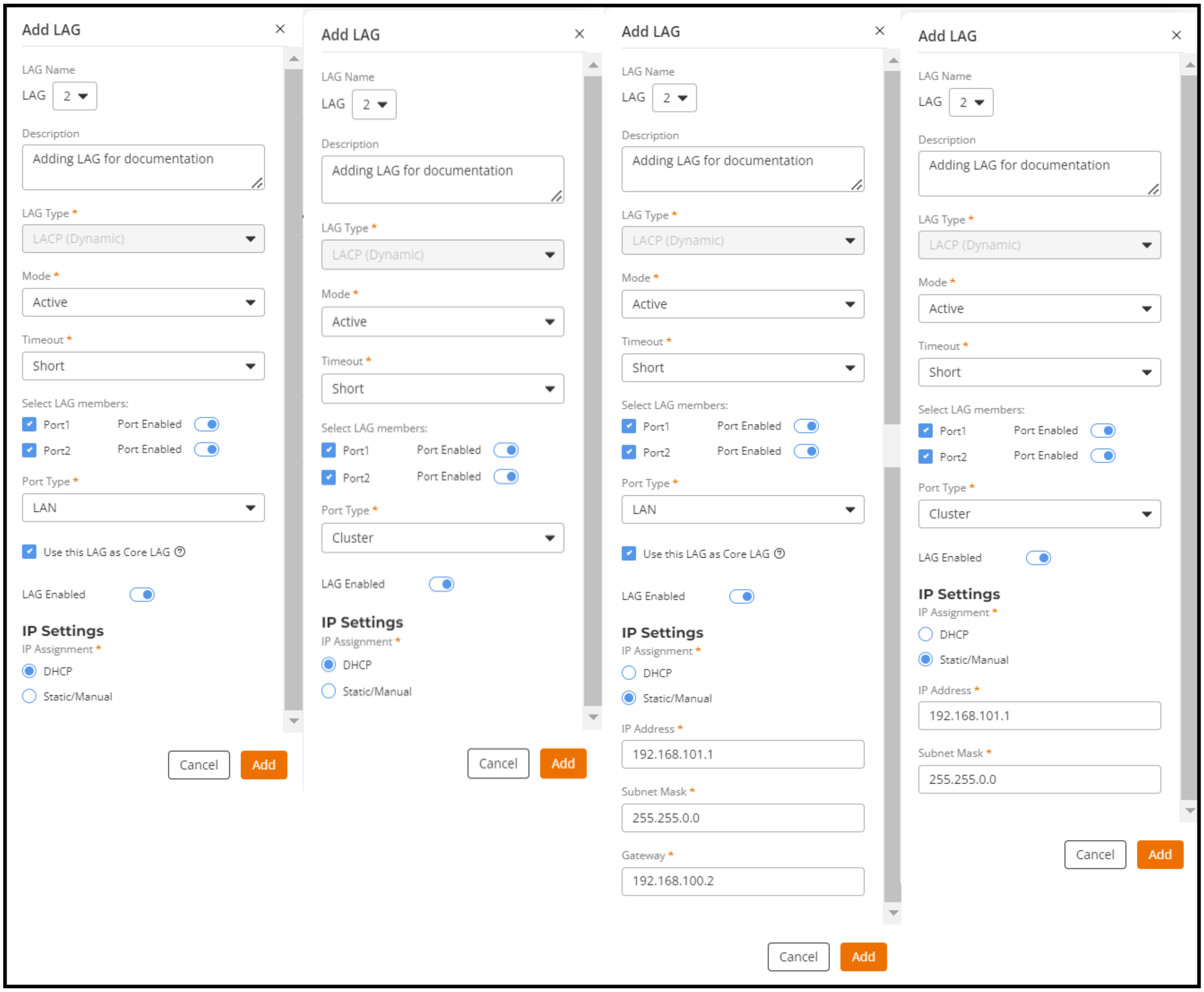
Enter the following details to add a LAG to the RUCKUS Edge device.

- **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 47 Add LAG - Examples of IP Settings Options



Add LAG ×
LAG Name: LAG 2
Description: Adding LAG for documentation
LAG Type *: LACP (Dynamic)
Mode *: Active
Timeout *: Short
Select LAG members:
☑ Port1 Port Enabled
☑ Port2 Port Enabled
Port Type *: LAN
☑ Use this LAG as Core LAG
LAG Enabled
IP Settings
IP Assignment *
● DHCP
○ Static/Manual
Cancel Add

Add LAG ×
LAG Name: LAG 2
Description: Adding LAG for documentation
LAG Type *: LACP (Dynamic)
Mode *: Active
Timeout *: Short
Select LAG members:
☑ Port1 Port Enabled
☑ Port2 Port Enabled
Port Type *: Cluster
LAG Enabled
IP Settings
IP Assignment *
● DHCP
○ Static/Manual
Cancel Add

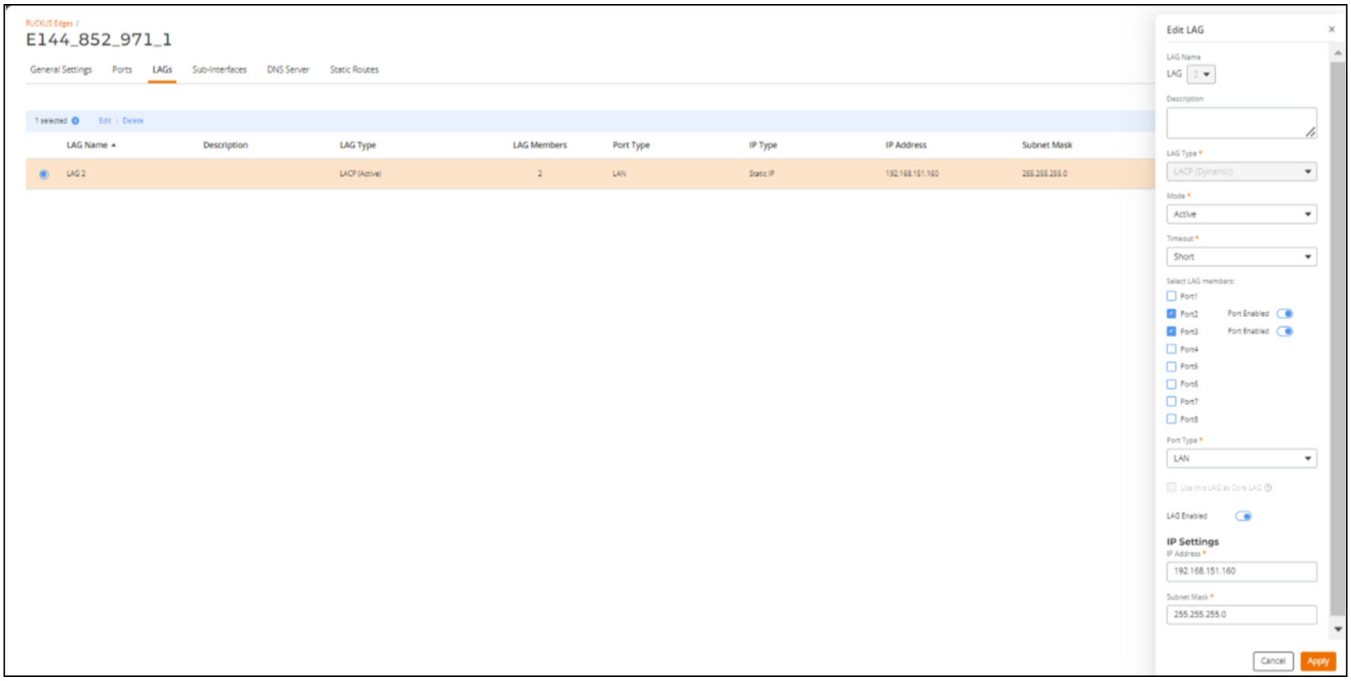
Add LAG ×
LAG Name: LAG 2
Description: Adding LAG for documentation
LAG Type *: LACP (Dynamic)
Mode *: Active
Timeout *: Short
Select LAG members:
☑ Port1 Port Enabled
☑ Port2 Port Enabled
Port Type *: LAN
☑ Use this LAG as Core LAG
LAG Enabled
IP Settings
IP Assignment *
○ DHCP
● Static/Manual
IP Address *: 192.168.101.1
Subnet Mask *: 255.255.0.0
Gateway *: 192.168.100.2
Cancel Add

Add LAG ×
LAG Name: LAG 2
Description: Adding LAG for documentation
LAG Type *: LACP (Dynamic)
Mode *: Active
Timeout *: Short
Select LAG members:
☑ Port1 Port Enabled
☑ Port2 Port Enabled
Port Type *: Cluster
LAG Enabled
IP Settings
IP Assignment *
○ DHCP
● Static/Manual
IP Address *: 192.168.101.1
Subnet Mask *: 255.255.0.0
Cancel Add

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 48 New LAG with Port Information

   RUCKUS Edges /
   E144_852_971_1

	LAG Name ▲	Description	LAG Type	LAG Members	Port Type	IP Type	IP Address	Subnet Mask
●	LAG 2		LACP (Active)	2	LAN	Static IP	192.168.151.160	255.255.255.0

   Edit LAG

   LAG Name: LAG 2

   Description:

   LAG Type *: LACP (Dynamic)

   Mode *: Active

   Timeout *: Short

   Select LAG members:
   ☐ Port1
   ☑ Port2 Port Enabled
   ☑ Port3 Port Enabled
   ☐ Port4
   ☐ Port5
   ☐ Port6
   ☐ Port7
   ☐ Port8

   Port Type *: LAN

   ☐ Use this LAG as Core LAG

   LAG Enabled

   IP Settings

   IP Address *: 192.168.151.160

   Subnet Mask *: 255.255.255.0

Editing a LAG

To edit a LAG port, follow these steps:

1. On the navigation bar, click **Gateway** > **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.

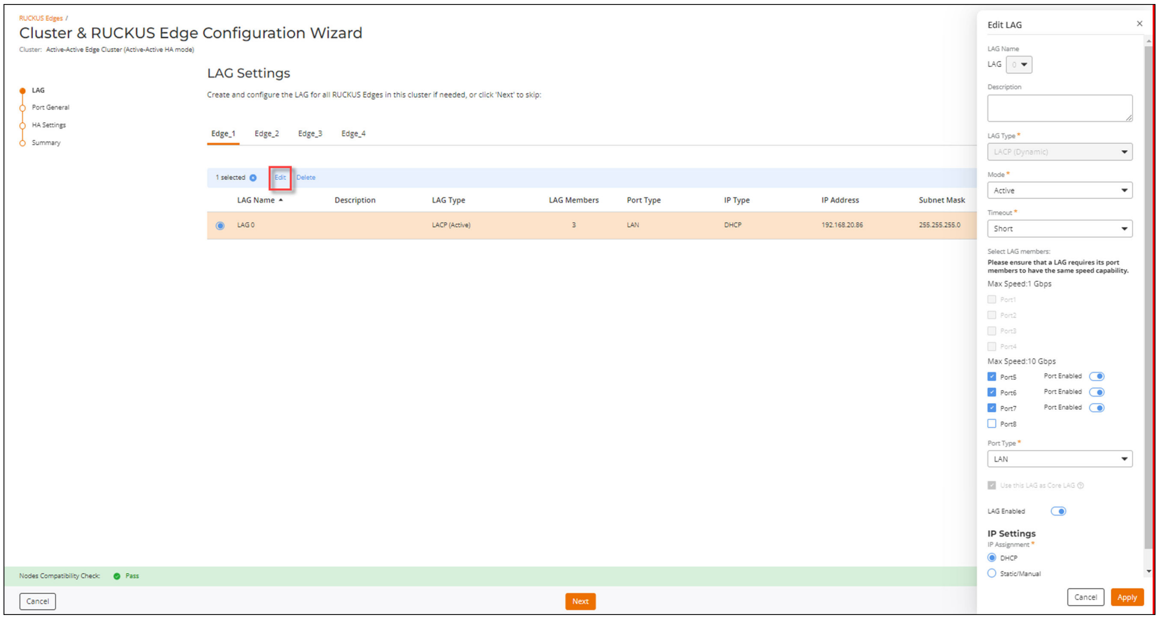
4. In the **General Settings** page, click the **LAGs** tab.

   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 49 Edit LAG



RUCKUS Edges /

Cluster & RUCKUS Edge Configuration Wizard

Cluster: Active-Active Edge Cluster (Active-Active HA mode)

● LAG
○ Port General
○ HA Settings
○ Summary

LAG Settings

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

Edge_1 | Edge_2 | Edge_3 | Edge_4

1 selected ⊗ Edit Delete

	LAG Name ▲	Description	LAG Type	LAG Members	Port Type	IP Type	IP Address	Subnet Mask
●	LAG 0		LACP (Active)	3	LAN	DHCP	192.168.20.86	255.255.255.0

Nodes Compatibility Check: ● Pass

Cancel Next

Edit LAG ×

LAG Name
LAG 0

Description

LAG Type *
LACP (Dynamic)

Mode *
Active

Timeout *
Short

Select LAG members:
Please ensure that a LAG requires its port members to have the same speed capability.

Max Speed:1 Gbps
□ Port1
□ Port2
□ Port3
□ Port4

Max Speed:10 Gbps
☑ Port5 Port Enabled
☑ Port6 Port Enabled
☑ Port7 Port Enabled
□ Port8

Port Type *
LAN

☑ Use this LAG as Core LAG

LAG Enabled

IP Settings
IP Assignment *
● DHCP
○ Static/Manual

Cancel Apply

Deleting a LAG

To delete a LAG port, follow these steps:

1. On the navigation bar, click **Gateway** > **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.

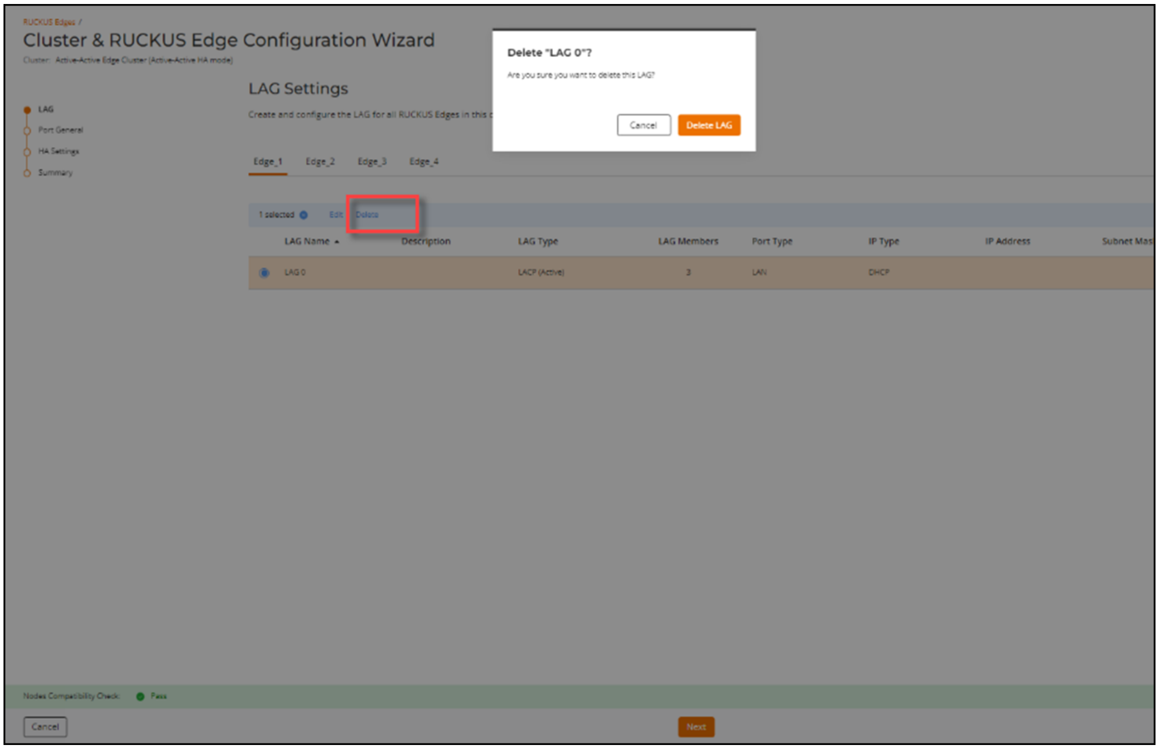
4. In the **General Settings** page, click the **LAGs** tab.

   This displays the **LAGs** page.

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

   This displays the confirm pop-up window. Click **Delete LAG**.

   FIGURE 50 Delete LAG



RUCKUS Edges /
Cluster & RUCKUS Edge Configuration Wizard
Cluster: Active-Active Edge Cluster (Active-Active HA mode)
LAG
Port General
HA Settings
Summary
LAG Settings
Create and configure the LAG for all RUCKUS Edges in this c
Edge_1
Edge_2
Edge_3
Edge_4
1 selected
Edit
Delete

	LAG Name	Description	LAG Type	LAG Members	Port Type	IP Type	IP Address	Subnet Mas
●	LAG 0		LACP (Active)	3	LAN	DHCP		

Delete "LAG 0"?

Are you sure you want to delete this LAG?

Cancel
Delete LAG
Nodes Compatibility Check: Pass
Cancel
Next

Configuring a RUCKUS Edge Link Aggregation Group through Command Line Interface

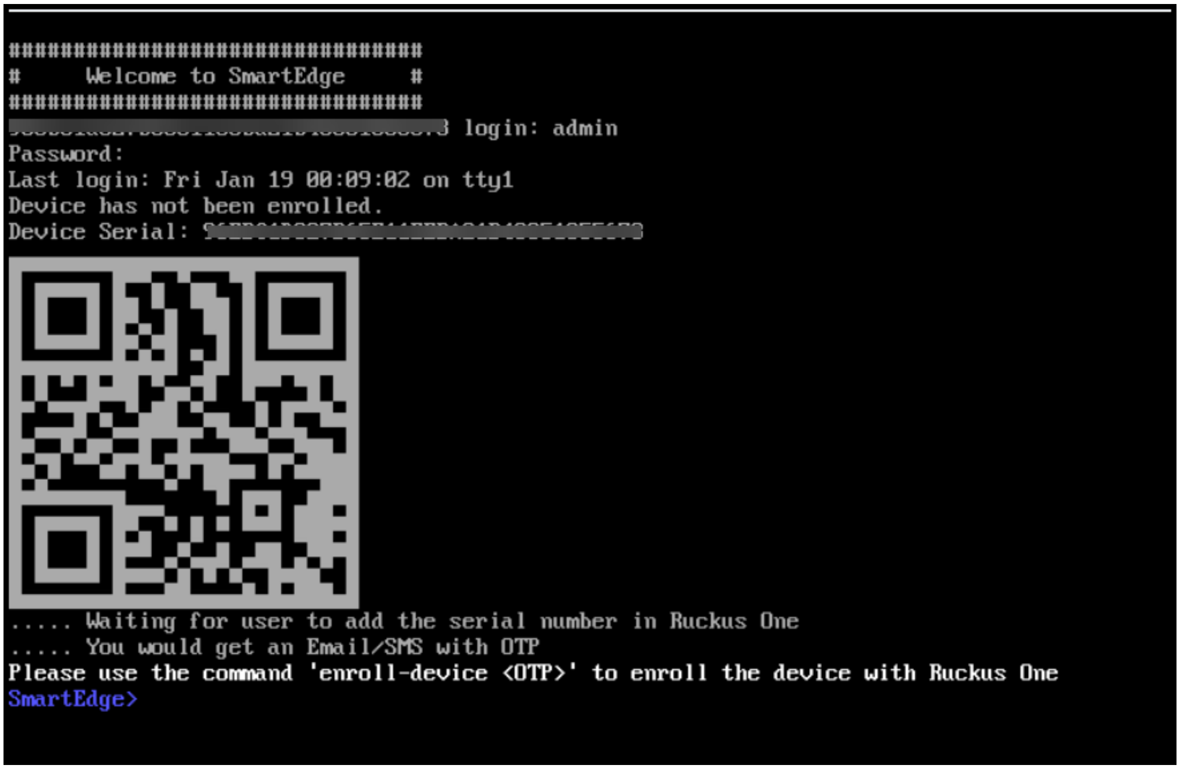
This procedure describes configuring a LAG using the command line interface (CLI). Using CLI enables quick execution of commands and allows more precise control over the system.

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 51 Device Details

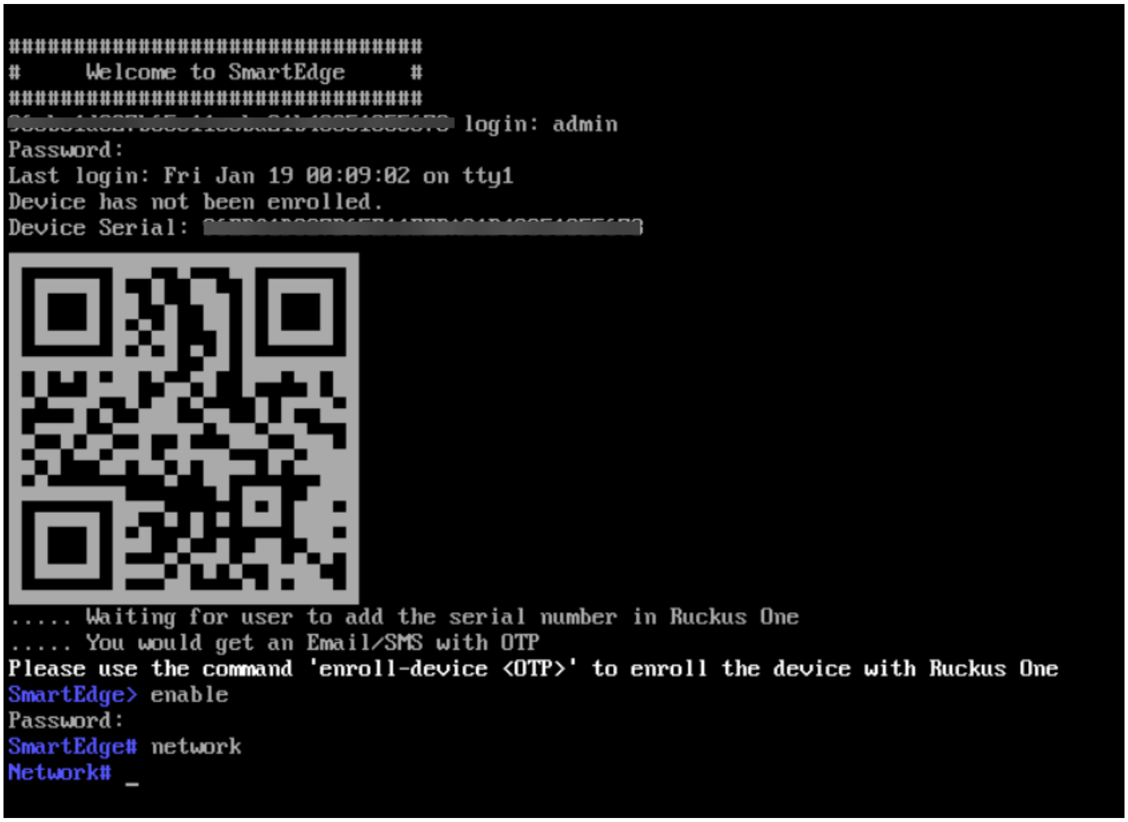


```
###################################
#      Welcome to SmartEdge       #
###################################
[redacted] login: admin
Password:
Last login: Fri Jan 19 00:09:02 on tty1
Device has not been enrolled.
Device Serial: [redacted]
..... Waiting for user to add the serial number in Ruckus One
..... 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.

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

FIGURE 52 enable and network Commands

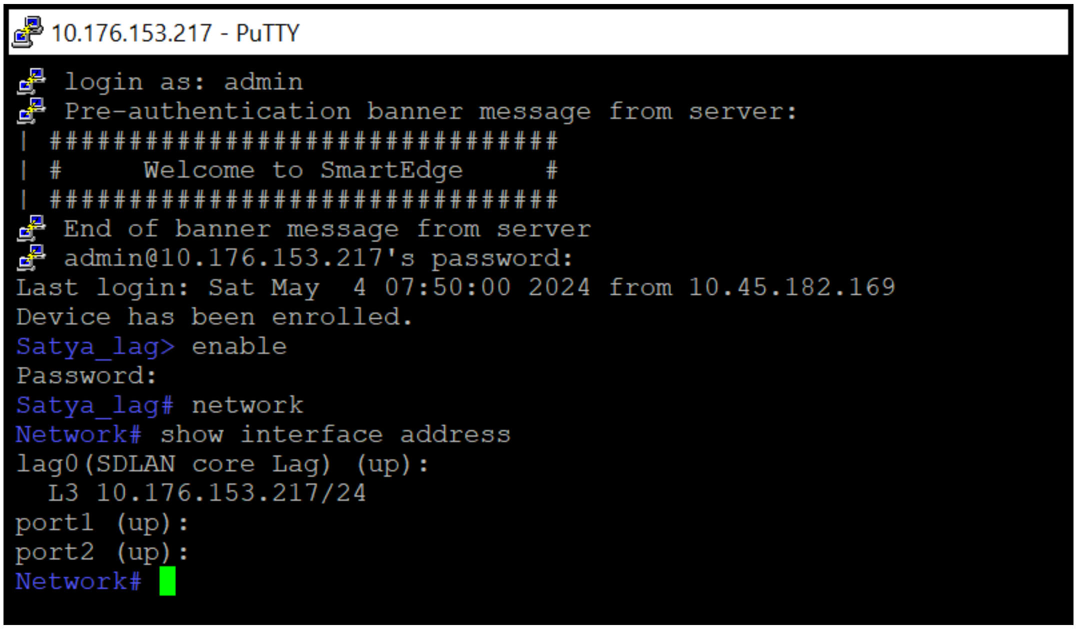


```
##################################
#     Welcome to SmartEdge     #
##################################
[redacted] login: admin
Password:
Last login: Fri Jan 19 00:09:02 on tty1
Device has not been enrolled.
Device Serial: [redacted]
..... Waiting for user to add the serial number in Ruckus One
..... 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# _
```

4. 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 53 show interface address Command



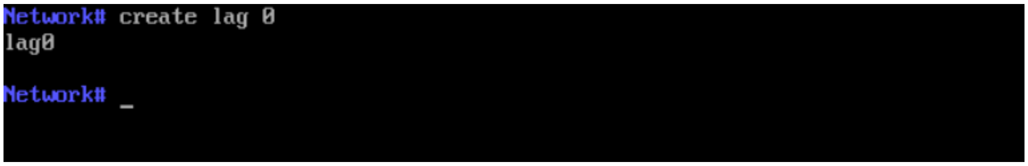
10.176.153.217 - PuTTY

```
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#
```

5. 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 54 Creating a LAG

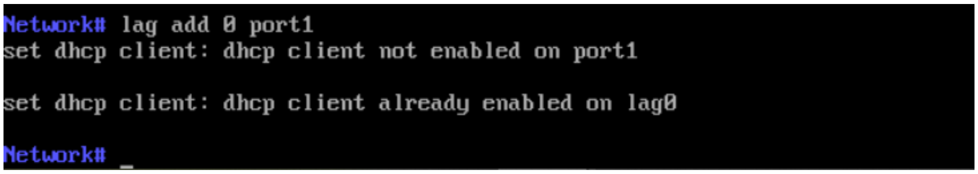


```
Network# create lag 0
lag0

Network# _
```

6. 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 55 Adding a LAG Port

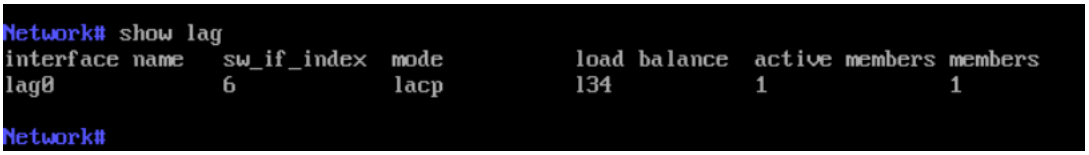
    ```
    Network# lag add 0 port1
    set dhcp client: dhcp client not enabled on port1

    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.

7. (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.

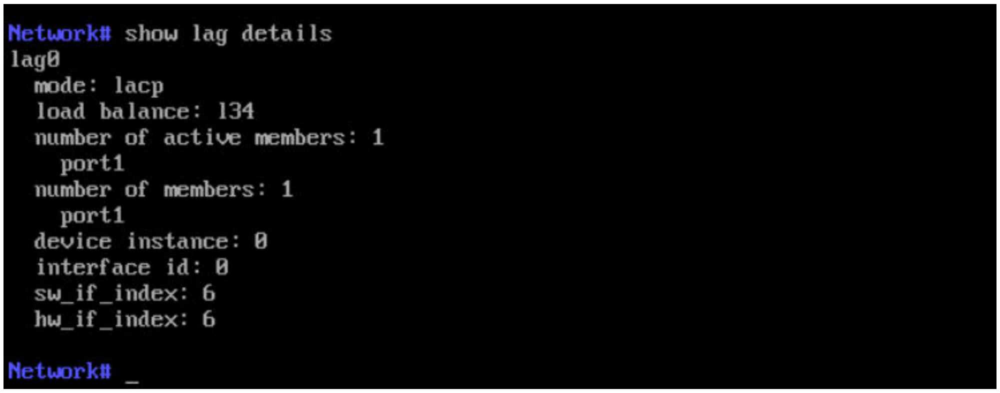
    FIGURE 56 show lag Command

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

    Network#
    ```

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

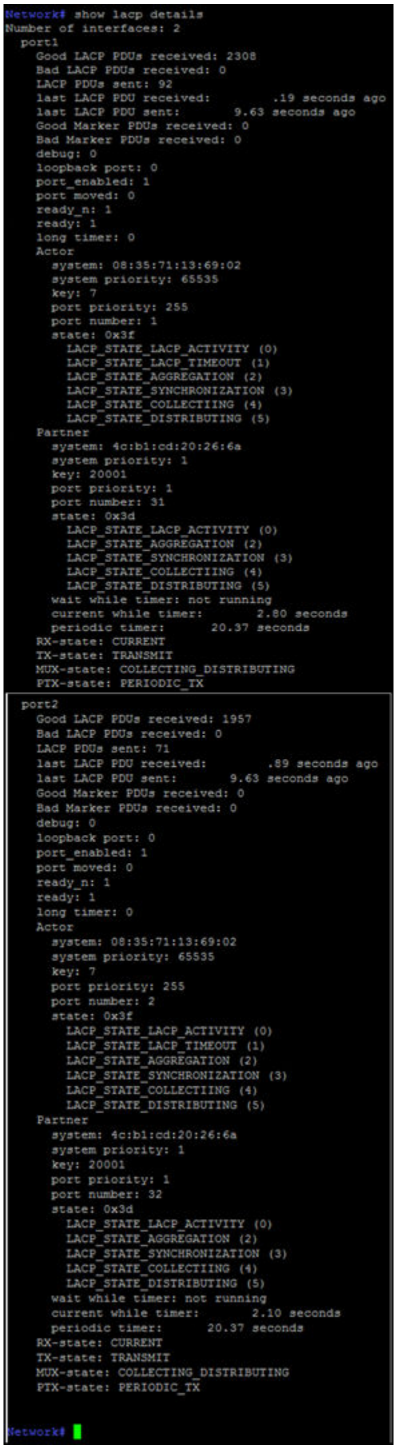
    FIGURE 57 show lag details Command

    ```
    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.

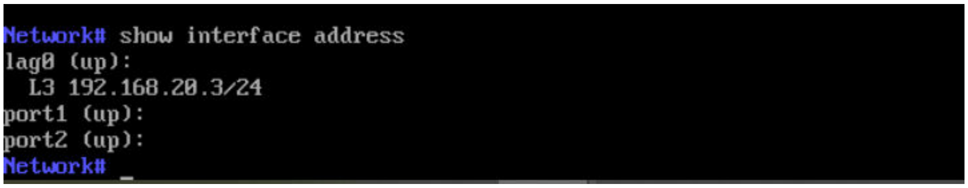
FIGURE 58 show lacp details Command



```
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_COLLECTIING (4)
        LACP_STATE_DISTRIBUTING (5)
    Partner
      system: 4c:b1: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_COLLECTIING (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_COLLECTIING (4)
        LACP_STATE_DISTRIBUTING (5)
    Partner
      system: 4c:b1: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_COLLECTIING (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#
```

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

    FIGURE 59 show interface address Command

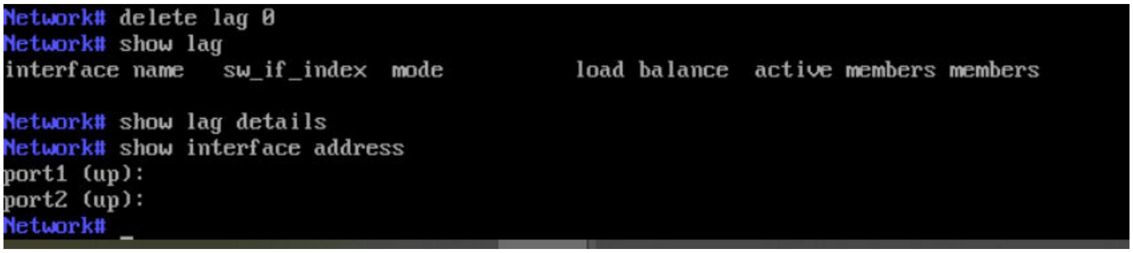
    ```
    Network# show interface address
    lag0 (up):
      L3 192.168.20.3/24
    port1 (up):
    port2 (up):
    Network# _
    ```

    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 60 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

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:

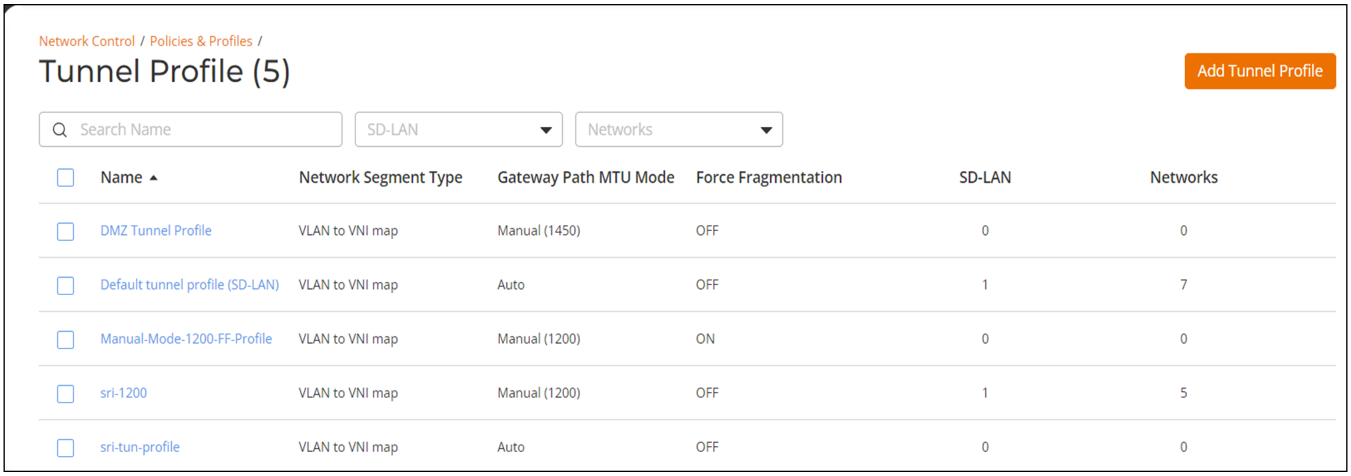
1. From the navigation bar, select **Network Control** > **Policies & Profiles**.

   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 61 Tunnel Profile Page



Network Control / Policies & Profiles /

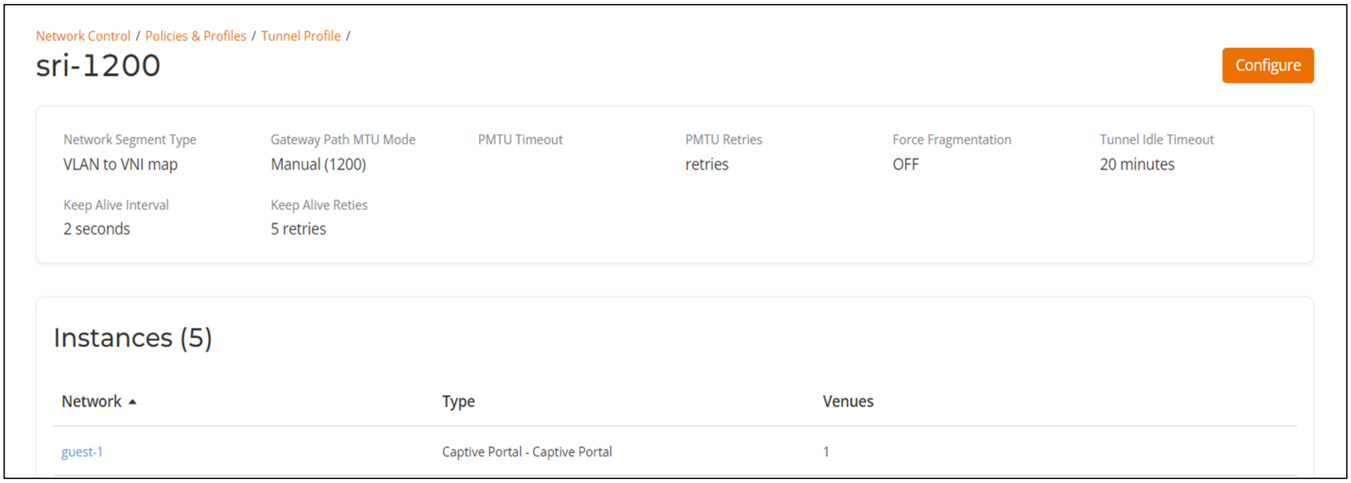
Tunnel Profile (5)

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

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 62 Details Page for a Tunnel Profile



Network Control / Policies & Profiles / Tunnel Profile /

sri-1200

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 Reties
2 seconds	5 retries

Instances (5)

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:

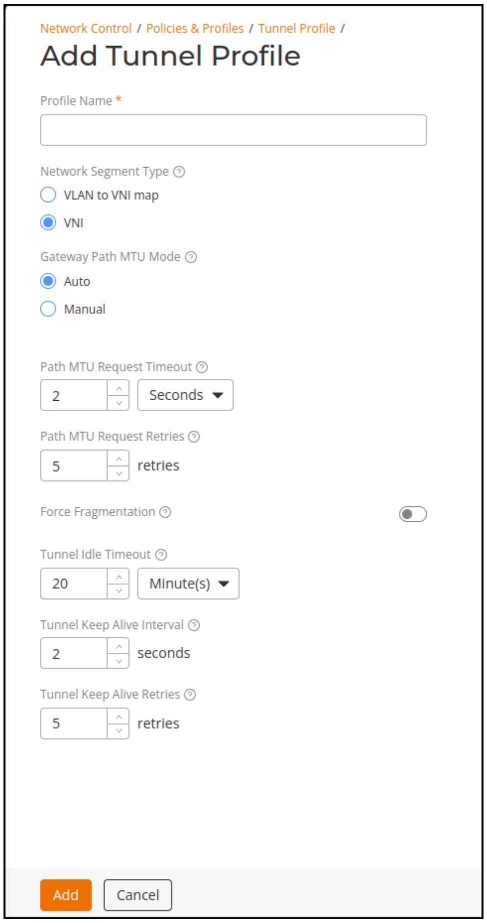
1. From the navigation bar, select **Network Control** > **Policies & Profiles**.

   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 63 Add Tunnel Profile Page



Network Control / Policies & Profiles / Tunnel Profile /

Add Tunnel Profile

Profile Name *

Network Segment Type
○ VLAN to VNI map
● VNI

Gateway Path MTU Mode
● Auto
○ Manual

Path MTU Request Timeout: 2 Seconds

Path MTU Request Retries: 5 retries

Force Fragmentation: off

Tunnel Idle Timeout: 20 Minute(s)

Tunnel Keep Alive Interval: 2 seconds

Tunnel Keep Alive Retries: 5 retries

3. 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. The **VNI** option is used for the PIN feature.
   - **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.

4. 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:

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

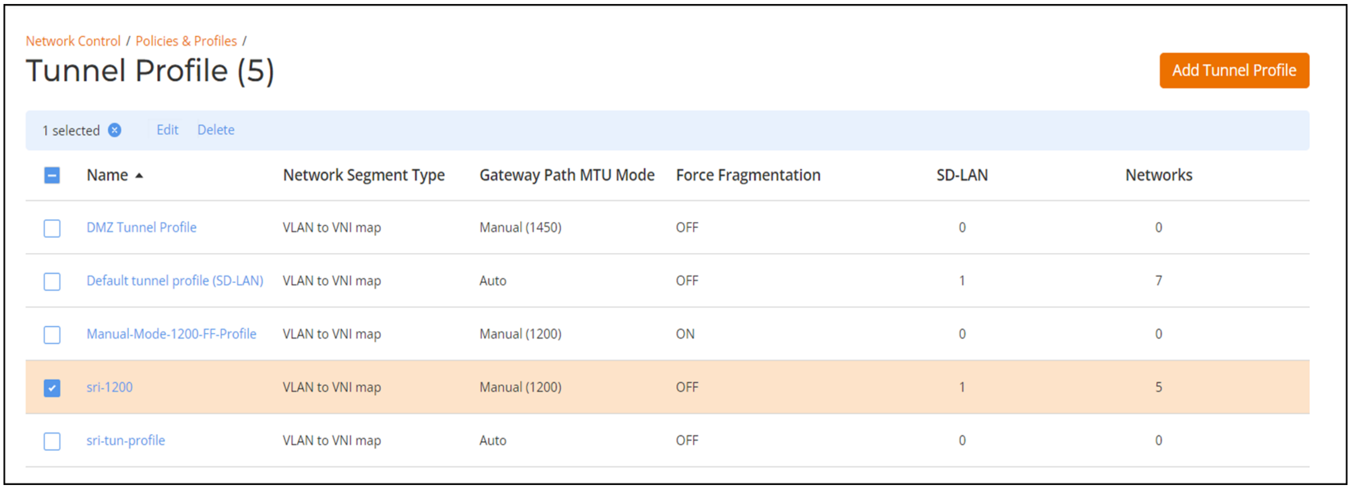
   The **Policies & Profiles** page is displayed.

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

   The **Tunnel Profile** page is displayed.

3. 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 64 Tunnel Profile Page



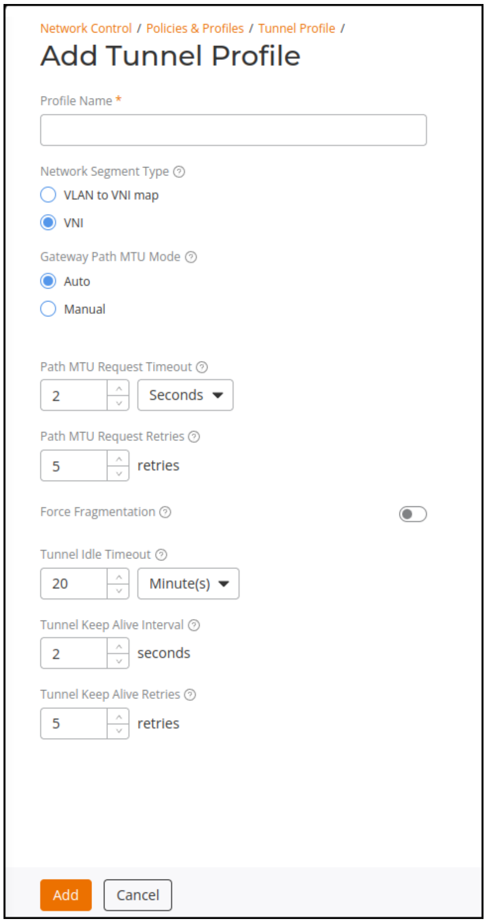
Network Control / Policies & Profiles /

Tunnel Profile (5)

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

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

FIGURE 65 Edit Tunnel Profile



Network Control / Policies & Profiles / Tunnel Profile /

Add Tunnel Profile

Profile Name *

Network Segment Type

○ VLAN to VNI map

● VNI

Gateway Path MTU Mode

● Auto

○ Manual

Path MTU Request Timeout

2 Seconds

Path MTU Request Retries

5 retries

Force Fragmentation

Tunnel Idle Timeout

20 Minute(s)

Tunnel Keep Alive Interval

2 seconds

Tunnel Keep Alive Retries

5 retries

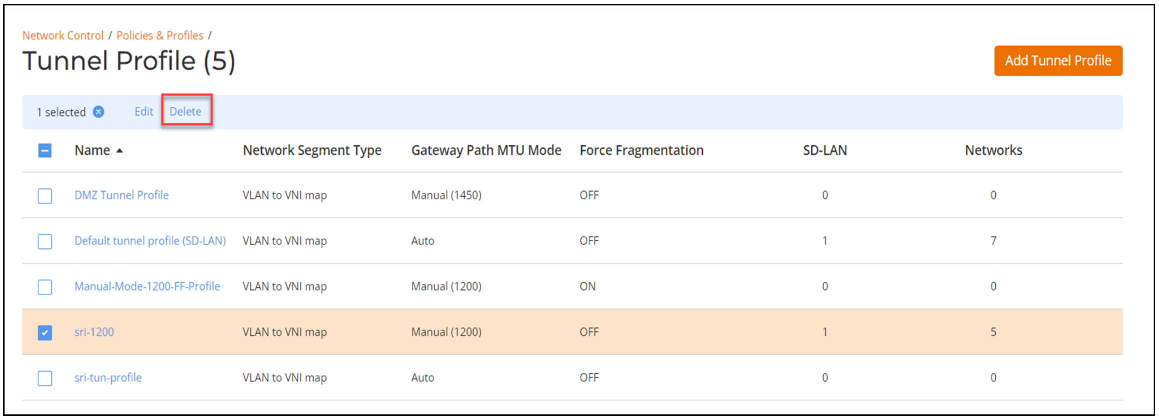
4. Update the **Profile Name**, **Network Segmentation Type**, **Gateway Path MTU Mode**, **Path MTU Request Timeout**, **Path MTU Request Retries**, **Force Fragmentation**, **Tunnel Idle Timeout**, **Tunnel Keep Alive Interval**, or **Tunnel Keep Alive Retries** options, as necessary, and click **Apply**.

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 66 Delete a Tunnel Profile

      Network Control / Policies & Profiles /

      Tunnel Profile (5)

☐	Name ▲	Network Segment Type	Gateway Path MTU Mode	Force Fragmentation	SD-LAN	Networks
☐	DMZ Tunnel Profile	VLAN to VNI map	Manual (1450)	OFF	0	0
☐	Default tunnel profile (SD-LAN)	VLAN to VNI map	Auto	OFF	1	7
☐	Manual-Mode-1200-FF-Profile	VLAN to VNI map	Manual (1200)	ON	0	0
☑	sri-1200	VLAN to VNI map	Manual (1200)	OFF	1	5
☐	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.

Software Defined Local Area Network (SD-LAN)

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.

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.

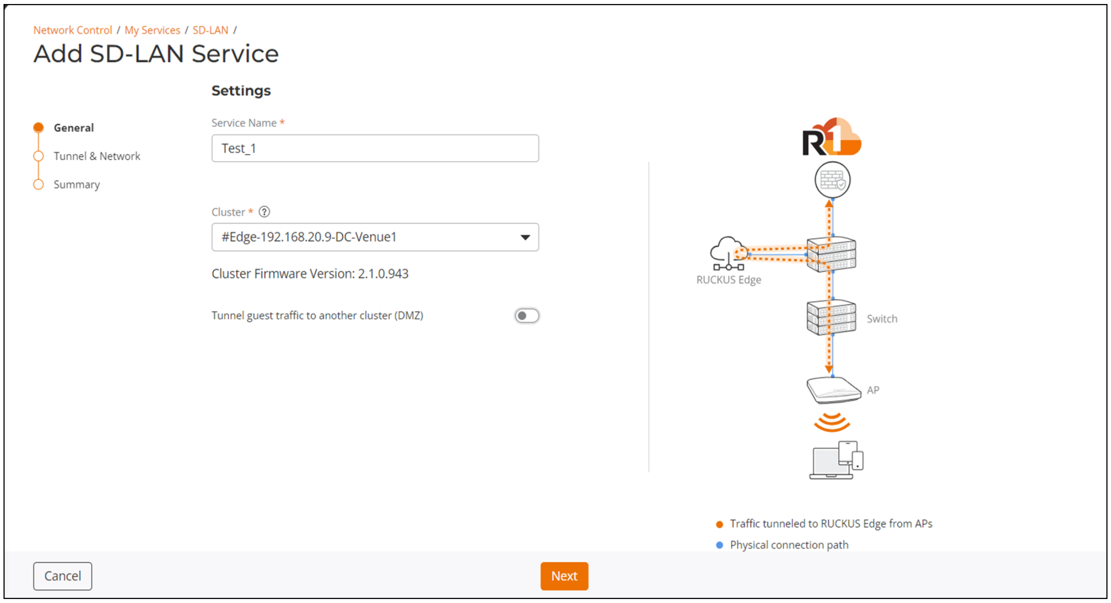
3. In the **Add SD-LAN Service** page, configure the following:

   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 67 Tunnel Guest Traffic to Another Cluster (DMZ) Disabled



Network Control / My Services / SD-LAN /

Add SD-LAN Service

Settings

Service Name *: Test_1

Cluster *: #Edge-192.168.20.9-DC-Venue1

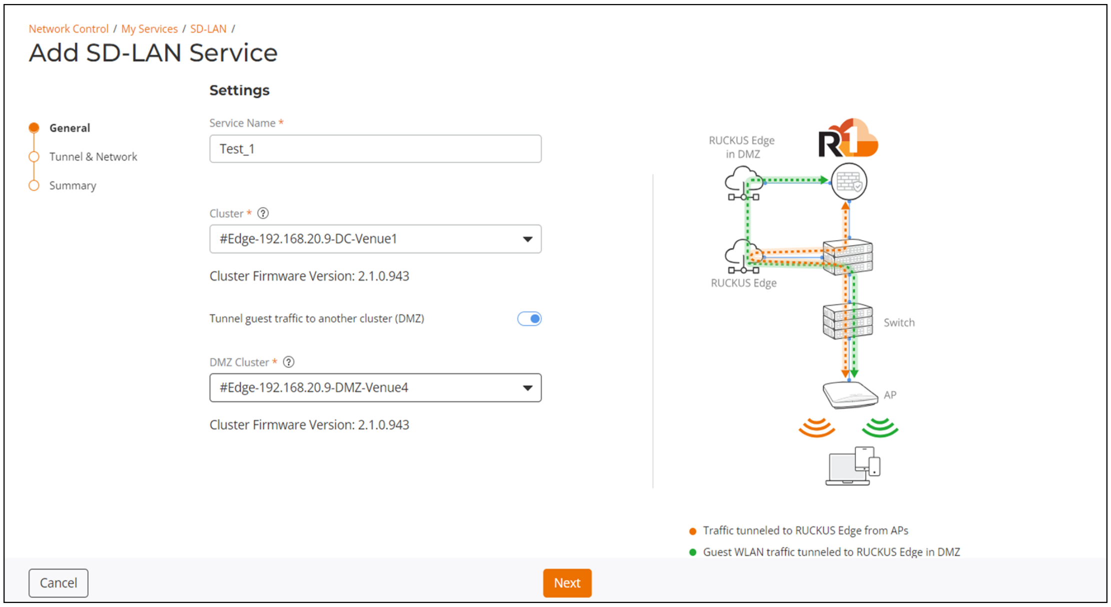
Cluster Firmware Version: 2.1.0.943

Tunnel guest traffic to another cluster (DMZ): ○ (off)

General
Tunnel & Network
Summary
RUCKUS Edge
Switch
AP
● Traffic tunneled to RUCKUS Edge from APs
● Physical connection path
Cancel
Next

     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 68 Tunnel Guest Traffic to Another Cluster (DMZ) Enabled



Network Control / My Services / SD-LAN /

Add SD-LAN Service

General
Tunnel & Network
Summary

Settings

Service Name *: Test_1

Cluster * ⓘ: #Edge-192.168.20.9-DC-Venue1

Cluster Firmware Version: 2.1.0.943

Tunnel guest traffic to another cluster (DMZ) ●

DMZ Cluster * ⓘ: #Edge-192.168.20.9-DMZ-Venue4

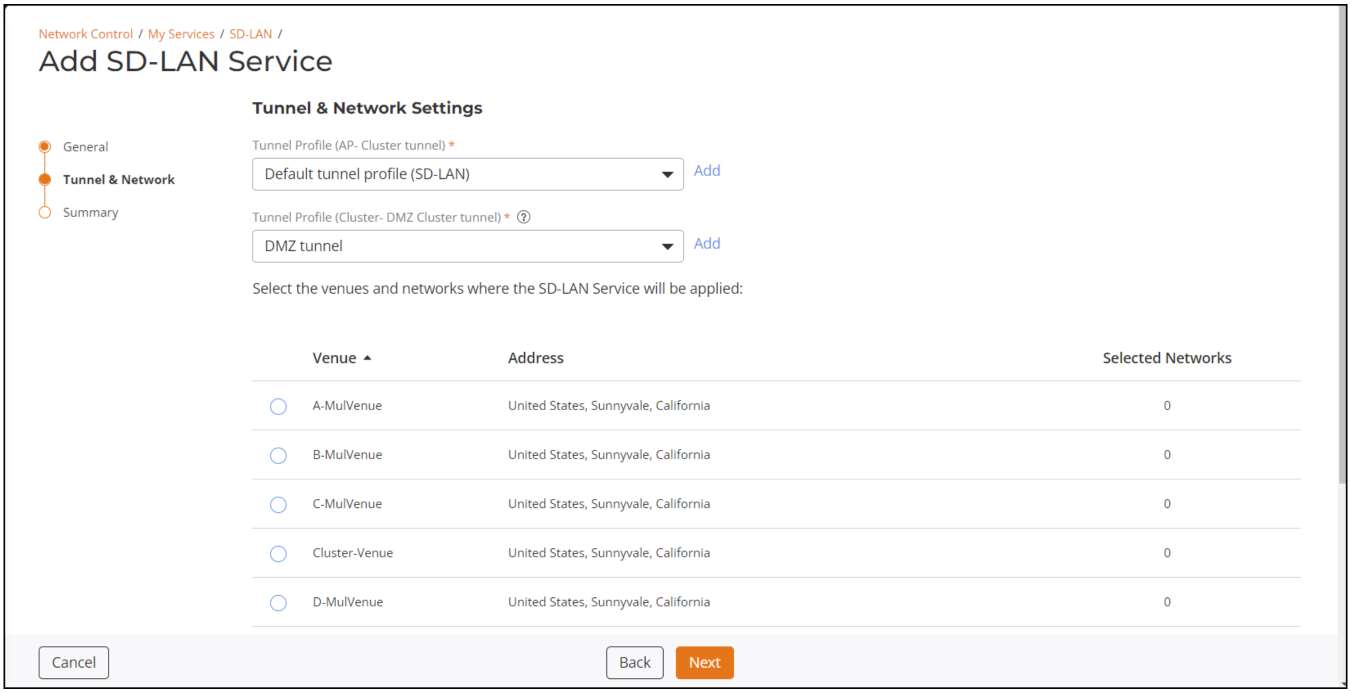
Cluster Firmware Version: 2.1.0.943

RUCKUS Edge in DMZ
RUCKUS Edge
Switch
AP
● Traffic tunneled to RUCKUS Edge from APs
● Guest WLAN traffic tunneled to RUCKUS Edge in DMZ
Cancel
Next

- **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 69 Tunnel and Network Settings



Network Control / My Services / SD-LAN /

Add SD-LAN Service

Tunnel & Network Settings

Tunnel Profile (AP- Cluster tunnel) *: Default tunnel profile (SD-LAN) Add

Tunnel Profile (Cluster- DMZ Cluster tunnel) * ⓘ: DMZ tunnel Add

Select the venues and networks where the SD-LAN Service will be applied:

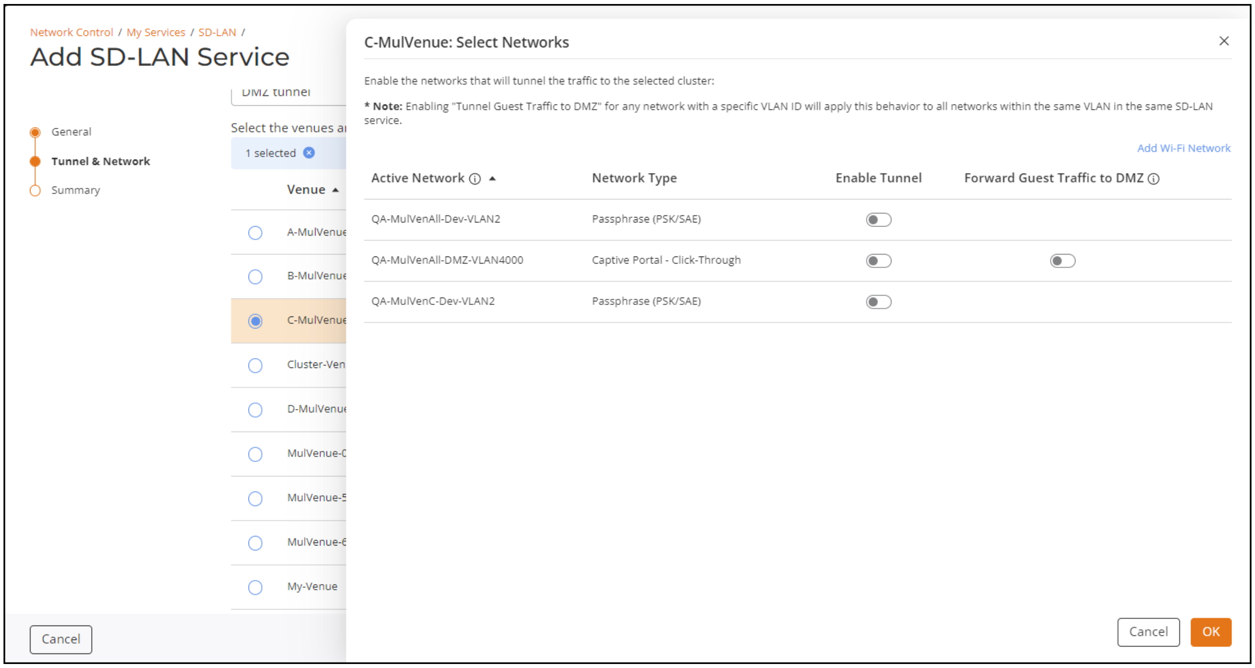
	Venue ▲	Address	Selected Networks
○	A-MulVenue	United States, Sunnyvale, California	0
○	B-MulVenue	United States, Sunnyvale, California	0
○	C-MulVenue	United States, Sunnyvale, California	0
○	Cluster-Venue	United States, Sunnyvale, California	0
○	D-MulVenue	United States, Sunnyvale, California	0

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 80 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 80 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 70 Select Networks

  Enable the networks that will tunnel the traffic to the selected cluster:

  * **Note:** Enabling "Tunnel Guest Traffic to DMZ" for any network with a specific VLAN ID will apply this behavior to all networks within the same VLAN in the same SD-LAN service.

Active Network	Network Type	Enable Tunnel	Forward Guest Traffic to DMZ
QA-MulVenAll-Dev-VLAN2	Passphrase (PSK/SAE)	○	
QA-MulVenAll-DMZ-VLAN4000	Captive Portal - Click-Through	○	○
QA-MulVenC-Dev-VLAN2	Passphrase (PSK/SAE)	○	

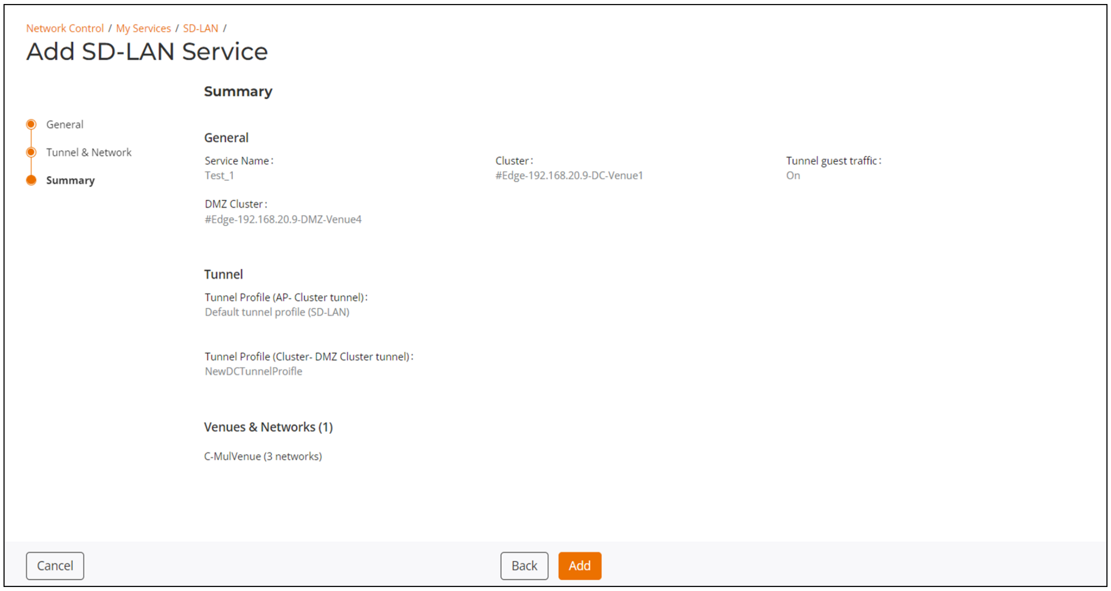
- In the resulting sidebar, you can click the **Enable Tunnel** toggle switch and the **Forward Guest Traffic to DMZ** toggle switch (applicable for captive portal networks) for each Wi-Fi network, as desired, then click **OK** to close the sidebar. Repeat this for each venue to which you want this SD-LAN 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 71 SD-LAN Summary



Add SD-LAN Service

Summary

General

Service Name: Test_1

Cluster: #Edge-192.168.20.9-DC-Venue1

Tunnel guest traffic: On

DMZ Cluster: #Edge-192.168.20.9-DMZ-Venue4

Tunnel

Tunnel Profile (AP- Cluster tunnel): Default tunnel profile (SD-LAN)

Tunnel Profile (Cluster- DMZ Cluster tunnel): NewDCTunnelProifle

Venues & Networks (1)

C-MulVenue (3 networks)

Viewing the SD-LAN Service

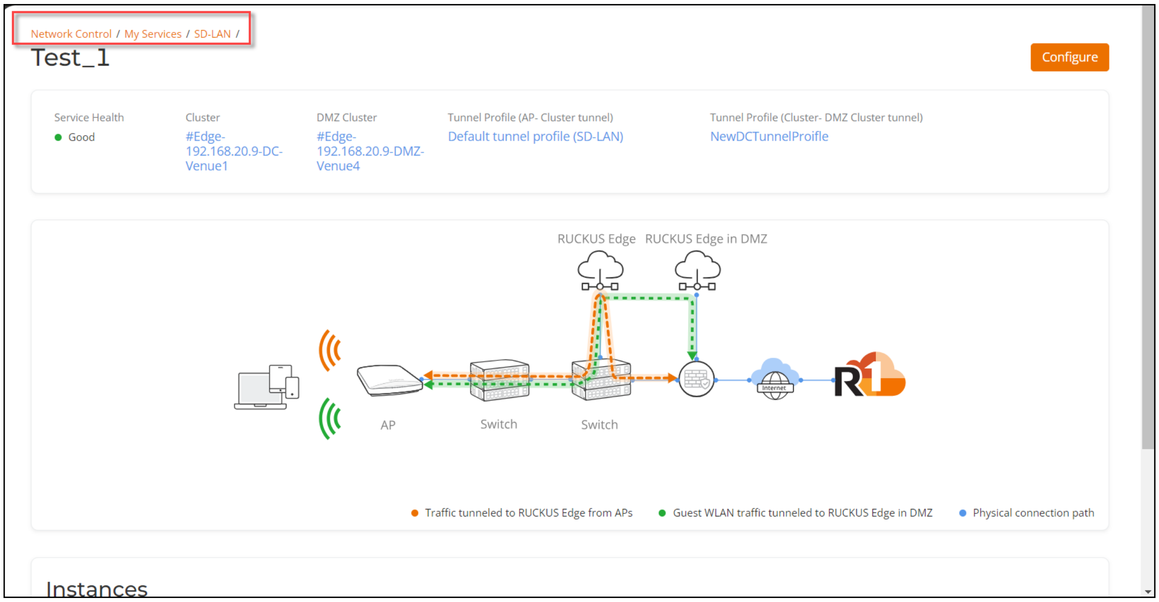
You can view information pertaining to a configured SD-LAN service from the perspective of the service itself, the RUCKUS Edge cluster, or the venue.

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.

FIGURE 72 Viewing an SD-LAN Service via Network Control



Network Control / My Services / SD-LAN /

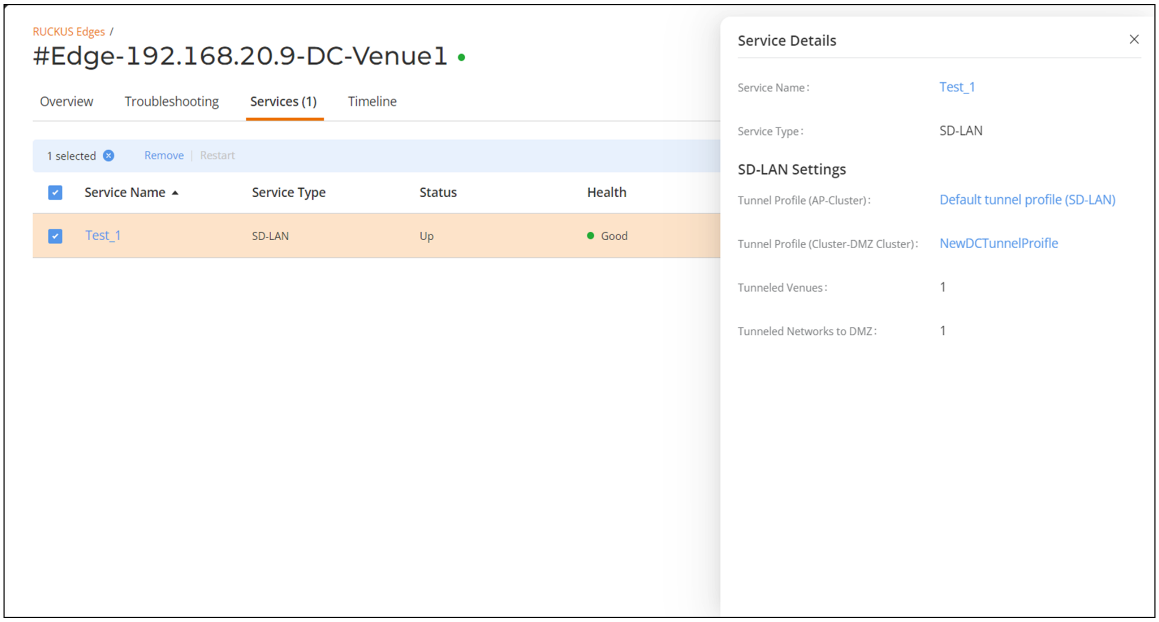
Test_1

Service Health	Cluster	DMZ Cluster	Tunnel Profile (AP- Cluster tunnel)	Tunnel Profile (Cluster- DMZ Cluster tunnel)
● Good	#Edge-192.168.20.9-DC-Venue1	#Edge-192.168.20.9-DMZ-Venue4	Default tunnel profile (SD-LAN)	NewDCTunnelProifle

Configure
RUCKUS Edge
RUCKUS Edge in DMZ
AP
Switch
Switch
Internet
● Traffic tunneled to RUCKUS Edge from APs
● Guest WLAN traffic tunneled to RUCKUS Edge in DMZ
● Physical connection path
Instances

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 73 Viewing an SD-LAN Service via RUCKUS Edge



RUCKUS Edges /

#Edge-192.168.20.9-DC-Venue1 ●

☑	Service Name ▲	Service Type	Status	Health
☑	Test_1	SD-LAN	Up	● Good

Service Details ×

Service Name: Test_1

Service Type: SD-LAN

SD-LAN Settings

Tunnel Profile (AP-Cluster): Default tunnel profile (SD-LAN)

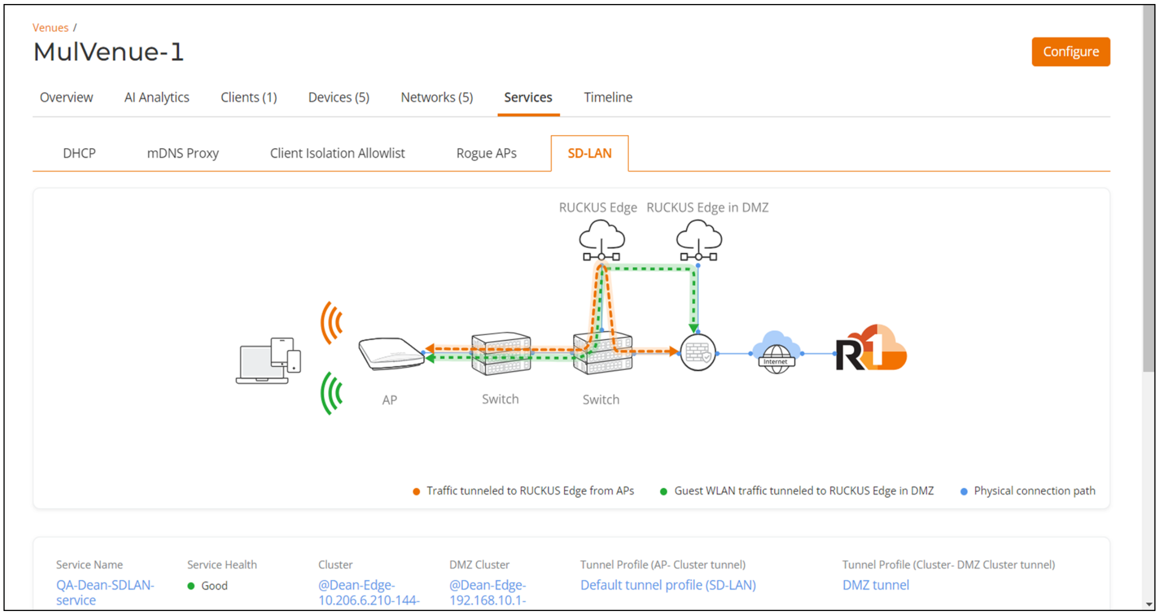
Tunnel Profile (Cluster-DMZ Cluster): NewDCTunnelProifle

Tunneled Venues: 1

Tunneled Networks to DMZ: 1

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 74 View an SD-LAN Service via Venues



Venues /

MulVenue-1

Service Name	Service Health	Cluster	DMZ Cluster	Tunnel Profile (AP- Cluster tunnel)	Tunnel Profile (Cluster- DMZ Cluster tunnel)
QA-Dean-SDLAN-service	● Good	@Dean-Edge-10.206.6.210-144-	@Dean-Edge-192.168.10.1-	Default tunnel profile (SD-LAN)	DMZ tunnel

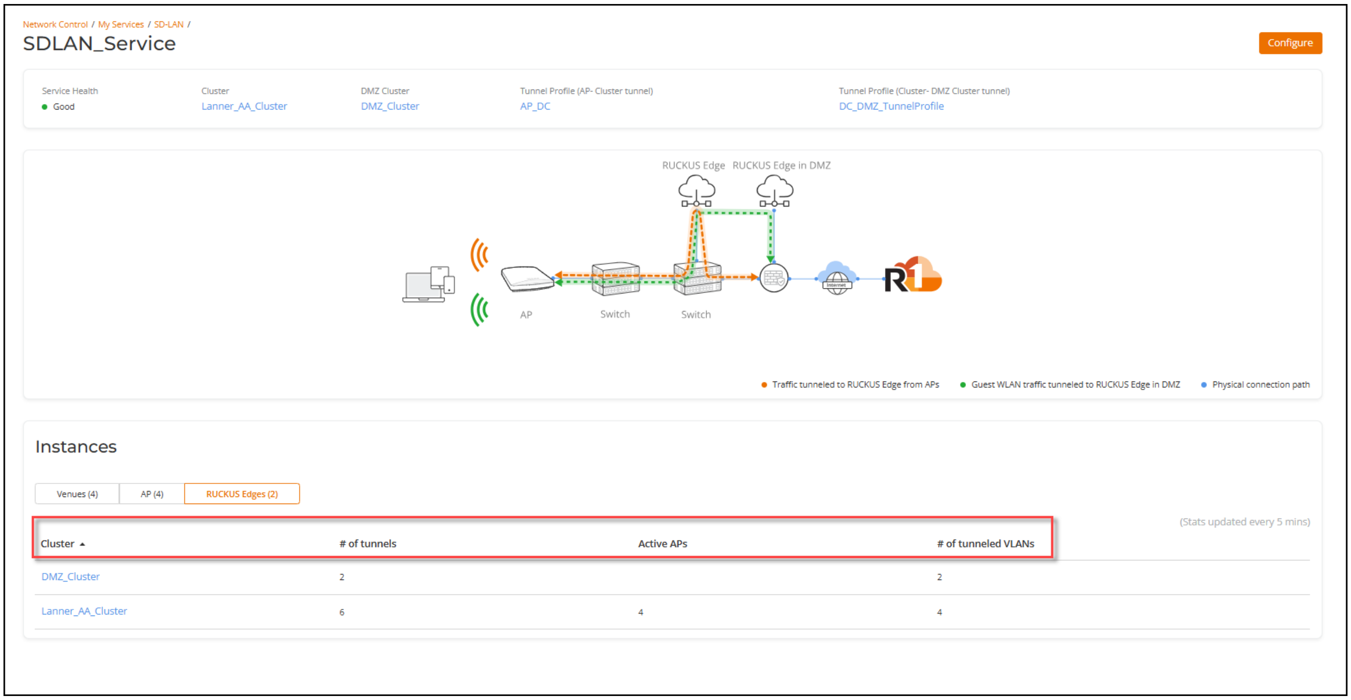
Viewing SD-LAN Statistics

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.

FIGURE 75 SD-LAN Statistics



Network Control / My Services / SD-LAN /

SDLAN_Service

Service Health	Cluster	DMZ Cluster	Tunnel Profile (AP- Cluster tunnel)	Tunnel Profile (Cluster- DMZ Cluster tunnel)
● Good	Lanner_AA_Cluster	DMZ_Cluster	AP_DC	DC_DMZ_TunnelProfile

RUCKUS Edge
RUCKUS Edge in DMZ
AP
Switch
Switch
● Traffic tunneled to RUCKUS Edge from APs
● Guest WLAN traffic tunneled to RUCKUS Edge in DMZ
● Physical connection path

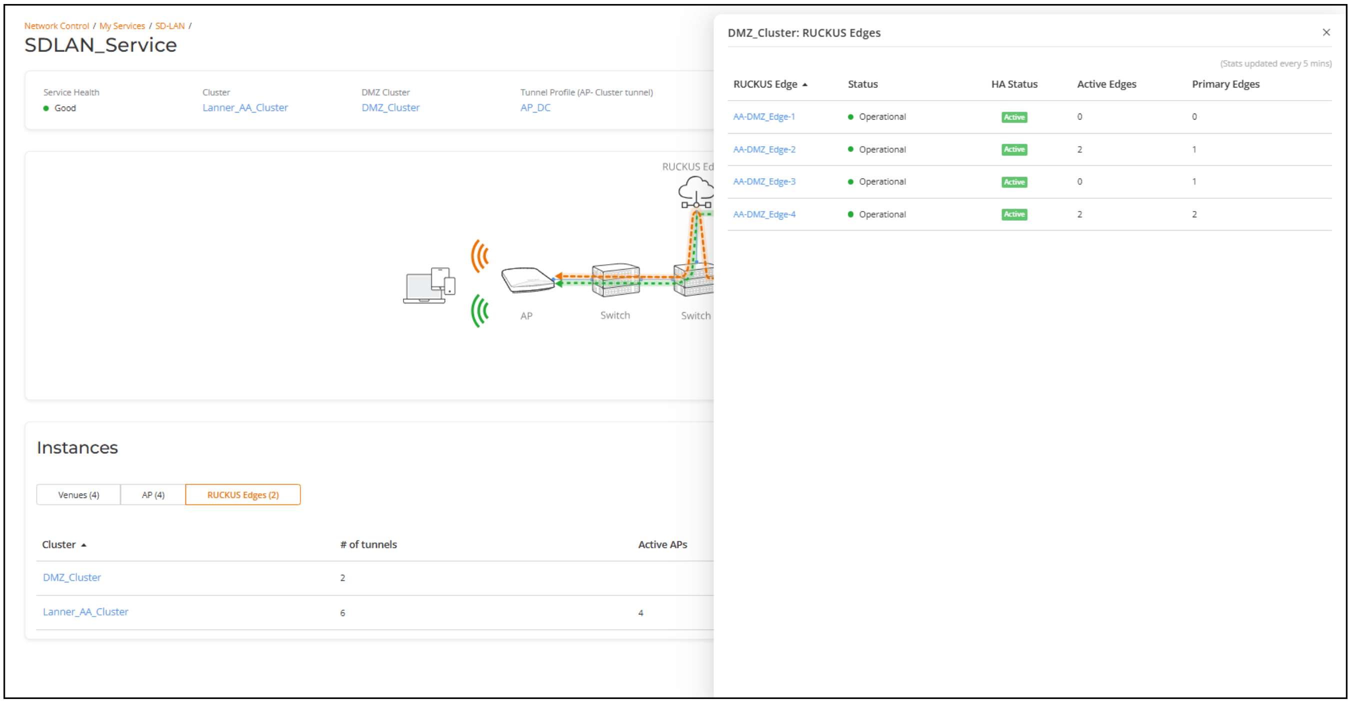
Instances

Venues (4)
AP (4)
RUCKUS Edges (2)

(Stats updated every 5 mins)

Cluster ▲	# of tunnels	Active APs	# of tunneled VLANs
DMZ_Cluster	2		2
Lanner_AA_Cluster	6	4	4

FIGURE 76 AP Load Distribution Between Edges of a Cluster



Network Control / My Services / SD-LAN /

SDLAN_Service

Service Health	Cluster	DMZ Cluster	Tunnel Profile (AP- Cluster tunnel)
● Good	Lanner_AA_Cluster	DMZ_Cluster	AP_DC

Instances

Venues (4) | AP (4) | RUCKUS Edges (2)

Cluster ▲	# of tunnels	Active APs
DMZ_Cluster	2	
Lanner_AA_Cluster	6	4

DMZ_Cluster: RUCKUS Edges ×

(Stats updated every 5 mins)

RUCKUS Edge ▲	Status	HA Status	Active Edges	Primary Edges
AA-DMZ_Edge-1	● Operational	Active	0	0
AA-DMZ_Edge-2	● Operational	Active	2	1
AA-DMZ_Edge-3	● Operational	Active	0	1
AA-DMZ_Edge-4	● Operational	Active	2	2

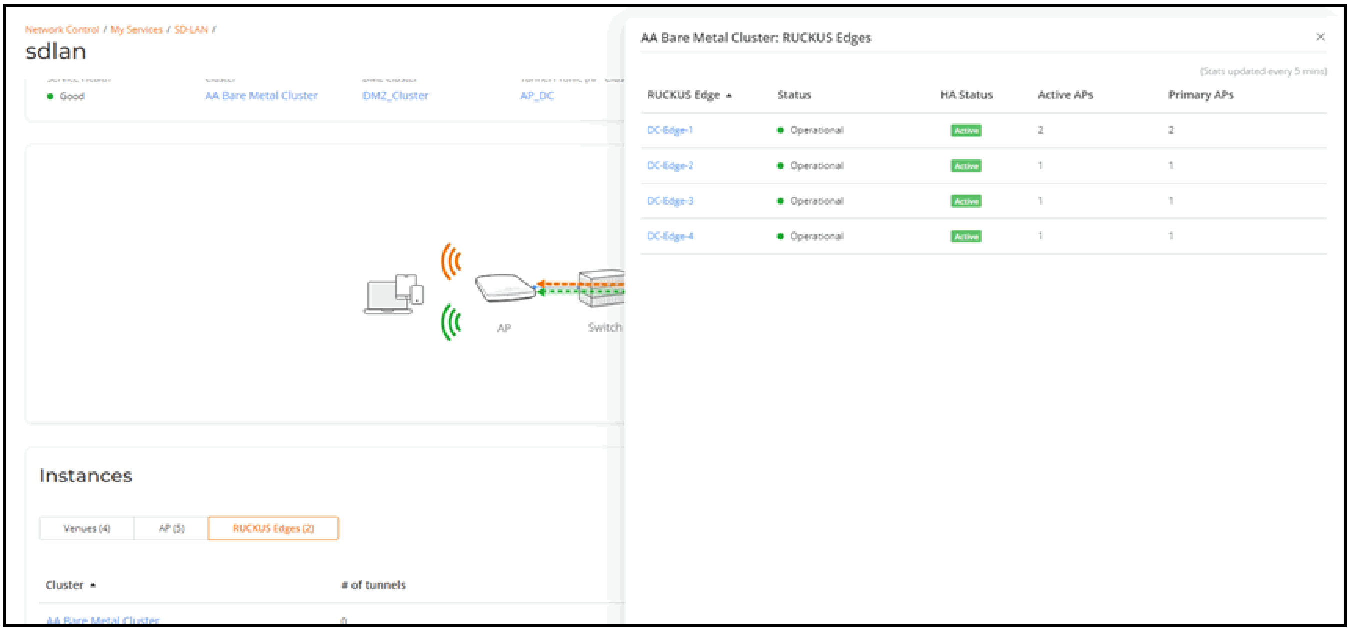
Statistics for AA DC Cluster

Active APs: This shows the number of APs currently connected to the given DC Edge and have an active VXLAN-GPE tunnel with the Edge.

Primary APs: This shows the number of APs that have selected the given DC Edge as their primary Edge. The primary Edge is the first Edge in the randomized list generated by the AP and is the preferred Edge for forming the VXLAN-GPE tunnel. If the primary Edge is not available, the AP forms a tunnel to the next available Edge in the randomized list. Therefore, the Primary APs count might differ from the Active APs count.

At the time of fallback, the APs fall back to the primary Edge. If all the edges are available, the Active APs and Primary APs count for a given Edge will be equal.

FIGURE 77 Statistics for AA DC cluster



Cluster ▲	# of tunnels
AA Bare Metal Cluster	0

AA Bare Metal Cluster: RUCKUS Edges

(Stats updated every 5 mins)

RUCKUS Edge ▲	Status	HA Status	Active APs	Primary APs
DC-Edge-1	● Operational	Active	2	2
DC-Edge-2	● Operational	Active	1	1
DC-Edge-3	● Operational	Active	1	1
DC-Edge-4	● Operational	Active	1	1

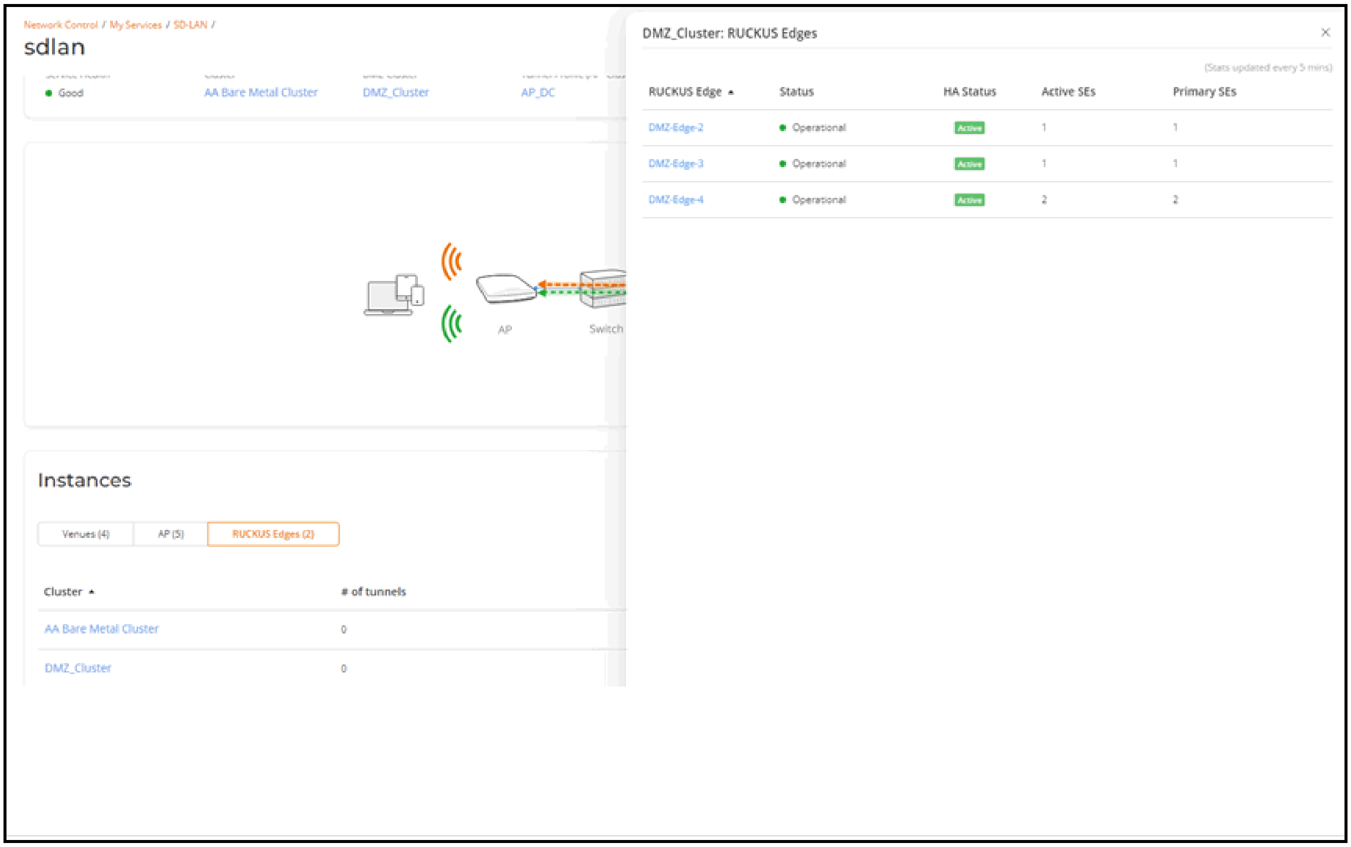
Statistics for DMZ Cluster

Active SEs: This shows the number of DC Edge devices currently connected to the given DMZ edge. There is an active VXLAN-GPE tunnel between the number shown under Active SEs and the given DMZ Edge.

Primary SEs: This shows the number of DC Edge devices that have the given DMZ Edge as their primary Edge. The primary Edge is the first Edge in the randomized list generated by the DC Edge and is the preferred Edge for forming the VXLAN-GPE tunnel. If the primary DMZ Edge is not available, the DC Edge forms a tunnel to the next available Edge in the randomized list. Therefore, the Primary SEs count might differ from the Active SEs count

At the time of fallback, the DC Edges fallback to the primary Edge. In a case where all the DMZ edges are available, the Active SEs and Primary SEs count for a given Edge will be equal.

FIGURE 78 Statistics for DMZ Cluster



Network Control / My Services / SD-LAN /

sdlan

● Good | AA Bare Metal Cluster | DMZ_Cluster | AP_DC

Instances

Venues (4) | AP (5) | RUCKUS Edges (2)

Cluster ▲	# of tunnels
AA Bare Metal Cluster	0
DMZ_Cluster	0

DMZ_Cluster: RUCKUS Edges

(Stats updated every 5 mins)

RUCKUS Edge ▲	Status	HA Status	Active SEs	Primary SEs
DMZ-Edge-2	● Operational	Active	1	1
DMZ-Edge-3	● Operational	Active	1	1
DMZ-Edge-4	● Operational	Active	2	2

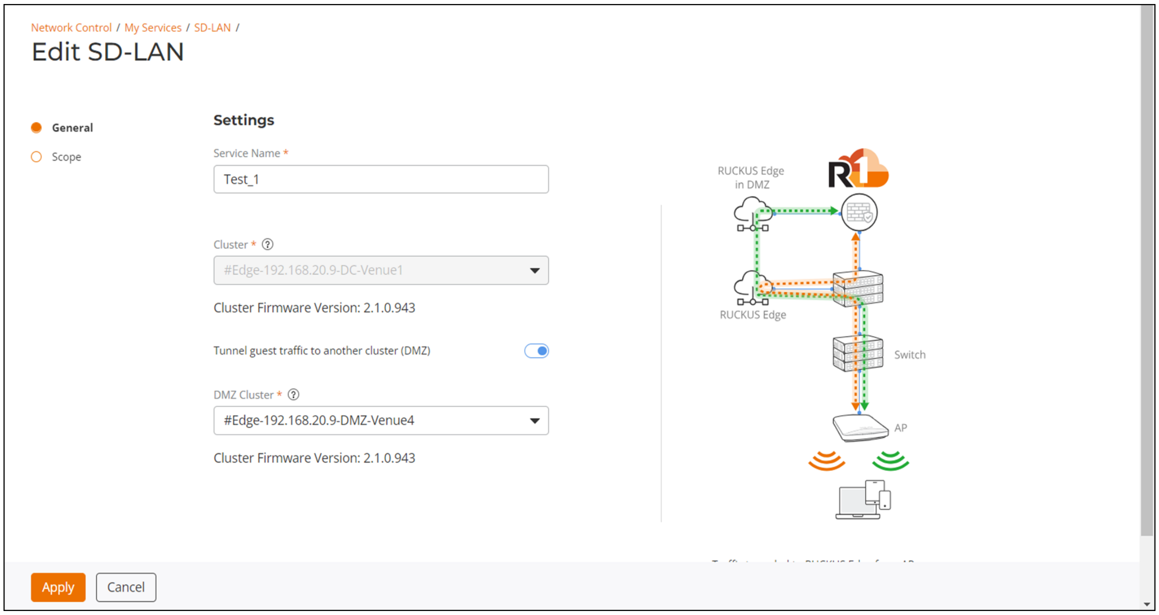
Editing an SD-LAN Service

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 79 Edit SD-LAN



Network Control / My Services / SD-LAN /

Edit SD-LAN

● General
○ Scope

Settings

Service Name *
Test_1

Cluster *
#Edge-192.168.20.9-DC-Venue1

Cluster Firmware Version: 2.1.0.943

Tunnel guest traffic to another cluster (DMZ)

DMZ Cluster *
#Edge-192.168.20.9-DMZ-Venue4

Cluster Firmware Version: 2.1.0.943

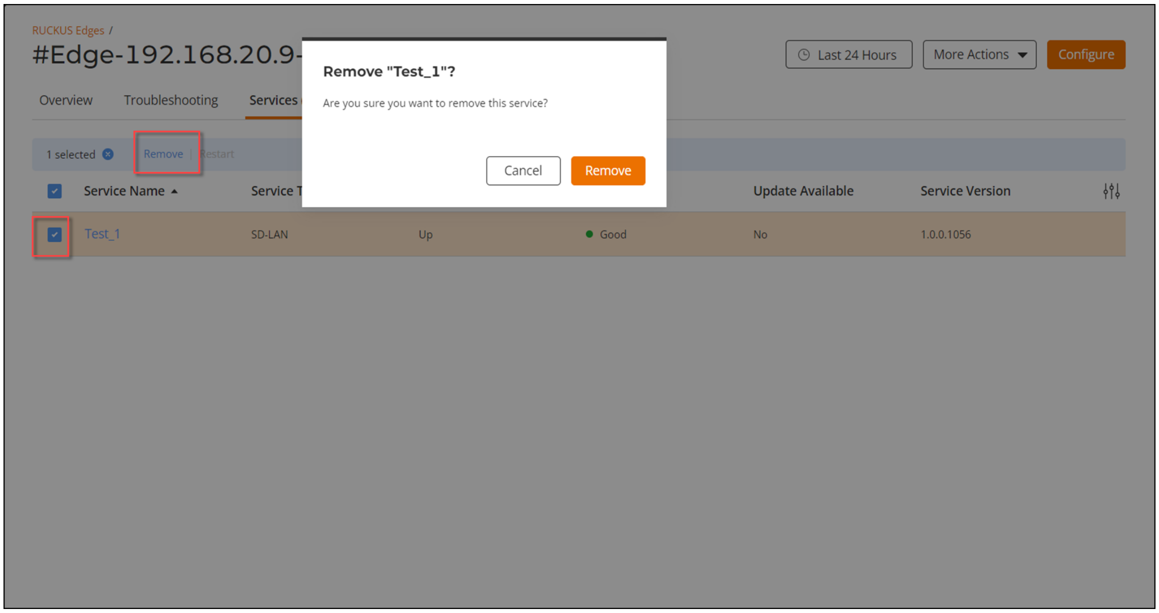
NOTE
If the **Tunnel Guest Traffic to another Cluster (DMZ)** option is disabled, the VxLAN-GPE tunnels connecting the access points (APs) to the Data Center are still communicating. However, the data traffic is disabled between the Data Center and the DMZ as this SD-LAN service is deleted from DMZ RUCKUS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

FIGURE 80 Remove SD-LAN Service from RUCKUS Edge



Remove "Test_1"?

Are you sure you want to remove this service?

Service Name	Service T			Update Available	Service Version
Test_1	SD-LAN	Up	● Good	No	1.0.0.1056

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.

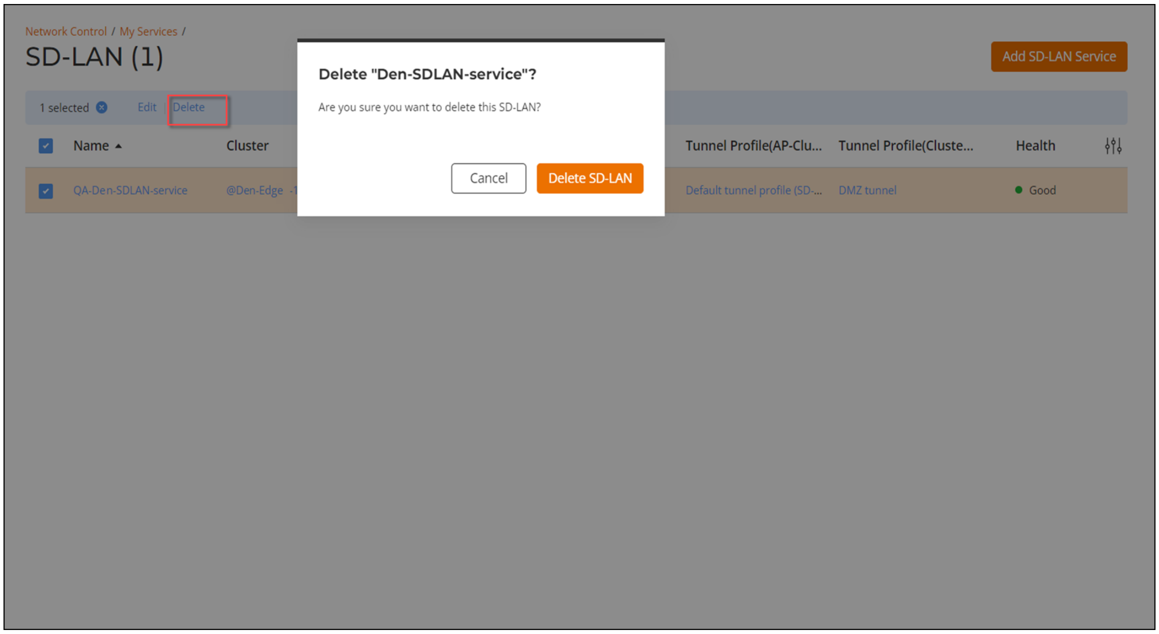
Deleting an SD-LAN Service

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 81 Delete SD-LAN Service



Delete "Den-SDLAN-service"?

Are you sure you want to delete this SD-LAN?

☑	Name ▲	Cluster	Tunnel Profile(AP-Clu...	Tunnel Profile(Cluste...	Health
☑	QA-Den-SDLAN-service	@Den-Edge -1	Default tunnel profile (SD-...	DMZ tunnel	● Good

Multiple Venue Support for an SD-LAN Service

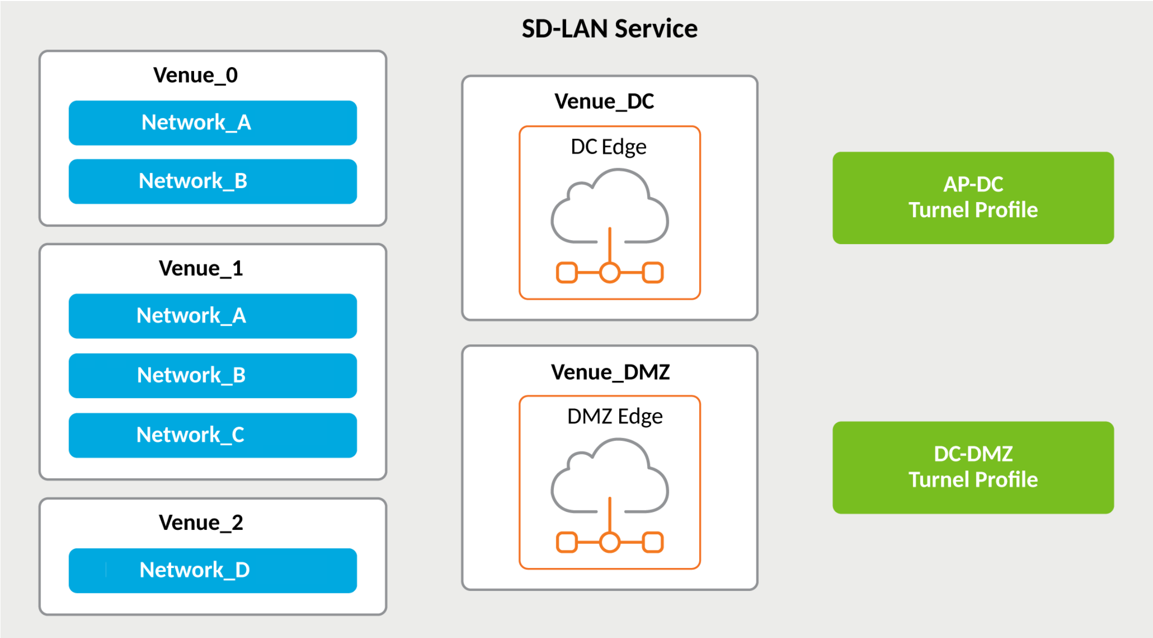
The Multiple Venue Support for an SD-LAN service feature offers a scalable and efficient way to manage multiple venues within an SD-LAN.

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 82 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.

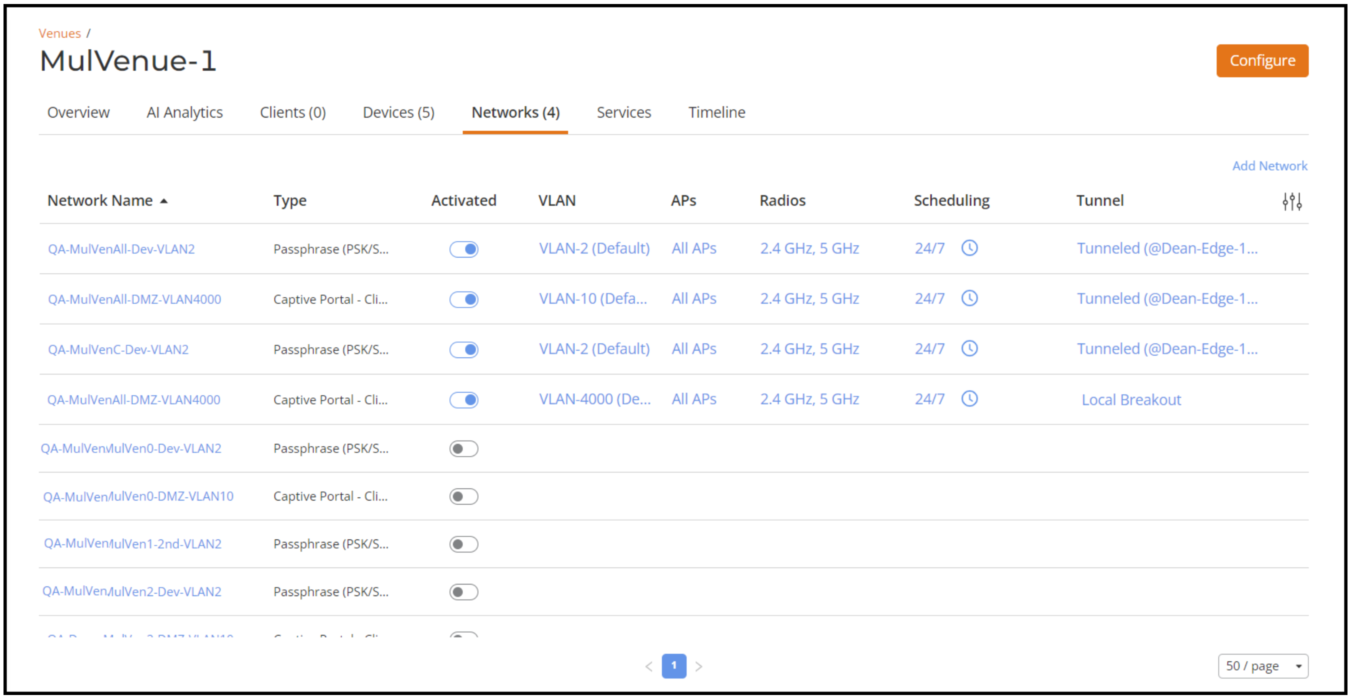
1. On the navigation bar, click **Venues**.

   The **Venues** page is displayed.

2. 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 83 Configured Networks in a Venue



Venues /

MulVenue-1

Configure

Overview | AI Analytics | Clients (0) | Devices (5) | Networks (4) | Services | Timeline

Add Network

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

< 1 >

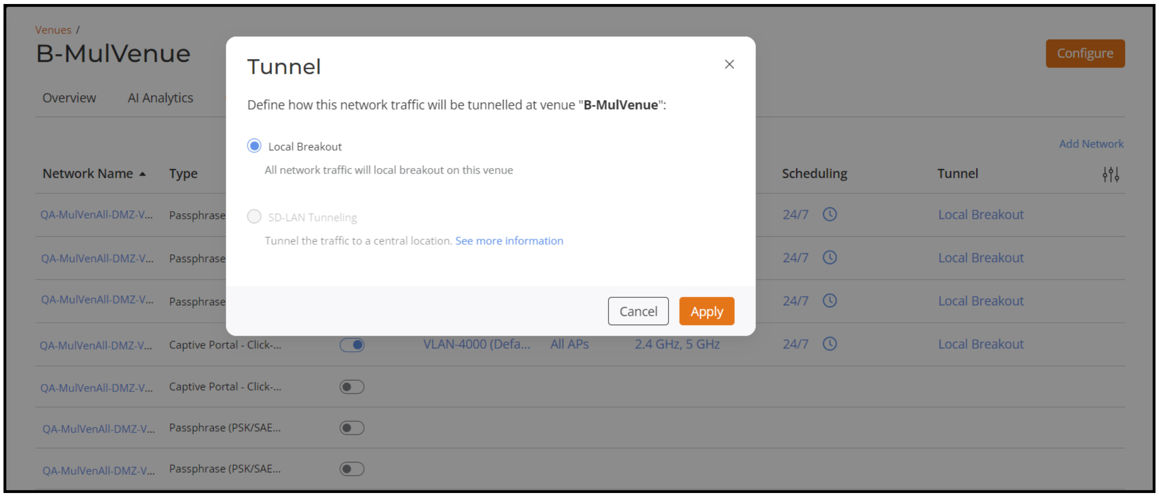
50 / page

- **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:
  - Passphrase (PSK/SAE)
  - 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)
  - Captive Portal: Active Directory/LDAP Server
  - Open Network
- **Activated**: Shows ON or OFF to display whether the network is activated in the venue. When this option is toggled OFF, only the network name and type appear on this page; no other network information is displayed.
- **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 the radio bandwidths on which this network is available. 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 the tunneling service or profile associated with each active network. The Tunnel column entry is clickable, allowing you to modify the tunneling type or configuration, as appropriate for the network and venue. Tunnel types follow:
  - **Local Breakout**: This option is automatically chosen when the venue is not linked to any tunneling service. When connected to any SD-LAN service, the network traffic will not be tunneled to the Edge cluster. APs will bridge this network traffic on its uplink ethernet port with appropriate VLAN on the ethernet network.

    FIGURE 84 Local Breakout

    Tunnel

    Define how this network traffic will be tunnelled at venue "**B-MulVenue**":

    ● Local Breakout

    All network traffic will local breakout on this venue

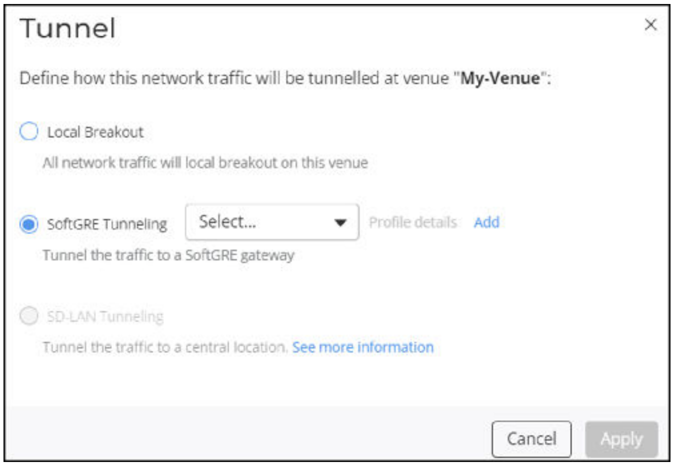
    ○ SD-LAN Tunneling

    Tunnel the traffic to a central location. See more information

  - **SoftGRE Tunneling**: A SoftGRE profile tunnels the traffic to a SoftGRE gateway.
    - Select a preconfigured SoftGRE gateway from the drop-down list and click **Apply**, or click **Add** to create a SoftGRE profile. Refer to #unique_62 for more information.
    - Click **Profile details** to view the associated tunnel gateway addresses and tunnel usage configurations for the selected SoftGRE profile.

For exceptions, refer to #unique_63.

FIGURE 85 SoftGRE Tunneling



Tunnel

Define how this network traffic will be tunnelled at venue "**My-Venue**":

○ Local Breakout

All network traffic will local breakout on this venue

● SoftGRE Tunneling Select... Profile details Add

Tunnel the traffic to a SoftGRE gateway

○ SD-LAN Tunneling

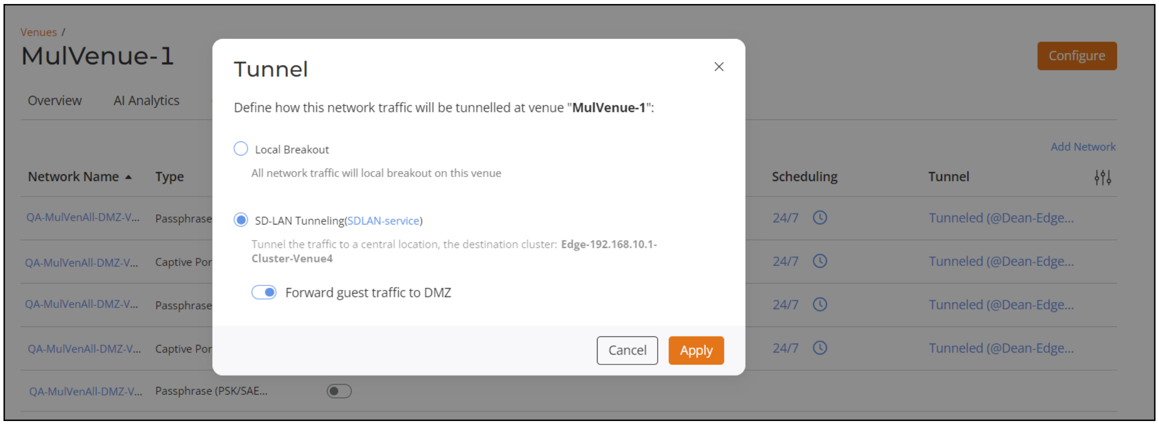
Tunnel the traffic to a central location. See more information

- **SD-LAN Tunneling**: The SD-LAN service tunnels traffic to a RUCKUS Edge device. Click the **See more information** link, to view information on Configuring an SD-LAN service.
  - For all network types except Captive Portal, traffic is tunneled between the AP and a Data Center Edge device, meaning you will not see the **Forward guest traffic to DMZ** option in the dialog box.
  - For Captive Portal networks, traffic is tunneled between a Data Center Edge device and a DMZ Edge device if the **Forward guest traffic to DMZ** option is enabled in the dialog box.

Refer to Software Defined Local Area Network and Configuring the SD-LAN Service for additional information.

> **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**.

FIGURE 86 Tunneling Options



Venues /

MulVenue-1

Overview AI Analytics

Network Name ▲	Type	Scheduling	Tunnel
QA-MulVenAll-DMZ-V...	Passphrase	24/7	Tunneled (@Dean-Edge...
QA-MulVenAll-DMZ-V...	Captive Por	24/7	Tunneled (@Dean-Edge...
QA-MulVenAll-DMZ-V...	Passphrase	24/7	Tunneled (@Dean-Edge...
QA-MulVenAll-DMZ-V...	Captive Por	24/7	Tunneled (@Dean-Edge...
QA-MulVenAll-DMZ-V...	Passphrase (PSK/SAE...		

Tunnel

Define how this network traffic will be tunnelled at venue "**MulVenue-1**":

○ Local Breakout

All network traffic will local breakout on this venue

● SD-LAN Tunneling(SDLAN-service)

Tunnel the traffic to a central location, the destination cluster: **Edge-192.168.10.1-Cluster-Venue4**

Forward guest traffic to DMZ

Personal Identity Network

Personal Identity Network

Personal Identity Networks (PIN) use VxLAN tunneling to extend Wi-Fi client and wired client via RUCKUS switch access to the RUCKUS Edge, creating seamless connectivity across the network domain. It enables Wi-Fi and wired clients to securely access their networks and connected devices while also establishing Personal Area Networks (PAN) for secure, individualized connectivity.

Personal Identity Network referred as PIN involves creating Personal Area Networks (PAN) for each unit in Multi Dwelling Unit (MDU) or dorm room in a university campus, using a shared network (access points, switches, internet gateway). In the PIN solution, the main role of RUCKUS Edge is to provide the following services to the PANs.

The following architecture types are supported on PIN -

- **RUCKUS Edge**
- **Distribution Switch (DS)** - Acts as an aggregation point for all the access layer switches.
- **Access Switch (AS)** - This facilitates the connection of end node devices to the network.
- **Access Point (AP)** - A wireless network device acts as portal for devices to connect to a local network.

Limitations

SD-LAN and Personal Identity Network are mutually exclusive features. If RUCKUS Edge or Network is chosen for one service, it cannot be utilized for the other service.

Only DPSK networks are supported, and the DPSK service must remain consistent within the Identity group.

The venue must have an Edge cluster and must enable Property Management within the Identity Group.

Once a PIN has been created, the cluster, DHCP service, and DHCP pool cannot be modified in the profile.

The tunnel profile is restricted to using only the VNI type within the PIN.

A maximum of 16 sub-interfaces is supported per physical port or LAG.

Only physical ports and LAGs can be configured as cluster interfaces.

To complete the LAG/Port & Virtual IP settings in the cluster configuration wizard, the user must create at least one physical LAN.

Only Active-Backup HA support is available.

Workflow of Personal Identity Network

Personal Identity Network workflow has a recommended sequence.

Pre-conditions before creating a Personal Identity Network:

1. **Property Management Service** for the venue should be already enabled.
2. **RUCKUS Edge** should be deployed to the venue.

User workflow of Personal Identity Network

Service Catalog: Create a new Personal Identity Network

1. Select property management enabled **Venue**.
2. Select Edge, DHCP pool, and set segment settings.
3. Select VxLAN tunnel profile and DPSK networks.
4. Select DS/AS and set DS settings.
5. Select AS settings.

   NOTE
   If no switch under the selected venue then skip step 4 and 5.

   The new **Personal Identity Network** creation is complete.

- **Wireless Access Point (AP)** - Enable the **Personal Identity Network** flag for networks. If **No** enable the **Personal Identity Network** in **DPSK Network** configuration window.
- **Wired Access Point (AP)** - To enable wired AP:
  - Navigate to **Venue/Property** unit and select the unit.
  - Select AP from the dropt-down list and assign LAN port.

Personal Identity Network Service Deployment

Personal Identity Network can be deployed in the following stages:

1. Connect the RUCKUS Edge, switches and APs in the desired topology.
2. Add the RUCKUS Edge, switches and APs in the RUCKUS One for management.
3. Create users/PANs (Network Segments) and associated PIN configuration for RUCKUS Edge, switches and APs.
4. RUCKUS Edge is on-boarded on the RUCKUS One device, followed by switches and APs. All the configuration is applied and network is ready for operation.
5. UEs connect to the switches and APs, authentication is completed. The UEs are associated with the PAN and is online.

Pre-requisites for Configuring Personal Identity Network

Associated DHCP service should be configured before configuring the Personal Identity Network.

The Personal Identity Network service can be applied to a RUCKUS Edge after the device is onboarded and the DHCP service is applied to the specific device.

Before starting the configuration, make sure APs, Identities, and DPSK settings are configured on the device.

For PIN configuration flow, RUCKUS Edge cluster must be selected instead of the RUCKUS Edge node.

Configuring Personal Identity Network for Access Points

Adding DPSK Service

Dynamic Pre-Shared Key is a encryption technology developed to provide robust and secure wireless access.

To add a DPSK service to configure PIN, perform the following steps.

1. On the RUCKUS One navigation bar, hover on **Network Control** and click **My Services**.

   This displays the **My Services** menu.

2. Click **DPSK** option in the menu.

   This displays **DPSK** page.

3. Click **Add DPSK Service**.

   This displays **Add DPSK Service** page.

4. In the **Add DPSK Service** page, enter the following details:

   Under **Settings** enter the service name

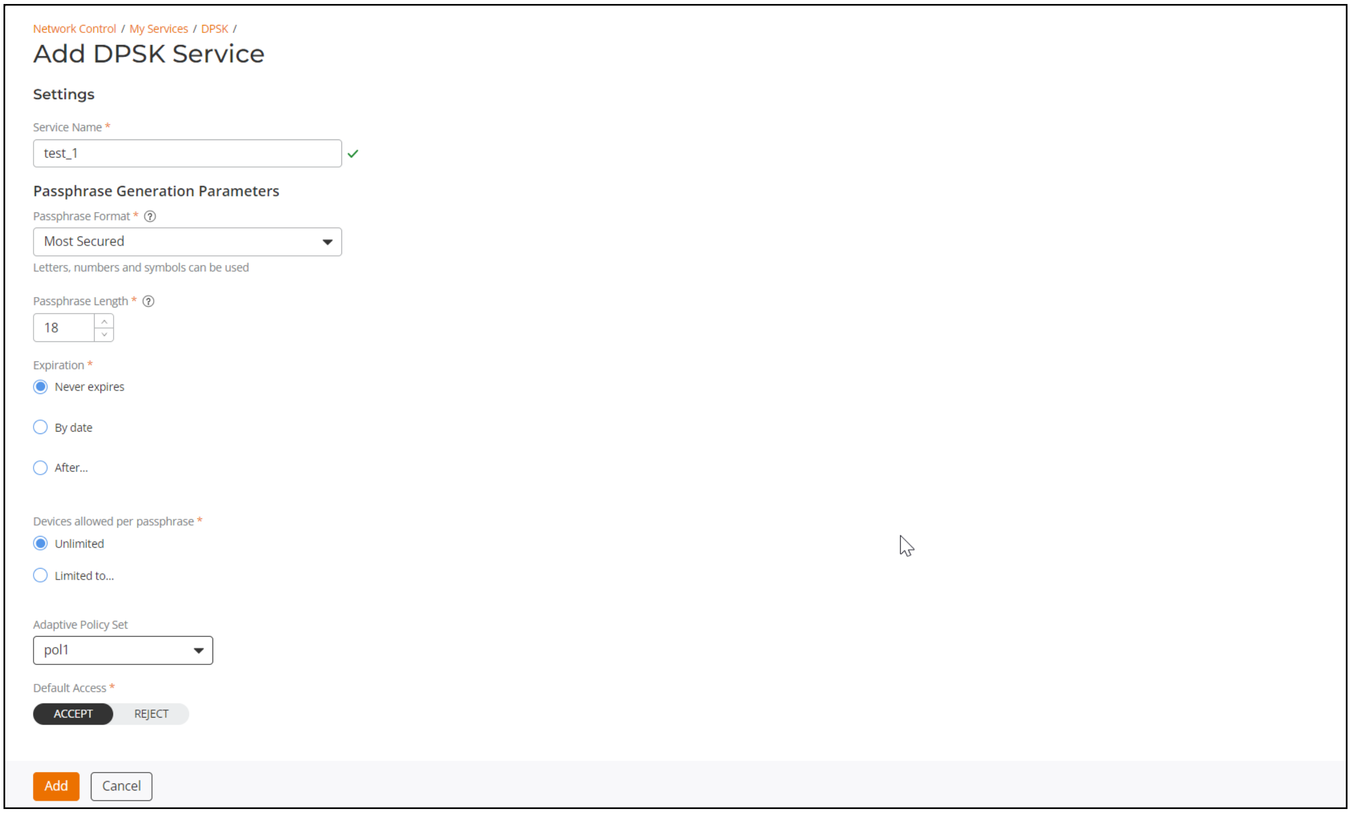
   - **Service Name** - Enter a name for the DPSK service.

   Under **Passphrase Generation Parameters** enter the following details:

   - **Passphrase Format** - Click on the drop-down menu and select the passphrase format.
     - Most Secured - Allows the user to use all ASCII characters.
     - Keyboard Friendly - Only Alphabets and numbers can be used.
     - Numbers Only - Only numbers can be used.
   - **Passphrase Length** - Enter the passpharse length. Valid range 8 to 63.
   - **Expiration** - Select the expiration type,
     - Never Expires - Have no expiry date.
     - By Date - Select a date from the corresponding calendar.
     - After - Enter a number in the corresponding field and choose the option from the drop-down list.
   - **Devices Allowed per Passphrase** - Select the number of devices to be allowed per passphrase.
     - Unlimited - No restrictions in terms of number of devices.
     - Limited To - Enter the number of devices that can be used with one passphrase in the corresponding field.
   - **Adaptive Policy Set** - Select the policy set from the drop-down list.
   - **Default Access** - Select the access method.

   After entering all the fields, click **Add**. The newly created DPSK service is added to the list.

FIGURE 87 Add DPSK Service



Network Control / My Services / DPSK /

Add DPSK Service

Settings

Service Name *
test_1

Passphrase Generation Parameters

Passphrase Format *
Most Secured
Letters, numbers and symbols can be used

Passphrase Length *
18

Expiration *
● Never expires
○ By date
○ After...

Devices allowed per passphrase *
● Unlimited
○ Limited to...

Adaptive Policy Set
pol1

Default Access *
ACCEPT REJECT

Creating a New DPSK Network

Create a new DPSK network using the newly created DPSK service from Wi-Fi networks.

To create a new DPSK network, perform the following steps.

1. On the RUCKUS One navigation bar, hover on **Wi-Fi** and click **Wi-Fi Networks List**.

   This displays **Create a New Network** page.
2. In the **Create a New Network** page, enter the details in each section.

Network Details

Enter the following details in this section.

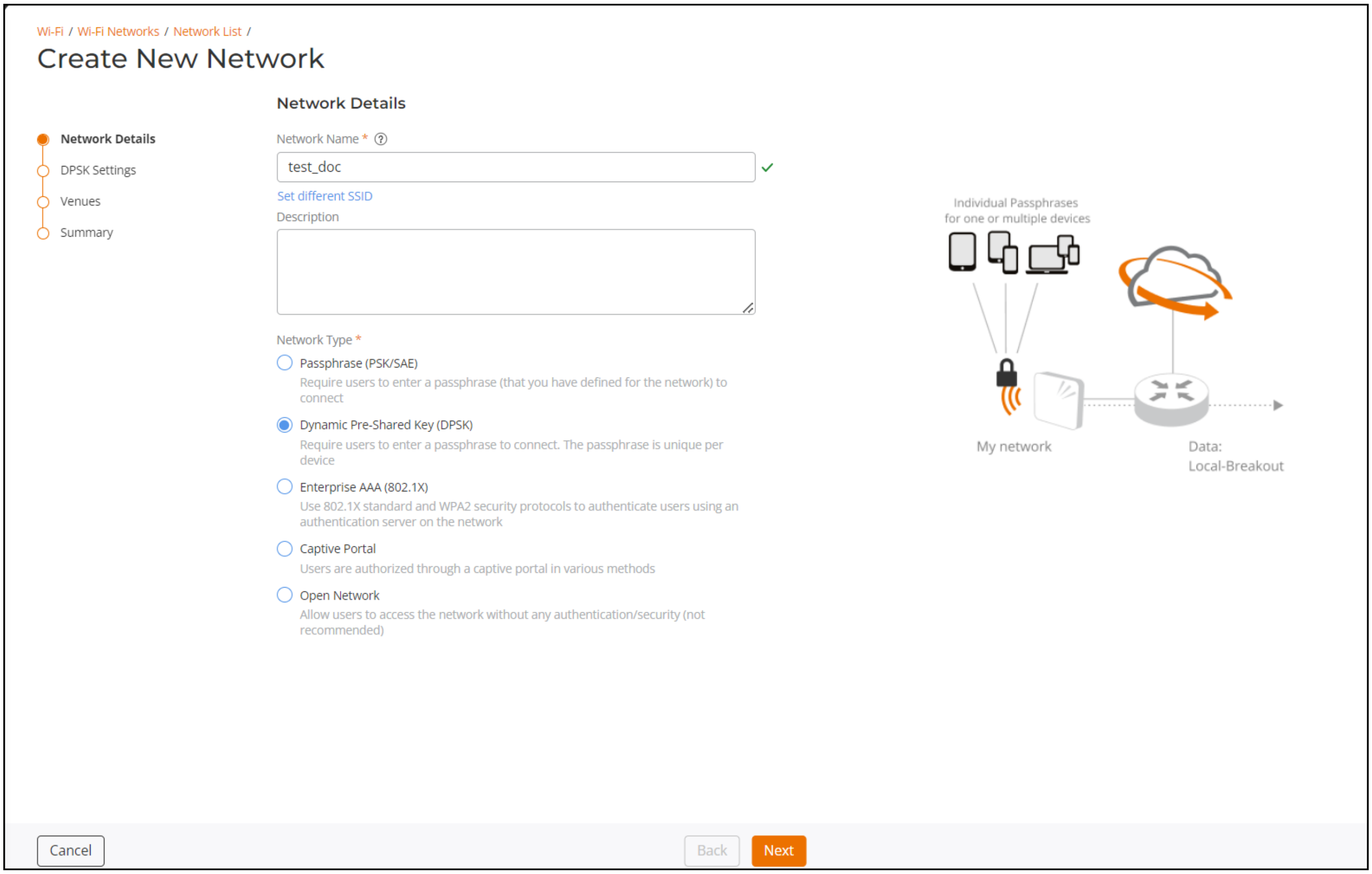
- **Network Name** - By default, network SSID is used as the network name, however, enter a network name for easier usage. Length of the network name is limited to 2-32 characters.

  > **NOTE**
  > To set a different SSID, click **Set different SSID** link.

- **Description** - Enter a purposeful description for the network name.
- **Network Type** - Select a network type from the options listed in the network type.

Click **Next**.

FIGURE 88 Create New Network



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

Create New Network

Network Details

- ● Network Details
- ○ DPSK Settings
- ○ Venues
- ○ Summary

Network Details

Network Name * ⓘ

test_doc ✓

Set different SSID

Description

Network Type *

○ Passphrase (PSK/SAE)
Require users to enter a passphrase (that you have defined for the network) to connect

● Dynamic Pre-Shared Key (DPSK)
Require users to enter a passphrase to connect. The passphrase is unique per device

○ Enterprise AAA (802.1X)
Use 802.1X standard and WPA2 security protocols to authenticate users using an authentication server on the network

○ Captive Portal
Users are authorized through a captive portal in various methods

○ Open Network
Allow users to access the network without any authentication/security (not recommended)

DPSK Settings

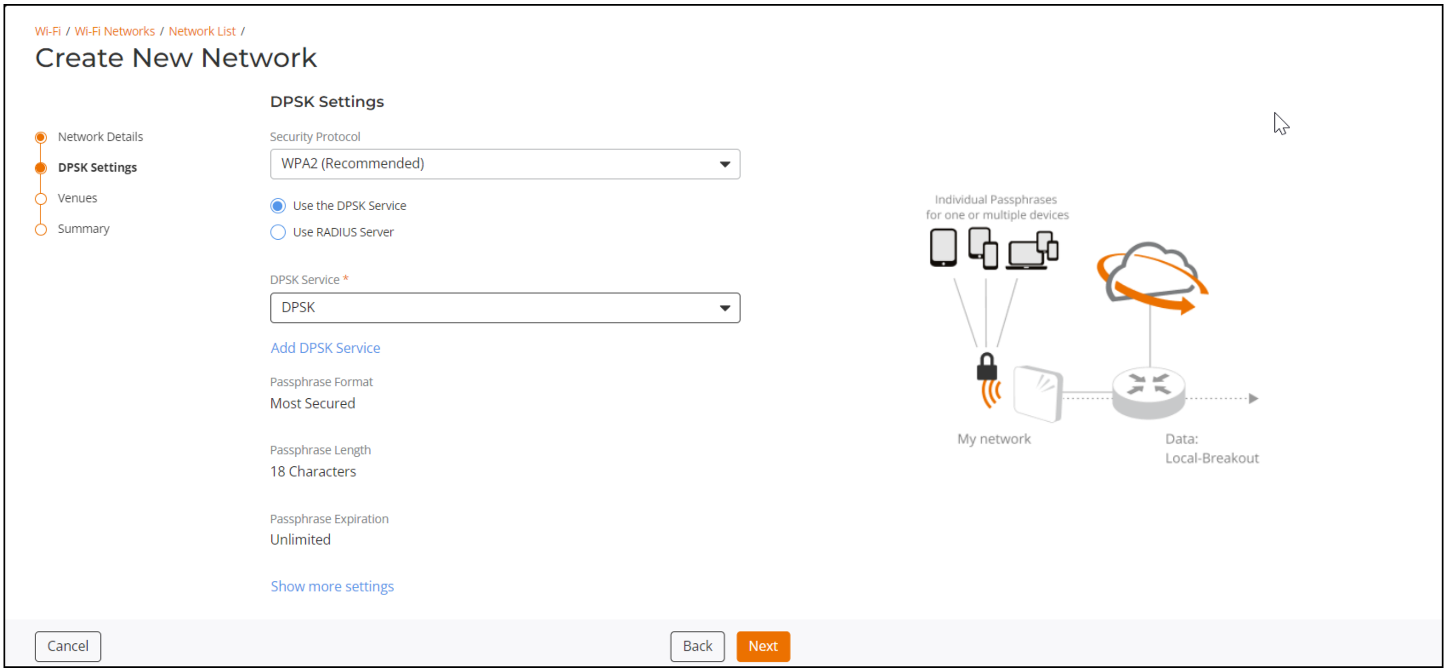
Enter the following details in this section.

- **Security Protocol** - Select the protocol from the drop-down list. Recommended protocol is WPA2 (Wi-Fi Protected Access 2) as it is an encrypted security protocol that protects internet traffic on wireless networks.
- **DPSK Service** - Select the DPSK service from the drop-down list. The list displays all the DPSK service names which are created in the **Network Control** > **My Services** > **DPSK**.

The other options are auto selected as per the DPSK service.

Click **Next**.

FIGURE 89 DPSK Settings



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

Create New Network

DPSK Settings

- ● Network Details
- ● **DPSK Settings**
- ○ Venues
- ○ Summary

Security Protocol
WPA2 (Recommended)

● Use the DPSK Service
○ Use RADIUS Server

DPSK Service *
DPSK

Add DPSK Service

Passphrase Format
Most Secured

Passphrase Length
18 Characters

Passphrase Expiration
Unlimited

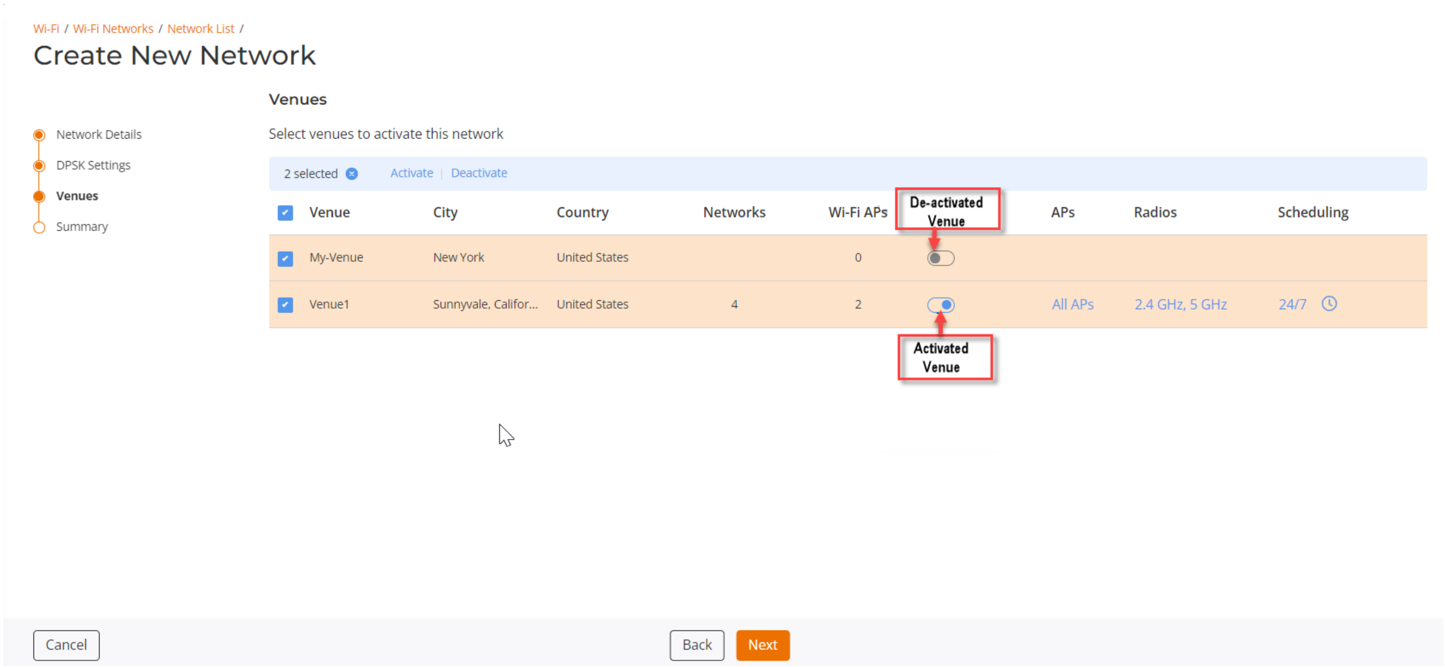
Show more settings

Venues

Select the venue or venues (multiple venues can be selected) and click **Activate**. Likewise, select the a venue or venues and click **Deactivate** to shutdown the venue or venues.

After activating the venue, click **Next**.

FIGURE 90 Activating/De-activating Venue



Create New Network

Venues

Select venues to activate this network

2 selected ⊗ Activate | Deactivate

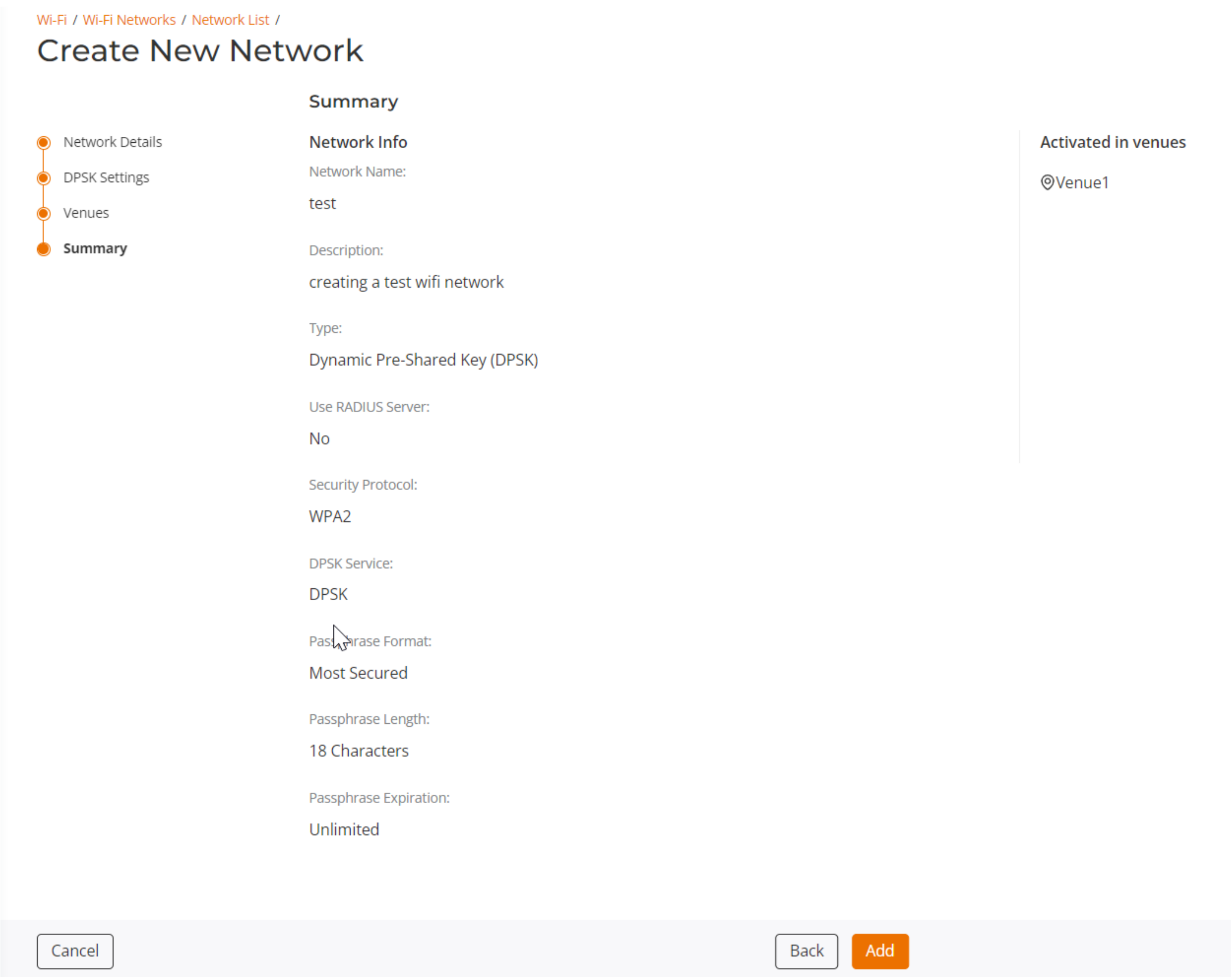
☑	Venue	City	Country	Networks	Wi-Fi APs	De-activated Venue	APs	Radios	Scheduling
☑	My-Venue	New York	United States		0	○			
☑	Venue1	Sunnyvale, Califor...	United States	4	2	●	All APs	2.4 GHz, 5 GHz	24/7

Activated Venue

Summary

The summary section displays the complete configuration of the newly created DPSK network. Verify the content and click **Add**.

FIGURE 91 Summary



Summary

Network Info

Network Name:
test

Description:
creating a test wifi network

Type:
Dynamic Pre-Shared Key (DPSK)

Use RADIUS Server:
No

Security Protocol:
WPA2

DPSK Service:
DPSK

Passphrase Format:
Most Secured

Passphrase Length:
18 Characters

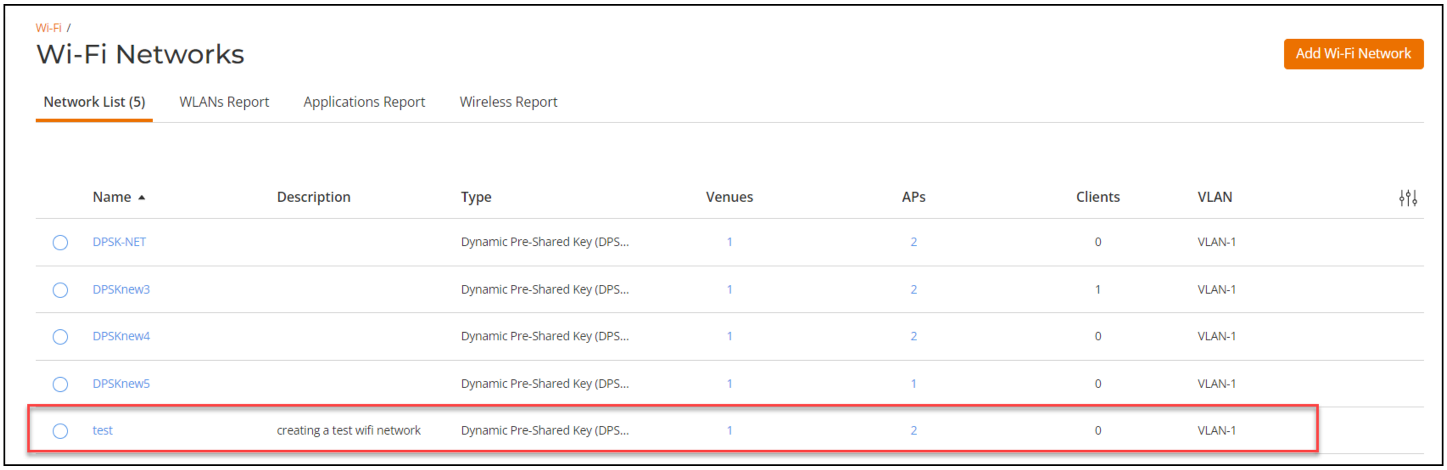
Passphrase Expiration:
Unlimited

Activated in venues

Venue1

The newly added Wi-Fi Network is displayed in the **Wi-Fi Networks** list.

FIGURE 92 Newly created Wi-Fi Network



Wi-Fi /

Wi-Fi Networks

	Name ▲	Description	Type	Venues	APs	Clients	VLAN
○	DPSK-NET		Dynamic Pre-Shared Key (DPS...	1	2	0	VLAN-1
○	DPSKnew3		Dynamic Pre-Shared Key (DPS...	1	2	1	VLAN-1
○	DPSKnew4		Dynamic Pre-Shared Key (DPS...	1	2	0	VLAN-1
○	DPSKnew5		Dynamic Pre-Shared Key (DPS...	1	1	0	VLAN-1
○	test	creating a test wifi network	Dynamic Pre-Shared Key (DPS...	1	2	0	VLAN-1

Creating a new Tunnel Profile

Tunnel profile allows the user to verify connectivity between VPN peers. Configuring tunnel interface can be used to ping a destination IP at specified intervals if the communication across the tunnel is broken.

To configure a tunnel profile, perform the following steps:

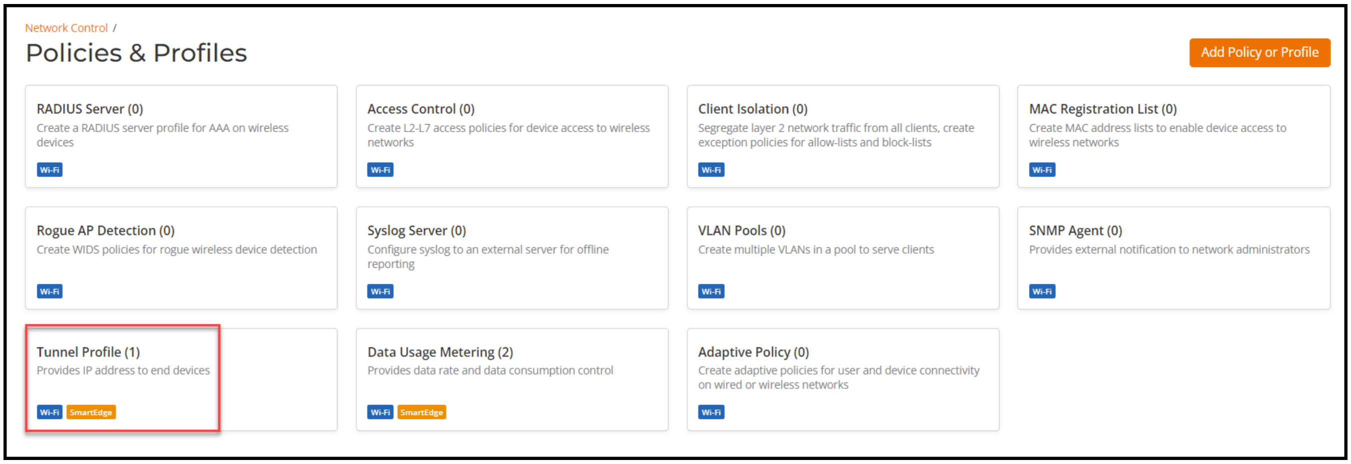
1. On the RUCKUS One navigation bar, hover mouse on **Network Control** and select **Policies and Profiles**. .

   This displays **Policies and Profiles** page.

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

   This displays **Tunnel Profile** page.

   FIGURE 93 Tunnel Profile



Network Control /

Policies & Profiles

RADIUS Server (0)
Create a RADIUS server profile for AAA on wireless devices
Wi-Fi

Access Control (0)
Create L2-L7 access policies for device access to wireless networks
Wi-Fi

Client Isolation (0)
Segregate layer 2 network traffic from all clients, create exception policies for allow-lists and block-lists
Wi-Fi

MAC Registration List (0)
Create MAC address lists to enable device access to wireless networks
Wi-Fi

Rogue AP Detection (0)
Create WIDS policies for rogue wireless device detection
Wi-Fi

Syslog Server (0)
Configure syslog to an external server for offline reporting
Wi-Fi

VLAN Pools (0)
Create multiple VLANs in a pool to serve clients
Wi-Fi

SNMP Agent (0)
Provides external notification to network administrators
Wi-Fi

Tunnel Profile (1)
Provides IP address to end devices
Wi-Fi SmartEdge

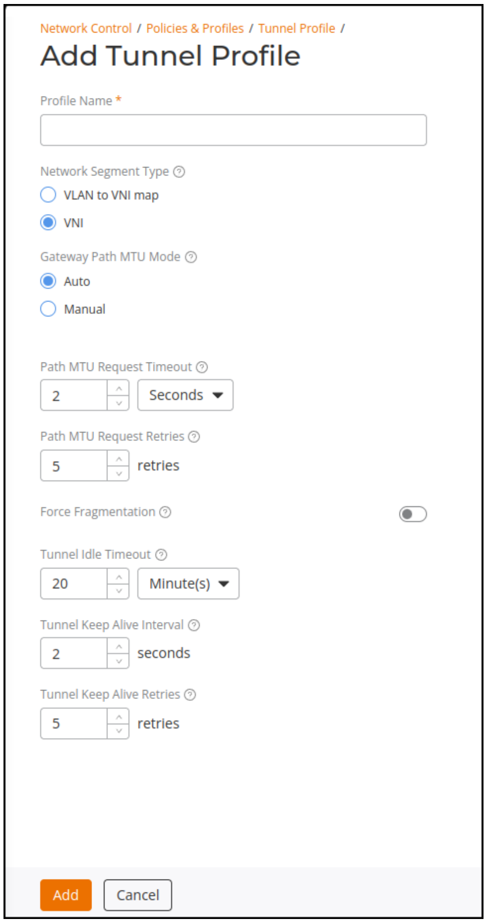
Data Usage Metering (2)
Provides data rate and data consumption control
Wi-Fi SmartEdge

Adaptive Policy (0)
Create adaptive policies for user and device connectivity on wired or wireless networks
Wi-Fi

3. Click **Add Tunnel Profile** and enter the following details:
   - **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. The **VNI** option is used for the PIN feature.
   - **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.

FIGURE 94 Add Tunnel Profile



Network Control / Policies & Profiles / Tunnel Profile /

Add Tunnel Profile

Profile Name *

Network Segment Type
○ VLAN to VNI map
● VNI

Gateway Path MTU Mode
● Auto
○ Manual

Path MTU Request Timeout: 2 Seconds

Path MTU Request Retries: 5 retries

Force Fragmentation

Tunnel Idle Timeout: 20 Minute(s)

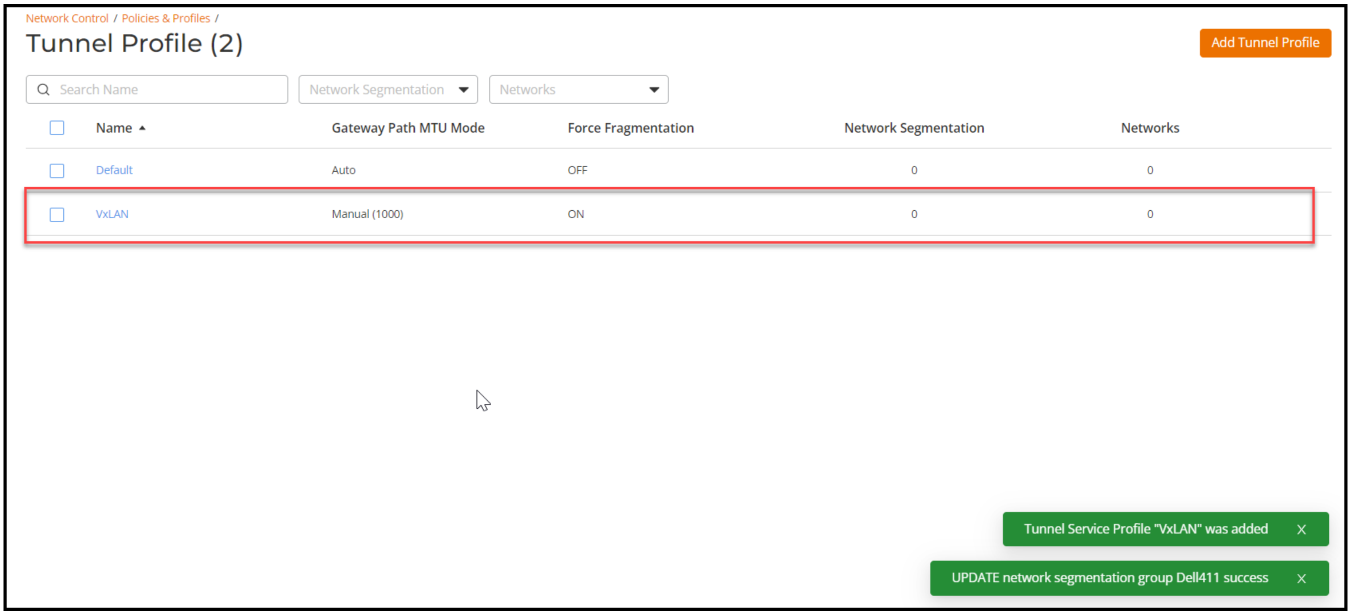
Tunnel Keep Alive Interval: 2 seconds

Tunnel Keep Alive Retries: 5 retries

4. After entering all the fields, click **Add**.

   The newly created tunnel profile is displayed in the **Tunnel Profile** page.

   FIGURE 95 New Tunnel Profile



	Name	Gateway Path MTU Mode	Force Fragmentation	Network Segmentation	Networks
□	Default	Auto	OFF	0	0
□	VxLAN	Manual (1000)	ON	0	0

Tunnel Service Profile "VxLAN" was added X

UPDATE network segmentation group Dell411 success X

Creating a New Identity Group

Identity group stores user related data.

To create a new Identity group, perform the following steps.

1. On the RUCKUS One navigation bar, hover on **Clients** and click **Identity Groups**.

   This displays **Identity Management** page.

2. In the **Identity Management** page, click **Add Identity Group** link.

   This displays **Create Identity Group** window.

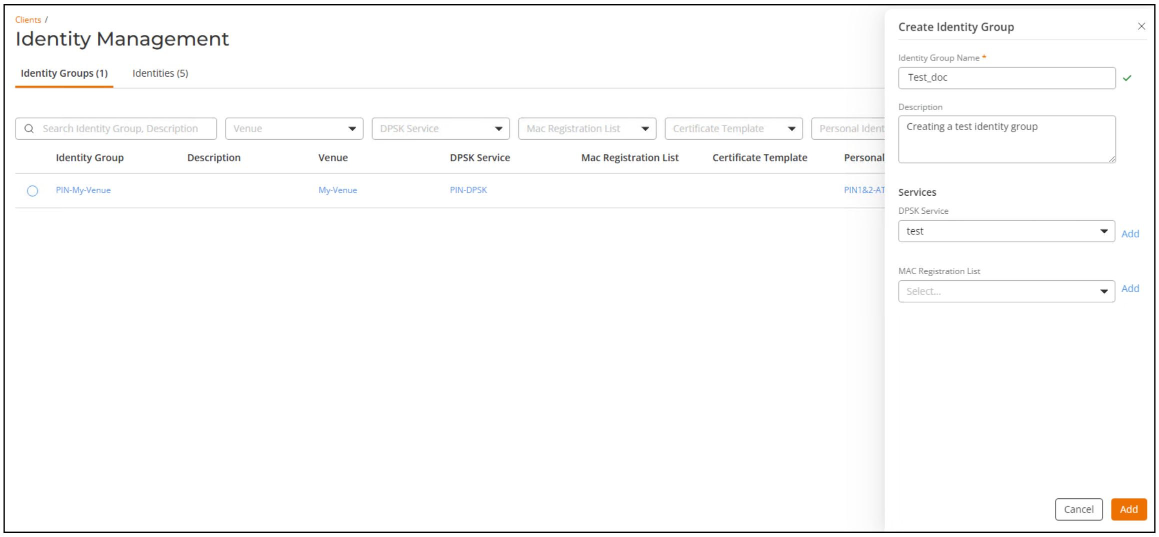
3. In the **Create Identity Group**, enter the following details

- **Identity Group Name** - Select identity group name from the drop-down list.
- **Description** - Enter a meaningful description for the identity group.

  Under **Services**,

- **DPSK Service** - Select a DPSK service from the drop-down list or add a DPSK service by clicking **Add** link.
- **MAC Registrationi List** - Select a MAC ID from the drop-down list or add a MAC by clicking **Add** link.

FIGURE 96 Creating a new Identity Group



Clients /

Identity Management

Identity Groups (1) Identities (5)

	Identity Group	Description	Venue	DPSK Service	Mac Registration List	Certificate Template	Personal
○	PIN-My-Venue		My-Venue	PIN-DPSK			PIN1&2-AT

Create Identity Group

Identity Group Name *: Test_doc

Description: Creating a test identity group

Services

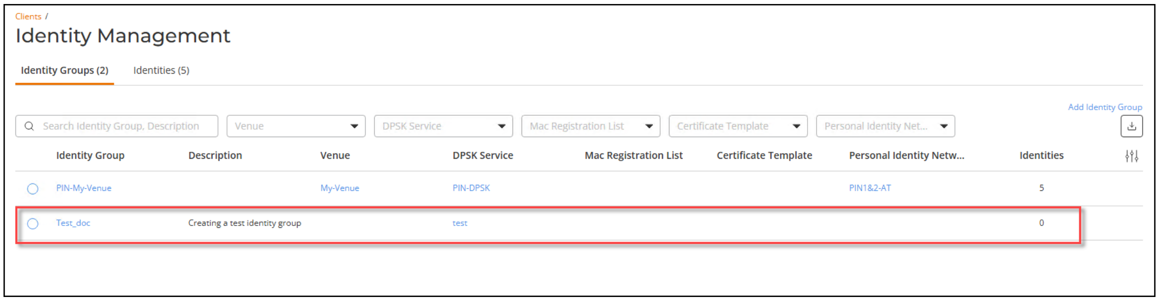
DPSK Service: test

MAC Registration List: Select...

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

   The newly added identity group is displayed in the **Identity Management** page.

FIGURE 97 Newly created Identity Group in the Identity Management List



Clients /

Identity Management

Identity Groups (2) Identities (5)

	Identity Group	Description	Venue	DPSK Service	Mac Registration List	Certificate Template	Personal Identity Netw...	Identities
○	PIN-My-Venue		My-Venue	PIN-DPSK			PIN1&2-AT	5
○	Test_doc	Creating a test identity group		test				0

Enabling Property Management

Enable property management in the venue. To enable property management, perform the following steps.

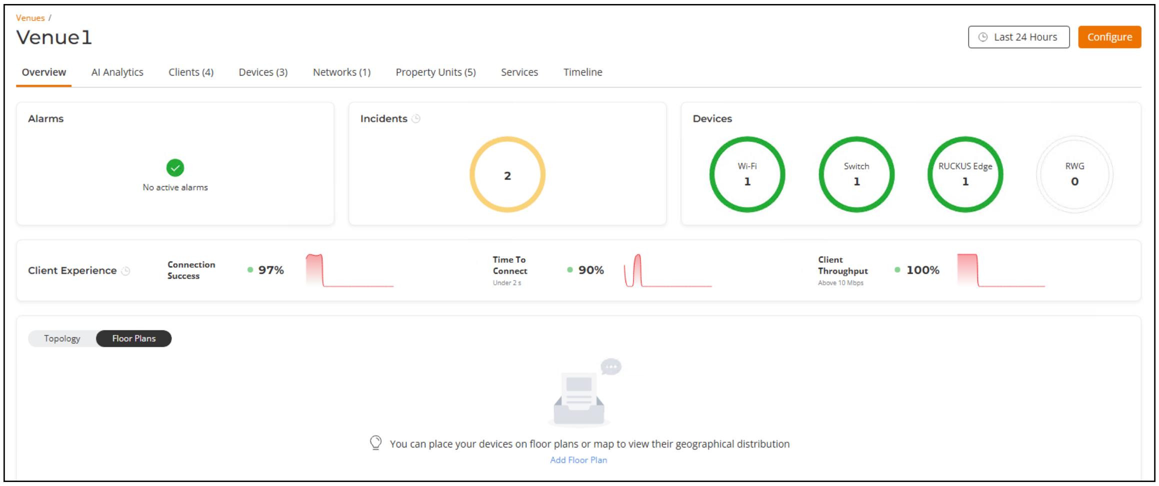
1. On the RUCKUS One navigation bar, click **Venue**.

   This displays **Venues** page with the list of venues.

2. Select and click on the **Venue** in the list.

   This displays the venue details.

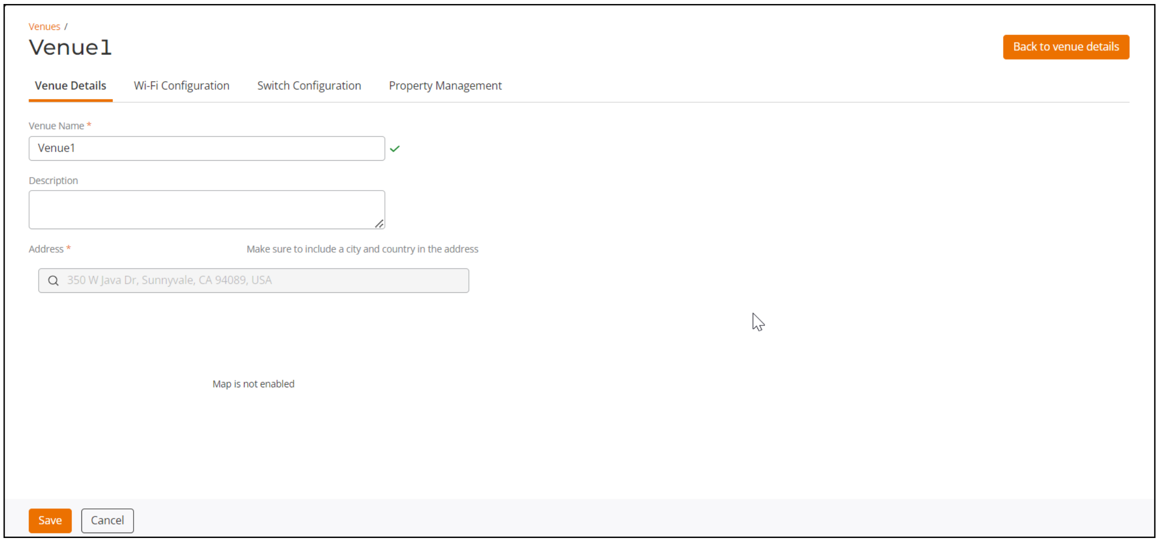
FIGURE 98 Venue Details



3. In the **Venue** page, click **Configure**.

   This displays the selected venue configuration details.

FIGURE 99 Venue Details



Venue Name * Venue1

Description

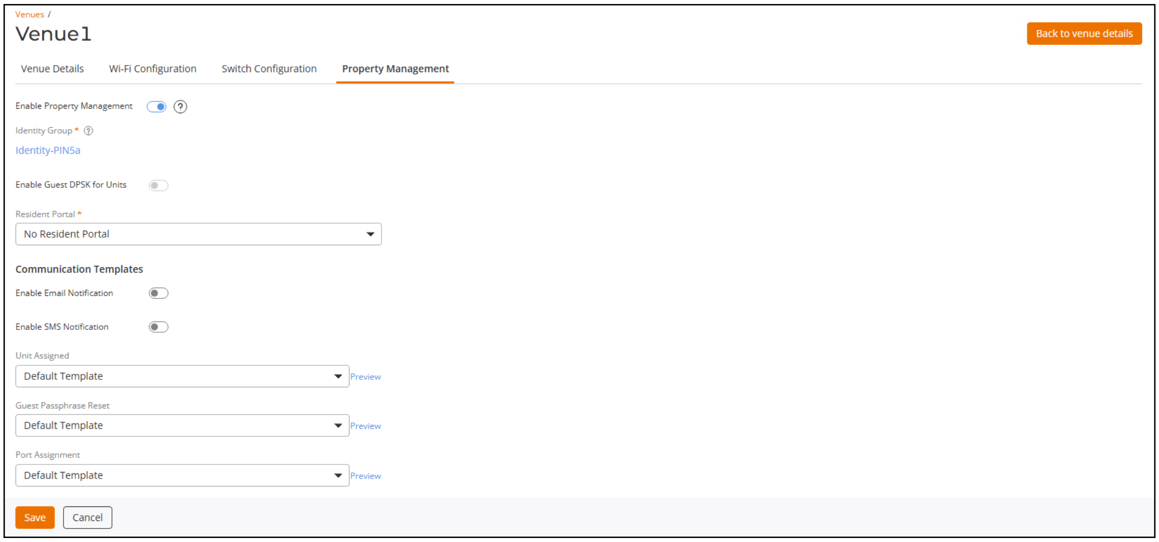
Address * 350 W Java Dr, Sunnyvale, CA 94089, USA

4. In the **Venue** details page, click **Property Management** tab.

   This displays the **Property Management** switch.

   NOTE
   By default, the **Property Management** switch is disabled, if the property management is swtiched off, all the related configuration is deleted and the network service is lost.

   FIGURE 100 Enable Property Management



Venues /

Venue1

Back to venue details

Venue Details | Wi-Fi Configuration | Switch Configuration | Property Management

Enable Property Management ●

Identity Group *

Identity-PIN5a

Enable Guest DPSK for Units ○

Resident Portal *

No Resident Portal

Communication Templates

Enable Email Notification ○

Enable SMS Notification ○

Unit Assigned

Default Template Preview

Guest Passphrase Reset

Default Template Preview

Port Assignment

Default Template Preview

Save Cancel

Personal Identity Network Configuration

To configure the Personal Identity Network, follow the sequence:

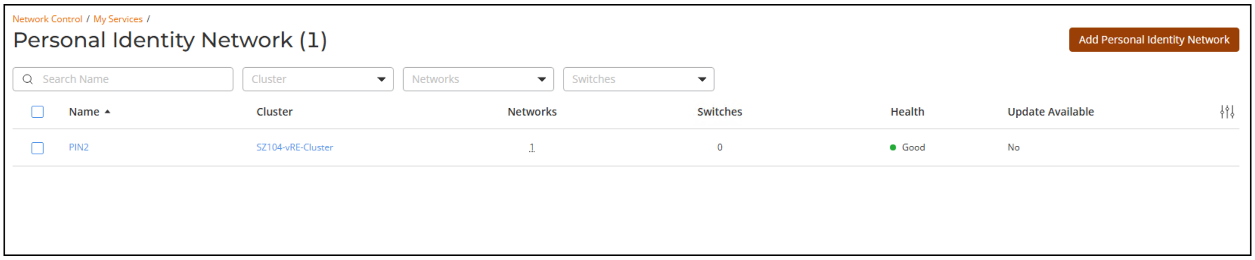
1. On the RUCKUS One navigation bar, navigate and hover the mouse on **Network Control** option.

   This displays options in the **Network Control**, click **My Services**.
2. In the **My Services** screen, click **Personal Identity Network**.

   This displays the **Personal Identity Network** screen.
3. Click **Add Personal Identity Network** button.

   This displays **Add Personal Identity Network** screen.

   FIGURE 101 Add Personal Identity Network



Network Control / My Services /

Personal Identity Network (1)

Add Personal Identity Network

Search Name | Cluster | Networks | Switches

□	Name ▲	Cluster	Networks	Switches	Health	Update Available
□	PIN2	SZ104-vRE-Cluster	1	0	● Good	No

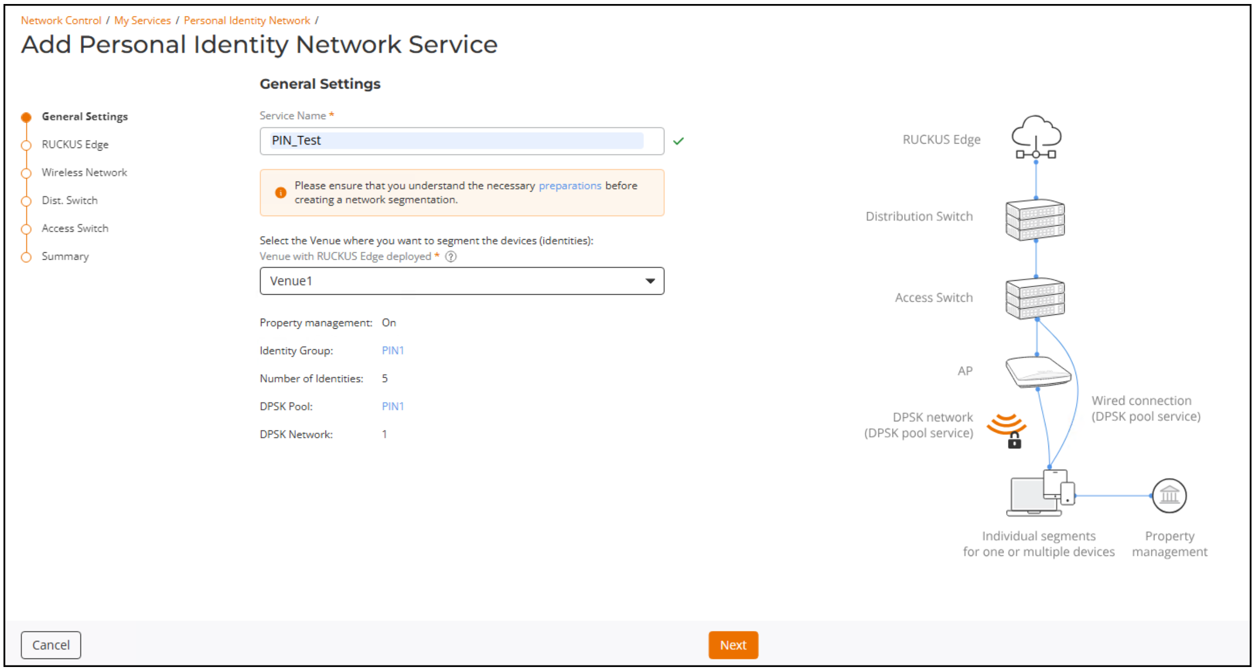
General Settings

In the **General Settings** screen, enter the following details:

- **Service Name** - Enter a name of the service.
- **Venue** - Select the venue to segment the devices (identities). To select the **Venue**, click **Venue with Property Management enabled** drop-down list and choose the venue. The selected venue displays the name of the **Identity Group**, **Number of Identity**, **DSPK Service** name and number of **DPSK Networks** available.

  After entering the above details, click **Next**

FIGURE 102 Add Personal Identity Network Service



Network Control / My Services / Personal Identity Network /

Add Personal Identity Network Service

- ● General Settings
- ○ RUCKUS Edge
- ○ Wireless Network
- ○ Dist. Switch
- ○ Access Switch
- ○ Summary

General Settings

Service Name *
PIN_Test ✓

Please ensure that you understand the necessary preparations before creating a network segmentation.

Select the Venue where you want to segment the devices (identities):
Venue with RUCKUS Edge deployed *
Venue1

Property management:	On
Identity Group:	PIN1
Number of Identities:	5
DPSK Pool:	PIN1
DPSK Network:	1

RUCKUS Edge
Distribution Switch
Access Switch
AP
DPSK network (DPSK pool service)
Wired connection (DPSK pool service)
Individual segments for one or multiple devices
Property management
Cancel
Next

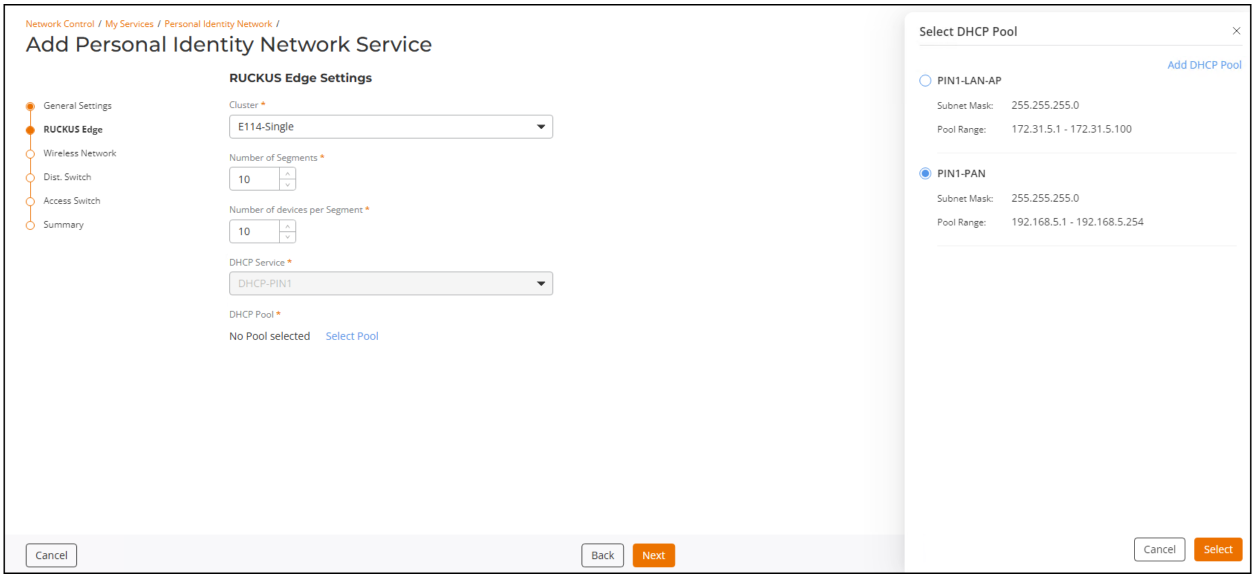
RUCKUS Edge Settings

In the **RUCKUS Edge Settings** screen, enter the following details:

- **RUCKUS Edge** - Select the device from the **RUCKUS Edge** drop-downlist.
- **Number of Segments** - Enter the number of segments required in the platform.
- **Number of Devices per Segment** - Enter the number of devices required in each segment.
- **DHCP Service** - The DHCP service associated with the selected **RUCKUS Edge** device is automatically selected.
- **DHCP Pool** - User should select one of the DHCP Pool as per the requirement. When selected the details of the pool are displayed on the screen.

After entering the above details, click **Next**.

FIGURE 103 RUCKUS Edge Settings



Network Control / My Services / Personal Identity Network /

Add Personal Identity Network Service

RUCKUS Edge Settings

Cluster *: E114-Single

Number of Segments *: 10

Number of devices per Segment *: 10

DHCP Service *: DHCP-PIN1

DHCP Pool *: No Pool selected

Select DHCP Pool

PIN1-LAN-AP
Subnet Mask: 255.255.255.0
Pool Range: 172.31.5.1 - 172.31.5.100

PIN1-PAN
Subnet Mask: 255.255.255.0
Pool Range: 192.168.5.1 - 192.168.5.254

Wireless Network Settings

In the **Wireless Network Settings** screen, select the **Tunnel Profile** from the drop-downlist or to add tunnel profile, click **Add**.

This displays **Add Tunnel Profile** window. Enter the following details:

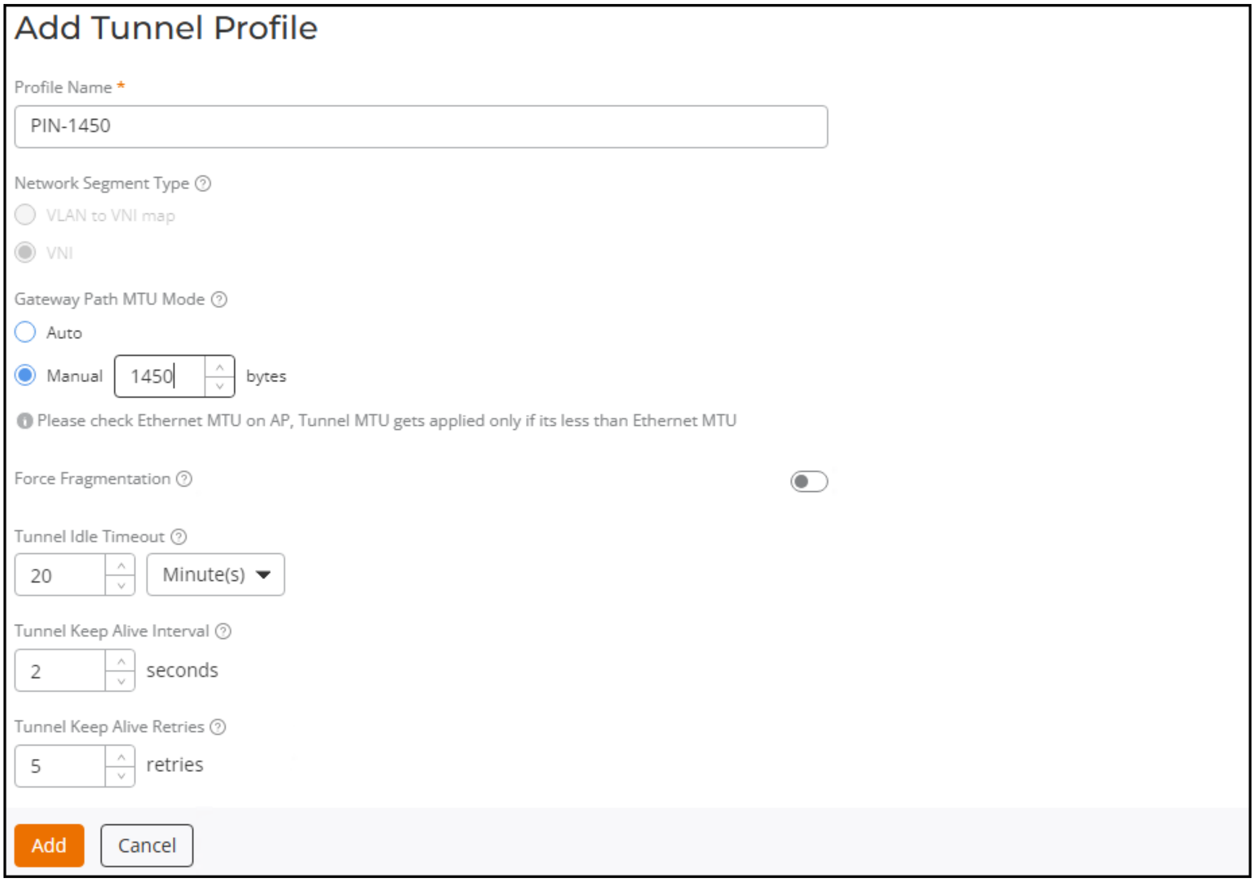
- **Profile Name**: Enter the name for the tunnel policy.
- **Network Segmentation Type**: The **VLAN to VNI map** option is selected by default. The **SD-LAN** service maps the VLAN ID to the VNI for tunneling. The **VNI** option is used for the PIN feature.
- **Gateway Path MTU Mode**: Select one of 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.

FIGURE 104 Add Tunnel Profile



Add Tunnel Profile

Profile Name *
PIN-1450

Network Segment Type
○ VLAN to VNI map
● VNI

Gateway Path MTU Mode
○ Auto
● Manual 1450 bytes

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

Force Fragmentation

Tunnel Idle Timeout
20 Minute(s)

Tunnel Keep Alive Interval
2 seconds

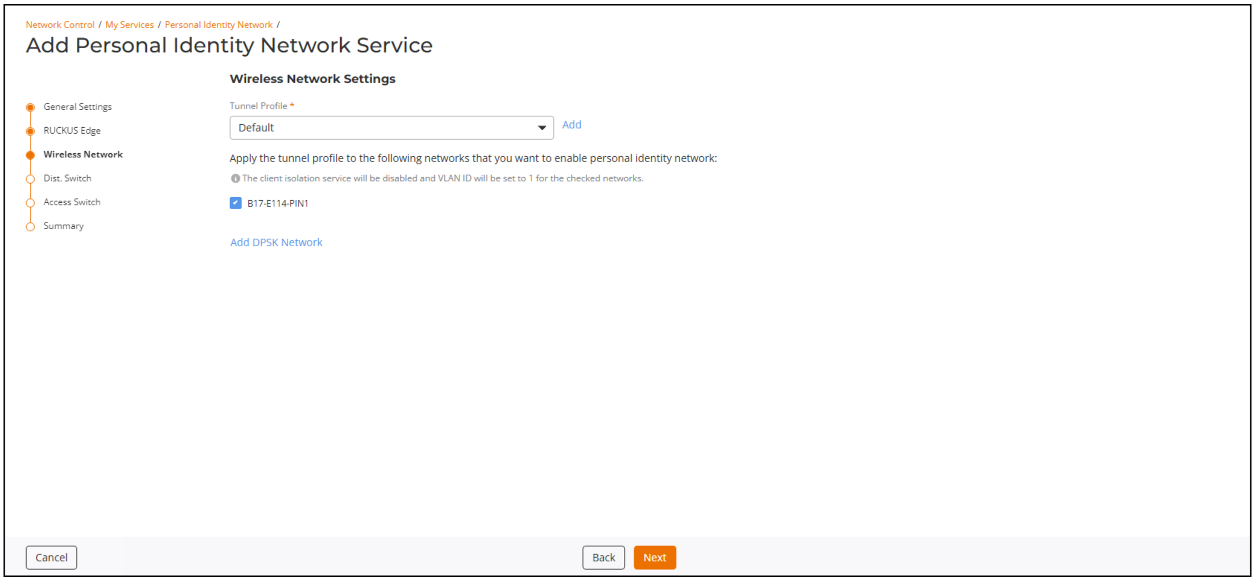
Tunnel Keep Alive Retries
5 retries

After entering the details, click **Add**. The newly added **Tunnel Profile** is displayed in the drop-down list.

Select the DPSK Network for PIN Service.

Click **Next**.

FIGURE 105 Wireless Network



Add Personal Identity Network Service

Wireless Network Settings

Tunnel Profile *: Default

Apply the tunnel profile to the following networks that you want to enable personal identity network:

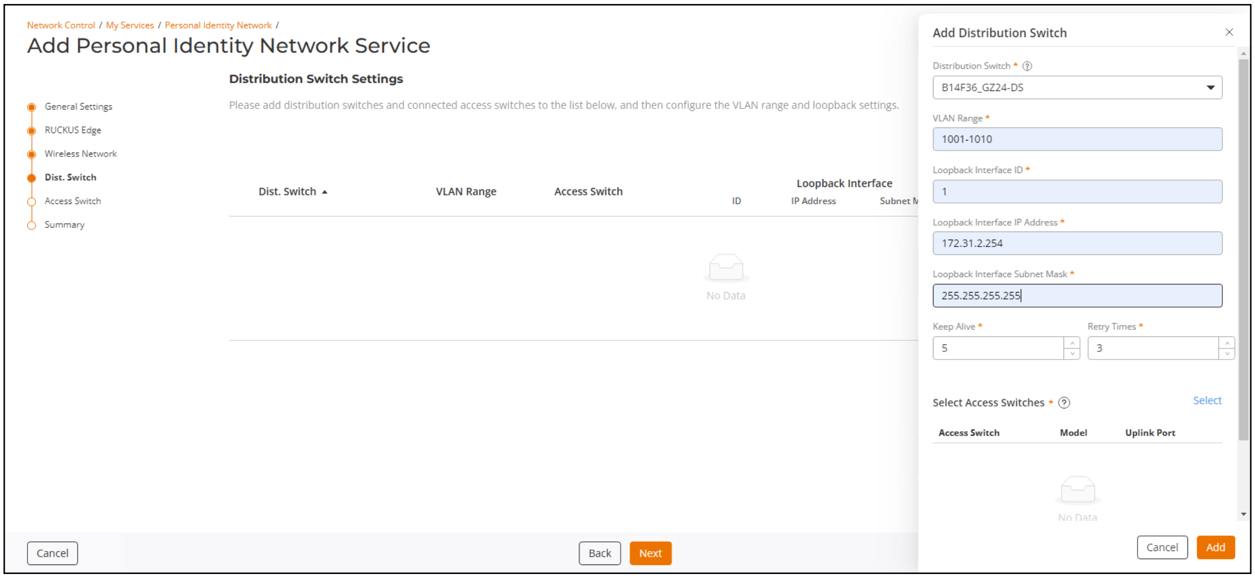
The client isolation service will be disabled and VLAN ID will be set to 1 for the checked networks.

☑ B17-E114-PIN1

Distribution Switch Settings

In the **Distribution Switch Settings** screen, by default the distribution switch associated with the selected RUCKUS Edge device is displayed in the window. However, to add a new distribution switch, click **Add Distribution Switch** and enter the details in the **Add Distribution Switch** window.

FIGURE 106 Add Distribution Switch



Add Personal Identity Network Service

Distribution Switch Settings

Please add distribution switches and connected access switches to the list below, and then configure the VLAN range and loopback settings.

Dist. Switch ▲	VLAN Range	Access Switch	Loopback Interface		
			ID	IP Address	Subnet M

No Data

Add Distribution Switch

Distribution Switch *: B14F36_GZ24-DS

VLAN Range *: 1001-1010

Loopback Interface ID *: 1

Loopback Interface IP Address *: 172.31.2.254

Loopback Interface Subnet Mask *: 255.255.255.255

Keep Alive *: 5

Retry Times *: 3

Select Access Switches *

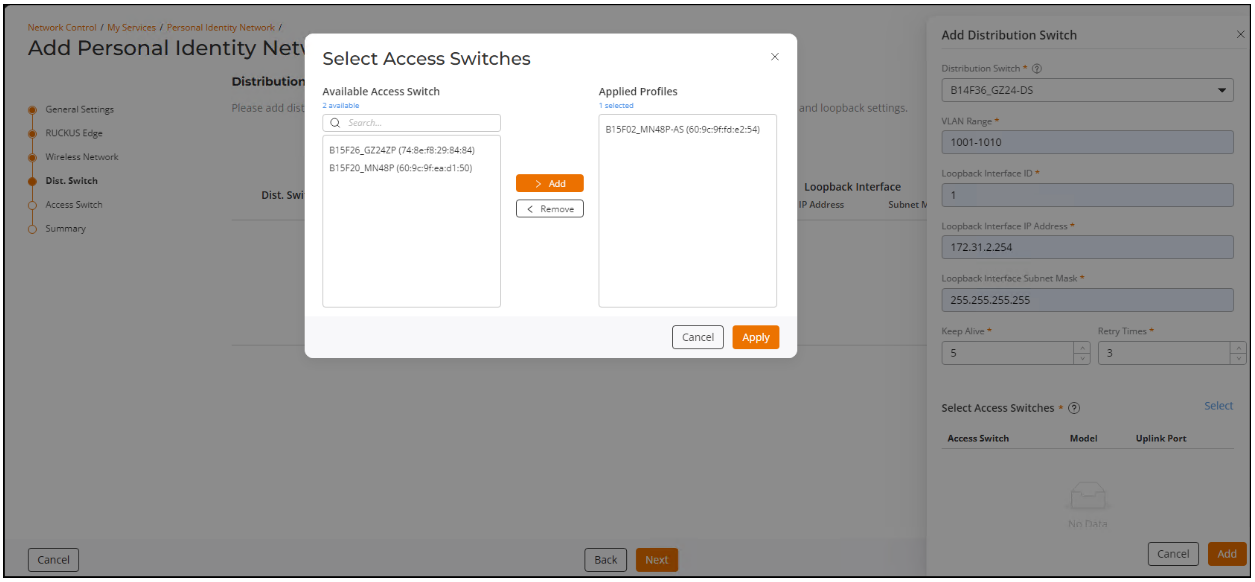
Access Switch	Model	Uplink Port

No Data

Access Switch Settings

Click the **Select** button to add associated Access Switch with the Distribution Switch.

FIGURE 107 Add Access Switch


Network Control / My Services / Personal Identity Network /

Add Personal Identity Netw

Distribution

Please add dist ... and loopback settings.

- General Settings
- RUCKUS Edge
- Wireless Network
- **Dist. Switch**
- Access Switch
- Summary

Dist. Swi | Loopback Interface IP Address | Subnet M

Select Access Switches

Available Access Switch
2 available

Search...

- B15F26_GZ24ZP (74:8e:f8:29:84:84)
- B15F20_MN48P (60:9c:9f:ea:d1:50)

Applied Profiles
1 selected

- B15F02_MN48P-AS (60:9c:9f:fd:e2:54)

Add Distribution Switch

Distribution Switch *: B14F36_GZ24-DS

VLAN Range *: 1001-1010

Loopback Interface ID *: 1

Loopback Interface IP Address *: 172.31.2.254

Loopback Interface Subnet Mask *: 255.255.255.255

Keep Alive *: 5

Retry Times *: 3

Select Access Switches *

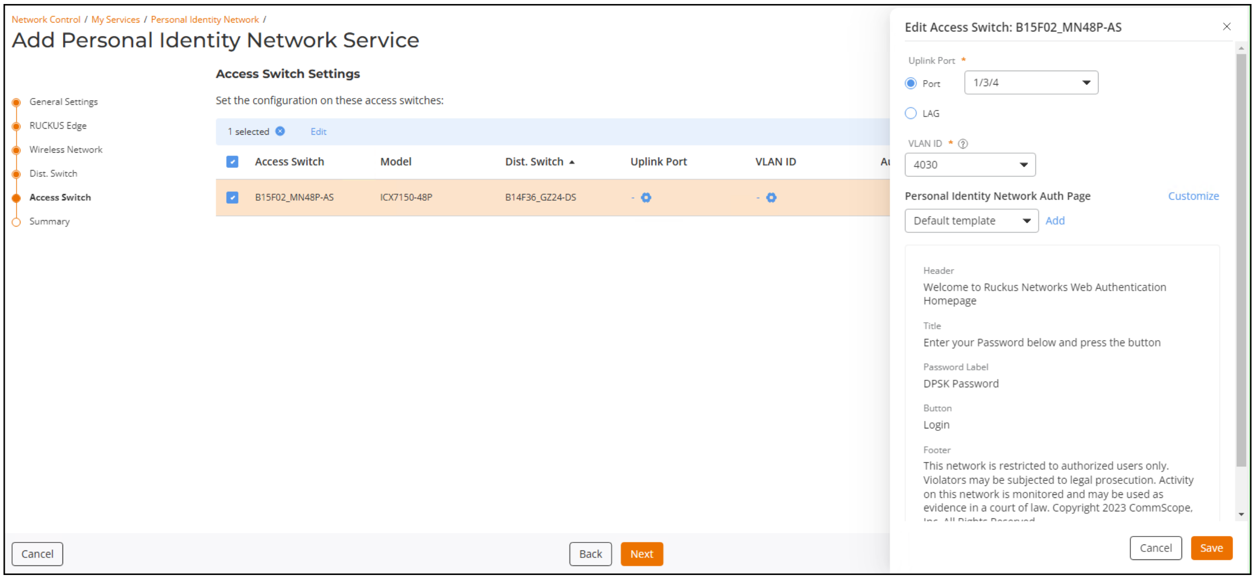
Access Switch	Model	Uplink Port

No Data

To add the associated access switch with the distribution switch, select the switch from the **Select Access Switches** list and click **Add** to move it to the **Applied Profiles**.

Click **Apply** to make the change effective.

FIGURE 108 Access Switch Settings


Network Control / My Services / Personal Identity Network /

Add Personal Identity Network Service

- General Settings
- RUCKUS Edge
- Wireless Network
- Dist. Switch
- **Access Switch**
- Summary

Access Switch Settings

Set the configuration on these access switches:

1 selected Edit

☑	Access Switch	Model	Dist. Switch ▲	Uplink Port	VLAN ID	Au
☑	B15F02_MN48P-AS	ICX7150-48P	B14F36_GZ24-DS	-	-	

Edit Access Switch: B15F02_MN48P-AS

Uplink Port *
● Port 1/3/4
○ LAG

VLAN ID *: 4030

Personal Identity Network Auth Page: Default template

Header
Welcome to Ruckus Networks Web Authentication Homepage

Title
Enter your Password below and press the button

Password Label
DPSK Password

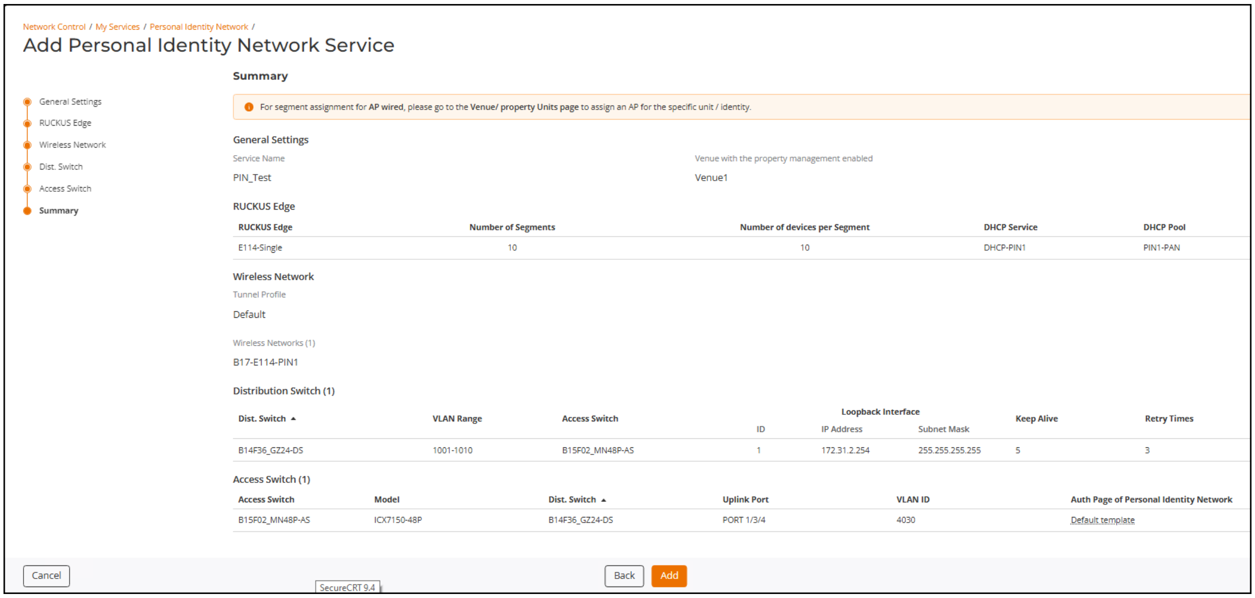
Button
Login

Footer
This network is restricted to authorized users only. Violators may be subjected to legal prosecution. Activity on this network is monitored and may be used as evidence in a court of law. Copyright 2023 CommScope, Inc. All Rights Reserved

Summary

The **Summary** screen displays all the selected entries, verify and click **Add** and edit or update any entry, click **Back**.

FIGURE 109 Summary



Add Personal Identity Network Service

Summary

For segment assignment for **AP wired**, please go to the **Venue/ property Units page** to assign an AP for the specific unit / identity.

General Settings

Service Name: PIN_Test

Venue with the property management enabled: Venue1

RUCKUS Edge

RUCKUS Edge	Number of Segments	Number of devices per Segment	DHCP Service	DHCP Pool
E114-Single	10	10	DHCP-PIN1	PIN1-PAN

Wireless Network

Tunnel Profile: Default

Wireless Networks (1): B17-E114-PIN1

Distribution Switch (1)

Dist. Switch ▲	VLAN Range	Access Switch	Loopback Interface			Keep Alive	Retry Times
			ID	IP Address	Subnet Mask		
B14F36_GZ24-DS	1001-1010	B15F02_MN48P-AS	1	172.31.2.254	255.255.255.255	5	3

Access Switch (1)

Access Switch	Model	Dist. Switch ▲	Uplink Port	VLAN ID	Auth Page of Personal Identity Network
B15F02_MN48P-AS	ICX7150-48P	B14F36_GZ24-DS	PORT 1/3/4	4030	Default template

Adding a Property Unit

A property unit is a Personal Area Network (PAN). PAN is described as a computer network that connects devices within a meters.

Property unit can be added Manually as well as imported from the local system through a .CSV file. To add a property unit to a Venue, perform the following steps.

1. On the RUCKUS One navigation bar, click **Venue**.

   This displays **Venues** page with the list of venues.

2. Select and click on the **Venue** in the list.

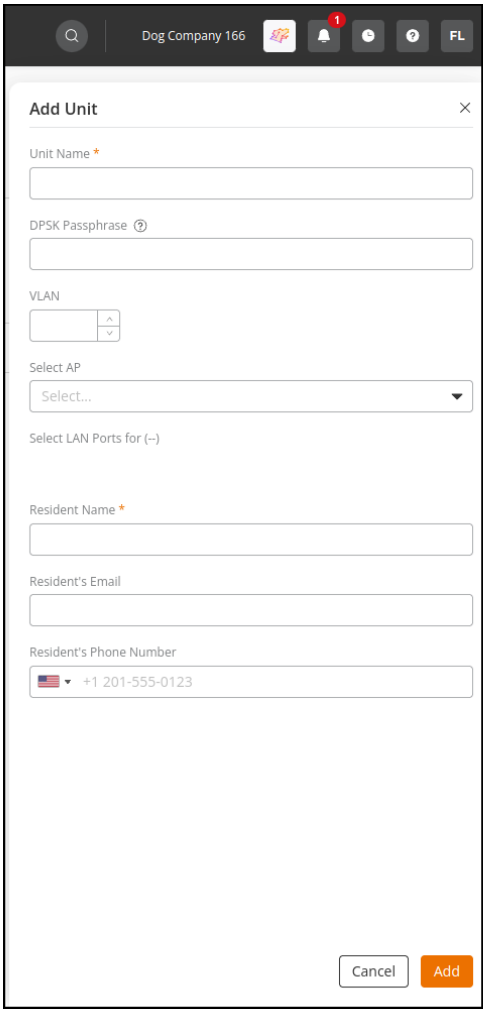
   This displays the venue details.

3. In the venue details, click **Add Unit** to add a unit manually.

   The **Add Unit** dialog box is displayed.

4. Complete the following fields:
   - **Unit Name**: Add a unit name for the propery units.
   - **DPSK Passphrase**: Enter a passphrase minimum eight characters that you want users to provide before they can access the network.
   - **VLAN**: Enter a VLAN ID (ranging from 1 through 4094).
   - **Select AP**: Select an access point from the drop-down list.
   - **Select LAN Ports**: Select LAN ports for the AP.
   - **Resident Name**: Enter a resident name.
   - **Resident's Email**: Enter a resident email.
   - **Resident's Phone Number**: Enter a resident phone number.

FIGURE 110 Add Unit



Dog Company 166

Add Unit

Unit Name *

DPSK Passphrase

VLAN

Select AP

Select...

Select LAN Ports for (--)

Resident Name *

Resident's Email

Resident's Phone Number

+1 201-555-0123

5. After entering the above fields, click **Add**.

   This displays the unit details.

6. In case of multiple units to be added, click **Import from File**.

   You can import multiple units at once, however it is not mandatory to import units in bulk.

   The **Import Units from File** dialog box is displayed.

7. Complete the following steps to import the unit.

   A CSV format of the file is available for download.

   a) Drag and drop a .CSV file or click **Browse** to locate the .CSV file, and click Open to upload it.

   b) (Optional) Click **Download template** to download the template or use file latest import.

   c) Using a spreadsheet application, open the .CSV file.

   d) Complete the following fields to identify the Unit:

      - **Unit Name**: Add a unit name for the propery units.
      - **DPSK Secret**: Enter a passphrase minimum eight characters that you want users to provide before they can access the network.
      - **Unit VLAN**: Enter a VLAN ID (ranging from 1 through 4094).
      - **Resident Name**: Enter a resident name.
      - **Email**: Enter a resident email.
      - **Phone Number**: Enter a resident phone number.

   e) Save the .CSV file.

   f) Click Import.

      If the import is successful, the **Import Units from File** dialog box displays with a message that units were imported successfully. If the import fails, the **Import Units from Files** dialog box displays an error message with details for each Units that failed to import.

8. Click **Add**.

   The personal units are added to the property.

Configuring Personal Identity Network for Switches

Adding a New Venue

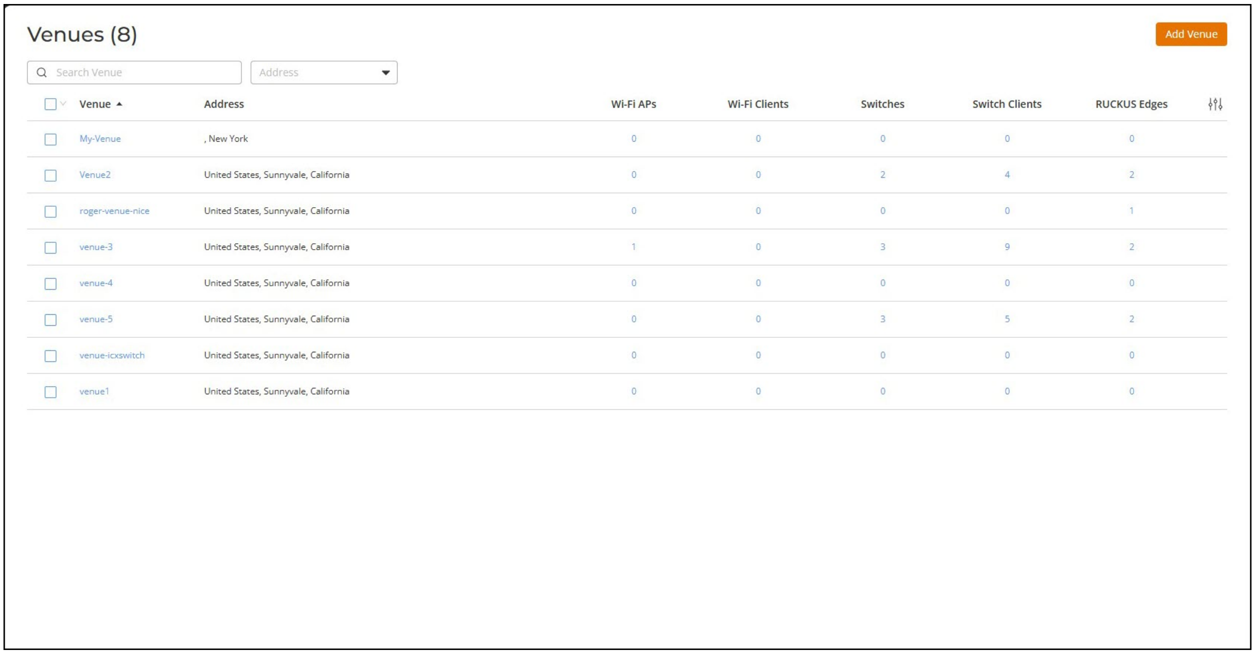
Venue is place where the Wi-Fi network is setup.

To add a new venue, perform the following steps.

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

   This displays the **Venues** page.

   FIGURE 111 Venues



Venues (8)

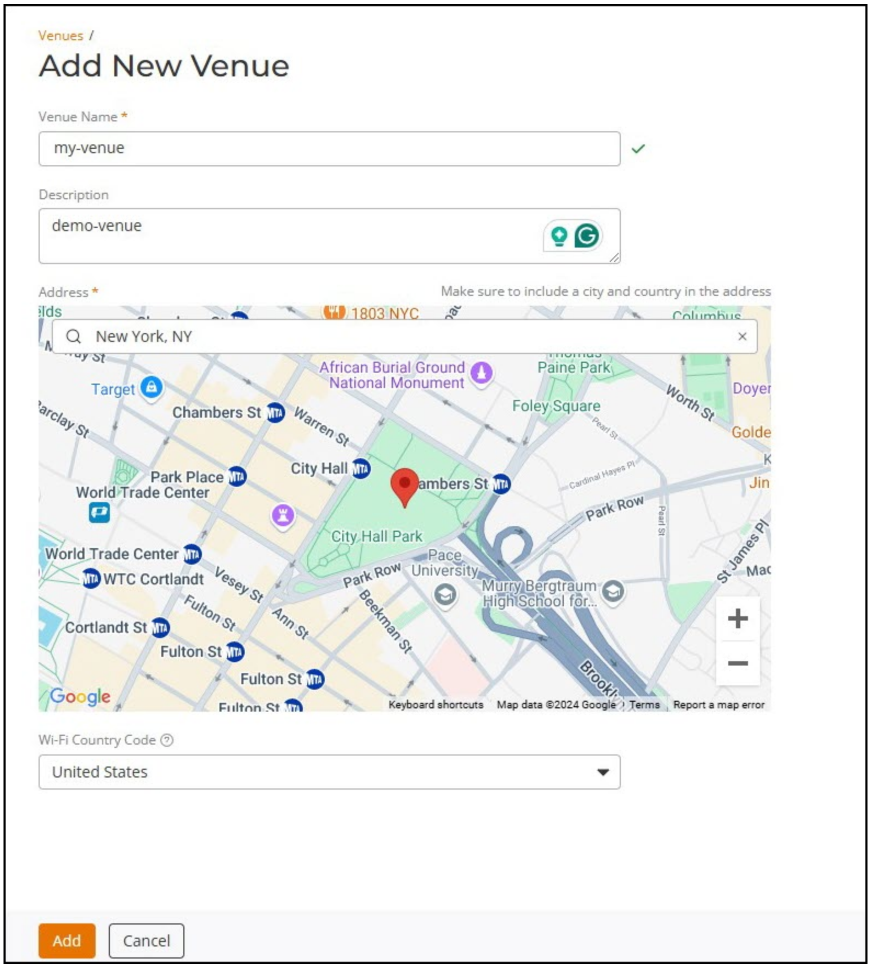
□	Venue ▲	Address	Wi-Fi APs	Wi-Fi Clients	Switches	Switch Clients	RUCKUS Edges
□	My-Venue	, New York	0	0	0	0	0
□	Venue2	United States, Sunnyvale, California	0	0	2	4	2
□	roger-venue-nice	United States, Sunnyvale, California	0	0	0	0	1
□	venue-3	United States, Sunnyvale, California	1	0	3	9	2
□	venue-4	United States, Sunnyvale, California	0	0	0	0	0
□	venue-5	United States, Sunnyvale, California	0	0	3	5	2
□	venue-icxswitch	United States, Sunnyvale, California	0	0	0	0	0
□	venue1	United States, Sunnyvale, California	0	0	0	0	0

2. In the **Venues** page, click **Add Venue** tab.

   This displays the **Add New Venue** page.

3. In the **Add New Venue**, enter the following details:
   - **Venue Name** - Enter a venue name for identifying the venue.
   - **Description** - Enter a description for the venue name.
   - **Address** - Enter the venue address or search by venue name to add the address of the venue.

FIGURE 112 Add a New Venue



Venues /

Add New Venue

Venue Name * my-venue

Description demo-venue

Address * Make sure to include a city and country in the address

New York, NY

Wi-Fi Country Code United States

Add Cancel

Configuring DHCP Service on RUCKUS Edge

The DHCP server assigns IP addresses to the hosts along configuration details.

In RUCKUS Edge, DHCP can be configured internally.

- Internal DHCP
- External DHCP

To configure DHCP internally, configure three DHCP pools.

- Pool One - (Optional) Configure IP addresses for switches or devices in the network.
- Pool Two - Webauth VLAN

- Pool Three - PIN Service

To configure DHCP internally, perform the following steps.

1. On the RUCKUS One navigation bar, hover on **Network Control** and click **My Services**.

   This displays **My Services** menu page.
2. Click **DHCP for RUCKUS Edge**.

   This displays **DHCP for RUCKUS Edge** page.

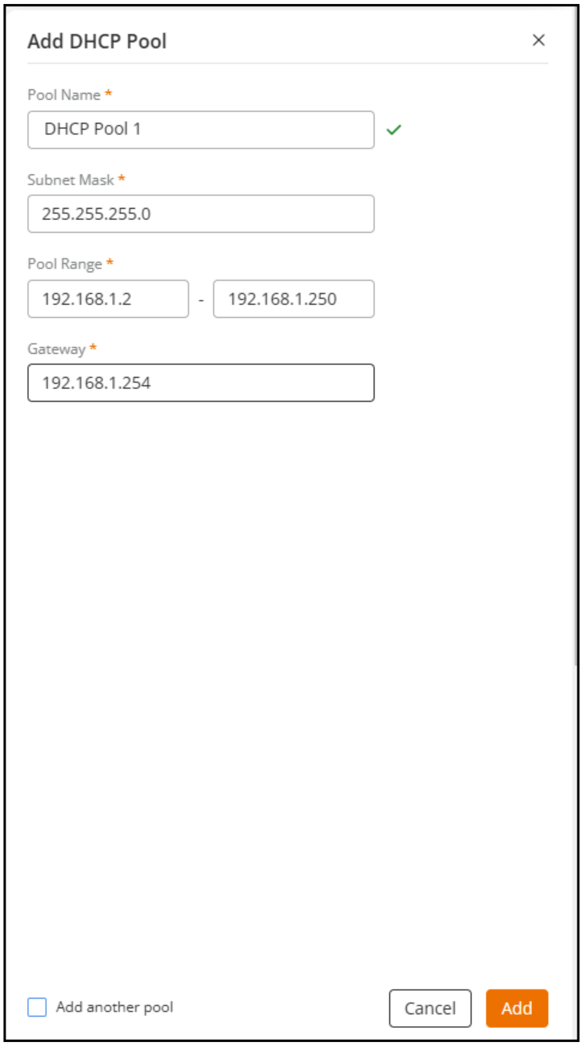
3. In the **DHCP for RUCKUS Edge** page, click **Add DHCP Service** and enter the following details -
   - **Service Name** - Enter service name.
   - **Primary DNS Server** - Primary DNS server is the main name server. This server stores IP address. Enter the IP address of the primary DNS server.

     NOTE
     A secondary DNS Server can be added by clicking the **Add Secondary DNS Server**, this server is used for reliability and to avoid over abundance.

   - **Lease Time** - Select the **Lease Time**.
     - **Limit To** - Enter any number and select the period from the corresponding drop-downlist.
     - **Infinite** - Have no expiry.
   - **Set DHCP Pool** - As described above, set three DHCP pools. To set DHCP pools, click **Add DHCP Pool**, this displays **Add DHCP Pool** window. Enter the following details -
     - Pool Name - Add a pool name.
     - Subnet Mask - Defines the range of IP addresses, it has two parts network bits and host bits. Enter a valid subnet mask.
     - Pool Range - Is a sequential range of IP addresses within a network. Enter a valid pool range.
     - Gateway - Is a node that connects one protocol to another protocol. Enter a valid gateway IP address.

     After entering the above details, click **Add**. The newly added DCHP pools are displayed in the list.

FIGURE 113 Add DHCP Pool



Add DHCP Pool

Pool Name *: DHCP Pool 1

Subnet Mask *: 255.255.255.0

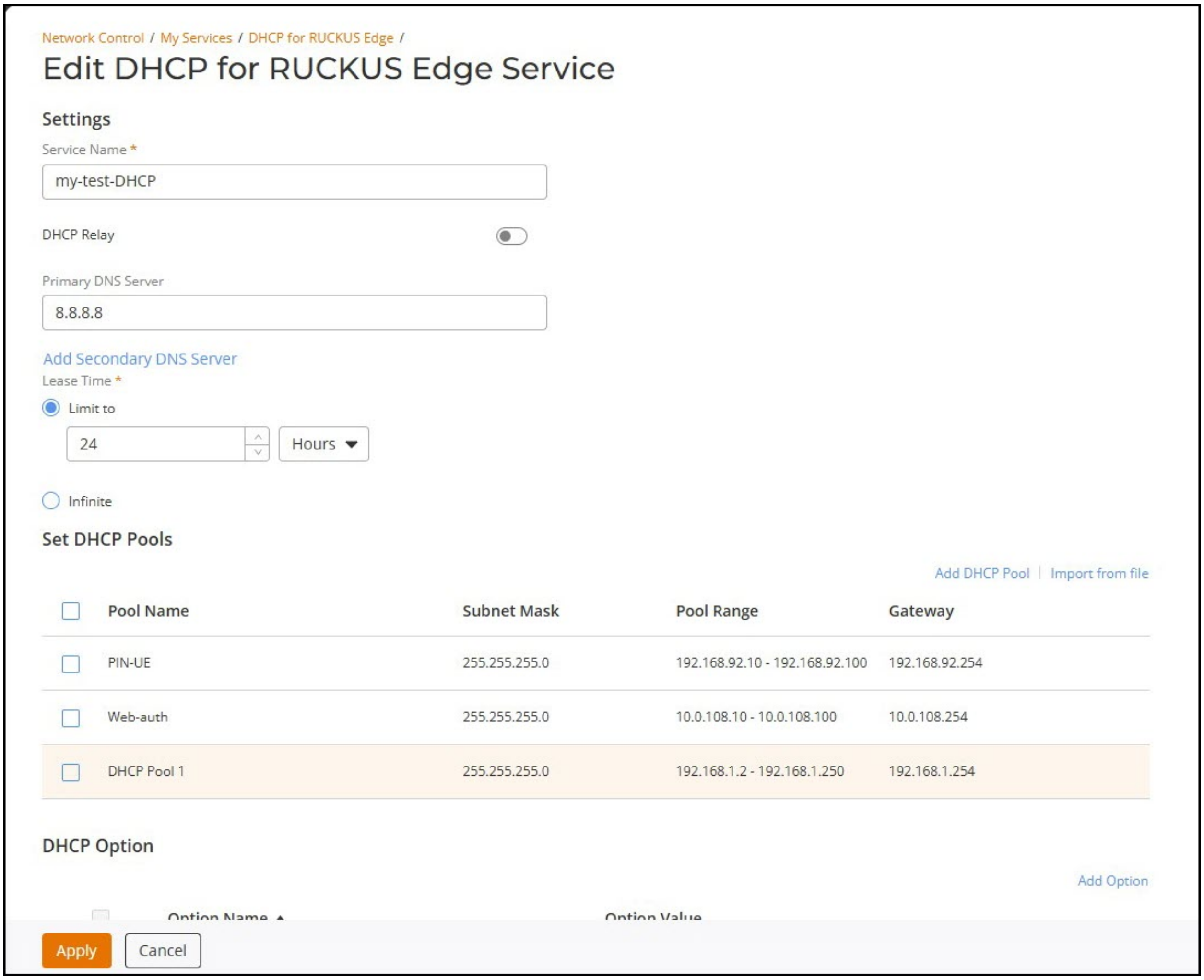
Pool Range *: 192.168.1.2 - 192.168.1.250

Gateway *: 192.168.1.254

□ Add another pool

- After creating the DHCP pools, click **Add**, the newly created DHCP service is displayed the list.

FIGURE 114 Set DHCP Pools



Network Control / My Services / DHCP for RUCKUS Edge /

Edit DHCP for RUCKUS Edge Service

Settings

Service Name *: my-test-DHCP

DHCP Relay

Primary DNS Server: 8.8.8.8

Lease Time *

● Limit to: 24 Hours

○ Infinite

Set DHCP Pools

□	Pool Name	Subnet Mask	Pool Range	Gateway
□	PIN-UE	255.255.255.0	192.168.92.10 - 192.168.92.100	192.168.92.254
□	Web-auth	255.255.255.0	10.0.108.10 - 10.0.108.100	10.0.108.254
□	DHCP Pool 1	255.255.255.0	192.168.1.2 - 192.168.1.250	192.168.1.254

DHCP Option

To Configure external DHCP, perform the following steps.

a) On the RUCKUS One navigation bar, hover on **Network Control** and click **My Services**.

This displays **My Services** menu page.

b) Click **DHCP for RUCKUS Edge**.

This displays **DHCP for RUCKUS Edge** page.

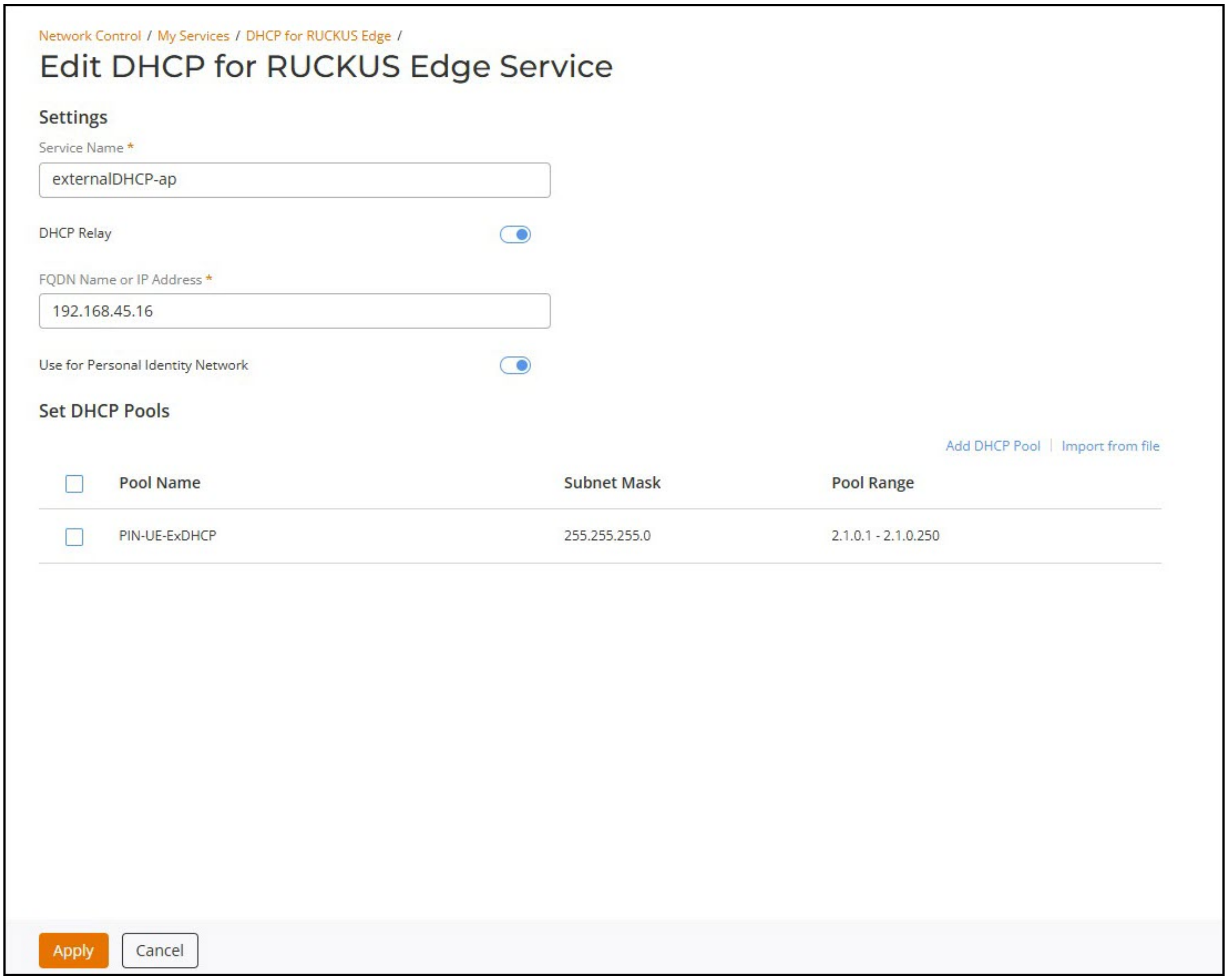
a) In the **DHCP for RUCKUS Edge** page, click **Add DHCP Service** and enter the following details -

NOTE
This pool is used only for PIN service.

- **Service Name** - Enter a service name.
- **DHCP Relay** - By default, this option is disabled, enable **DHCP Relay** to setup external DHCP.
- **FQDN Name or IP Address** - Fully Qualified Name or Address of the internet host.
- **Use for Personal Identity Network** - By default, this option is disabled, enable this option to use in PIN.

- **Set DHCP Pools** - As described above, follow the instructions to set the **DHCP Pool**

FIGURE 115 External DHCP



Network Control / My Services / DHCP for RUCKUS Edge /

Edit DHCP for RUCKUS Edge Service

Settings

Service Name *: externalDHCP-ap

DHCP Relay: ●

FQDN Name or IP Address *: 192.168.45.16

Use for Personal Identity Network: ●

Set DHCP Pools

	Pool Name	Subnet Mask	Pool Range
□	PIN-UE-ExDHCP	255.255.255.0	2.1.0.1 - 2.1.0.250

Configuring RUCKUS Edge Ports

IP static routes remain in the IP route table only as long as the port or virtual interface used by the route is available and the next-hop IP address is valid.

To configure ports, perform the following steps.

1. On the RUCKUS One navigation bar, click on **Gateway** > **RUCKUS Edge**.

   This displays the list of ports on the RUCKUS Edge devices.

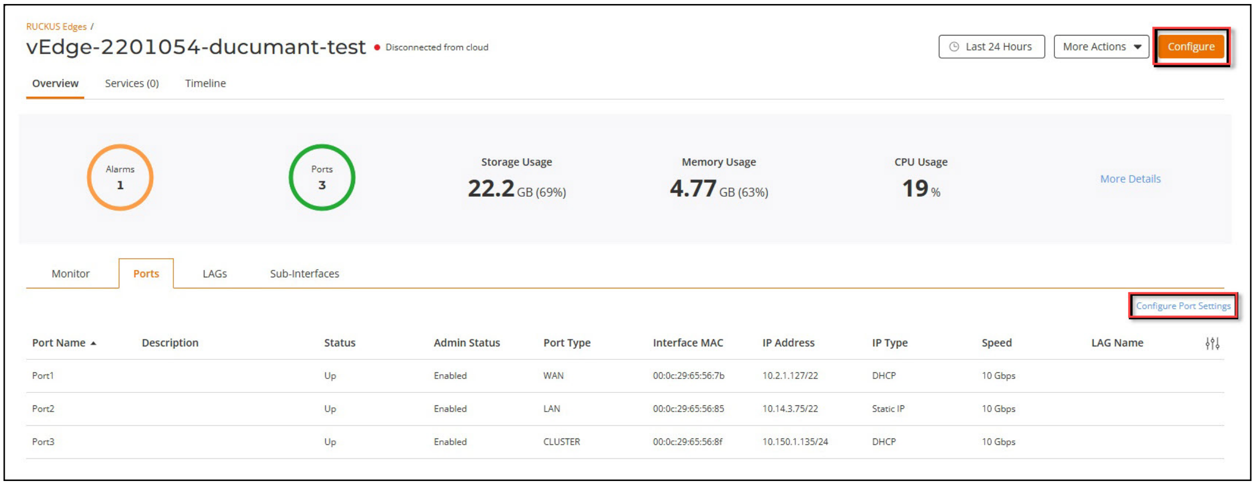
2. Click on the name of the **Port**.

   This displays port details screen.

3. In the **Port details** screen, click **Configure** or **Configure Port Settings**.

   This displays the **Port Configuration** details.

FIGURE 116 Ports Configuration



vEdge-2201054-ducumant-test ● Disconnected from cloud

Storage Usage 22.2 GB (69%)

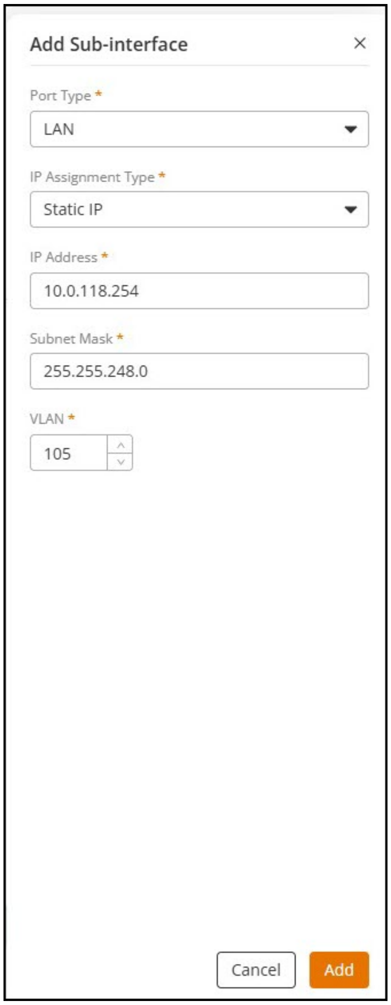
Memory Usage 4.77 GB (63%)

CPU Usage 19 %

Port Name ▲	Description	Status	Admin Status	Port Type	Interface MAC	IP Address	IP Type	Speed	LAG Name
Port1		Up	Enabled	WAN	00:0c:29:65:56:7b	10.2.1.127/22	DHCP	10 Gbps	
Port2		Up	Enabled	LAN	00:0c:29:65:56:85	10.14.3.75/22	Static IP	10 Gbps	
Port3		Up	Enabled	CLUSTER	00:0c:29:65:56:8f	10.150.1.135/24	DHCP	10 Gbps	

4. Click **Sub-interface** tab and enter the details.

FIGURE 117 Adding Sub-interface



Add Sub-interface

Port Type *
LAN

IP Assignment Type *
Static IP

IP Address *
10.0.118.254

Subnet Mask *
255.255.248.0

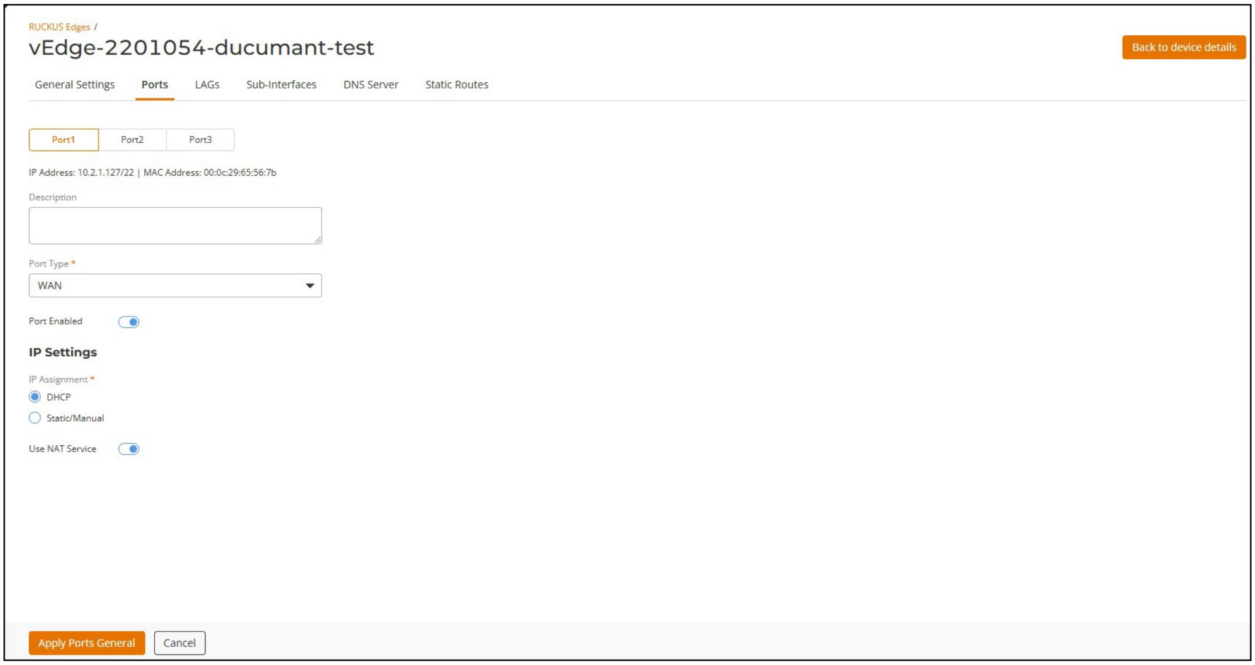
VLAN *
105

5. Click **Add**.

Ports General

1. Click **Port General** tab and enter the following details:
   - **Description** - Enter a short description to identify the port.
   - **Port Type** - Select the port type from the drop-down list. By default, WAN is selected and **Port Enabled** is **On**.
   - **IP Settings** - To manually configure the external DHCP, select **Static/Manual** and enter the **IP Address**, **Subnet Mask** and **Gateway** details in the respective fields. By default, the **Use NAT Service** is enabled.

   FIGURE 118 Port Settings

   vEdge-2201054-ducumant-test

   IP Address: 10.2.1.127/22 | MAC Address: 00:0c:29:65:56:7b

   Description

   Port Type *
   WAN

   Port Enabled ●

   IP Settings

   IP Assignment *
   ● DHCP
   ○ Static/Manual

   Use NAT Service ●

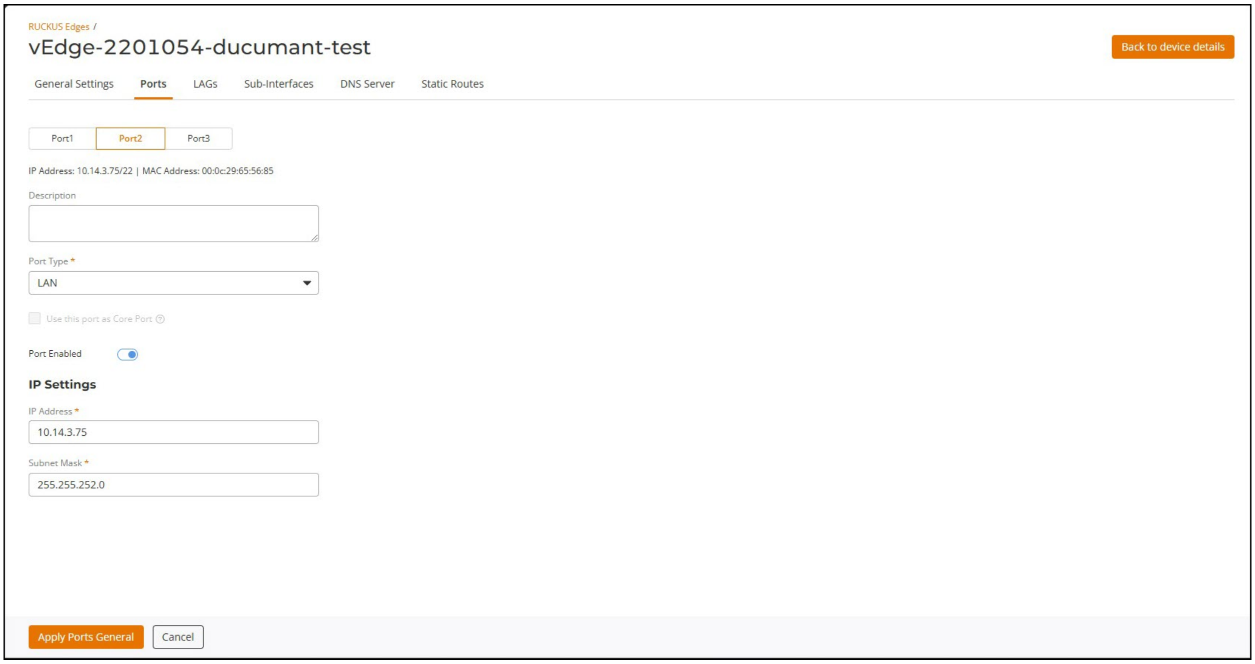
2. After entering all the details in the respective fields, click **Apply Port General** settings.

3. The application displays update successful message.

NOTE

Re-iterate the same steps for **Port 2** and **Port 3**, however, in the **Port Type** drop-down list, select **LAN**.

FIGURE 119 Port 2 Settings



vEdge-2201054-ducumant-test

IP Address: 10.14.3.75/22 | MAC Address: 00:0c:29:65:56:85

Description

Port Type * LAN

□ Use this port as Core Port

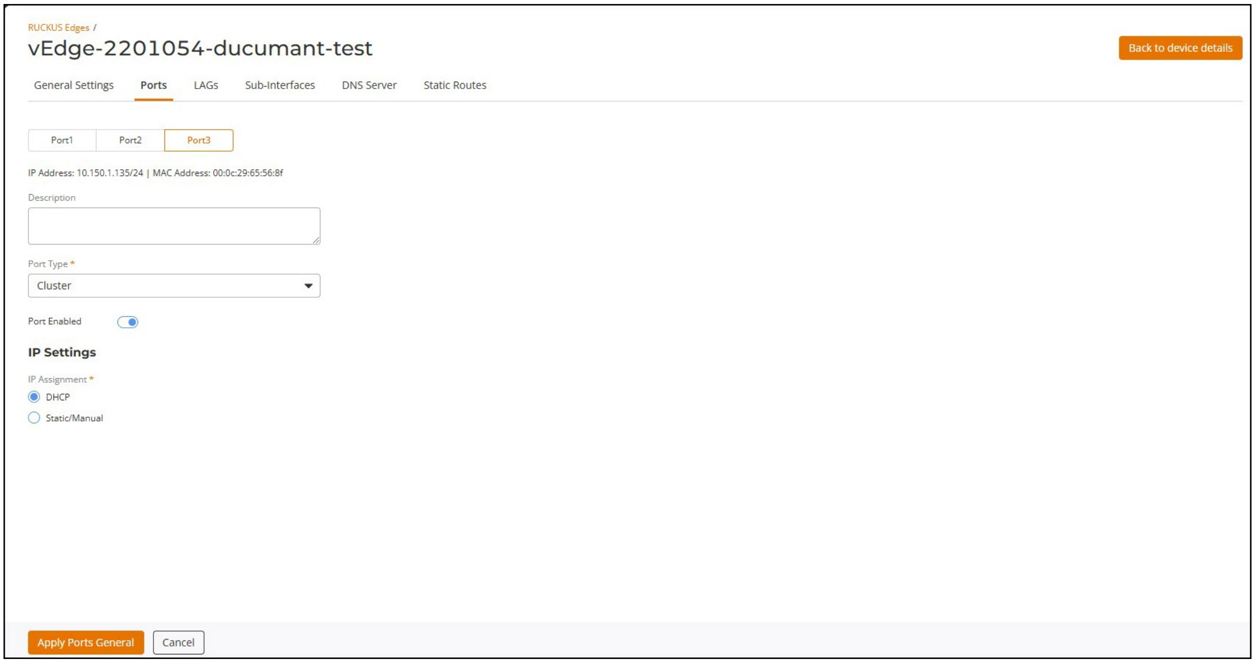
Port Enabled

IP Settings

IP Address * 10.14.3.75

Subnet Mask * 255.255.252.0

FIGURE 120 Port 3 Settings



vEdge-2201054-ducumant-test

IP Address: 10.150.1.135/24 | MAC Address: 00:0c:29:65:56:8f

Description

Port Type * Cluster

Port Enabled

IP Settings

IP Assignment *

● DHCP

○ Static/Manual

Sub-Interface

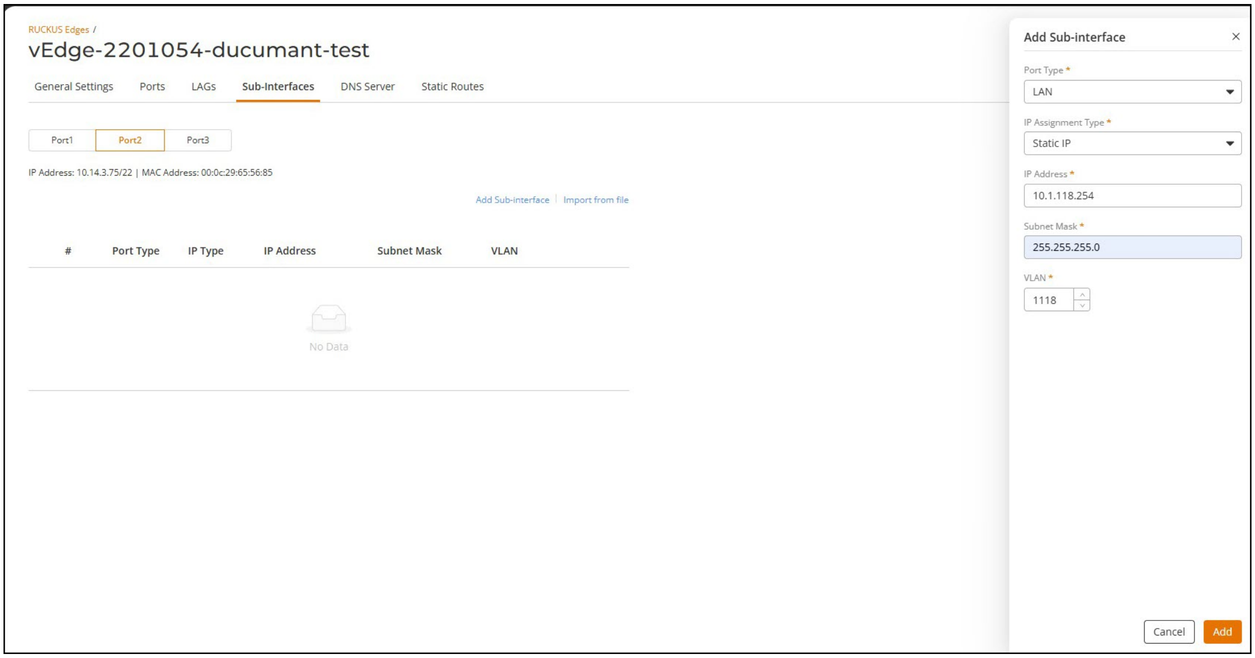
1. Click **Sub-Interface** tab and click **Add Sub-Interface**

   This displays **Add Sub-Interface** window.

2. In the **Add Sub-Interface** window, enter the following details:

   - **Port Type** - Select the port type from the drop-down list.
   - **IP Assignment Type** - By default, the IP assignment type is **DHCP**, however, to manually configure the ports, select **Static** from the drop-down list and enter the IP address.

   FIGURE 121 Sub-Interface Port Settings



RUCKUS Edges /

vEdge-2201054-ducumant-test

IP Address: 10.14.3.75/22 | MAC Address: 00:0c:29:65:56:85

#	Port Type	IP Type	IP Address	Subnet Mask	VLAN

No Data

Add Sub-interface

Port Type *: LAN

IP Assignment Type *: Static IP

IP Address *: 10.1.118.254

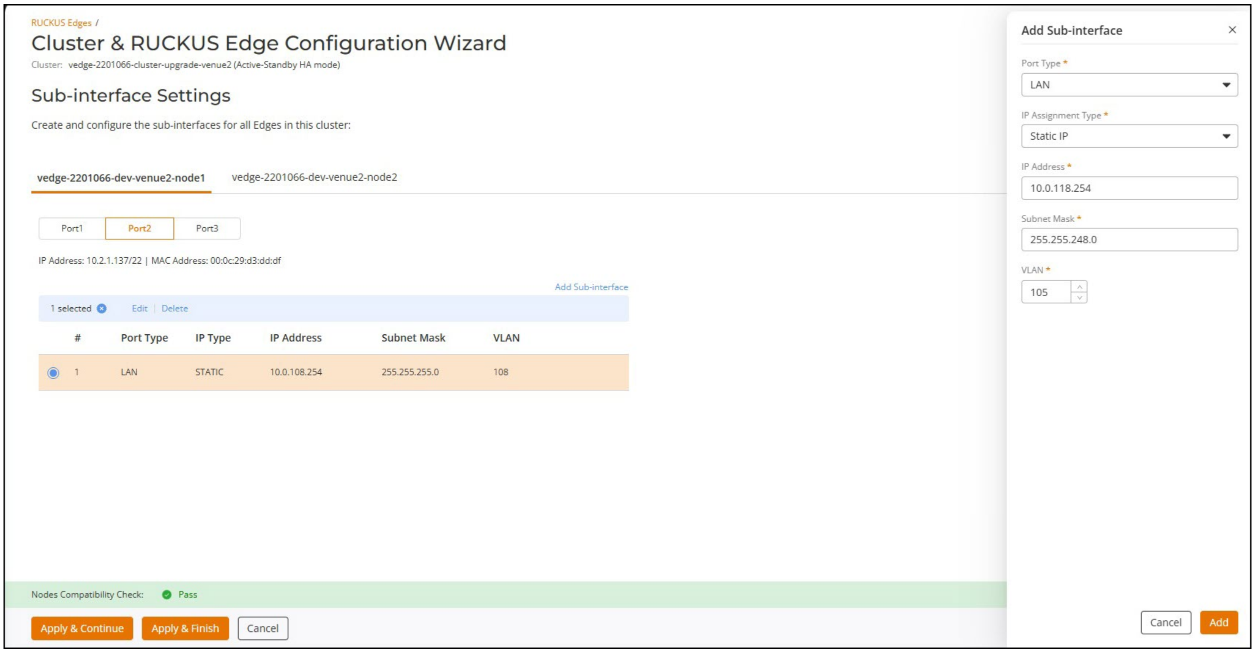
Subnet Mask *: 255.255.255.0

VLAN *: 1118

3. After entering all the details in the respective fields, click **Add**.

4. The sub-interface settings are displayed on the screen.

FIGURE 122 Sub-interface Settings



RUCKUS Edges /

Cluster & RUCKUS Edge Configuration Wizard

Cluster: vedge-2201066-cluster-upgrade-venue2 (Active-Standby HA mode)

Sub-interface Settings

Create and configure the sub-interfaces for all Edges in this cluster:

vedge-2201066-dev-venue2-node1
vedge-2201066-dev-venue2-node2
Port1
Port2
Port3

IP Address: 10.2.1.137/22 | MAC Address: 00:0c:29:d3:dd:df

Add Sub-interface
1 selected
Edit
Delete

	#	Port Type	IP Type	IP Address	Subnet Mask	VLAN
●	1	LAN	STATIC	10.0.108.254	255.255.255.0	108

Nodes Compatibility Check: Pass

Add Sub-interface

Port Type *: LAN

IP Assignment Type *: Static IP

IP Address *: 10.0.118.254

Subnet Mask *: 255.255.248.0

VLAN *: 105

NOTE
Repeat the same steps to add interfaces to **Port 2** and **Port 3**.

5. User can also import file from the local system by clicking **Import from file**. Only .csv (Comma Separated Values) file type with file size not exceeding more than 5MB is allowed to be uploaded.

NOTE
User should have routes to reach the loopback of Distribution Switch from RUCKUS Edge and if the user is using external DHCP server then another route to reach the external DHCP server.

Configuring Static Routes

IP static routes remain in the IP route table only as long as the port or virtual interface used by the route is available and the next-hop IP address is valid.

To configure static routes, perform the following steps.

1. On the RUCKUS One navigation bar, click on **Gateway** > **RUCKUS Edge**.

   This displays the list of RUCKUS Edge devices.

2. Click on the name of the **RUCKUS Edge** device.

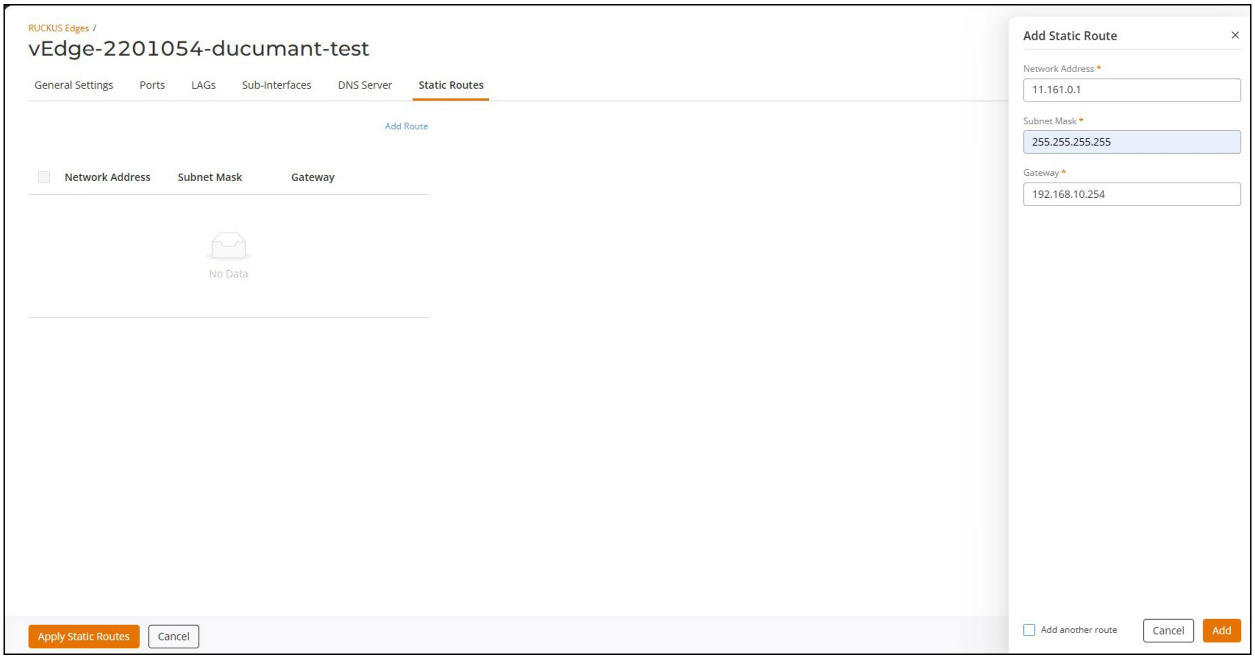
   This displays RUCKUS Edge details screen.

3. In the **RUCKUS Edge details** screen, click **Configure**.

   This displays the **RUCKUS Edge Configuration** details.

4. Click **Static Routes** tab.

FIGURE 123 Static Routes



☐	Network Address	Subnet Mask	Gateway

Add Static Route

Network Address * 11.161.0.1

Subnet Mask * 255.255.255.255

Gateway * 192.168.10.254

☐ Add another route

5. To add a new static route, click **Add Route**.

   This displays the **Add Static Route** window. Enter the following details:

   - **Network Address** - Enter the Network IP Address.
   - **Subnet Mask** - Enter a valid subnet mask for the network address.

     NOTE
     Each network address has a unique subnet mask and gateway.

   - **Gateway** - Enter the gateway IP address.

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

   This displays the new static route in the list.

On-Boarding Access and Distribution Switch

Make sure both the switches are able to reach RUCKUS One in order to connect to the cloud.

Both ICX switches should have DNS server configured (via DHCP or statically). Use the Command Line Interface (CLI) to connect both the switches.

Use the command **show manager status** to check connection status.

NOTE
For ICX7550 and ICX7850 model switches, ensure the Distribution switch has the forwarding profile configured for PIN. To configure the forwarding profile use the **forwarding-profile profile2** command.

Adding Switches

Add to two switches.

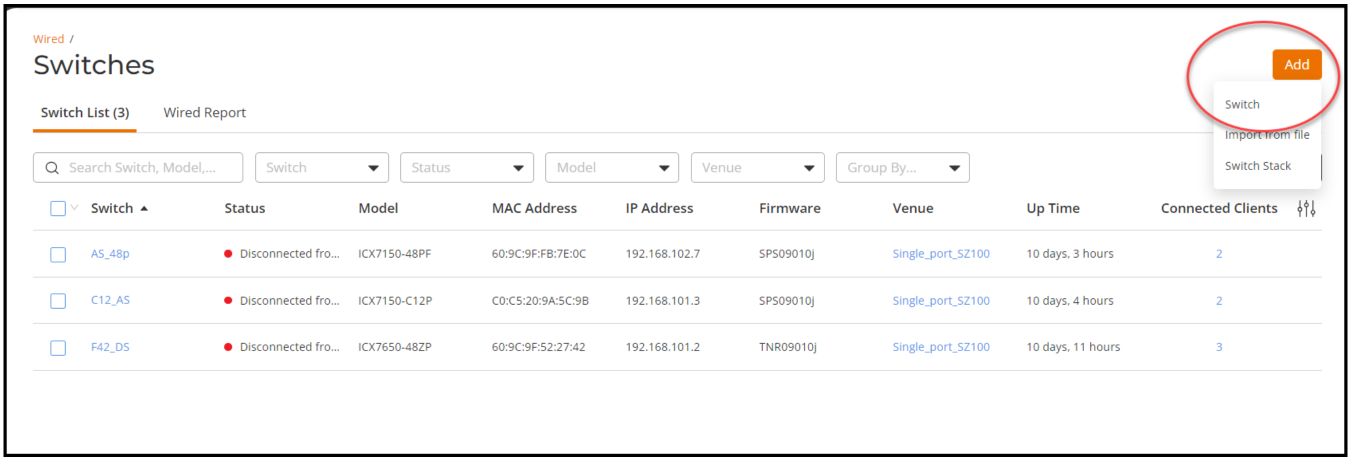
To add swtiches perform the following steps.

1. On the RUCKUS One navigation bar, hover on **Wired** and select **Switch List**.

   This displays the **Switches** page.

2. In the **Switches** page, click **Add** and select **Add Swtich**.

   FIGURE 124 Add Switch

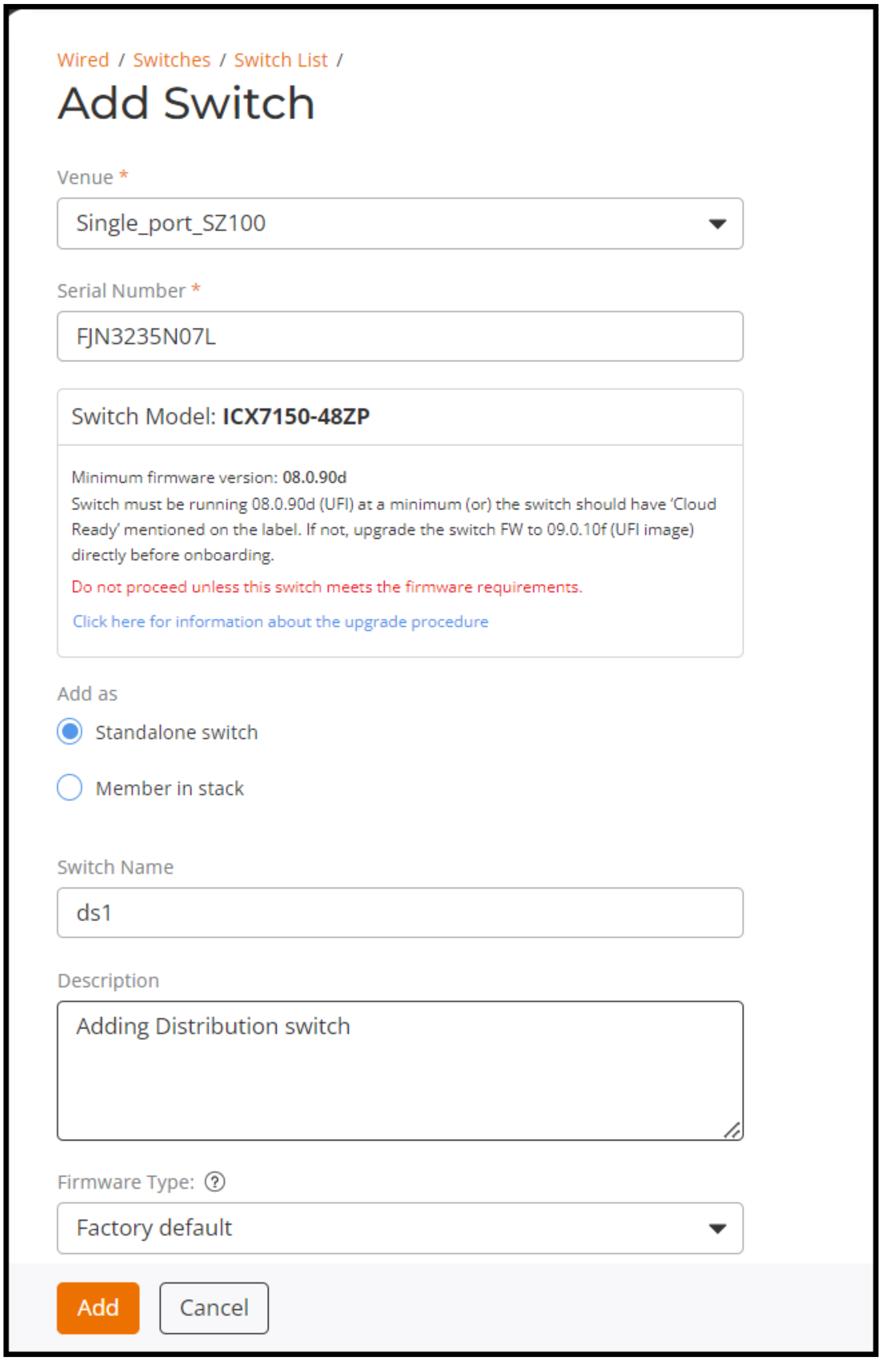
   

□	Switch ▲	Status	Model	MAC Address	IP Address	Firmware	Venue	Up Time	Connected Clients
□	AS_48p	● Disconnected fro...	ICX7150-48PF	60:9C:9F:FB:7E:0C	192.168.102.7	SPS09010j	Single_port_SZ100	10 days, 3 hours	2
□	C12_AS	● Disconnected fro...	ICX7150-C12P	C0:C5:20:9A:5C:9B	192.168.101.3	SPS09010j	Single_port_SZ100	10 days, 4 hours	2
□	F42_DS	● Disconnected fro...	ICX7650-48ZP	60:9C:9F:52:27:42	192.168.101.2	TNR09010j	Single_port_SZ100	10 days, 11 hours	3

   This displays the **Add Switch** page.

3. In the **Add Switch** page, enter the following details:
   - **Venue** - Select the venue name from the drop-down list.
   - **Serial Number** - Enter the serial number of the device.
   - **Add as** - Select either **Standalone Switch** (standalone switches are managed and configured as a single entity) or **Member in Stack.** (a group of switches work togeather as a single entity).
   - **Switch Name** - Enter the name of the switch.
   - **Description** - Enter short description for the switch.
   - **Firmware Type** - Select only if the switch is a factory default switch.
   - **DHCP Client** - Select only if the switch is a factroy default switch.

FIGURE 125 Add Switch



Wired / Switches / Switch List /

Add Switch

Venue *

Single_port_SZ100

Serial Number *

FJN3235N07L

Switch Model: **ICX7150-48ZP**

Minimum firmware version: **08.0.90d**

Switch must be running 08.0.90d (UFI) at a minimum (or) the switch should have 'Cloud Ready' mentioned on the label. If not, upgrade the switch FW to 09.0.10f (UFI image) directly before onboarding.

Do not proceed unless this switch meets the firmware requirements.

Click here for information about the upgrade procedure

Add as

● Standalone switch

○ Member in stack

Switch Name

ds1

Description

Adding Distribution switch

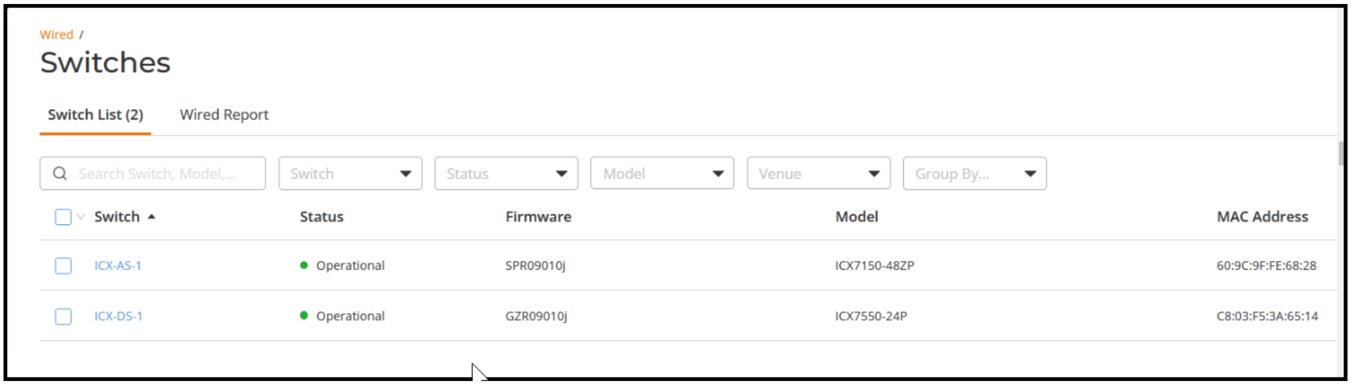
Firmware Type:

Factory default

4. After entering the above details, click **Add**.

   The newly added switch is displayed in the switch list.

   FIGURE 126 Access and Distribution Switches added to RUCKUS One



Wired /

Switches

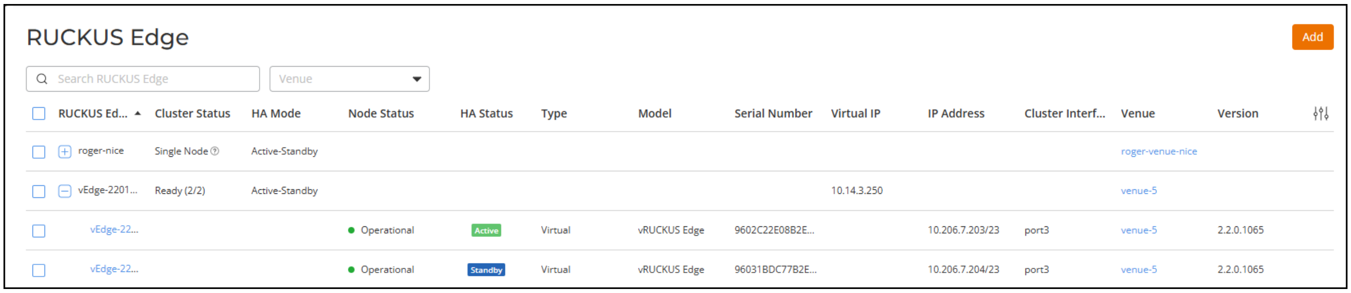
Switch List (2) | Wired Report

Switch	Status	Firmware	Model	MAC Address
ICX-AS-1	● Operational	SPR09010j	ICX7150-48ZP	60:9C:9F:FE:68:28
ICX-DS-1	● Operational	GZR09010j	ICX7550-24P	C8:03:F5:3A:65:14

5. After the switches are onboarded, tag downlink/uplink ports through RUCKUS One to approriate values.

   The ICX switches and RUCKUS Edge is onboarded and the status is displayed as **Operational** .

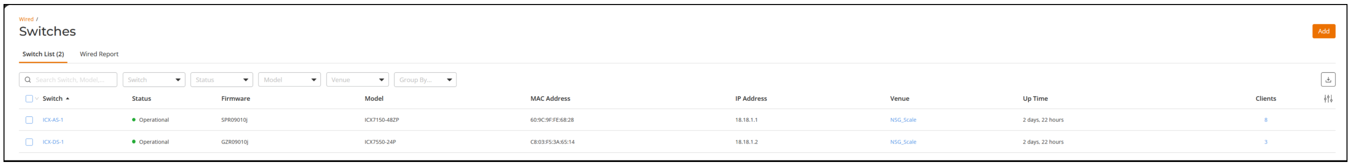
   FIGURE 127 Status of the RUCKUS Edge Swtich is Operational



RUCKUS Edge

RUCKUS Ed...	Cluster Status	HA Mode	Node Status	HA Status	Type	Model	Serial Number	Virtual IP	IP Address	Cluster Interf...	Venue	Version
roger-nice	Single Node	Active-Standby									roger-venue-nice	
vEdge-2201...	Ready (2/2)	Active-Standby						10.14.3.250			venue-5	
vEdge-22...			● Operational	Active	Virtual	vRUCKUS Edge	9602C22E08B2E...		10.206.7.203/23	port3	venue-5	2.2.0.1065
vEdge-22...			● Operational	Standby	Virtual	vRUCKUS Edge	96031BDC77B2E...		10.206.7.204/23	port3	venue-5	2.2.0.1065

   FIGURE 128 Status of the ICX Switch is Operational



Wired /

Switches

Switch List (2) | Wired Report

Switch	Status	Firmware	Model	MAC Address	IP Address	Venue	Up Time	Clients
ICX-AS-1	● Operational	SPR09010j	ICX7150-48ZP	60:9C:9F:FE:68:28	18.18.1.1	NSG_Scale	2 days, 22 hours	8
ICX-DS-1	● Operational	GZR09010j	ICX7550-24P	C8:03:F5:3A:65:14	18.18.1.2	NSG_Scale	2 days, 22 hours	3

Adding VLAN Profile

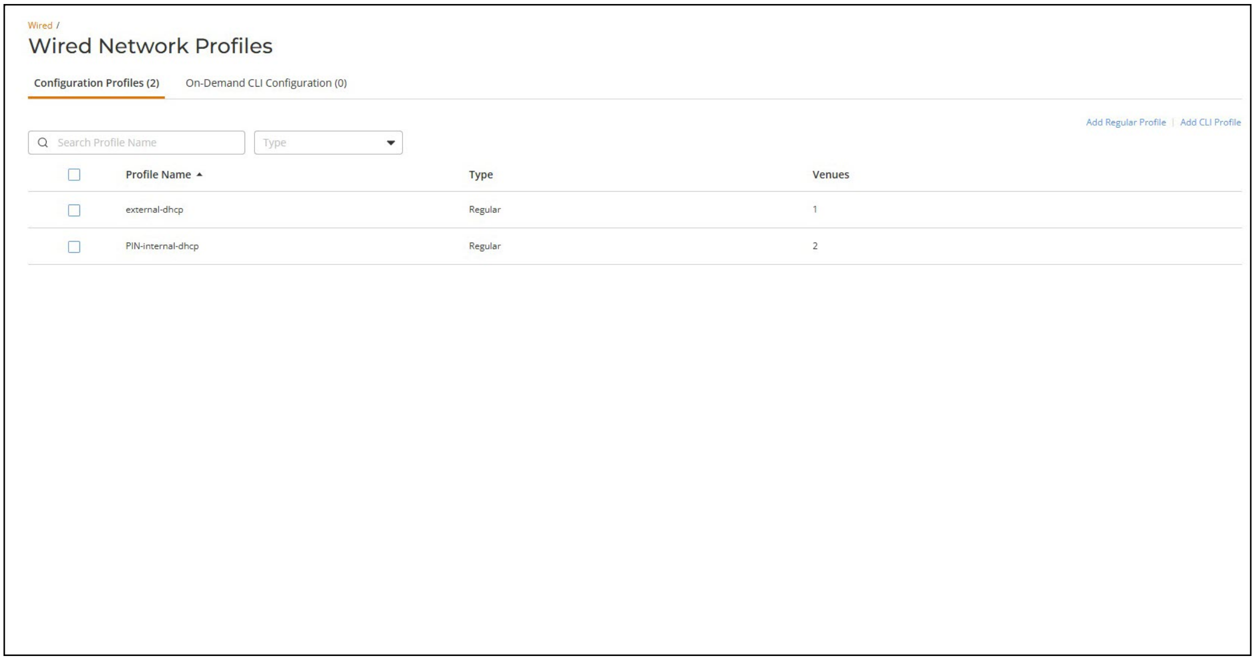
Virtual Local Area Network connects multiple devices and network nodes from different LANs to one logical network.

To add a VLAN profile, perform the following steps.

1. On the RUCKUS One navigation bar, navigate and hover the mouse on **Wired** option and select **Configuration Profiles**.

   This displays **Wired Network Profiles** page.

   FIGURE 129 Wired Network Profiles

   Wired /
Wired Network Profiles
Configuration Profiles (2)
On-Demand CLI Configuration (0)
Add Regular Profile | Add CLI Profile
Search Profile Name
Type

□	Profile Name ▲	Type	Venues
□	external-dhcp	Regular	1
□	PIN-internal-dhcp	Regular	2

2. In **Wired Network Profiles** page, click **Add Regular Profile** link.

   This displays **Add Switch Configuration Profile** page. In this page enter the details in the respective section as mentioned below.

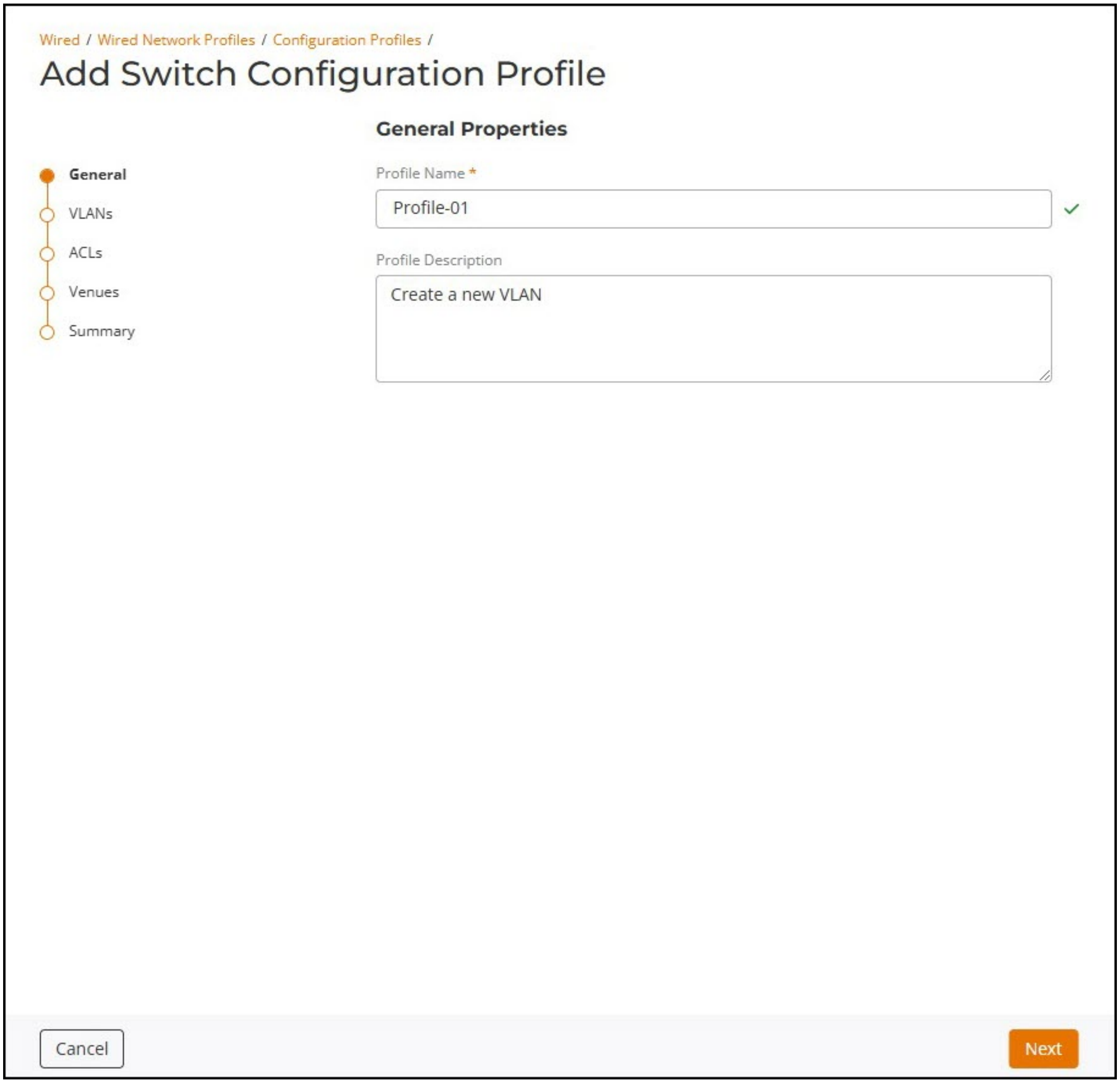
General Properties

In this section, enter the following details:

- **Profile Name** - Enter a profile to identify the VLAN.
- **Description** - Enter a short description of the VLAN profile.

After enter the above details, click **Next**. This displays the **VLANs** section.

FIGURE 130 General Properties_VLAN



Wired / Wired Network Profiles / Configuration Profiles /

Add Switch Configuration Profile

General Properties

Profile Name *: Profile-01

Profile Description: Create a new VLAN

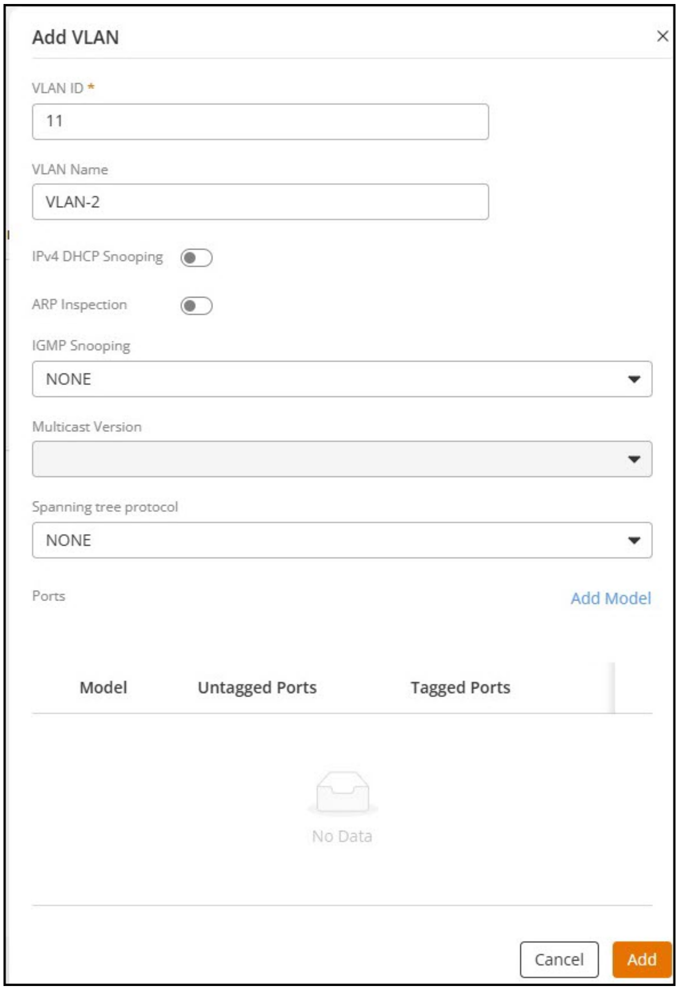
VLANs

In the **VLANs** section, click **Add VLAN** and enter the following details:

- **VLAN ID** - Each port on a switch can be assigned to be a member of VLAN. VLAN ID is a number between 0-4095. Enter a **VLAN ID**.
- **VLAN Name** - Enter a name to identify the VLAN.
- **IPv4 DHCP Snooping** - Internet Protocol version 4 is a protocol and DHCP snooping a security that prevents unauthorised servers from accessing the network. By default, this option is disabled.
- **ARP Inspection** - It is a security feature to inspect Address Resolution Protocol (ARP) packets in a network. By default, this option is disabled.

- **IGMP Snooping** - Internet Group Management Protocol (IGMP) is a method switches use to identify multicast groups. Click on the drop-down list and select the **IGMP Snooping** option.
- **Multicast Version** - There are three versions of IGMP. Click on the drop-down list and select the **Multicast Version**.
- **Spanning Tree Protocol** - It is a network protocol used to prevent looping within a network. Click on the drop-down list and select the **Spanning Tree Protocol** option.

FIGURE 131 Add VLAN



Add VLAN

VLAN ID *: 11

VLAN Name: VLAN-2

IPv4 DHCP Snooping: ○

ARP Inspection: ○

IGMP Snooping: NONE

Multicast Version:

Spanning tree protocol: NONE

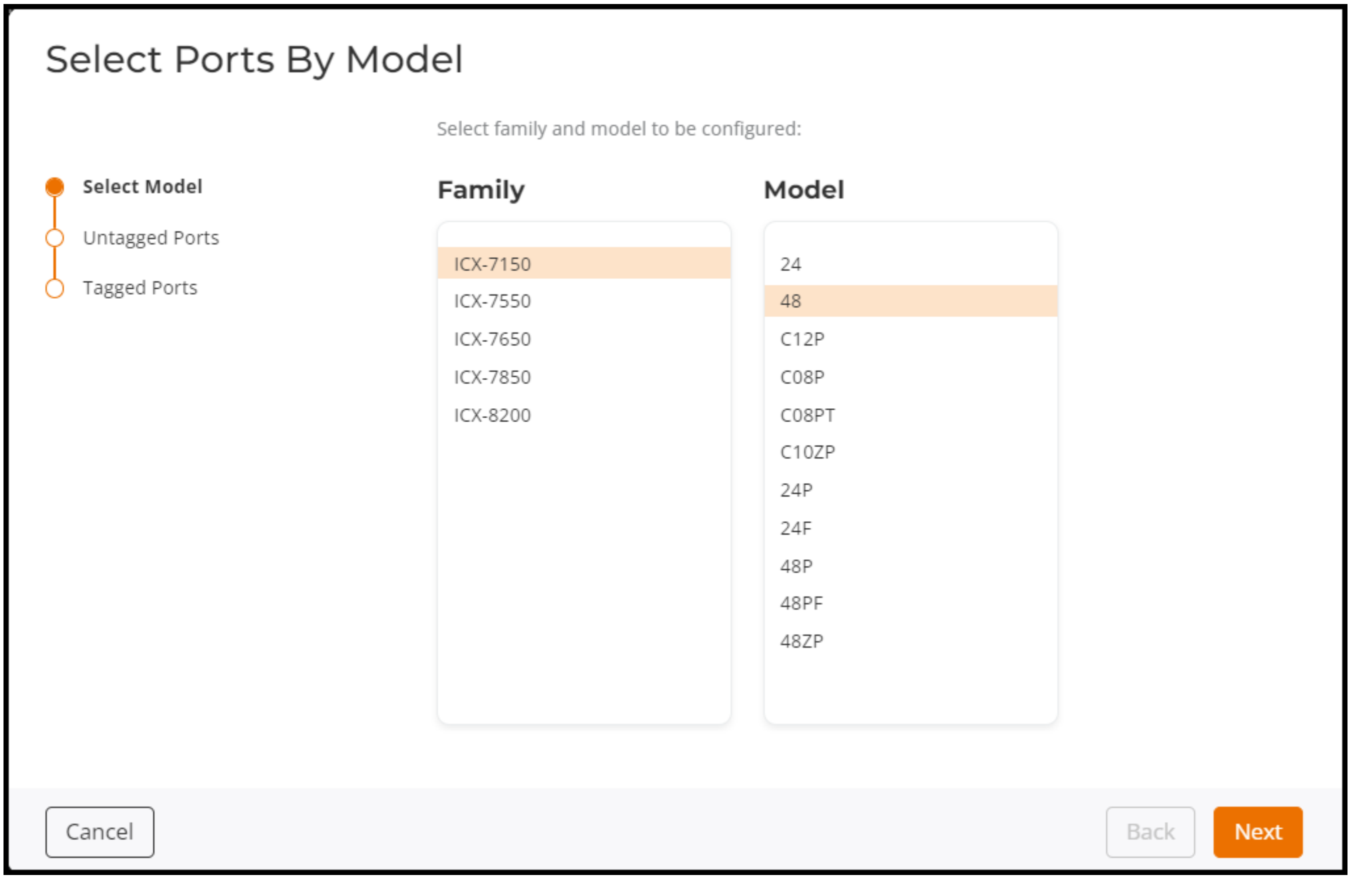
Ports

Model	Untagged Ports	Tagged Ports

No Data

- **Add Model** - Click **Add Model** link, this displays **Select Ports by Model** page, Selec the **Family** and **Model** and click **Next**.

FIGURE 132 Select the Ports by Model

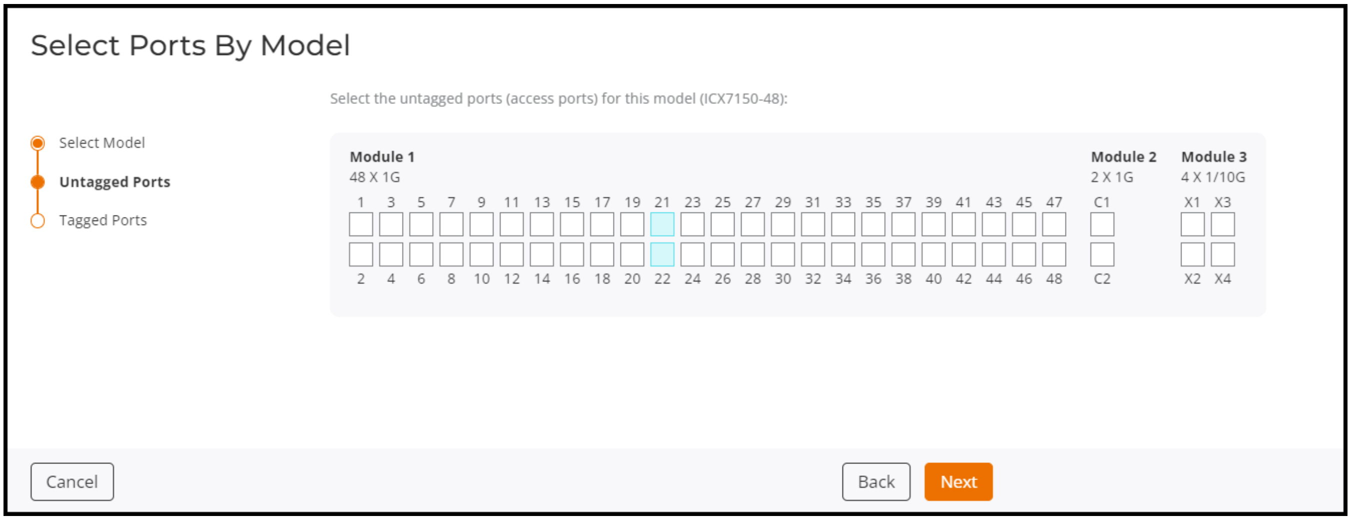


Select Ports By Model

Select family and model to be configured:

- **Untagged Ports** - Select the untagged ports (Access Ports) for this model. To select the ports, click on the **Port Numbers** and the selected ports are highlighted. Click **Next**.

FIGURE 133 Untagged Ports

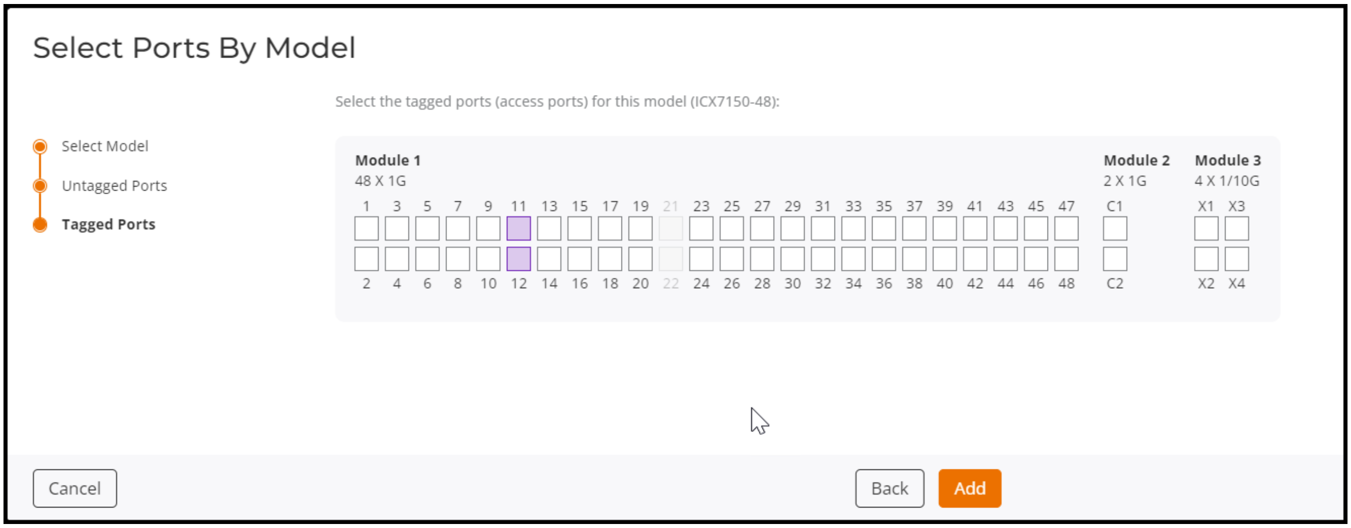


Select Ports By Model

Select the untagged ports (access ports) for this model (ICX7150-48):

- **Tagged Ports** - Select the tagged ports (Access Ports) for this model. To select the ports, click on the **Port Numbers** and the selected ports are highlighted. Click **Add**.

FIGURE 134 Tagged Ports

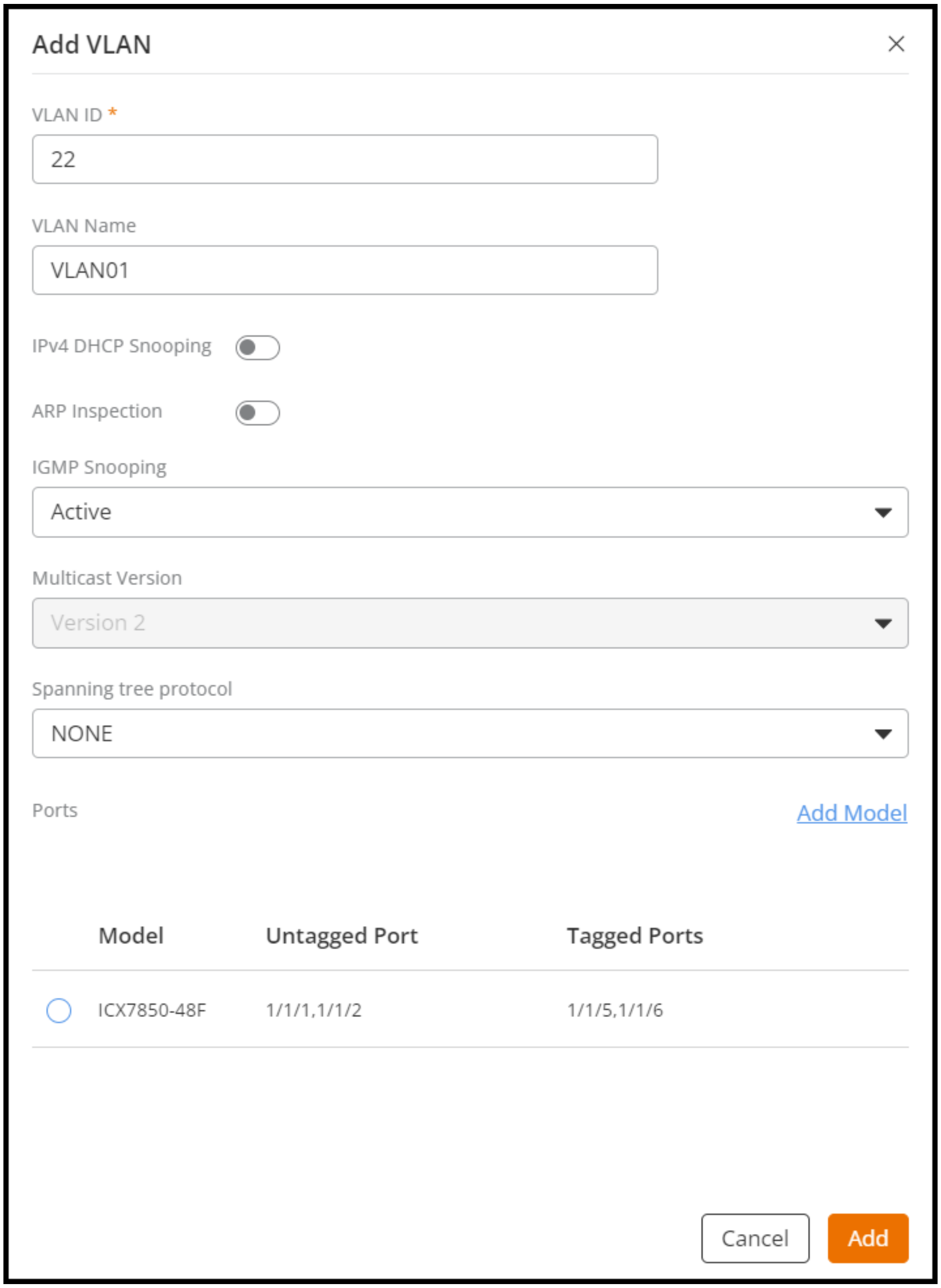


Select Ports By Model

Select the tagged ports (access ports) for this model (ICX7150-48):

- The newly added model with port details are displayed in the **Add VLAN** window.

FIGURE 135 Add VLAN Model



Add VLAN

VLAN ID *: 22

VLAN Name: VLAN01

IPv4 DHCP Snooping: Off

ARP Inspection: Off

IGMP Snooping: Active

Multicast Version: Version 2

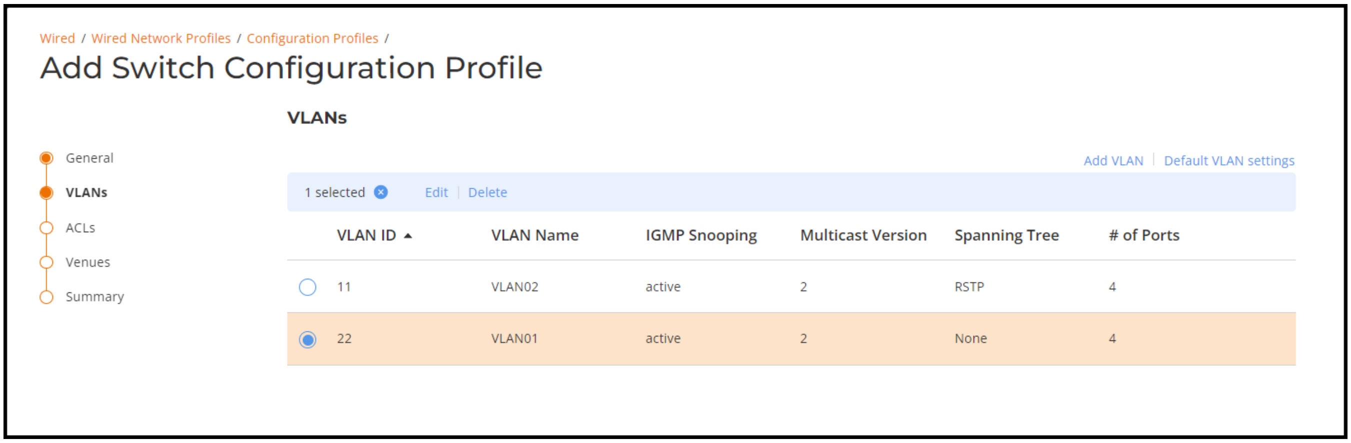
Spanning tree protocol: NONE

Ports

	Model	Untagged Port	Tagged Ports
○	ICX7850-48F	1/1/1,1/1/2	1/1/5,1/1/6

- Select the model and click **Add**. The new VLAN ID is displayed in the **VLANs** section.

FIGURE 136 List of VLANs



Wired / Wired Network Profiles / Configuration Profiles /

Add Switch Configuration Profile

VLANs

	VLAN ID ▲	VLAN Name	IGMP Snooping	Multicast Version	Spanning Tree	# of Ports
○	11	VLAN02	active	2	RSTP	4
●	22	VLAN01	active	2	None	4

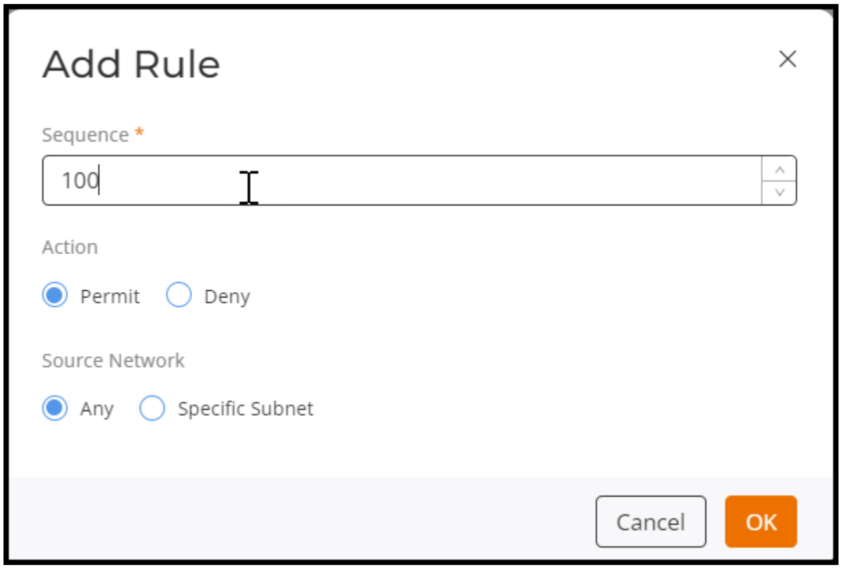
- Click **Next**. This displays the **ACLs** section

ACLs

In the ACLs section, click **Add ACL**. This displays the **Add ACL** window. Enter the following details:

- **ACL Name** - Enter a name to identify the ACL.
- **Type** - Select the ACL type. There are two types of access list.
  - Standard Access-List - Made up of using source IP address only.
  - Extended Access List - Made up of sourc IP, destination IP, source port and destination port.
- **Rules** - To add rules to the ACL, click **Add Rule** and enter the following details:
  - Sequence - Enter a number between 1-65000.
  - Action - Select **Permit** or **Deny**.
  - Source Network - Select **Any** or **Specific Subnet**.

FIGURE 137 Add ACL Rules



Add Rule

Sequence * 100

Action

● Permit ○ Deny

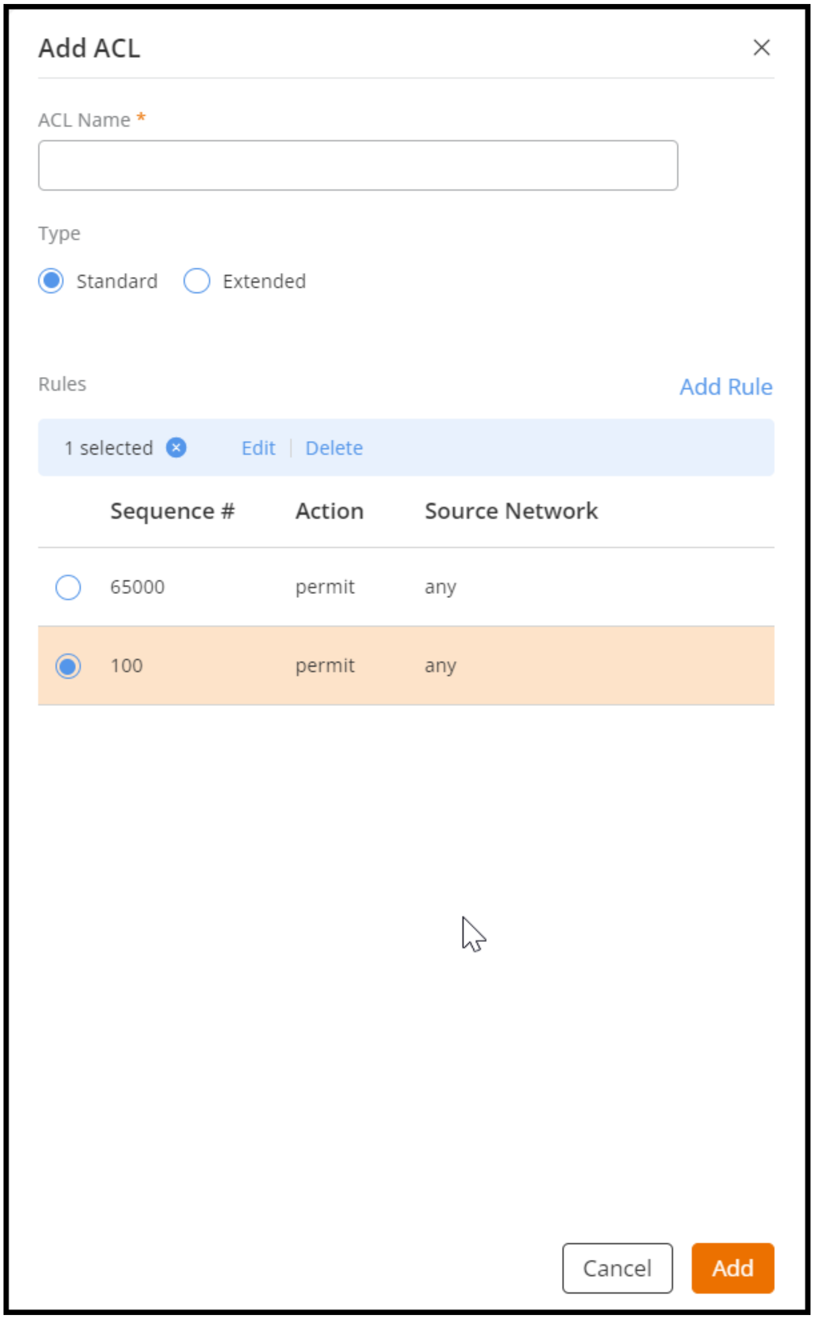
Source Network

● Any ○ Specific Subnet

Enter the details and click **Ok**. The new rule is displayed in the **Add ACL** window.

- Select the rule and click **Add**.

FIGURE 138 ACL Rules



Add ACL

ACL Name *

Type

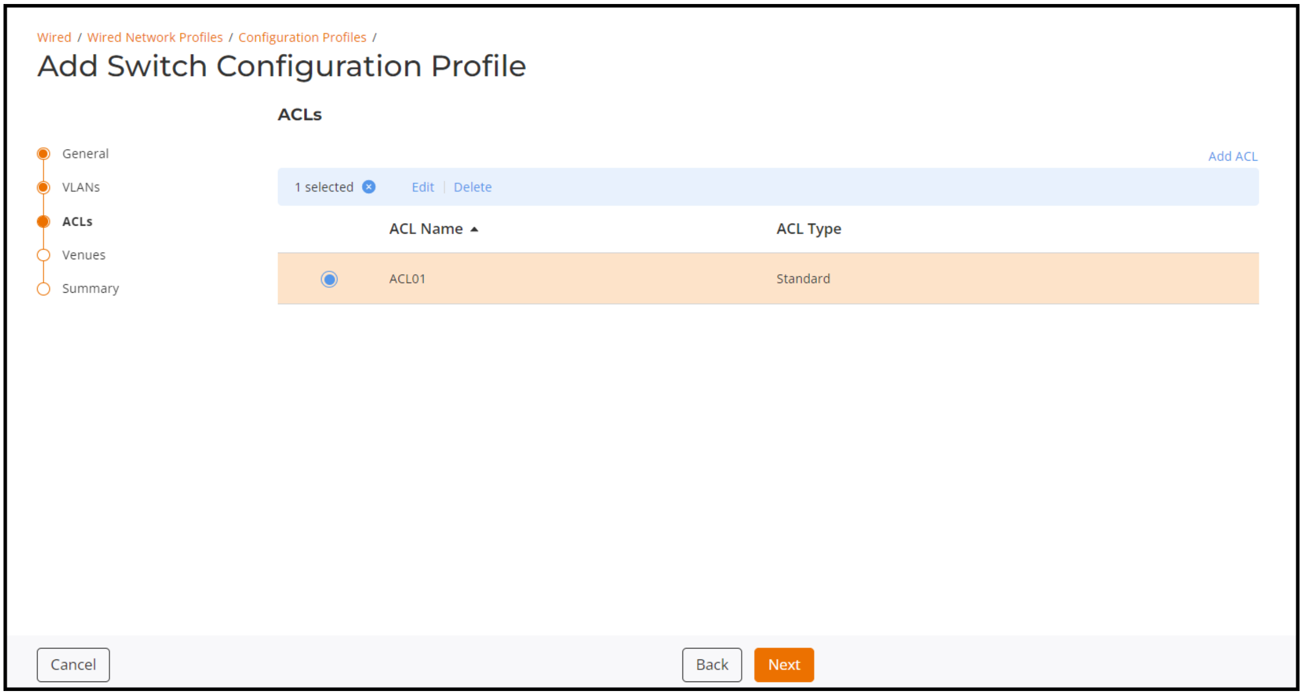
● Standard ○ Extended

Rules

	Sequence #	Action	Source Network
○	65000	permit	any
●	100	permit	any

The new ACL rule is displayed in the **ACLs** page. Click **Next**. This displays **Venues** section

FIGURE 139 List of ACLs Added



Wired / Wired Network Profiles / Configuration Profiles /

Add Switch Configuration Profile

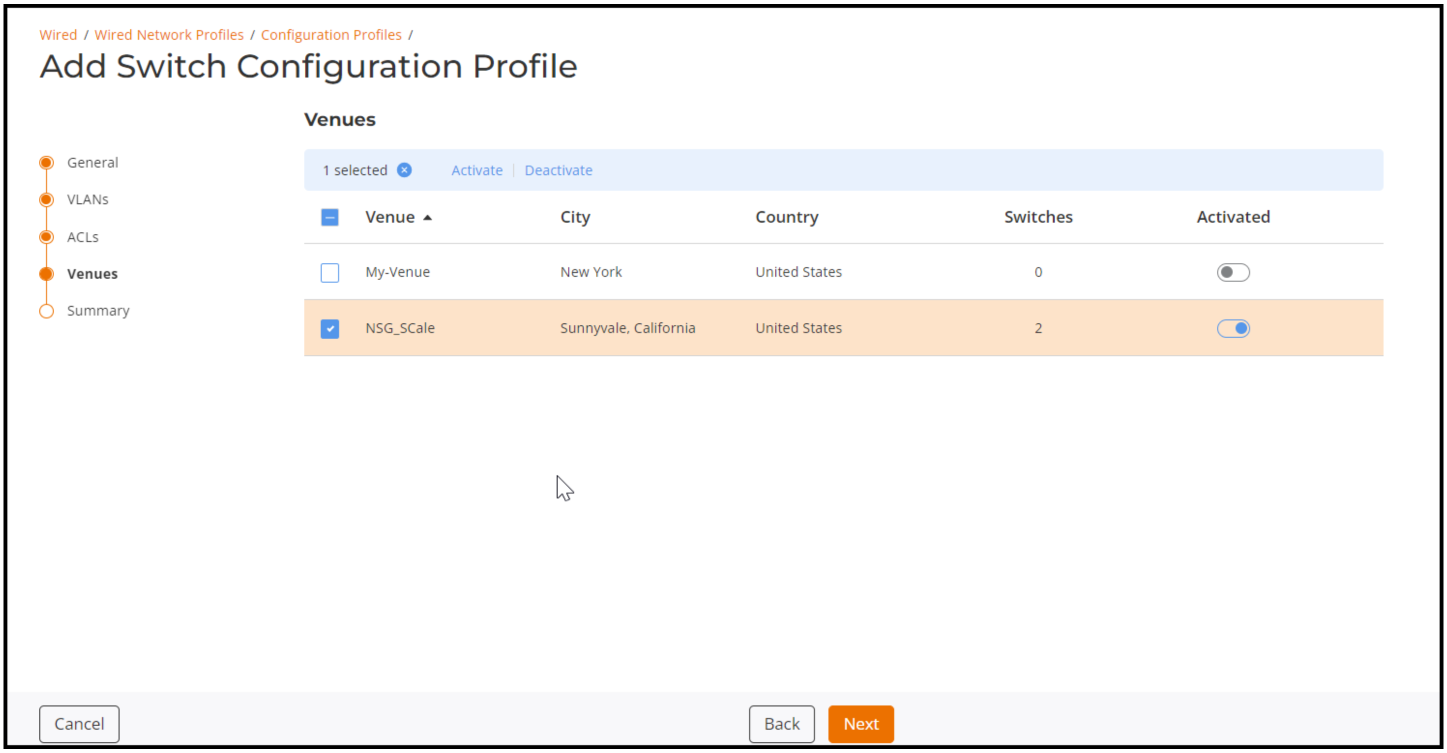
ACLs

	ACL Name ▲	ACL Type
●	ACL01	Standard

Venues

The venues list is auto-populated. All the associated venues are displayed in the list. Check the box corresponding to the **Venue** and click **Activate**.

FIGURE 140 Activate Venue



Wired / Wired Network Profiles / Configuration Profiles /

Add Switch Configuration Profile

- General
- VLANs
- ACLs
- **Venues**
- Summary

Venues

1 selected ⊗ Activate | Deactivate

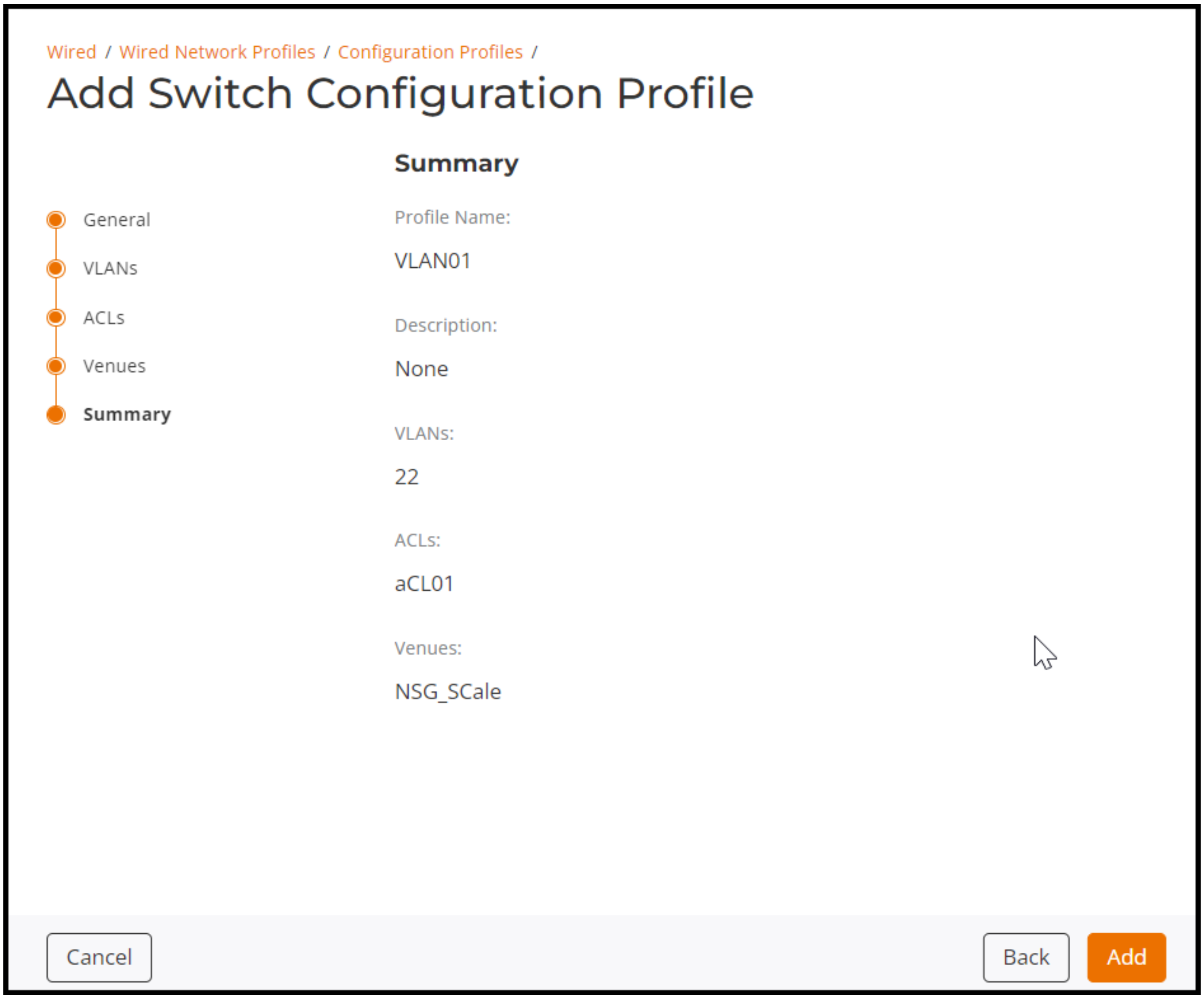
☐	Venue ▲	City	Country	Switches	Activated
□	My-Venue	New York	United States	0	○
☑	NSG_SCale	Sunnyvale, California	United States	2	●

After activating the selected venue, click **Next**. This displays the **Summary** section.

Summary

Verify all the details in the **Summary** section and click **Add**

FIGURE 141 Summary



Wired / Wired Network Profiles / Configuration Profiles /

Add Switch Configuration Profile

Summary

Profile Name:

VLAN01

Description:

None

VLANs:

22

ACLs:

aCL01

Venues:

NSG_SCale

The new **VLAN Configuration Profile** is displayed in the **Wired Network Profiles** page.

Tagging Uplink/Downlink Ports

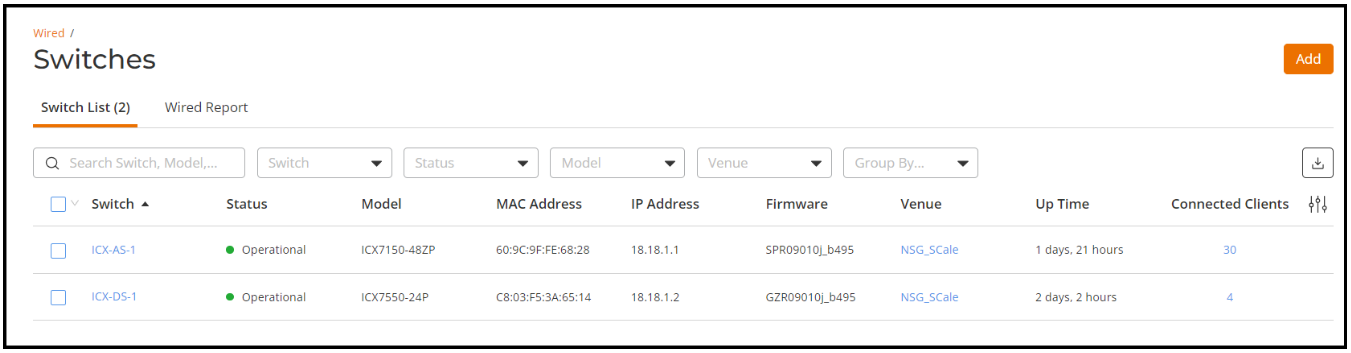
After the switches are onboarded, RUCKUS One should be tagged with uplink and downlink ports.

To tag the uplink and downlink ports, perform the following steps.

1. On the RUCKUS One navigation bar, navigate and hover the mouse on **Wired** option and select **Switch List**.

   This displays the onboarded switch list.

   FIGURE 142 Switches

	Switch ▲	Status	Model	MAC Address	IP Address	Firmware	Venue	Up Time	Connected Clients
□	ICX-AS-1	● Operational	ICX7150-48ZP	60:9C:9F:FE:68:28	18.18.1.1	SPR09010j_b495	NSG_SCale	1 days, 21 hours	30
□	ICX-DS-1	● Operational	ICX7550-24P	C8:03:F5:3A:65:14	18.18.1.2	GZR09010j_b495	NSG_SCale	2 days, 2 hours	4

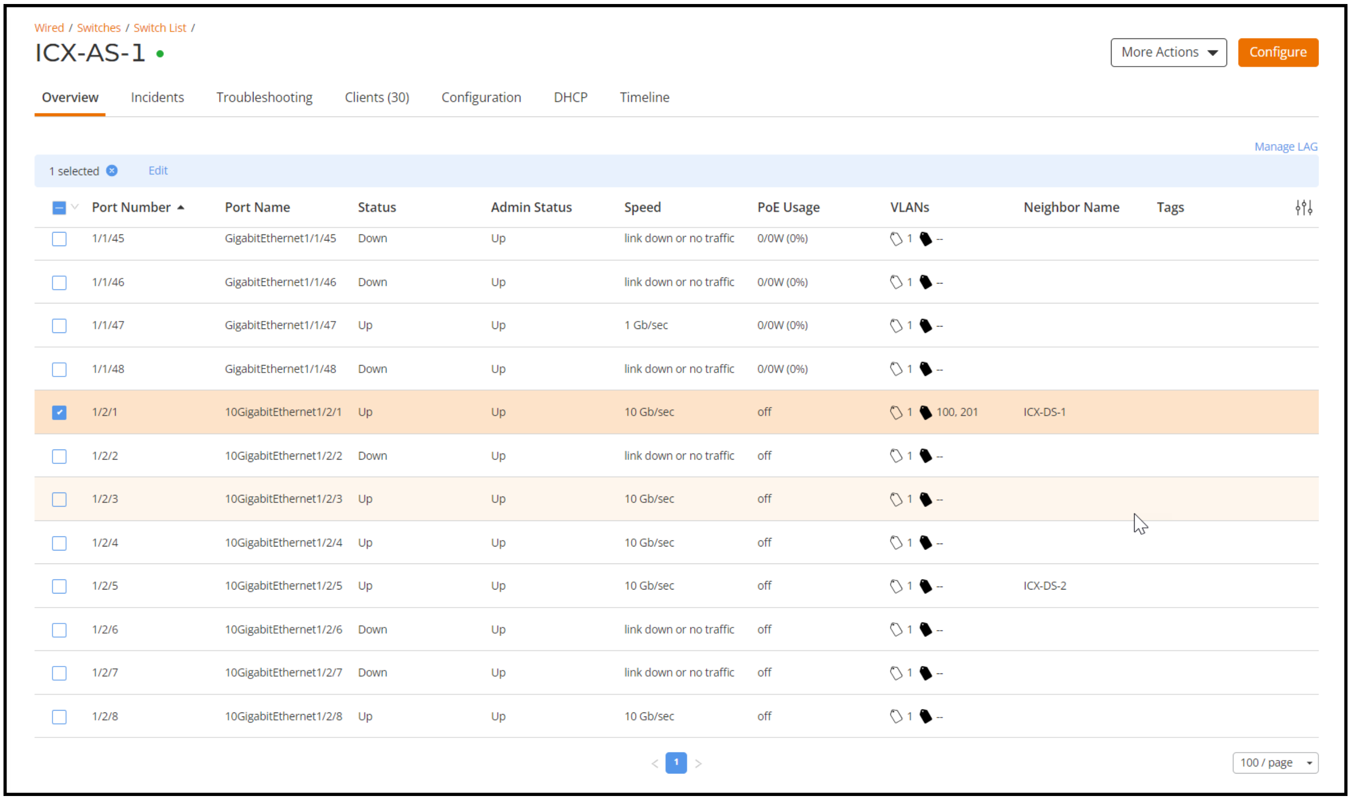
2. Click on switch **ICX-AS-1** to tag uplink port.

   This displays details of the switch.

3. In the details page, click **Ports** tab.

   This displays the list of ports configured on the switch.

   FIGURE 143 List of Ports

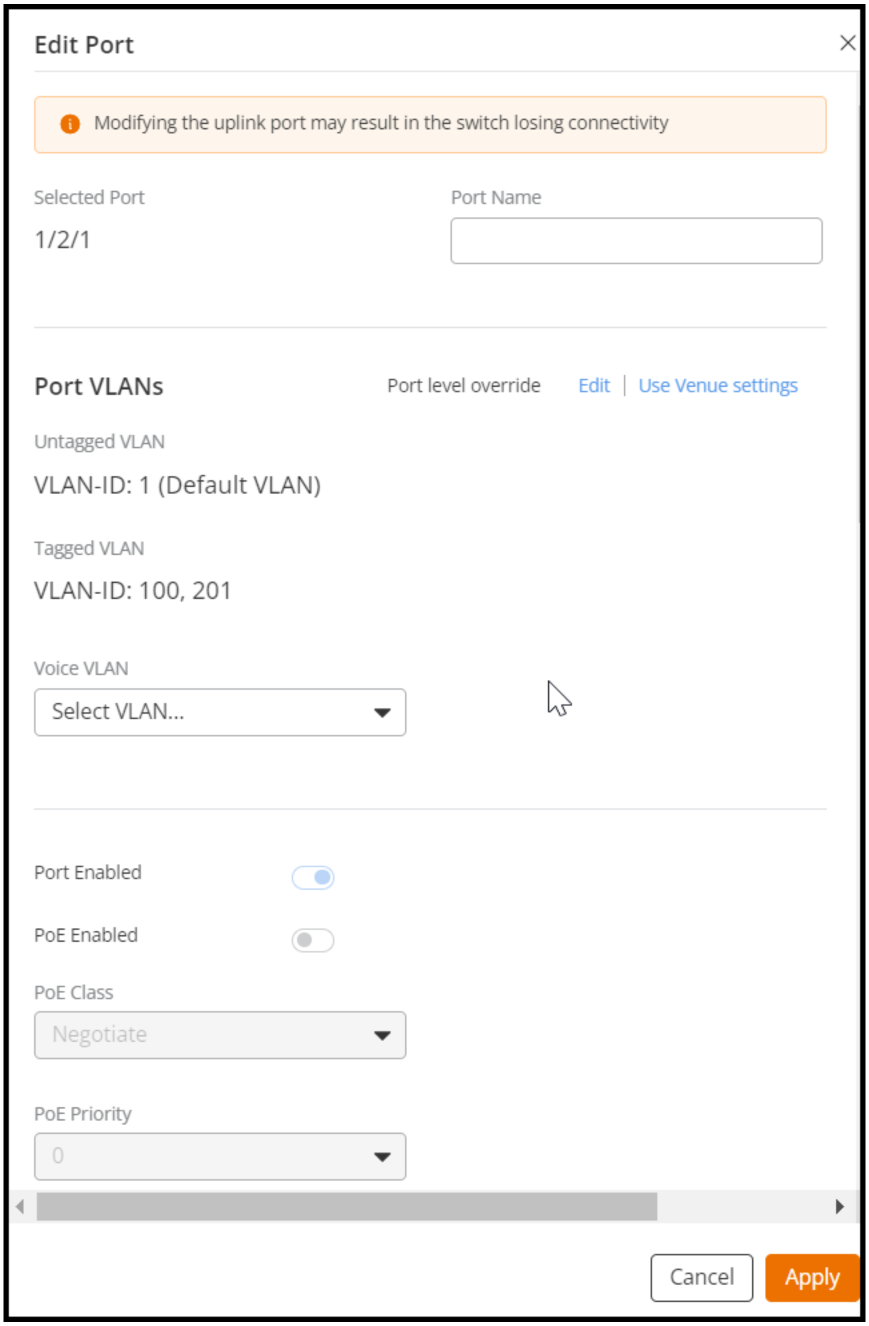


☐	Port Number ▲	Port Name	Status	Admin Status	Speed	PoE Usage	VLANs	Neighbor Name	Tags
☐	1/1/45	GigabitEthernet1/1/45	Down	Up	link down or no traffic	0/0W (0%)	◇ 1 ◆ --		
☐	1/1/46	GigabitEthernet1/1/46	Down	Up	link down or no traffic	0/0W (0%)	◇ 1 ◆ --		
☐	1/1/47	GigabitEthernet1/1/47	Up	Up	1 Gb/sec	0/0W (0%)	◇ 1 ◆ --		
☐	1/1/48	GigabitEthernet1/1/48	Down	Up	link down or no traffic	0/0W (0%)	◇ 1 ◆ --		
☑	1/2/1	10GigabitEthernet1/2/1	Up	Up	10 Gb/sec	off	◇ 1 ◆ 100, 201	ICX-DS-1	
☐	1/2/2	10GigabitEthernet1/2/2	Down	Up	link down or no traffic	off	◇ 1 ◆ --		
☐	1/2/3	10GigabitEthernet1/2/3	Up	Up	10 Gb/sec	off	◇ 1 ◆ --		
☐	1/2/4	10GigabitEthernet1/2/4	Up	Up	10 Gb/sec	off	◇ 1 ◆ --		
☐	1/2/5	10GigabitEthernet1/2/5	Up	Up	10 Gb/sec	off	◇ 1 ◆ --	ICX-DS-2	
☐	1/2/6	10GigabitEthernet1/2/6	Down	Up	link down or no traffic	off	◇ 1 ◆ --		
☐	1/2/7	10GigabitEthernet1/2/7	Down	Up	link down or no traffic	off	◇ 1 ◆ --		
☐	1/2/8	10GigabitEthernet1/2/8	Up	Up	10 Gb/sec	off	◇ 1 ◆ --		

4. Selec the port and click **Edit**.

   This displays the tagged and untagged VLAN ports .i.e. uplink and downlink ports for the swtich.

FIGURE 144 Uplink/Downlink VLAN Ports



Edit Port

Modifying the uplink port may result in the switch losing connectivity

Selected Port: 1/2/1

Port Name:

Port VLANs

Untagged VLAN: VLAN-ID: 1 (Default VLAN)

Tagged VLAN: VLAN-ID: 100, 201

Voice VLAN: Select VLAN...

Port Enabled: on

PoE Enabled: off

PoE Class: Negotiate

PoE Priority: 0

Adding DPSK Service

Dynamic Pre-Shared Key is a encryption technology developed to provide robust and secure wireless access.

To add a DPSK service to configure PIN, perform the following steps.

1. On the RUCKUS One navigation bar, hover on **Network Control** and click **My Services**.

   This displays the **My Services** menu.
2. Click **DPSK** option in the menu.

   This displays **DPSK** page.
3. Click **Add DPSK Service**.

   This displays **Add DPSK Service** page.

4. In the **Add DPSK Service** page, enter the following details:

   Under **Settings** enter the service name

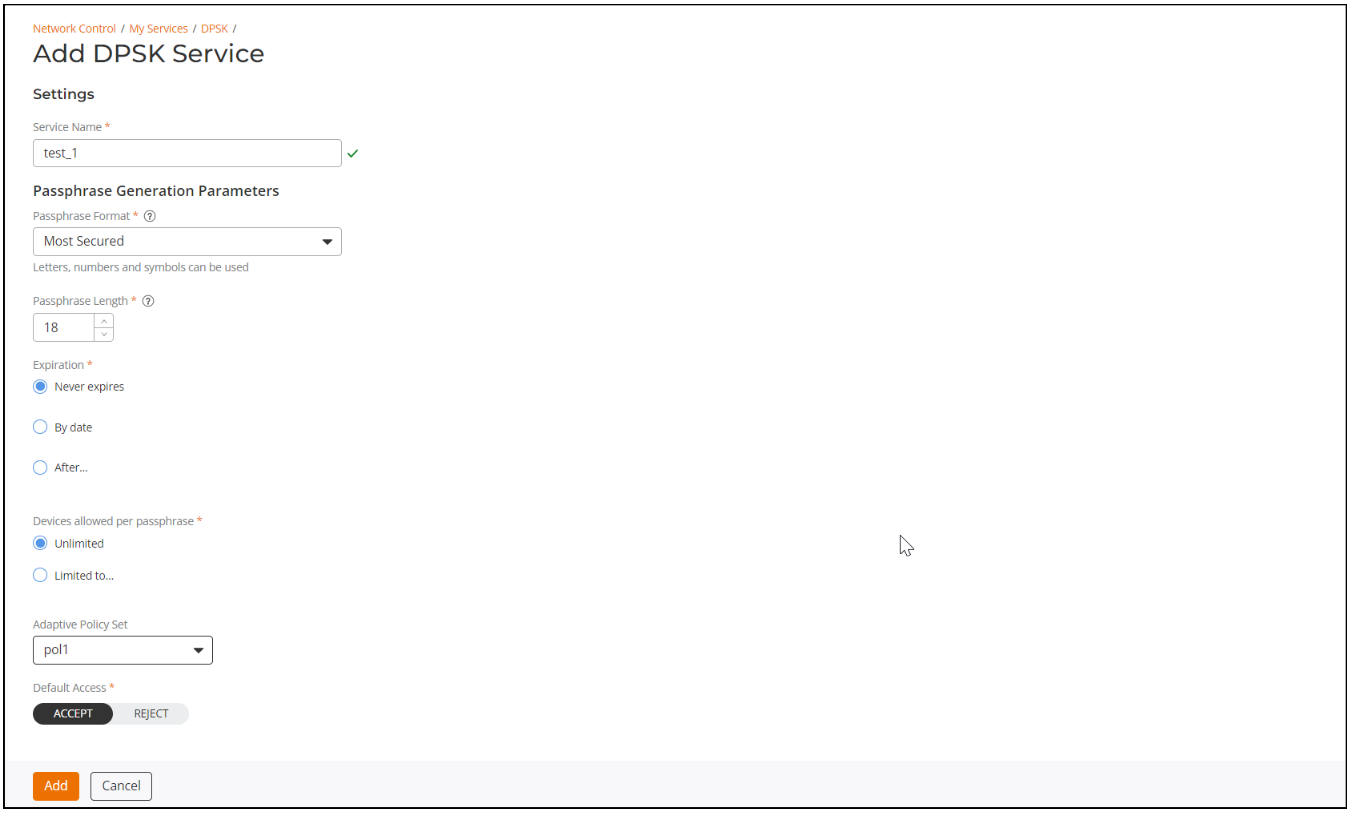
   - **Service Name** - Enter a name for the DPSK service.

   Under **Passphrase Generation Parameters** enter the following details:

   - **Passphrase Format** - Click on the drop-down menu and select the passphrase format.
     - Most Secured - Allows the user to use all ASCII characters.
     - Keyboard Friendly - Only Alphabets and numbers can be used.
     - Numbers Only - Only numbers can be used.
   - **Passphrase Length** - Enter the passpharse length. Valid range 8 to 63.
   - **Expiration** - Select the expiration type,
     - Never Expires - Have no expiry date.
     - By Date - Select a date from the corresponding calendar.
     - After - Enter a number in the corresponding field and choose the option from the drop-down list.
   - **Devices Allowed per Passphrase** - Select the number of devices to be allowed per passphrase.
     - Unlimited - No restrictions in terms of number of devices.
     - Limited To - Enter the number of devices that can be used with one passphrase in the corresponding field.
   - **Adaptive Policy Set** - Select the policy set from the drop-down list.
   - **Default Access** - Select the access method.

   After entering all the fields, click **Add**. The newly created DPSK service is added to the list.

FIGURE 145 Add DPSK Service



Network Control / My Services / DPSK /

Add DPSK Service

Settings

Service Name *: test_1 ✓

Passphrase Generation Parameters

Passphrase Format *: Most Secured

Letters, numbers and symbols can be used

Passphrase Length *: 18

Expiration *

● Never expires

○ By date

○ After...

Devices allowed per passphrase *

● Unlimited

○ Limited to...

Adaptive Policy Set: pol1

Default Access *: [✓ ACCEPT] REJECT

Creating a New Identity Group

Identity group stores user related data.

To create a new Identity group, perform the following steps.

1. On the RUCKUS One navigation bar, hover on **Clients** and click **Identity Groups**.

   This displays **Identity Management** page.

2. In the **Identity Management** page, click **Add Identity Group** link.

   This displays **Create Identity Group** window.

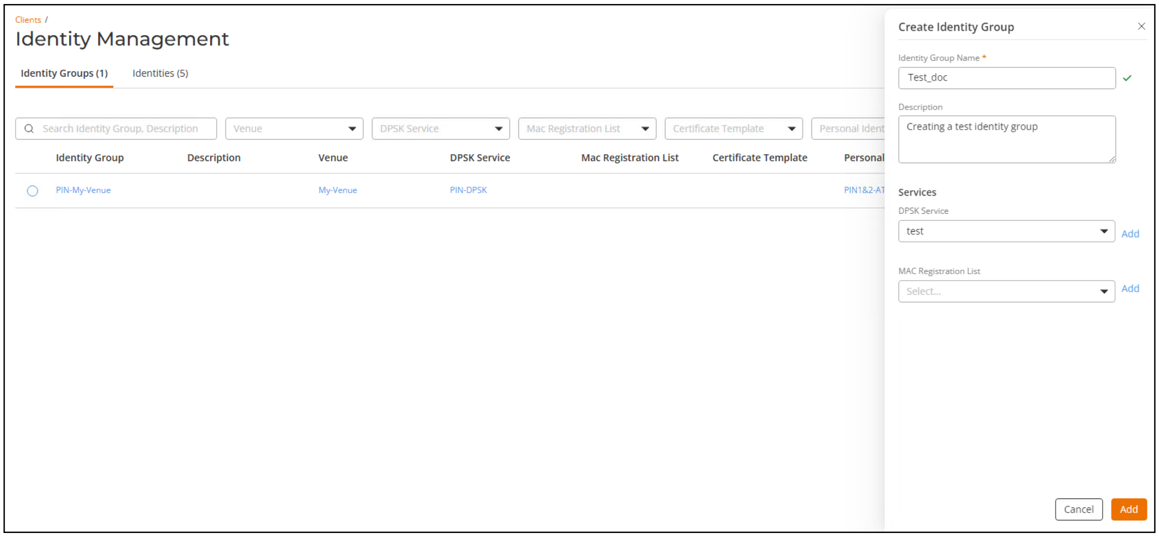
3. In the **Create Identity Group**, enter the following details

   - **Identity Group Name** - Select identity group name from the drop-down list.
   - **Description** - Enter a meaningful description for the identity group.

     Under **Services**,

   - **DPSK Service** - Select a DPSK service from the drop-down list or add a DPSK service by clicking **Add** link.
   - **MAC Registrationi List** - Select a MAC ID from the drop-down list or add a MAC by clicking **Add** link.

   FIGURE 146 Creating a new Identity Group

	Identity Group	Description	Venue	DPSK Service	Mac Registration List	Certificate Template	Personal
○	PIN-My-Venue		My-Venue	PIN-DPSK			PIN1&2-AT

   Create Identity Group

   Identity Group Name *: Test_doc ✓

   Description: Creating a test identity group

   Services

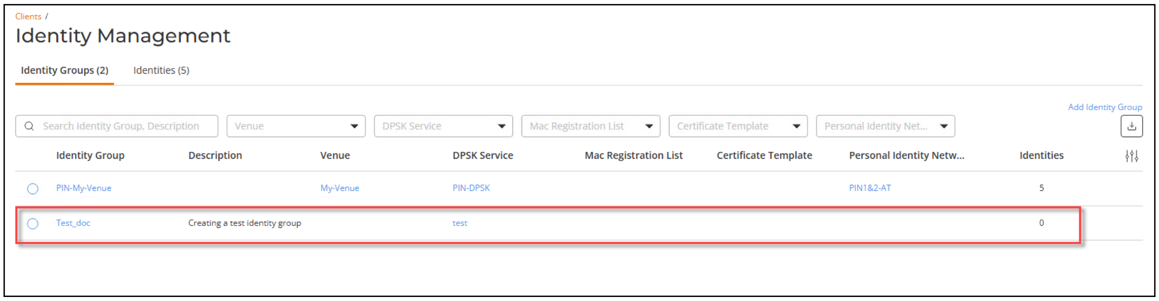
   DPSK Service: test

   MAC Registration List: Select...

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

   The newly added identity group is displayed in the **Identity Management** page.

   FIGURE 147 Newly created Identity Group in the Identity Management List



Identity Group	Description	Venue	DPSK Service	Mac Registration List	Certificate Template	Personal Identity Netw...	Identities
○ PIN-My-Venue		My-Venue	PIN-DPSK			PIN1&2-AT	5
○ Test_doc	Creating a test identity group		test				0

Enabling Property Management

Enable property management in the venue. To enable property management, perform the following steps.

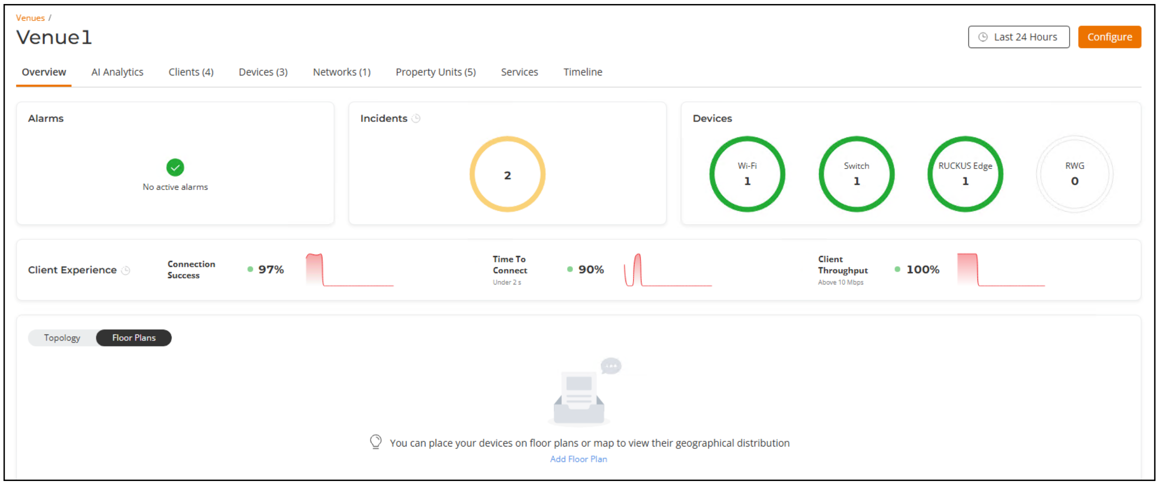
1. On the RUCKUS One navigation bar, click **Venue**.

   This displays **Venues** page with the list of venues.

2. Select and click on the **Venue** in the list.

   This displays the venue details.

   FIGURE 148 Venue Details



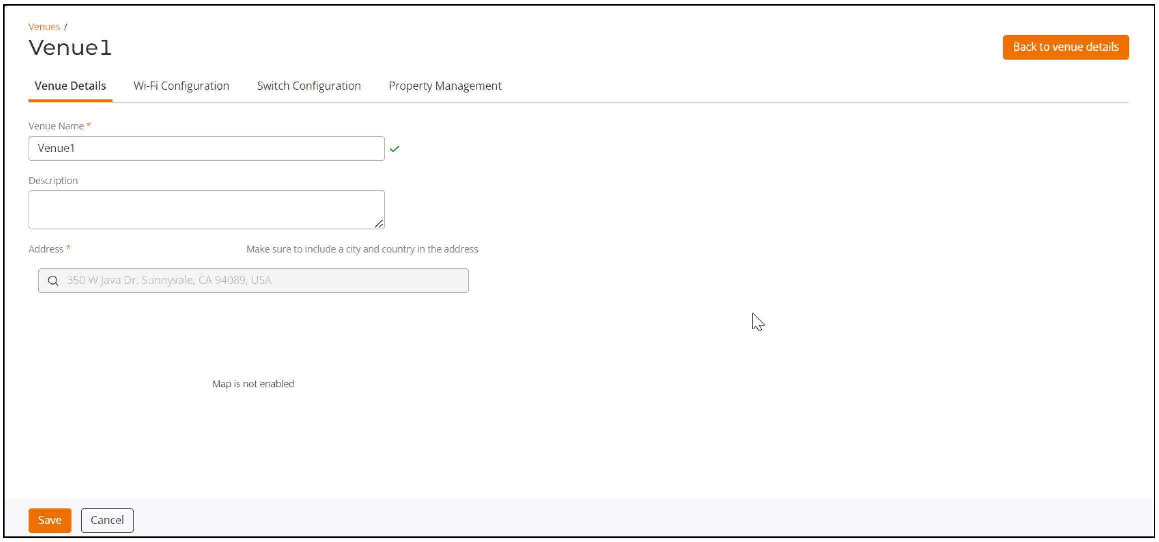
No active alarms

You can place your devices on floor plans or map to view their geographical distribution

3. In the **Venue** page, click **Configure**.

   This displays the selected venue configuration details.

   FIGURE 149 Venue Details



Venues /

Venue1

Back to venue details

Venue Details | Wi-Fi Configuration | Switch Configuration | Property Management

Venue Name *

Venue1 ✓

Description

Address * — Make sure to include a city and country in the address

350 W Java Dr, Sunnyvale, CA 94089, USA

Map is not enabled

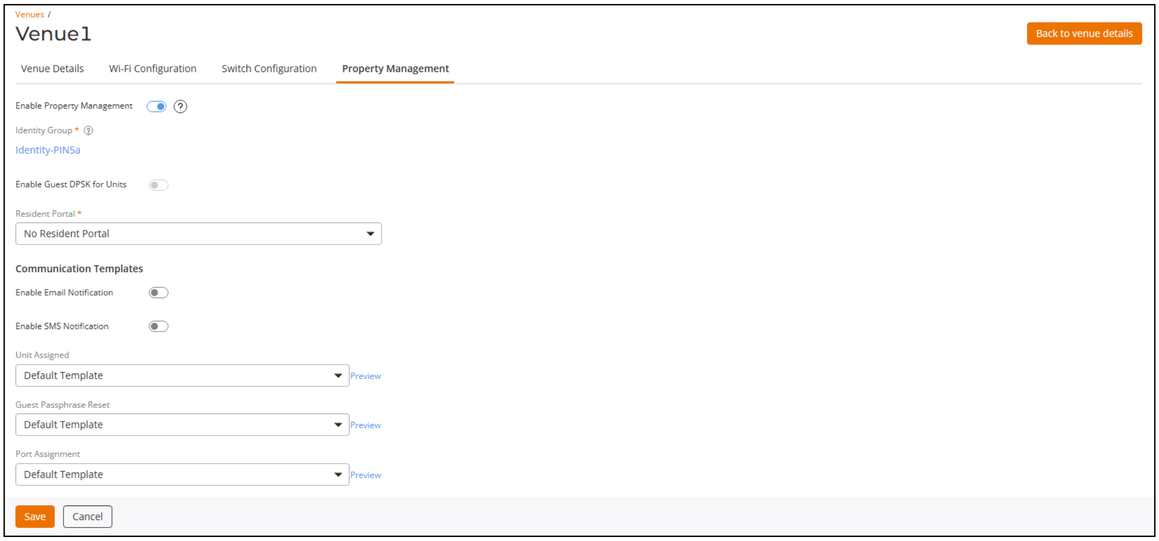
Save | Cancel

4. In the **Venue** details page, click **Property Management** tab.

   This displays the **Property Management** switch.

   NOTE
   By default, the **Property Management** switch is disabled, if the property management is swtiched off, all the related configuration is deleted and the network service is lost.

   FIGURE 150 Enable Property Management



Venues /

Venue1

Back to venue details

Venue Details | Wi-Fi Configuration | Switch Configuration | Property Management

Enable Property Management ●

Identity Group *

Identity-PIN5a

Enable Guest DPSK for Units ○

Resident Portal *

No Resident Portal

Communication Templates

Enable Email Notification ○

Enable SMS Notification ○

Unit Assigned

Default Template — Preview

Guest Passphrase Reset

Default Template — Preview

Port Assignment

Default Template — Preview

Save | Cancel

Dynamic Host Configuration Protocol (DHCP)

Configuring DHCP for RUCKUS Edge Service

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automatically assign IP addresses and other communications to the devices connected in the network.

When DHCP relay is enabled, there is a property called ‘For Personal Identification Network. If you enable this property, you need to enter the pool information, excluding the gateway.
To configure DHCP service for RUCKUS Edge, perform the following steps.

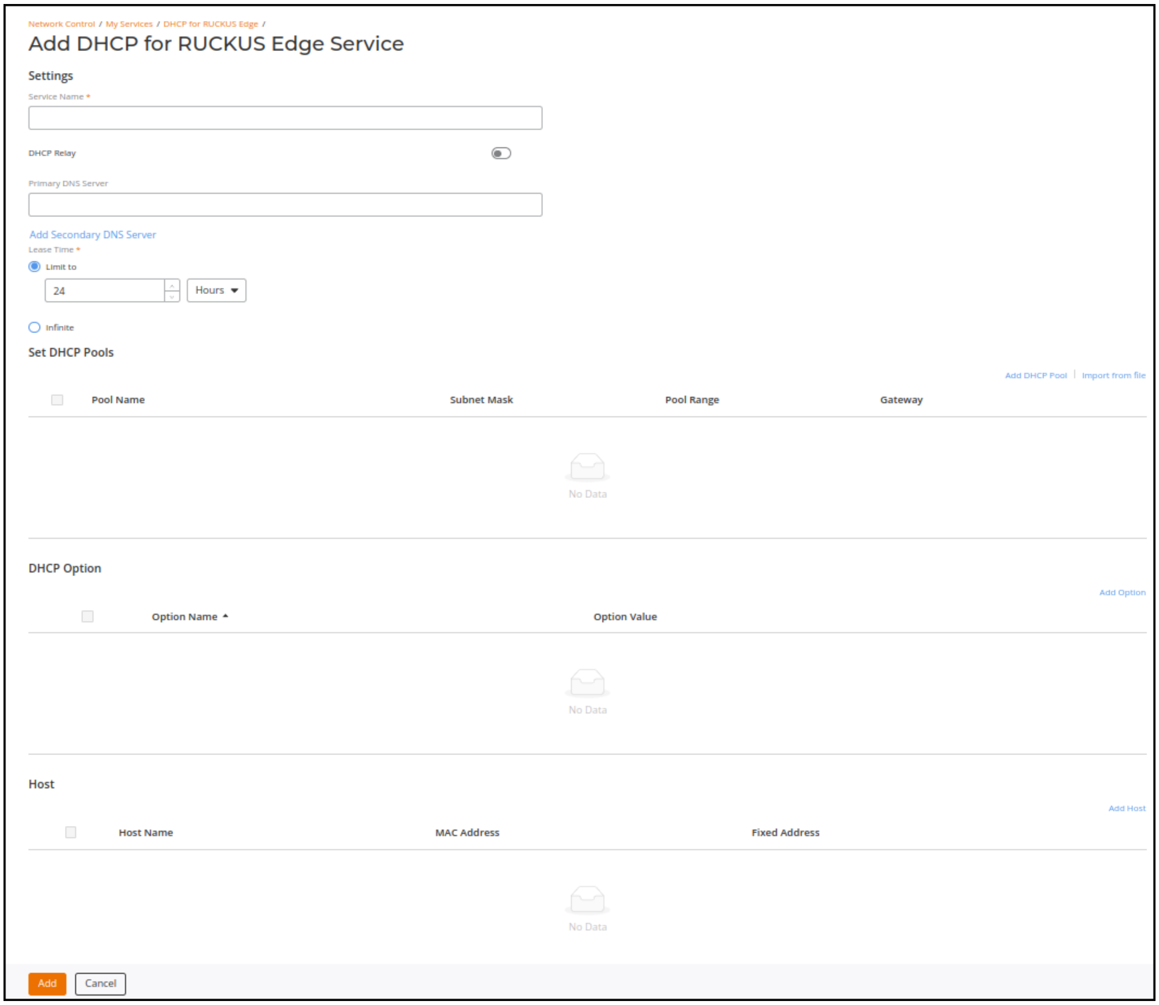
1. On the RUCKUS One navigation bar, hover on **Network Control** and click **My Services**.

   This displays the **My Services** menu.
2. Click **DHCP for RUCKUS Edge**.

3. In the **DHCP for RUCKUS Edge** page, click **Add DHCP Service**.

   This displays **Add DHCP for RUCKUS Edge Service** page. In the **Add DHCP for RUCKUS Edge Service** enter all the details in the sections listed below.

   FIGURE 151 Add DHCP for RUCKUS Edge Service



Network Control / My Services / DHCP for RUCKUS Edge /

Add DHCP for RUCKUS Edge Service

Settings

Service Name *

DHCP Relay

Primary DNS Server

Add Secondary DNS Server

Lease Time *

● Limit to

24 Hours

○ Infinite

Set DHCP Pools

Add DHCP Pool | Import from file

□	Pool Name	Subnet Mask	Pool Range	Gateway

No Data

DHCP Option

Add Option

□	Option Name	Option Value

No Data

Host

Add Host

□	Host Name	MAC Address	Fixed Address

No Data

Settings

- **Service Name** - Enter a valid service name for the DHCP service.
- **DHCP Relay** - By default, this option is disabled. Enable this option for DHCP clients to communicate with DHCP servers.
- **Primary DNS Server** - Enter primary DNS server details. This is an optional field. To add a secondary DNS server, click **Add Secondary DNS Server** link and the field is displayed below.
- **Lease Time** - There are two options:
  - Limit To - Choose or enter a number from the scroll bar and select an option between Days, Hours and minutes from the drop-down. The **Lease Time** expires as per the selection.
  - Infinite - Select this option for limitless lease time.

Set DHCP Pools

- **Add DHCP Pool** - To add a DHCP pool, click the **Add DHCP Pool** link. This displays **Add DHCP Pool** window. Enter the details of the DHCP and click **Add**. The newly added DHCP details are displayed in the section.
- **Import from file** - To import a file from the local computer, click **Import from file** link. This displays **Import from file** window. Click **Browse** or **Drag and drop the file** from local computer and click **Import**. Make sure the file format is **.csv**, file size should be less or equal to **5MB** and the file may have only **128** entries.

DHCP Option

- **Add Option** - To add DHCP option, click **Add Option** link. This displays the **Add Option** window, select the **Option Name** from the drop-down list. The option supported are -
  - Domain Server
  - Domain Name
  - NTP Server
  - vendor-encapsulated-options
  - vendor-class-identifier
  - NETBIOS Scope
  - Server Name
  - Bootfile-Name

  Enter a value in the **Option Value**. Both the fields are mandatory. After entering the details, click **Add**. The newly added DHCP option is displayed in the section.

Add Host

- **Add Host** - To add a host, click **Add Host** link. This displays the **Add Host** window. Enter the details in the Add Host window and click **Add**. The newly added host is displayed in the section.

The newly added DHCP for RUCKUS Edge Service is displayed in the **DHCP for RUCKUS Edge** page.

Deploying DHCP for RUCKUS Edge Service

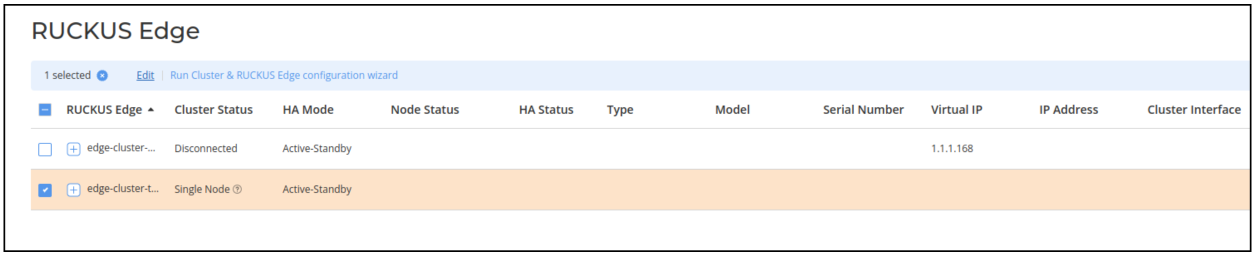
After configuring a DHCP for RUCKUS Edge, user should deploy the service.

To deploy the DHCP for RUCKUS Edge service, perform the following steps.

1. On the RUCKUS One navigation bar, click **Gateway** > **RUCKUS Edge**.

   This displays the **RUCKUS Edge** page.

FIGURE 152 RUCKUS Edge



RUCKUS Edge

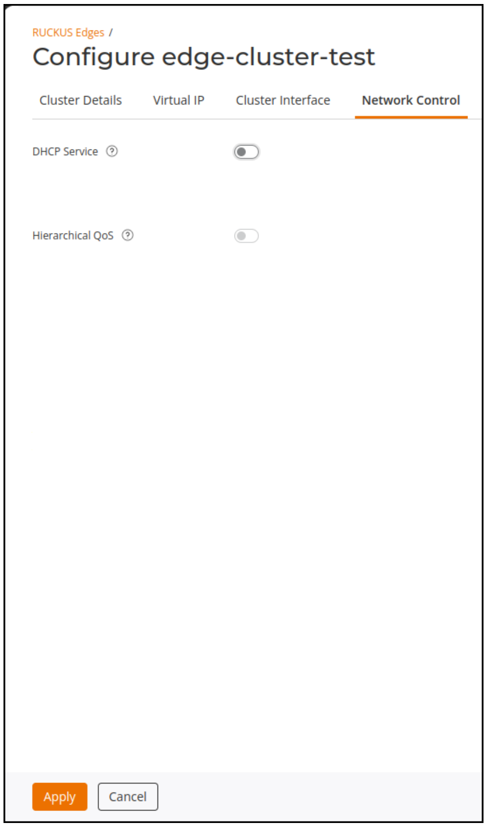
1 selected ⊗ Edit | Run Cluster & RUCKUS Edge configuration wizard

▣	RUCKUS Edge ▲	Cluster Status	HA Mode	Node Status	HA Status	Type	Model	Serial Number	Virtual IP	IP Address	Cluster Interface
□	⊞ edge-cluster-...	Disconnected	Active-Standby						1.1.1.168		
☑	⊞ edge-cluster-t...	Single Node ⓘ	Active-Standby								

2. Select the RUCKUS Edge from the list and click **Edit**.

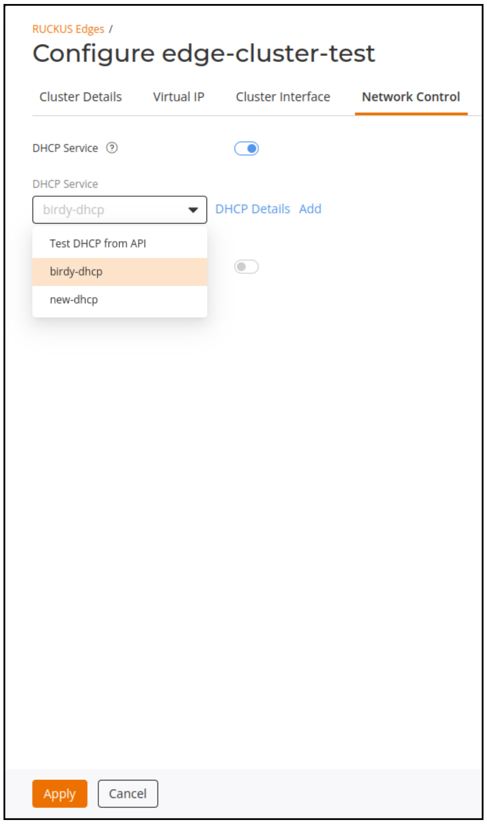
   This displays the selected Edge **Cluster Details**.

   FIGURE 153 RUCKUS Edge with Details

3. Click the **Network Control** tab.

FIGURE 154 Network Control



4. Select the **DHCP Service** and click **Apply**.
5. To apply the DHCP settings, go to **Network Control** > **My Services** > **DHCP for RUCKUS Edge**.

   This displays the **DHCP for RUCKUS Edge Service** window.
6. In the **DHCP for RUCKUS Edge Service** window, click the **DHCP Service** drop-down list and select the service and click **Apply**.

   The selected DHCP service is displayed in the RUCKUS Edge page.

Editing a DHCP for RUCKUS Edge Service

To edit a DHCP for RUCKUS Edge service, perform the following steps.

1. On the RUCKUS One navigation bar, hover on **Network Control** and click **My Services**.

   This displays the **My Services** menu.
2. Click **DHCP for RUCKUS Edge**.

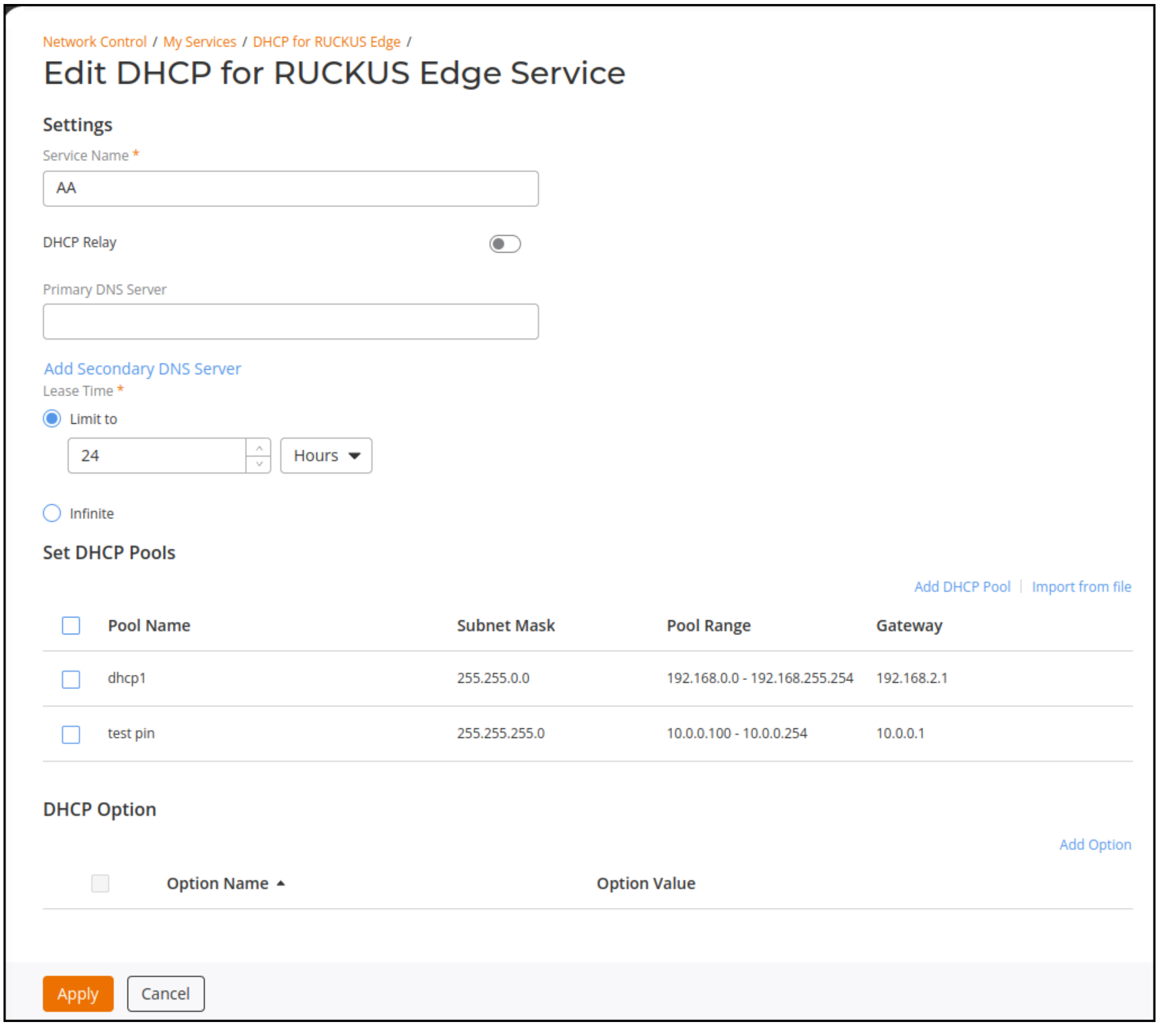
   This displays the list of DHCPs in the **DHCP for RUCKUS Edge Service**.
3. Select check box corresponding to the name of the DHCP for RUCKUS Edge Service.

   This displays the **Edit**, **Delete** links on top of the section.

4. Click **Edit**.

   This displays **Edit DHCP for RUCKUS Edge Service** page.

   FIGURE 155 Edit DHCP for RUCKUS Edge Service



Network Control / My Services / DHCP for RUCKUS Edge /

Edit DHCP for RUCKUS Edge Service

Settings

Service Name *: AA

DHCP Relay: ○

Primary DNS Server:

Add Secondary DNS Server

Lease Time *

● Limit to: 24 Hours

○ Infinite

Set DHCP Pools

Add DHCP Pool | Import from file

□	Pool Name	Subnet Mask	Pool Range	Gateway
□	dhcp1	255.255.0.0	192.168.0.0 - 192.168.255.254	192.168.2.1
□	test pin	255.255.255.0	10.0.0.100 - 10.0.0.254	10.0.0.1

DHCP Option

Add Option

□	Option Name ▲	Option Value

5. Edit the DHCP settings as required and click **Apply**. A confirmation message is displayed and the selected DHCP is updated with the new information.

Deleting a DHCP for RUCKUS Edge Service

To delete a DHCP for RUCKUS Edge service, perform the following steps.

1. On the RUCKUS One navigation bar, hover on **Network Control** and click **My Services**.

   This displays the **My Services** menu.

2. Click **DHCP for RUCKUS Edge**.

   This displays the list of DHCPs in the **DHCP for RUCKUS Edge Service**.

3. Select check box corresponding to the name of the DHCP for RUCKUS Edge Service.

   This displays the **Edit**, **Delete** links on top of the section.

4. Click **Delete**.

   This displays a confirmation message.

5. Click **Delete DHCP**.

   The selected DHCP is removed from the list.

Appendix

Supported AP Models

Table 5 provides a list of APs that are supported by RUCKUS Edge release 2.1.0.

TABLE 5 Supported AP Models for Release 2.1.0

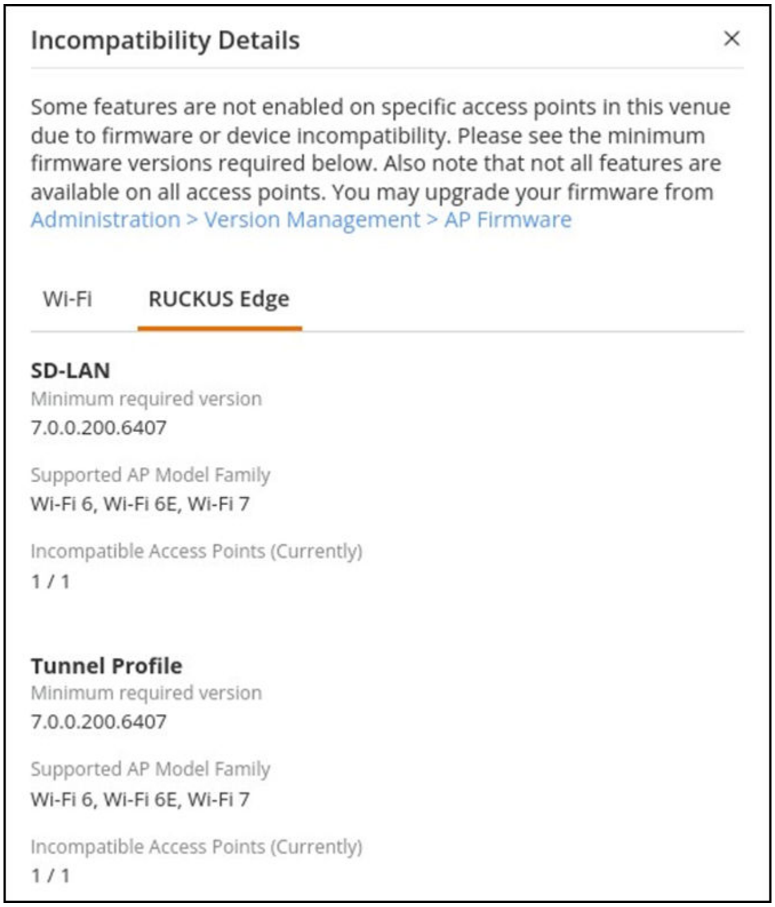
IEEE Standard	Profile ID	Image Type	Supported AP Models
802.11be	ap-arm-11beax	R770	R770
802.11ax	ap-arm-11ax	R730	R730, R750, R650, T750, T750SE, R850, R550, R760, R560
	ap-arm-cypress	H550	H550, T350C, T350D, T350SE, R350, H350
802.11ac Wave 2	ap-arm-dakota	R510	R320, M510, R510, H510, H320, E510, 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 156. 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 156 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

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

350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com