CONFIGURATION GUIDE

RUCKUS SmartZone (ST-GA) Tunnel and Data Plane Guide, 7.0.0

Supporting SmartZone Release 7.0.0

Part Number: 800-73598-001 Rev B
Publication Date: August 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

About This Guide

This guide aims to provide comprehensive insight into deploying and maintaining tunneled WLANs and Data Planes. It covers managing the Data Plane from the controller Web UI, customizing and troubleshooting traffic forwarding, and encryption. By following this guide, you will gain a deep understanding of how to effectively manage and optimize your network's tunneled WLANs and Data Planes.

New In This Document

TABLE 2 Key Features and Enhancements in *Tunnel and Data Plane Guide*, *7.0.0* (*August 2024*)

Feature	Description	Reference
Adding Icons	Throughout the guide.	-
Adding Animated GIFs	Throughout the guide.	-

Configuring the Data Plane

Configuring the Data Plane

By default, the controller sends traffic from its data plane from a single interface.

> **NOTE**
> This feature is managed only by vSZ-E and vSZ-H controllers.

If your organization's network requires separation of the access and core traffic, configure access and core separation on the controller.

To configure a data plane:

1. Go to **Network** > **Data and Control Plane** > **Cluster**.
2. Select the data plane from the list and click **Configure**.The Edit Data Plane Network Settings form appears.
3. Configure the settings as explained in Table 3.
4. Click **OK**.

TABLE 3 Configuring Data Plane

Field	Description	Your Action
Network		
Interface Mode	Indicates the traffic direction.	Choose the option: ● **Single Interface** (default)—For the controller to send traffic from its data plane from a single interface. ● **Access and Core Interface**—For the controller to send traffic to the access and core networks separately. **NOTE** To separate the access and core networks – Use static routes, if the data plane is required to connect to IP addresses in the core network (for example, for DHCP relay or L2oGRE termination) and the destination IP addresses are not part of the core subnet. ● **Keep original configuration**—For the controller to keep the original manual Data Plane setup.
Network > **Primary (Access) Interface**		
IP Mode	Indicates the mode of assigning the IP address to this interface.	Select the option: ● **Static** (*recommended*)—To manually assign an IP address to this interface manually. – Enter the **IP Address**. – Enter **Subnet Mask** for the IP address. – Enter the **Gateway** router address. – Enter the **Primary DNS Server** IP address. – Enter the **Secondary DNS Server** IP address. – Enter **VLAN** ID to tag traffic. – Choose the **Data NAT IP/Port Configured** option. – Enter **Data NAT IP** address. – Enter **Data NAT Port** address. ● **DHCP**—To automatically obtain an IP address from a DHCP server on the network. – Enter **VLAN** ID to tag traffic. – Choose the **Data NAT IP/Port Configured** option.
Network > **IPv6 Primary (Access) Interface**		
IP Mode	Indicates the mode of assigning the IP address to this interface.	Select the option: ● **Static** (*recommended*)—To manually assign an IP address to this interface manually. – Enter the **IP Address**. – Enter the **Gateway** router address. – Enter the **Primary DNS Server** IP address. – Enter the **Secondary DNS Server** IP address. ● **Auto**—To automatically obtain an IP address from a DHCP server on the network.
Network > **Secondary (Core) Interface** (applicable for **Interface Mode**: **Access and Core Interfaces**)		
IP Address	Indicates the IP address of the core network interface.	Enter the IP address. **NOTE** The secondary/core interface IP address must be configured manually; DHCP is unsupported.
Subnet Mask	Indicates the IP address of the subnet mask.	Enter the subnet mask.

TABLE 3 Configuring Data Plane (continued)

Field	Description	Your Action
VLAN	Indicates that the traffic is tagged with a VLAN ID.	Enter the VLAN ID. **NOTE** If VLANS are configured on both the access and core networks, the VLAN ID that you enter here must be different from the one that you entered for the primary/access interface. **NOTE** You cannot configure the IP address and VLAN settings for a virtual Data Plane from the Primary (Access) and Secondary (Core) Interface sections. Only vSZ-H supports virtual Data Plane.
Disconnect AP when core link down	Indicates that the AP is disconnected secondary core link is down.	Select the check box.
Static Routes		
Network Address	Indicates the destination IP address of this route.	Enter the IP address.
Subnet Mask	Indicates a subnet mask for the IP address.	Enter the subnet mask.
Gateway	Indicates the IP address of the gateway router.	Enter the IP address of the gateway router.
Add	Adds the static route settings.	Click **Add**.
CALEA Relay		
Mark this Data Plane as CALEA Relay (This feature is supported only for vSZ-E and vSZ-H controllers)	Indicates that the data plane uses CALEA relay.	Select the check box.
DHCP Profile		
DHCP Profile	Indicates the data plane DHCP service profile.	Choose the DHCP service profile from the drop-down.
NAT Profile		
NAT Profile	Indicates the data plane NAT service profile.	Choose the NAT service profile from the drop-down.
Syslog		
Enable DHCP syslog	Enables syslog to record the DHCP logs.	Select the check box.
Enable NAT syslog	Enables syslog to record the NAT logs.	Select the check box.
Syslog Server IP	Indicates the IP address of the remote syslog server.	Enter the IP address of the remote syslog server.
Syslog Server Port	Indicates the port number of the remote syslog server.	Enter the Port number of the remote syslog server.

NOTE
You can restart a data plane. To do so, select the data plane from the list and click **Restart**.

NOTE
You can approve or delete a data plane. To do so, select the data plane from the list and click **Approve** or **Delete** respectively. You can also download debug logs or switch over clusters. To do so, select the data plane from the list, click **More** and select **Download** or **Switch Over Clusters** respectively.

NOTE
All configuration changes applicable to vSZ-H are also applicable to SZ100-D.

Creating a DP Group

Creating a DP Group

The vSZ-D version in the same DP group must be the same for consistent AP/DP functioning.

> **NOTE**
> Creating a DP group affinity profile is supported only for vSZ-E and vSZ-H platforms.

Complete the following steps to create a DP group.

1. Select **Network** > **Data and Control Plane** > **DP group**.
2. Click **Create**.

   The **Create DP group** form is displayed.
3. Enter a **Name** and **Description** for the DP group.
4. Click **Add**.

   The **Add DP** page is displayed.
5. Select Data Plane from the list and click **OK**.

   NOTE

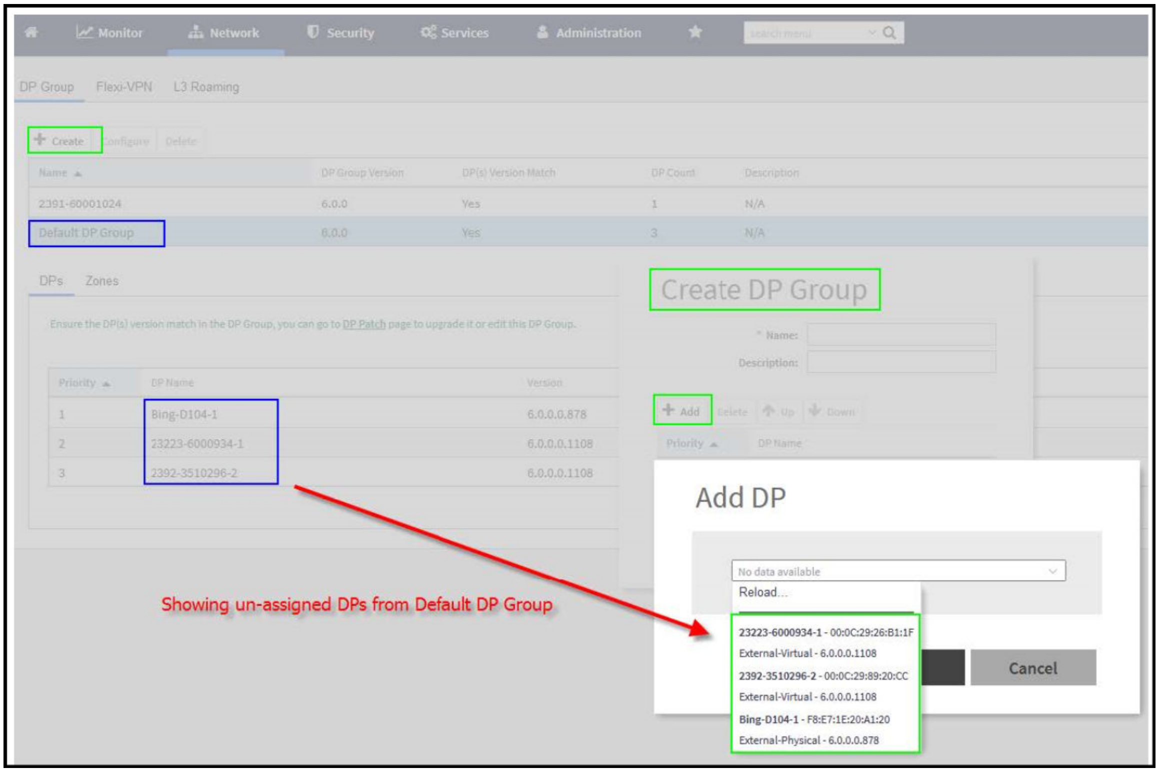
   - While SZ is upgrading from an older version to a newer version, the system validates whether any DP is assigned a duplicate. If a duplicate is encountered, the following warning message is displayed:

     ```
     There is an over-assigned DP in the DP Zone Affinity profiles. Please go to the
     DP Zone Affinity page to edit and make sure only one DP profile is assigned at
     the same time.
     ```
     Once the over-assigned DPs are removed, SZ can upgrade the system.
   - After the configuration that included the over-assigned profiles has been restored, the following message notifies you to correct the configuration:

     ```
     The overlapping DP Group has been detected. There is the over-assigned DP in DP
     Group. Please go to DP Group page to edit and make sure the DP only one DP Group
     assigned at the same time.
     ```

   .

FIGURE 1 Creating a DP Group



Name ▲	DP Group Version	DP(s) Version Match	DP Count	Description
2391-60001024	6.0.0	Yes	1	N/A
Default DP Group	6.0.0	Yes	3	N/A

Ensure the DP(s) version match in the DP Group, you can go to DP Patch page to upgrade it or edit this DP Group.

Priority ▲	DP Name	Version
1	Bing-D104-1	6.0.0.0.878
2	23223-6000934-1	6.0.0.0.1108
3	2392-3510296-2	6.0.0.0.1108

* Name:

Description:

Priority ▲	DP Name

No data available

23223-6000934-1 - 00:0C:29:26:B1:1F
External-Virtual - 6.0.0.0.1108
2392-3510296-2 - 00:0C:29:89:20:CC
External-Virtual - 6.0.0.0.1108
Bing-D104-1 - F8:E7:1E:20:A1:20
External-Physical - 6.0.0.0.878

.

6. Click **OK**.

   NOTE
   You can edit or delete a DP group. To do so, select the DP Group from the list and click **Configure** or **Delete** respectively.

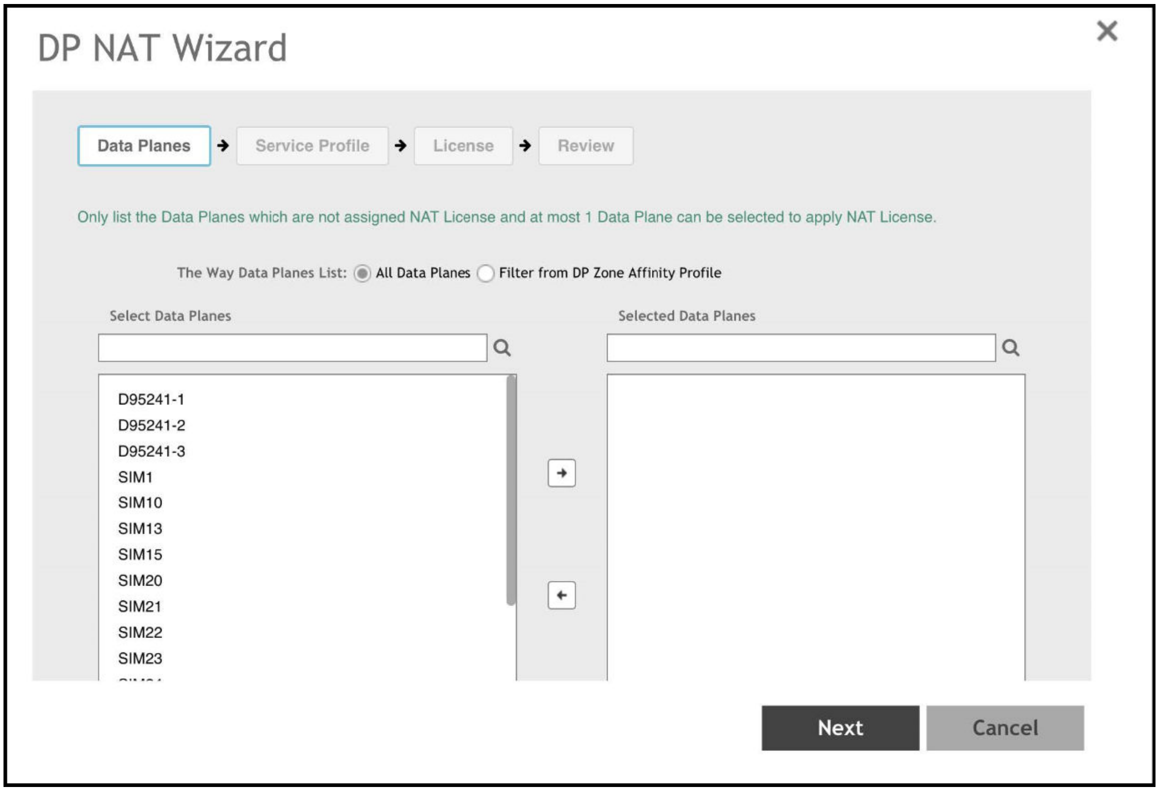
Verifying DP Version Match

From the list, the **DP(s) Version Match** column indicates **Yes** if all the DPs have the same version in the DP Group and **No** if the DPs have different versions in the DP group. You can click the **DP(s)** tab to verify the version of the DP.

DP NAT License Assignment

1. Select the data plane.
2. Option 1 let the user select filter to apply.
3. The "Select Data Planes" is listing DP(s) filtering by option 1.
4. In "Select Data Planes" area, only list DP(s) which has not assigned NAT license.

FIGURE 2 DP NAT WIZARD



Only list the Data Planes which are not assigned NAT License and at most 1 Data Plane can be selected to apply NAT License.

The Way Data Planes List: ● All Data Planes ○ Filter from DP Zone Affinity Profile

Select Data Planes

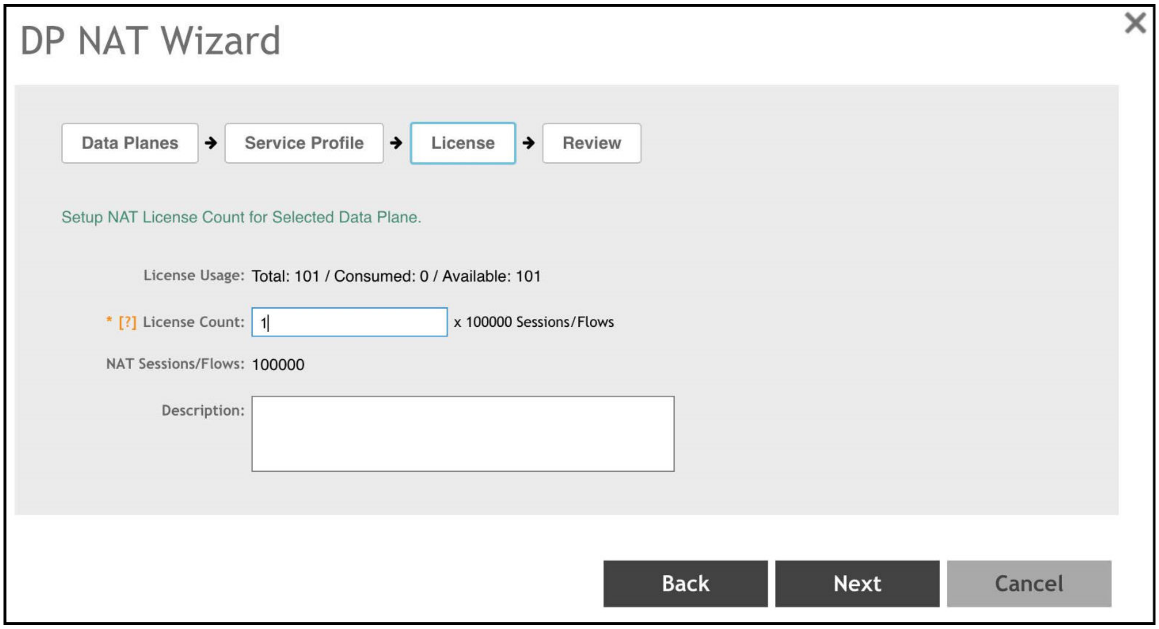
D95241-1
D95241-2
D95241-3
SIM1
SIM10
SIM13
SIM15
SIM20
SIM21
SIM22
SIM23

Selected Data Planes

1. Select the NAT service profile.
2. In NAT service profile option, only list the profile which has not assigned to DP.
3. The existed service profile on DP will be replaced after the wizard completed.

Allocate the sufficient license for DP NAT.

FIGURE 3 DP NAT WIZARD License



Setup NAT License Count for Selected Data Plane.

License Usage: Total: 101 / Consumed: 0 / Available: 101

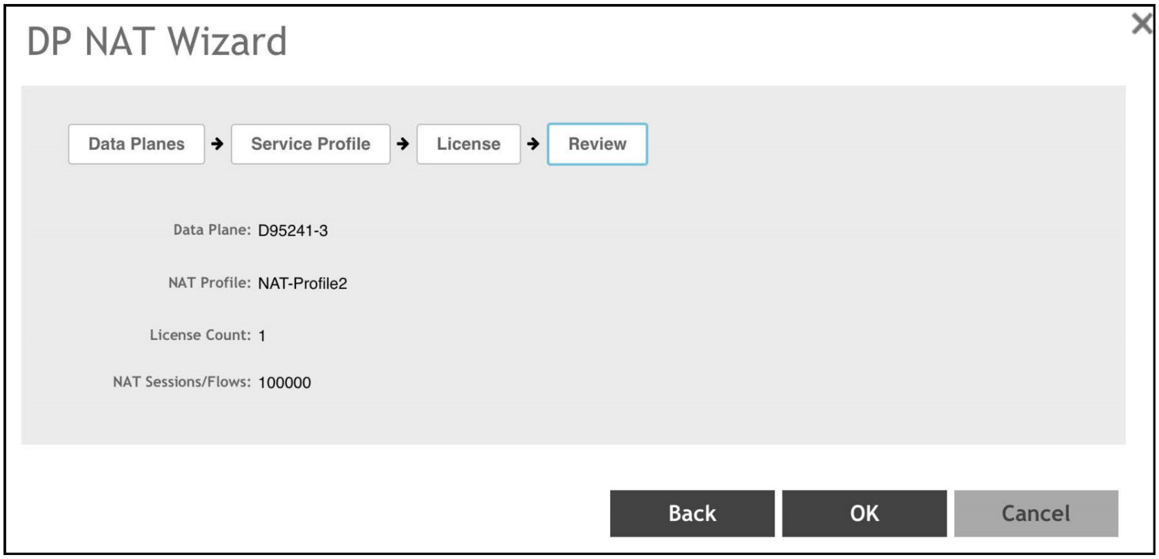
* [?] License Count: 1 x 100000 Sessions/Flows

NAT Sessions/Flows: 100000

Description:

Review all DP NAT configuration before applying.

FIGURE 4 DP NAT WIZARD Review



Data Plane: D95241-3

NAT Profile: NAT-Profile2

License Count: 1

NAT Sessions/Flows: 100000

Enabling Flexi VPN

Enabling Flexi VPN

You can enable Flexi-VPN and limit the network resources that a UE can access. Flexi-VPN allows an administrator to customize the network topology, and is thereby able to control the network resources accessible to the end-user. This feature is only supported on vSZ-E and vSZ-H, and is enabled by purchasing the Flexi-VPN license.

1. From the main menu, go to **Network** > **Data and Control Plane** > **Flexi-VPN**.

   The **Flexi-VPN** status page is displayed.

2. Select **Flexi-VPN**.

   NOTE
   The Flexi-VPN option is available only if the Access-VLAN ID is configured in manual mode, and when VLAN Pooling, Dynamic VLAN and Core Network VLAN options, and Tunnel NAT are disabled.

   NOTE
   Flexi-VPN is activated when a Flexi-VPN profile is assigned to a WLAN.

   NOTE
   A maximum of 1024 WLAN IDs can be applied to a Flexi-VPN profile.
   Flexi-VPN supports IPv4 addressing formats and Ruckus GRE tunnel protocol. It does not support IPv6 addressing formats.

The following record table indicates that the Flexi-VPN profile is successfully applied to the WLAN:

- WLAN: displays the name of the WLAN
- Zone: displays the name of the zone.
- Zone Affinity Profile: displays the name of the source data plane from which tunneled traffic starts
- Flexi-VPN Profile: displays the name of the destination data plane to where the tunneled traffic terminates

VIDEO
Flexi-VPN Overview. This video provides a brief overview of Flexi-VPN.

Click to play video in full screen mode.

Enabling L3 Roaming Criteria for DP

Enabling L3 Roaming Criteria for DP

Using the layer 3 roaming feature, clients can roam across APs in the network (from one data plane to another data plane). This is typically required when the number of clients in the network increases and clients have to roam from a network that they were connected to, to another WLAN network with similar access settings. This feature enables seamless roaming and ensures session continuity between the client and the network.

NOTE
L3 roaming is only supported on vSZ-H and vSZ-E.

You can configure the roaming criteria for a DP so that it uses one of these two options - UE subnet or WLAN VLAN to access another DP to connect to, within a network. Before this, you must ensure that the L3 roaming feature is enabled in the DP.

1. From the main menu, go to **Network** > **Data and Control Plane** > **L3 Roaming**.

   The **L3 Roaming** page is displayed.
2. Select **L3 Roaming**.
3. Click **Configure** to edit the L3 roaming settings.

   The **Edit L3 Roaming** page is displayed.
4. From **Activate**, you can enable the feature for the DP by selecting Enable or Disable from the drop-down menu.
5. From the **Roaming Criteria** list, select one of the following options to define the data format to establish connection between DPs: UE Subnet or WLAN VLAN.
6. Click **OK**.

You have successfully enabled L3 roaming, and also set the roaming criteria based on which DPs would connect within the network.

NOTE
If there are more than 40 DPs been approved, the controller limits you to use L3 Roaming.

NOTE
A fresh controller software installation or upgrade from a version that does not support L3 roaming resets the L3 roaming configuration and it remains disabled. You must enable L3 roaming on a DP again.

RUCKUS AP Tunnel Stats

Viewing Statistics for RUCKUS GRE Tunnels

The web interface displays the table and its corresponding graph chart. The two representations are synchronized and controlled by the search criteria. For performance reasons, the total counters per DP or per AP for each bin may be pre-calculated.

To view the RUCKUS GRE Tunnel Statistics:

1. Select **Monitor** > **Report** > **Ruckus AP Tunnel Stats**. The Ruckus GRE tab appears by default.
2. Update the parameters as explained in Table 4.
3. Click:
   - **Load Data**— To view the report in the workspace.
   - **Export CSV**—To open or save the report in CSV file format.

TABLE 4 RUCKUS GRE Report Parameters

Field	Description	Your Action
Time Period	Indicate the time period for which you want to view the report.	Move the slider to set the duration.
Data Plane	Indicates the Data Plane.	Select the Data Plane.
AP MAC or IP Address	Indicates the MAC of the Access Point or IP Address.	Enter the AP MAC or IP address.
Zone Name	Specifies the zone for which you want to view the report.	Enter the zone name or select the zone from the list.

Table 5 contains the report based on the statistics for RUCKUS GRE. Each entry contains the 15 minutes cumulative data.

TABLE 5 RUCKUS GRE report attributes

Attribute	Type	Description
Time	Long	Bin ID, which is stamped at a 15 minute interval. For example, 10:00, 10:15.
TXBytes	Long	Indicates the number of bytes sent.
RXBytes	Long	Indicates the number of bytes received.
TXPkts	Long	Indicates the number of packets sent.
RXPkts	Long	Indicates the number of packets received.
Dropped Packets	Long	Indicates the number of packets dropped.

Viewing Statistics for SoftGRE Tunnels

The web interface displays the table and its corresponding graph chart. The two representations are synchronized and controlled by the search criteria. For performance reasons, the total counters per DP or per AP for each bin may be pre-calculated. The tunneled flows are offloaded by default for 11ax and cypress profiles.

To view the SoftGRE Tunnel statistics:

1. Select **Monitor** > **Report** > **Ruckus AP Tunnel Stats**. The Ruckus GRE tab appears by default.
2. Select **SoftGRE**. Update the parameters as explained in Table 6.
3. Click:
   - **Load Data**— To view the report in the workspace.
   - **Export CSV**—To open or save the report in CSV file format.

TABLE 6 SoftGRE Report Parameters

Field	Description	Your Action
Time Period	Indicate the time period for which you want to view the report.	Move the slider to set the duration.
Zone Name	Specifies the zone for which you want to view the report.	Select the required zone.
Gateway Address	Specifies the gateway address	Enter the gateway address.
AP MAC or IP Address	Indicates the MAC of the Access Point or IP Address.	Enter the AP MAC or IP address.

Table 7 contains the report based on the statistics for SoftGRE. Each entry contains the 15 minutes cumulative data.

TABLE 7 SoftGRE Report Attributes

Attribute	Type	Description
Time	Long	Bin ID, which is stamped at a 15 minute interval. For example, 10:00, 10:15.
TXBytes	Long	Indicates the number of bytes sent.
RXBytes	Long	Indicates the number of bytes received.
TXPkts	Long	Indicates the number of packets sent.
RXPkts	Long	Indicates the number of packets received.
RX Dropped Packets	Long	Indicates the number of packets dropped.
TX Dropped Packets	Long	Indicates the number of packets dropped.
TX Error Packets	Long	Indicates the number of packets with a header error.
RX Error Packets	Long	Indicates the number of packets with a header error.

Viewing Statistics for SoftGRE IPsec Tunnels

The web interface displays the table and its corresponding graph chart. The two representations are synchronized and controlled by the search criteria. For performance reasons, total counters per DP or per AP for each bin may be pre-calculated.

To view the SoftGRE IPsec Tunnel Statistics:

1. elect **Monitor** > **Report** > **Ruckus AP Tunnel Stats**. The Ruckus GRE tab appears by default.
2. Select **SoftGRE + IPsec**. Update the parameters as explained in Table 8.

3. Click:
   - **Load Data**— To view the report in the workspace.
   - **Export CSV**—To open or save the report in CSV file format.

TABLE 8 SoftGRE + IPsec Report Parameters

Field	Description	Your Action
Time Period	Indicate the time period for which you want to view the report.	Move the slider to set the duration.
Zone Name	Specifies the zone for which you want to view the report.	Select the required zone.
Gateway Address	Specifies the gateway address	Enter the gateway address.
AP MAC or IP Address	Indicates the MAC of the Access Point or IP Address.	Enter the AP MAC or IP address.

Table 9 contains the report based on the statistics for access point IPsec. Each entry contains the 15 minutes cumulative data.

TABLE 9 SoftGRE + IPsecReport Attributes

Attribute	Type	Description
Time	Long	Bin ID, which is stamped at a 15 minute interval. For example, 10:00, 10:15.
TXBytes	Long	Indicates the number of bytes sent.
RXBytes	Long	Indicates the number of bytes received.
TXPkts	Long	Indicates the number of packets sent.
RXPkts	Long	Indicates the number of packets received.
TX Dropped Packets	Long	Indicates the number of packets dropped.
RX Dropped Packets	Long	Indicates the number of packets dropped.

Core Network Tunnel Stats

Viewing Statistics for the L2oGRE Core Network Tunnel

An L2oGRE forwarding profile defines the gateway and tunnel configuration for the core network of L2oGRE tunnels.

Complete the following steps to view the statistics for the L2oGRE core network tunnel.

1. From the main menu, go to **Monitor** > **Report** > **Core Network Tunnel Stats**. The **L2oGRE** dialog box is displayed.
2. Configure the following options:
   - **Time Period:** Move the slider to set the duration for which you want to view the report.
   - **Data Plane:** Select the data plane.
   - **Gateway IP Address:** Enter the gateway IP address.
   - **MVNO Name:** Select the mobile network operation name (MVNO).
3. Click **Load Data** to view the report in the workspace or **Export CSV** to open or save the report in CSV file format.

Table 10 contains the report attributes based on the statistics for the L2oGRE core network tunnel.

TABLE 10 L2oGRE Core Network Tunnel Attributes

Attribute	Type	Description
Time	Long	Bin ID, which is stamped at 15-minute intervals; for example, 10:00, 10:15, 10:30.
TX Bytes	Long	Indicates the number of bytes sent.
RX Bytes	Long	Indicates the number of bytes received.
TX Packets	Long	Indicates the number of packets sent.
RX Packets	Long	Indicates the number of packets received.
Dropped Packets	Long	Indicates the number of packets dropped.

Viewing Statistics for the GTP Core Network Tunnel

GPRS Tunneling Protocol (GTP) transmits user data packets and signals between the controller and the gateway GPRS support node (GGSN).You can view historical traffic statistics and trends of the GTP core tunnels.

GTP encapsulates traffic and creates GTP tunnels, which act as virtual data channels for transmission of data between the controller and the GGSN. A GTP tunnel is established between the controller and the GGSN for a data session initiated from the user equipment (UE).

Complete the following steps to view the GTP core network tunnel statistics.

1. From the main menu, go to **Monitor** > **Report** > **RUCKUS AP Tunnel Stats**. The **SoftGRE** dialog box is displayed.
2. Select GTP and configure the following options:
   - **Time Period:** Move the slider to set the duration for which you want to view the report.
   - **Zone Name:** Select the zone name.

- **Gateway IP Address:** Enter the gateway IP address.
- **AP MAC or IP Address:** Enter the AP MAC address or IP address.

3. Click **Load Data** to view the report in the workspace or **Export CSV** to open or save the report in CSV file format.

The below table lists the attributes based on the statistics for the GTP. Each entry contains the cumulative data for the 15-minute interval.

TABLE 11 GTP Report Attributes

Attribute	Type	Description
Time	Long	Bin ID, which is stamped at 15-minute intervals; for example, 10:00, 10:15, 10:30.
TX Bytes	Long	Indicates the number of bytes sent.
RX Bytes	Long	Indicates the number of bytes received.
TX Packets	Long	Indicates the number of packets sent.
RX Packets	Long	Indicates the number of packets received.
Tx Dropped Packets	Long	Indicates the number of packets dropped while sending.
Rx Dropped Packets	Long	Indicates the number of packets dropped while receiving.
Bad GTPU	Long	Indicates a tunneling mechanism that provides a service for carrying user data packets dropped.
RX TEID Invalid	Long	Indicates the number of invalid packets received by Tunnel End Point Identifiers (TEID).
TX TEID Invalid	Long	Indicates the number of invalid packets sent by the Tunnel End Point Identifiers (TEID).
Echo RX	Long	Indicates the echo message received.
Last Echo RX Time	Long	Indicates the time when the last echo message was received.

Working with Tunnels and Ports

Creating a RUCKUS GRE Profile

Generic Routing Encapsulation (GRE) provides a way to encapsulate arbitrary packets (payload packet) inside of a transport protocol, and transmit them from one tunnel endpoint to another. You can configure the RUCKUS GRE tunnel profile of the controller to manage AP traffic.

To create a GRE profile follow the below steps.

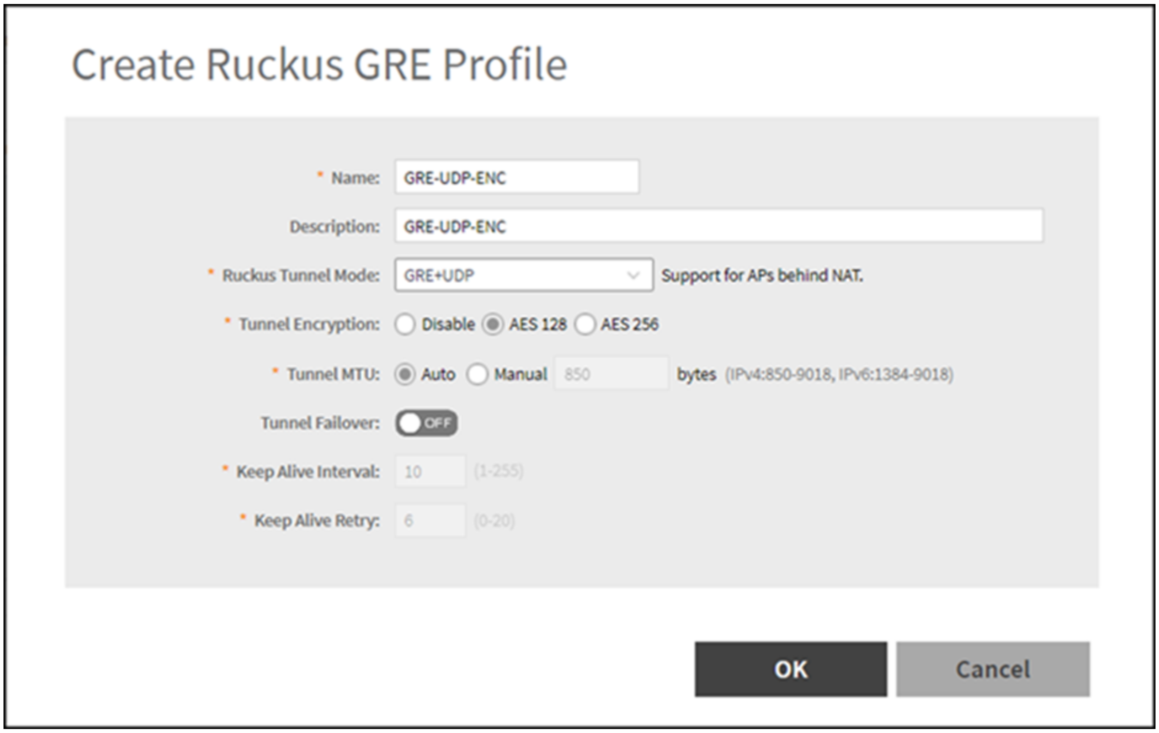
NOTE
You can also edit, clone and delete the profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Ruckus GRE** tab.

1. From the main menu go to **Services** > **Tunnels & Ports**.
2. Select the **Ruckus GRE** tab, and select the system to create the profile.

3. Click **Create**.

   The **Create Ruckus GRE Profile** page is displayed.

   FIGURE 5 Creating a Ruckus GRE Profile



Create Ruckus GRE Profile

* Name: GRE-UDP-ENC

Description: GRE-UDP-ENC

* Ruckus Tunnel Mode: GRE+UDP Support for APs behind NAT.

* Tunnel Encryption: ○ Disable ● AES 128 ○ AES 256

* Tunnel MTU: ● Auto ○ Manual 850 bytes (IPv4:850-9018, IPv6:1384-9018)

Tunnel Failover: OFF

* Keep Alive Interval: 10 (1-255)

* Keep Alive Retry: 6 (0-20)

4. Type a name for the profile in the **Name** box.
5. Type a description for the profile in the **Description** box.
6. Select a protocol to use for tunneling WLAN traffic back to the data plane by choosing one of the following after clicking the drop-down arrow in the **Ruckus Tunnel Mode** box:
   - **GRE + UDP**—Select this option to allow APs behind a NAT server to tunnel WLAN traffic back to the data plane.
   - **GRE**—Select this option to tunnel regular WLAN traffic only.
7. To allow managed APs to decrypt 802.11 packets, and then use an AES encrypted tunnel to send them to the data plane. Select one of the **Tunnel Encryption** options:
   - Click the **Disable** radio button to allow only the management traffic to be encrypted; data traffic is unencrypted. This is the default option.
   - Click the **AES 128** radio button to use an AES 128-byte encryption tunnel.
   - Click the **AES 256** radio button to use an AES 256-byte encryption tunnel.

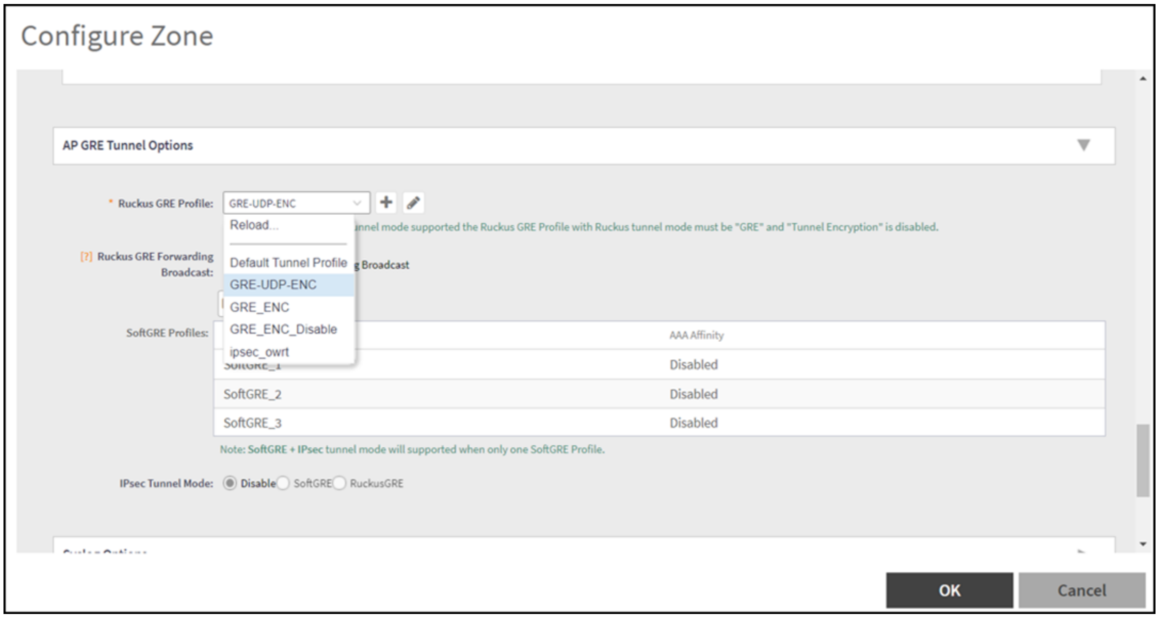
   MTU is the size of the largest protocol data unit that can be passed on the controller network.
8. Set the maximum transmission unit (MTU) for the tunnel using one of the **Tunnel MTU** options:
   - Click the **Auto** radio button. This is the default option.
   - Click the **Manual** radio button and enter the maximum number of bytes. For IPv4 traffic the range is from 850-1500 bytes, for IPv6 traffic the range is from 1384 to 1500 bytes.
9. Set the Tunnel failover option to either OFF or On. By default it is in OFF mode.

10. Enter the **Keep Alive Interval** value. By default the interval value is 10 and the range is between 1-255.
11. Enter the **Keep Alive Retry** value. By default the retry value is 06 and the range is between 0-20.
12. Click **OK**.

Using the created GRE profile in an AP Zone and WLAN

13. From the main menu go to **Network** > **Wireless** > **Access Points** > **Zone** profile to use the created GRE profile.
14. Select the GRE profile from the drop down list. Enable or disable the RUCKUS GRE forwarding broadcast. By default the option is turned OFF. Select the SoftGRE profiles and IPSec Tunnel Mode.

FIGURE 6 Applying the Ruckus GRE Profile



Configure Zone

AP GRE Tunnel Options

* Ruckus GRE Profile: GRE-UDP-ENC

...nnel mode supported the Ruckus GRE Profile with Ruckus tunnel mode must be "GRE" and "Tunnel Encryption" is disabled.

[?] Ruckus GRE Forwarding Broadcast: ...g Broadcast

SoftGRE Profiles:

	AAA Affinity
SoftGRE_1	Disabled
SoftGRE_2	Disabled
SoftGRE_3	Disabled

Note: SoftGRE + IPsec tunnel mode will supported when only one SoftGRE Profile.

IPsec Tunnel Mode: ● Disable ○ SoftGRE ○ RuckusGRE

15. From the main menu go to **Network** > **Wireless LANs** > **WLAN** profile to use the created GRE profile.
16. Another option is navigate to the Zone level configuration and find **AP GRE Tunnel**.
17. Click + to create a new profile.
18. Go to the required WLAN to use the GRE profile.

Creating a Soft GRE Profile

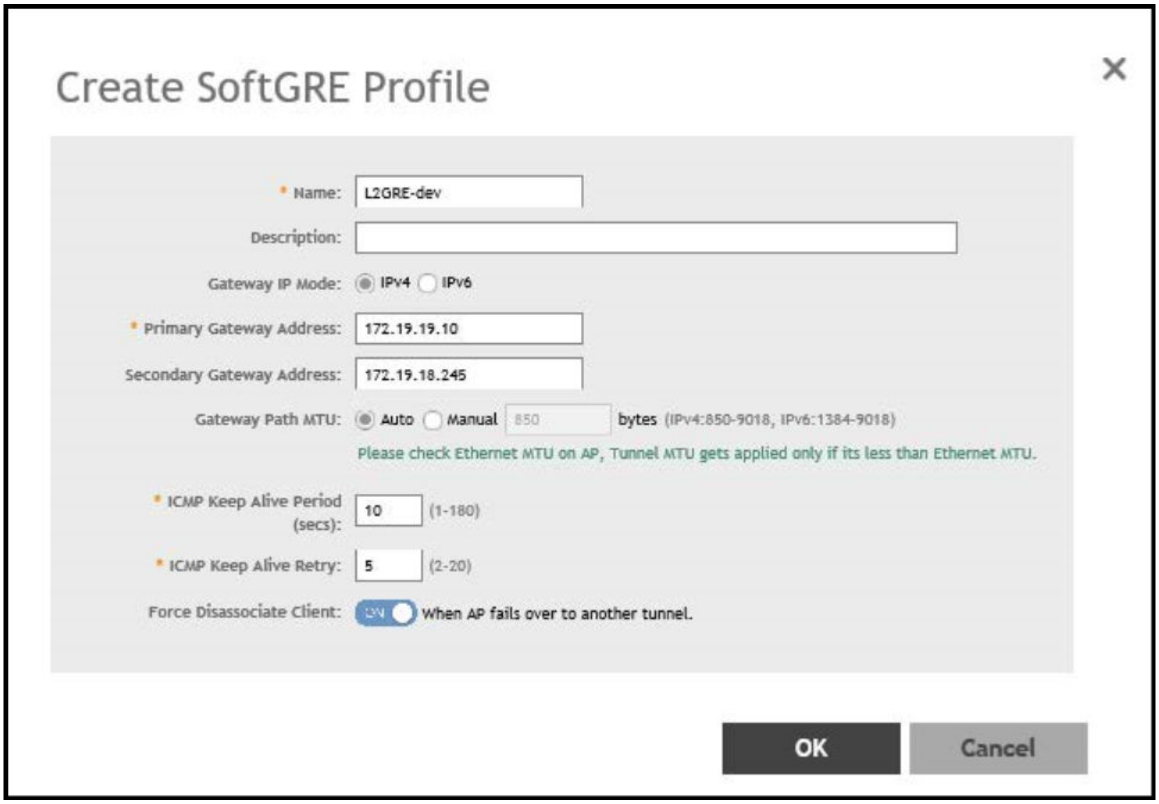
You can configure the Soft GRE tunnel profile of the controller to manage AP traffic.

1. From the main menu go to **Services** > **Tunnels and Ports**.

2. Select **SoftGRE** and click **Create**.

   The **Create SoftGRE Profile** page is displayed.

   FIGURE 7 Creating a SoftGRE Profile



Create SoftGRE Profile

* Name: L2GRE-dev

Description:

Gateway IP Mode: ● IPv4 ○ IPv6

* Primary Gateway Address: 172.19.19.10

Secondary Gateway Address: 172.19.18.245

Gateway Path MTU: ● Auto ○ Manual 850 bytes (IPv4:850-9018, IPv6:1384-9018)

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

* ICMP Keep Alive Period (secs): 10 (1-180)

* ICMP Keep Alive Retry: 5 (2-20)

Force Disassociate Client: ON When AP fails over to another tunnel.

3. Enter profile name and description.
4. Under **Gateway IP Mode**, select **IPv4** or **IPv6** addressing.
5. In the **Primary Gateway Address** field, enter the IP address or fully-qualified domain name (FQDN) of the primary gateway server.
6. In the **Secondary Gateway Address** field, enter the IP address or fully-qualified domain name (FQDN) of the secondary gateway server.

   NOTE
   If the controller is unable to reach the primary gateway server, the controller automatically attempts to reach the secondary gateway address at the IP address specified by you.

7. For **Gateway Path MTU**, set the maximum transmission unit (MTU) for the gateway path.

   Select one of the following options:

   - **Auto**: This is the default option.
   - **Manual**: The transmission range is from 850 through 1500 bytes.

8. In the **ICMP Keep Alive Period** field, enter the time interval in seconds.

   NOTE
   Time interval is the time taken by the APs to send a keep alive message to an active third party WLAN gateway. The range is from 1 through 180 seconds. The default value is 10 seconds.

9. In the **ICMP Keep Alive Retry** field, enter the number of keep alive attempts.

   NOTE
   Keep alive attempts are the number of attempts that the APs wait for a response from the active third party WLAN gateway before failing over to the standby WLAN gateway. The range is from 2 through 10 attempts. The default value is 5 attempts.

10. Under **Force Disassociate Client**, enable **Disassociate client when AP fails over to another tunnel** if you want to disassociate the client when AP fails over to another tunnel.

    NOTE
    You must select this option if you have enabled **AAA Affinity** while configuring the zone.

11. Click **OK**.

You have created the Soft GRE profile.

NOTE
You can also edit, clone, and delete the profile by selecting the options **Configure**, **Clone**, and **Delete** respectively from the **Soft GRE** tab.

Creating an IPsec Profile

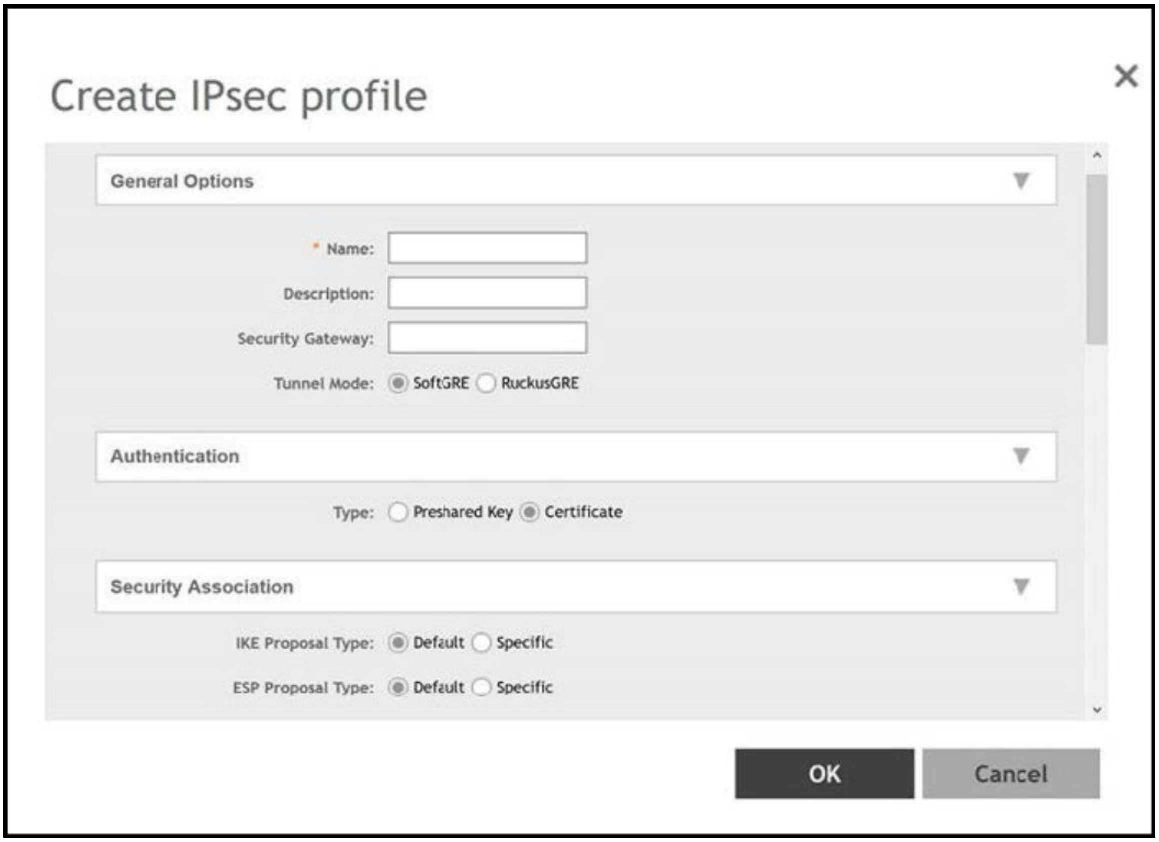
You can create an IPsec profile on 11ac and 11ax APs.

1. From the main menu, navigate to **Services** > **Tunnels & Ports**.
2. Select the **IPsec** tab, and then select the zone for which you want to create the profile.

3. Click **Create**.

   The **Create IPsec Profile** dialog box is displayed.

   FIGURE 8 Creating an IPsec Profile



Create IPsec profile

General Options

* Name:

Description:

Security Gateway:

Tunnel Mode: ● SoftGRE ○ RuckusGRE

Authentication

Type: ○ Preshared Key ● Certificate

Security Association

IKE Proposal Type: ● Default ○ Specific

ESP Proposal Type: ● Default ○ Specific

4. Under **General Options**, configure the following options:
   - **Name:** Enter a name for the profile.
   - **Description:** Enter a description for the profile.
   - **Security Gateway:** Enter the IP address or fully-qualified domain name (FQDN) of the IPsec server. If you use the IP address, the IP address format that you must enter will depend on the IP mode that is configured on the controller.
   - **Tunnel Mode:** Select **SoftGRE** or **RuckusGRE**.

     NOTE
     The **IP Mode** option is displayed only when **SoftGRE** is selected for **Tunnel Mode**.

   - **IP Mode:** Select **IPv4** or **IPv6**.
5. Under **Authentication**, configure the **Type** option.

   Select **Preshared Key** to use PSK for authentication or **Certificate** to use an X.509 certificate on the certificate authority (CA) or registration authority (RA) server. The controller uses the CMPv2 protocol to obtain the signed certificate from the **CA or RA** server. If you select **Preshared Key**, enter the **PSK**. The PSK must be 8 to 128 ASCII characters in length.

6. Under **Security Association**, configure the following options:
   - **IKE Proposal Type**: Select **Default** to use the default Internet Key Exchange (IKE) security association (SA) proposal type or select **Specific** to manually configure the IKE SA proposal. If you select **Specific**, you must configure the following settings:
     - **Encryption Algorithm:** Options include 3DES, AES128, AES192, and **AES256**.
     - **Integrity Algorithm:** Options include **MD5, SHA1, AES-XCBC, SHA256, SHA384**, and **SHA512**.
     - **Pseudo-Random Function:** Options include **Use integrity ALG, PRF-MD5, PRF-SHA1, PRF-AES-XCBC, PRF-AES-CMAC, PRF-SHA256,** and **PRF-SHA384**.
     - **DH Group:** Options for Diffie-Hellman (DH) groups for IKE include **modp768, modp1024, modp1536, modp2048, modp3072, modp4096, modp6144**, and **modp8192**.
   - **ESP Proposal Type:** Select **Default** to use the default Encapsulating Security Payload (ESP) SA proposal type or select **Specific** to manually configure the ESP proposal. If you select **Specific**, you must configure the following settings:
     - **Encryption Algorithm:** Options include **3DES, AES128, AES192, AES256**, and **NONE**.
     - **Integrity Algorithm:** Options include **MD5, SHA1, AES-XCBC, SHA256, SHA384**, and **SHA512**.
     - **DH Group:** Options for Diffie-Hellman (DH) groups for ESP include **None, modp768, modp1024, modp1536, modp2048, modp3072, modp4096, modp6144**, and **modp8192**.

       NOTE
       If you selected **RuckusGRE** for **Tunnel Mode**, the following IKE and ESP proposals are supported:

       - AES128-SHA1-MODP2048
       - AES256-SHA384-ECP384

         NOTE
         IKE encryption proposals should be greater than or equal to ESP encryption proposals. RuckusGRE over IPsec supports IKEv2 authentication by X.509 certificate only.

7. Under **Rekey Options**, configure the following options:
   - **Internet Key Exchange:** Select a time unit (day, hour, or minute) from the list, and enter a number to set the time interval at which the IKE key renews. Select the **Disable** check box to disable the IKE rekey.
   - **Encapsulating Security Payload:** Select a time unit (day, hour, or minute) from the list, and enter a number to set the time interval at which the ESP key renews. Select the **Disable** check box to disable the ESP rekey.
8. Under **Certificate Management Protocol**, configure the following options:
   - **DHCP Option 43 Sub Code for CA/RA Address:** Set the DHCP Option 43 subcode that will be used to discover the address of the CA or RA server on the network. The default subcode is 8.
   - **Server Path:** Enter the path to the X.509 certificate on the CA or RA server.
   - **DHCP Option 43 Sub Code for Subject Name of CA/RA**: Set the DHCP Option 43 subcode that will be used to discover the subject name of the CA or RA server on the network. The default subcode is 5.
   - **Subject Name of CA/RA:** Enter an ASCII string that represents the subject name of the CA or RA server.

9. Under **Advanced Options**, configure the following options:
   - **DHCP Option 43 Sub Code for Security Gateway**: Set the DHCP Option 43 subcode that will be used to discover the address of the security gateway on the network. The default subcode is 7.
   - **Retry Limit:** Set the number of times that the controller will attempt to discover the address of the security gateway. The default retry count is 5. Accepted values are 0 (disable) through 16.
   - **Replay Window:** Set the ESP replay window (in packets). The default size is 32 packets. Accepted values are 0 (disable) through 32 packets.
   - **IP Compression:** Click **Enable** to enable IP Payload Compression Protocol (IPComp) compression before encryption. The default value is Disable.
   - **Force NAT-T:** Click Enable to enforce UDP encapsulation of ESP packets. The default value is Disable.
   - **Dead Peer Detection:** By default, the IKE protocol runs a health check with the remote peer to ensure that it is alive. Click **Disable** to disable the health check.
   - **NAT-T Keep Alive Interval:** Enter a value (in seconds) to set the keepalive interval for NAT traversal. The default keep alive interval is 20 seconds. Accepted values are 1 to 65536. To disable the keep alive interval, click Disable.
   - **FailOver Options:** To configure the failover settings when APs are unable to connect, configure the following options:
     - **Retry Period:** Set the number of days (minimum 3 days) during which APs will keep attempting to connect. Select the **Forever** check box to keep trying indefinitely.
     - **Retry Interval:** Set the interval (in minutes) between each retry attempt. The default retry interval is 1 minute. Accepted values are from 1 through 30 minutes.
     - **Retry Mode:** Click **Revertive** if you want APs to fall back to the specified primary security gateway. Click **Non-revertive** if you want APs to maintain connectivity with the security gateway to which they are currently connected.
10. Click **OK**.

    NOTE
    You can also edit, clone, and delete the profile by selecting the Configure, Clone, and Delete options respectively from the IPsec tab.

Creating a Tunnel DiffServ Profile

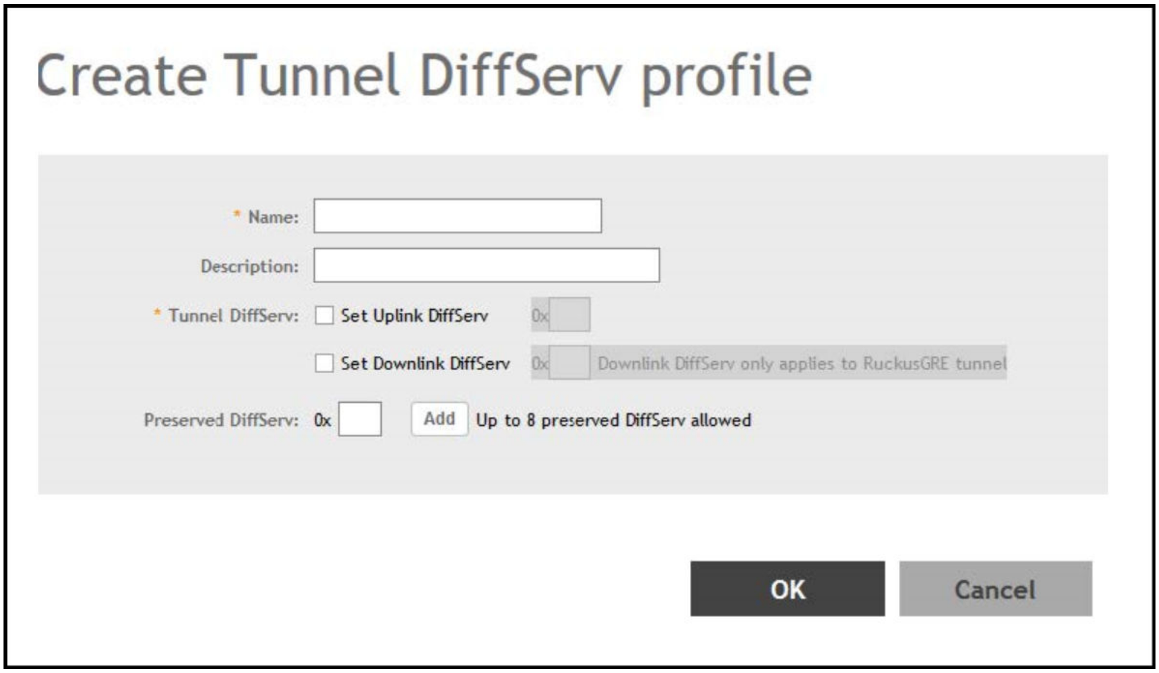
If you want to configure the type of service (ToS) bit settings for the access-side traffic from RUCKUS APs, complete the following steps to create a Differentiated Services (DiffServ) profile. This profile can only be applied to RuckusGRE and SoftGRE traffic.

1. From the main menu, go to **Services** > **Tunnels and Ports**.
2. Select the **DiffServ** tab, and then select the zone for which you want to create the profile.

3. Click **Create**.

   The **Create Tunnel DiffServ Profile** dialog box is displayed.

   FIGURE 9 Creating a Tunnel DiffServ Profile



Downlink DiffServ only applies to RuckusGRE tunnel

Up to 8 preserved DiffServ allowed

4. Configure the following options:
   - **Name:** Enter a name for the DiffServ profile that you are creating.
   - **Description:** Enter a brief description for the DiffServ profile.
   - **Tunnel DiffServ:** Configure the following options.
     - **Set Uplink DiffServ:** Select the check box if you want to set the **Differentiated Services** field for uplink user traffic from RUCKUS APs towards either the controller or a third-party gateway using SoftGRE, and enter the desired value to be set by the RUCKUS AP.
     - **Set Downlink DiffServ:** Select the check box if you want to set the **Differentiated Services** field for downlink user traffic from the controller towards the AP, and enter the desired value to be set by the RUCKUS AP.
   - **Preserved DiffServ:** Configure up to eight entries in the preserved DiffServ list. The Preserved DiffServ list allows the preservation of values that have been already marked in incoming packets either in uplink or downlink traffic.
5. Click **OK**.

   NOTE
   You can also edit, clone, and delete the profile by selecting the **Configure**, **Clone**, and **Delete** options respectively from the **DiffServ** tab.

Applying Communications Assistance for Law Enforcement Act

The Communications Assistance for Law Enforcement Act (CALEA) is a law passed by the United States. This is to enhance the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment, to modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities.

> **NOTE**
> CALEA applies only to the virtual SmartZone (vSZ-H) platform.

1. From the main menu, go to **Services** > **Tunnels and Ports**.
2. Select the **CALEA** tab.
3. For **Server IP**, enter the CALEA server IP address, and click **OK**.
4. Click **Create**.

   The **Create UE MAC** dialog box is displayed.

   > **NOTE**
   > Only the health of top 100 clients are displayed.

5. For **MAC Address**, enter the MAC address of the client or user equipment for which CALEA mirroring is required. The MAC address is sent by the controller to the vSZ-D.
6. Click **OK**.

Enabling Tunnel Encryption

You can use tunnel encryption to encrypt data for a private network through a public network. Tunnel encryption is available in virtual controller vSZ-H and vSZ-E platforms.

1. From the main menu, go to **Services** > **Tunnels and Ports**.
2. Select the **Tunnel Encryption(DP)** tab.

   The **Tunnel Encryption(DP)** tab is displayed.
3. Set **Enable Tunnel Encryption** to **ON**. By default the encryption is turned OFF.
4. Click **OK**.

Forwarding Multicast Packets

In multicast forwarding, a group of hosts is typically grouped under a multicast IP address. Data can then be transmitted from the source to the IP address, which in turn transmits data to the various hosts assigned to the multicast IP address. This is point-to-multipoint data transmission. Forwarding multicast packets is only available for the SZ100.

1. From the main menu, navigate to **Services** > **Tunnels and Ports**.
2. Select the **Multicast Forwarding** tab.

   The **Multicast Forwarding** tab is displayed.
3. Under **Global Setting**, set **Enable forwarding multicast packet on tunnel mode** to **ON**. By default the setting is set to OFF.

4. Click **OK**.

Split Tunnel Profile

A Split Tunnel Profile can be created to manage corporate and local traffic by sending only corporate traffic to the controller. A split tunnel ensures that local traffic does not incur the overhead of the round trip to the controller, which decreases traffic on the WAN link and minimizes latency for local application traffic. Using a split tunnel, a remote user is associated with a single SSID (rather than multiple SSIDs) to access corporate resources, such as a mail server, and local resources (for example, a local printer).

Split Tunnel Profile Limitations

Before enabling the Split Tunnel Profile, consider the following limitations:

- The Split Tunnel Profile does not support a zone where Mesh-enabled APs are present.
- The Split Tunnel Profile and Express Wi-Fi are not supported together on the same WLAN.
- For the Split Tunnel Profile and Express Wi-Fi to work properly, the configured IP rules for a split tunnel and a walled garden must be different.
- The Split Tunnel Profile does not support DHCP server or NAT router.
- The Split Tunnel Profile does not support wired clients.
- The limitations applicable to DHCP or NAT also apply to the Split Tunnel Profile.
- WISPr-related (web-authentication) WLANs are not supported on a split tunnel WLAN.
- ICMP is not supported towards a line buildout (LBO) split path where Source Network Address Translation (SNAT) occurs.
- IPv6 addresses are not supported in the Split Tunnel Profile.
- Multicast discovery of Bonjour devices will not occur over the LBO.
- As the data traffic is established from the server side, TFTP is not supported.
- As the server rejects the data connection that does not have the NAT IP address sent by the client, the FTP active mode is not supported with a split tunnel.

Creating a Split Tunnel Profile

A Split Tunnel profile is created to manage corporate and local traffic by sending only corporate traffic to the controller.

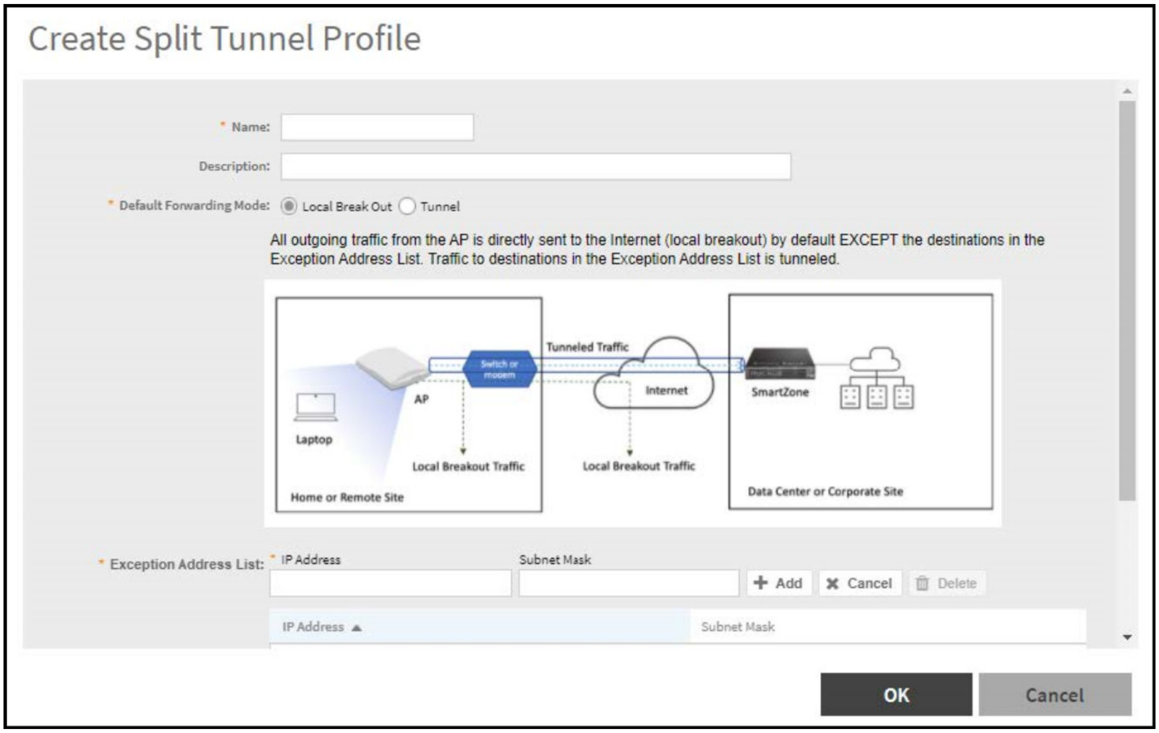
Complete the following steps to configure a split tunnel profile.

1. From the main menu go to **Services** > **Tunnels and Ports** > **Split Tunnel**.

2. Select the zone for which you want to create the profile and click **Create**.

   The **Create Split Tunnel Profile** window is displayed.

   FIGURE 10 Creating a Split Tunnel Profile



Create Split Tunnel Profile

* Name:

Description:

* Default Forwarding Mode: ● Local Break Out ○ Tunnel

All outgoing traffic from the AP is directly sent to the Internet (local breakout) by default EXCEPT the destinations in the Exception Address List. Traffic to destinations in the Exception Address List is tunneled.

* Exception Address List: * IP Address Subnet Mask

IP Address ▲	Subnet Mask

3. Enter the split tunnel profile information:

   NOTE
   RuckusGRE or SoftGRE must be enabled on the WLAN before mapping it to a Split Tunnel Profile.

   a. In the **Name** field, type a name for the split tunnel profile.

   b. In the **Description** field, type a short description for the split tunnel profile.

   c. In **Default Forwarding Mode** field, select one of the following option:

      - **Local Break Out**: All outgoing traffic from the AP is by default sent to the Internet (local breakout) except for the destinations in the Exception Address List. Traffic to destinations in the Exception Address List is tunneled.
      - **Tunnel**: All outgoing traffic from the AP is tunneled except for the destinations in the Exception Address List. Traffic to destinations in the Exception Address List is directly sent to the Internet (local breakout).

   d. In the **IP Address** field, enter the destination IP address.

   e. In the **Subnet Mask** field, enter the destination IP subnet mask.

   f. Click **Add** to add the destination IP details.

   g. Click **OK**.

   NOTE
   You can also edit, clone or delete the profile by selecting the options **Configure**, **Clone**, and **Delete** respectively from the **Split Tunnel** tab.

Managing Core Network Tunnels

Tunneling protocols allows users to access or provide a network service that the network does not support or provide directly.

Creating Bridge Forwarding Profiles

An Bridge forwarding profile defines the DHCP configuration for the core network.

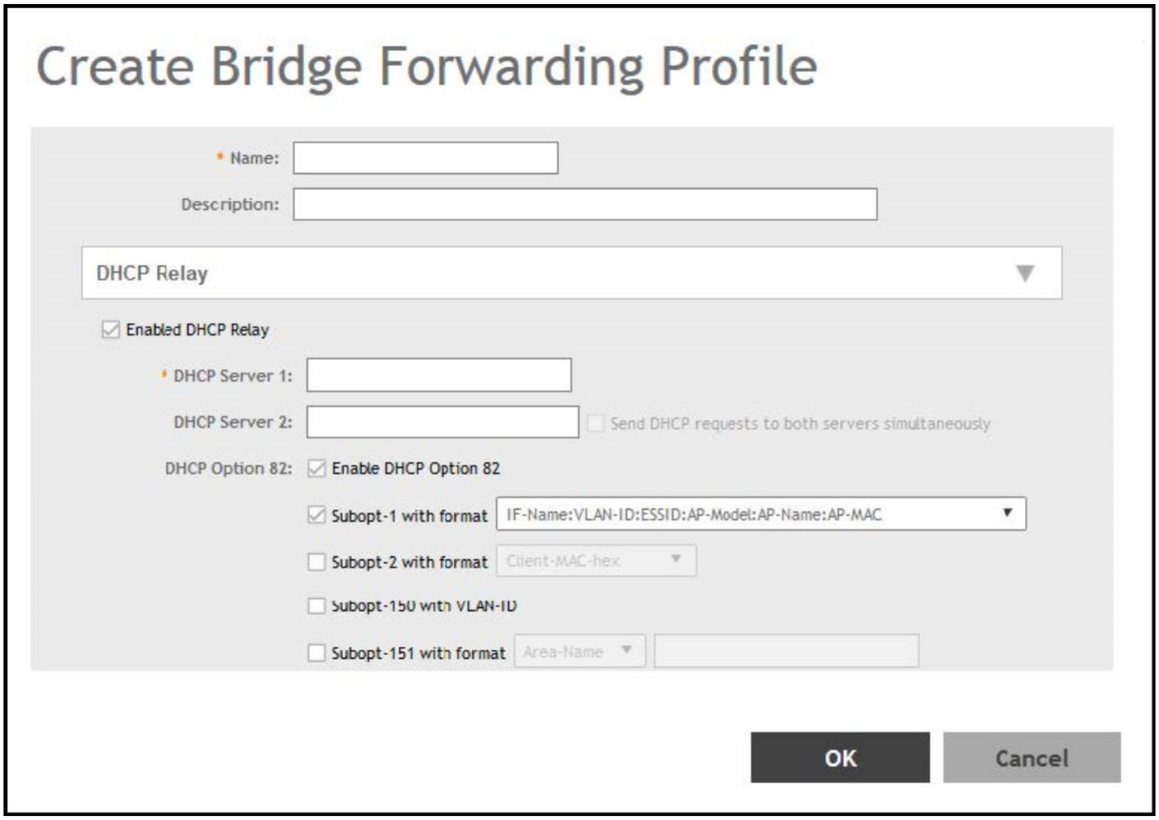
Follow the below steps to create a Bridge Forwarding Profile.

NOTE
This feature is applicable only for SZ300 and vSZ-H platforms.

1. From the main menu go to **Services** > **Tunnels and Ports** > **Core Network Tunnel** > **Bridge**.
2. Select the zone for which you want to create the profile.
3. Click **Create**.

   The **Create Bridge Forwarding Profile** page is displayed.

FIGURE 11 Creating a Bridge Forwarding Profile



Create Bridge Forwarding Profile

* Name:

Description:

DHCP Relay ▼

☑ Enabled DHCP Relay

* DHCP Server 1:

DHCP Server 2: □ Send DHCP requests to both servers simultaneously

DHCP Option 82: ☑ Enable DHCP Option 82

☑ Subopt-1 with format IF-Name:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC ▼

□ Subopt-2 with format Client-MAC-hex ▼

□ Subopt-150 with VLAN-ID

□ Subopt-151 with format Area-Name ▼

4. Configure the following:
   a. Name: Type a name for the profile that you are creating.
   b. Description: Type a brief description for the profile.
   c. DHCP Relay: Select the **Enable DHCP Relay**check-box and configure the DHCP server IP address and DHCP option 82 settings.
      1. DHCP Server 1: Type the IPv4 address of the DHCP server that will allocate IP addresses to DHCP clients.
      2. DHCP Server 2: If a secondary DHCP server exists on the network, type the IPv4 address of the secondary server.
      3. DHCP Option 82: Select this check box if you want the DHCP relay agent (in this case, the controller) to insert specific identification information into requests that are forwarded to the DHCP server. If you enabled DHCP Option 82, you can configure the following Option 82 sub-options by selecting the corresponding check boxes:
         - Subopt-1 with format: You can customize sub-option 1 (Circuit ID) to send only the AP's MAC address in hexadecimal format or the MAC address and ESSID. The default format is: IFName:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC.
         - Subopt 2 with format: You can customize sub-option 2 (Remote ID), which sends the client's MAC address by default, to send the AP's MAC address, or the client MAC plus ESSID or AP MAC plus ESSID.
         - Subopt-150 with VLAN ID: This sub-option encapsulates the VLAN ID.
         - Subopt-151 with format: This sub-option can encapsulate either the ESSID or a configurable Area Name.
   d. Click **OK**.

You have created the Bridge forwarding profile.

> **NOTE**
> You can also edit and delete the profile by selecting the options **Configure** and **Delete** respectively, from the **Bridge** tab.

Creating L2oGRE Forwarding Profiles

An L2oGRE forwarding profile defines the gateway and tunnel configuration for the core network of L2oGRE tunnels. This feature is applicable only for SZ300 and vSZ-H platforms.

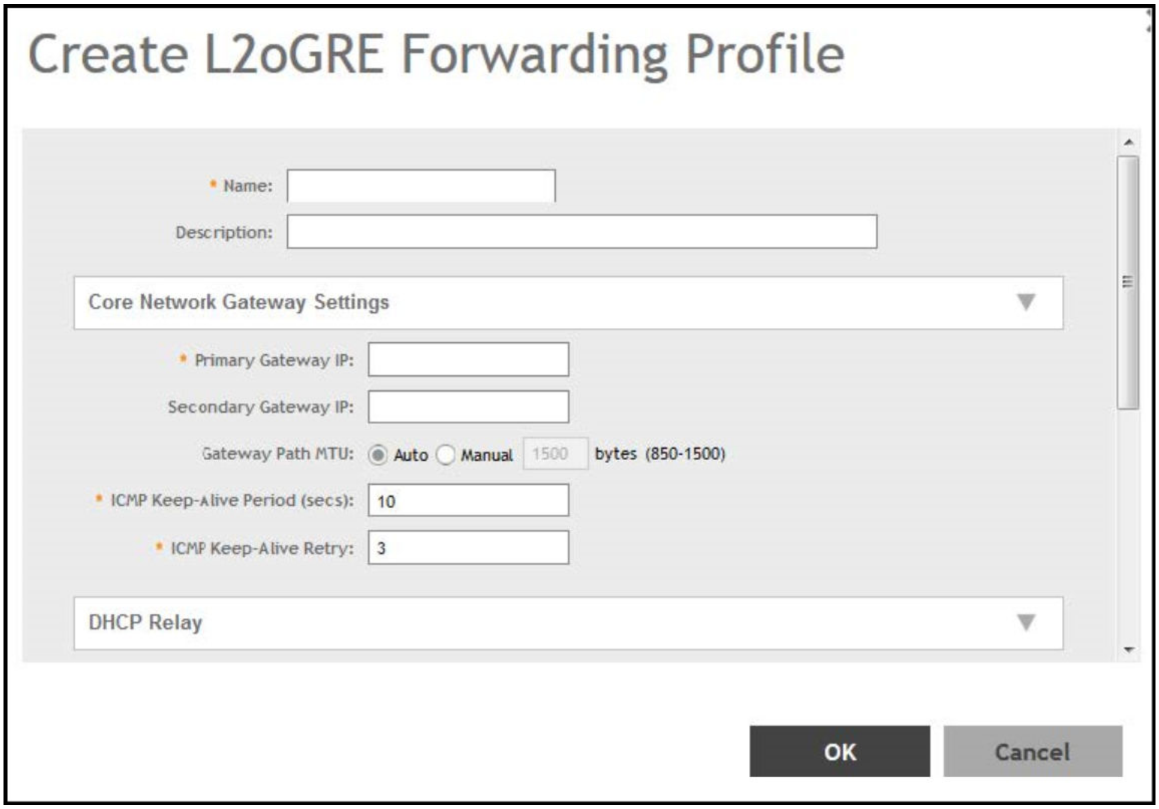
Follow the below steps to create a L2oGRE Forwarding Profile.

1. From the main menu go to **Services** > **Core Network Tunnel** > **L2oGRE**.
2. Select the zone for which you want to create the profile.

3. Click **Create**.

   The **Create L2oGRE Forwarding Profile** page is displayed.

FIGURE 12 Creating a L2oGRE Forwarding Profile



Create L2oGRE Forwarding Profile

* Name:

Description:

Core Network Gateway Settings

* Primary Gateway IP:

Secondary Gateway IP:

Gateway Path MTU: ● Auto ○ Manual 1500 bytes (850-1500)

* ICMP Keep-Alive Period (secs): 10

* ICMP Keep-Alive Retry: 3

DHCP Relay

4. Configure the following:

   a. Name: Type a name for the profile that you are creating.

   b. Description: Type a brief description for the profile.

   c. Core Network Gateway Settings

      1. Primary Gateway IP: Type the IP address of the primary gateway for the L2oGRE tunnel.

      2. Secondary Gateway IP: Type the IP address of the secondary gateway for the L2oGRE tunnel. If the primary gateway is unreachable, this gateway will be used for the L2oGRE tunnel.

      3. Gateway Path MTU: Set it the MTU manually or use Auto (default). MTU is the size of the largest protocol data unit (in bytes) that can be passed on the controller network.

      4. ICMP Keep-Alive Period (secs): Set the time in seconds between sending retry messages to the keep alive IP address. Enter an integer between 2 and 255. The default is 10 seconds.

      5. ICMP Keep-Alive Retry: Set the retry period to send messages to the keep alive IP address. The default value is 3 retries.

   d. DHCP Relay: Select the **Enable DHCP Relay**check-box and configure the DHCP server IP address and DHCP option 82 settings.

      1. DHCP Server 1: Type the IPv4 address of the DHCP server that will allocate IP addresses to DHCP clients.

      2. DHCP Server 2: If a secondary DHCP server exists on the network, type the IPv4 address of the secondary server.

      3. DHCP Option 82: Select this check box if you want the DHCP relay agent (in this case, the controller) to insert specific identification information into requests that are forwarded to the DHCP server. If you enabled DHCP Option 82, you can configure the following Option 82 sub-options by selecting the corresponding check boxes:

         - Subopt-1 with format: You can customize sub-option 1 (Circuit ID) to send only the AP's MAC address in hexadecimal format or the MAC address and ESSID. The default format is: IFName:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC.

         - Subopt 2 with format: You can customize sub-option 2 (Remote ID), which sends the client's MAC address by default, to send the AP's MAC address, or the client MAC plus ESSID or AP MAC plus ESSID.

         - Subopt-150 with VLAN ID: This sub-option encapsulates the VLAN ID.

         - Subopt-151 with format: This sub-option can encapsulate either the ESSID or a configurable Area Name.

   e. Click **OK**.

You have created the L2oGRE forwarding profile.

> **NOTE**
> You can also edit and delete the profile by selecting the options **Configure** and **Delete** respectively, from the **L2oGRE** tab.

SoftGRE Support

This section describes the SoftGRE support that the controller provides and the supported deployment topology.

Overview of SoftGRE Support

There are numerous equipment vendors serving the service provider market today. Among these vendors, the more prominent ones include Alcatel-Lucent (ALU), Ericsson, NSN, Huawei and Cisco. Most of these vendors support different tunneling and mobility management protocols at their packet gateways.

Since most (if not all) of these equipment vendors do not develop access points themselves, they are publishing SoftGRE specifications to enable access point vendors (such as RUCKUS) to support SoftGRE on their devices.

Configuring And Monitoring AP Zones

If no tunneled WLANs exist in the zone, you can change the tunnel type from SoftGRE to GRE or GRE + UDP.

MVNO accounts are currently unsupported by SoftGRE tunnels. If you create an MVNO account and assign an AP zone that is using a SoftGRE tunnel, an error message appears.

1. Follow the steps as described in *Creating an AP Zone* in *RUCKUS SmartZone Network Administration Guide* to change the tunnel type from SoftGRE.
2. Scroll down to the **AP GRE Tunnel Options** section and select the **Ruckus GRE Profile** or click **Add** to create a new profile.
3. From the Create Ruckus GRE Profile window, select the **Ruckus Tunnel Mode** to change from SoftGRE.

   If you attempt to change the tunnel type when a tunneled WLAN exists within the zone, the following error message appears:

   ```
   Unable to update the configuration of the AP zone. Reason: It is disallowed to change the
   tunnel type, because it
   has tunneled WLAN.
   ```
4. Click **OK**.

   The zone configuration information is displayed.

SoftGRE SNMP MIBs

The following table lists the SoftGRE OIDs.

TABLE 12 OIDs related to SoftGRE

Parent Node	Node Name	OID
ruckusWLANAPInfo	ruckusSCGWLANAPMacAddr	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.1
	ruckusSCGWLANAPSoftGREServer	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.2
	ruckusSCGWLANAPSoftGREGWAddr	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.3
	ruckusSCGWLANAPSoftGREActive	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.4
	ruckusSCGWLANAPSoftGRETxPkts	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.5
	ruckusSCGWLANAPSoftGRETxBytes	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.6
	ruckusSCGWLANAPSoftGRERxPkts	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.7
	ruckusSCGWLANAPSoftGRERxBytes	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.8
	ruckusSCGWLANAPSoftGRETxPktsErr	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.9
	ruckusSCGWLANAPSoftGRERxPktsErr	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.10
	ruckusSCGWLANAPSoftGRETxPktsDropped	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.11
	ruckusSCGWLANAPSoftGRERxPktsDropped	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.12
	ruckusSCGWLANAPSoftGRETxPktsFrag	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.13
	ruckusSCGWLANAPSoftGREICMPTotal	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.14
	ruckusSCGWLANAPSoftGREICMPNoReply	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.15
	ruckusSCGWLANAPSoftGREDisconnect	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.16

SoftGRE Events and Alarms

If there is no downstream traffic in the tunnel, APs that belong to the zone configured for SoftGRE send out-of-band ICMP keep-alive messages (interval is configurable) to the active third party WLAN gateway. If an AP does not receive a response from the active WLAN gateway, it triggers an alarm and it automatically creates a SoftGRE tunnel to the standby WLAN gateway.

If the AP does not receive a response from the standby WLAN gateway either, the AP disconnects all tunneled WLAN services. It continues to send keep-alive messages to both the active WLAN gateway (primary GRE remote peer) and standby WLAN gateway (secondary GRE remote peer). If it receives a response from either WLAN gateway, the AP restores all tunneled WLAN services automatically.

There are four types of events that APs send to the controller:

- Failover from primary GRE remote peer to secondary GRE remote peer
- Failover from secondary GRE remote peer to primary GRE remote peer.
- Tunnel disconnected because both primary and secondary GRE remote peers are unreachable
- Tunnel restored because either primary or secondary GRE remote peer is reachable

For the list of alarms and events related to SoftGRE that APs generate, refer to SoftGRE Events on page 47 and SoftGRE Alarms on page 46.

SoftGRE Alarms

SoftGRE related alarms that APs send to the controller.

Following are the SoftGRE related alarms:

apSoftGRETunnelFailoverPtoS AP[{apname@apMac}] fails over from primaryGRE[{address}] to secondaryGRE[{address}]
Code: 611
Default to Trap: true
Severity: major
Attributes:

- "apMac"="xx:xx:xx:xx:xx:xx"
- "primaryGRE"="xxx.xxx.xxx.xxx
- "secondaryGRE"="xxx.xxx.xxx.xxx

apSoftGRETunnelFailoverStoP AP[{apname@apMac}] fails over from secondaryGRE[{address }] to primaryGRE[{address}]
Code: 612
Default to Trap: true
Severity: major
Attributes:

- "apMac"="xx:xx:xx:xx:xx:xx
- "secondaryGRE"="xxx.xxx.xxx.xxx"
- "primaryGRE"="xxx,xxx.xxx.xxx"

apSoftGREGatewayReachable AP [{apname@apMac}] is able to reach [{softgreGW}] [{softgreGWAddress}] successfully
Code: 613
Default to Trap: true
Severity: informational
Attributes:

- "apMac"="xx:xx:xx:xx:xx:xx"
- "softgreGW"="primaryGRE"
- "softgreGWAddress"="xxx.xxx.xxx.xxx"

apSoftGREGatewayNotReachable AP [{apname@apMac }] is unable to reach the following gateways: [{gateway list}]
Code: 614
Default to Trap: true
Severity: major
Attributes:

- “apMac"="xx:xx:xx:xx:xx:xx"

- "softGREGatewayList"="xxx.xxx.xxx.xxx, yyy,yyy.yyy.yyy"

SoftGRE Events

SoftGRE related events that APs send to the controller.

Following are the events related to SoftGRE that AP generates.

apSoftGRETunnelFailoverPtoS
AP [{apname@apMac}] fails over from primaryGRE [{address}] to secondaryGRE [{address}].
Code: 611
Severity:
Attributes:

- "apMac"="xx:xx:xx:xx:xx:xx"
- "primaryGRE"="xxx.xxx.xxx.xxx"
- "secondaryGRE"="xxx.xxx.xxx.xxx"

apSoftGRETunnelFailoverStoP
AP [{apname@apMac}] fails over from secondaryGRE [{address }] to primaryGRE [{address}].
Code: 612
Severity: Warning
Attributes:

- "apMac"="xx:xx:xx:xx:xx:xx"
- "secondaryGRE"="xxx.xxx.xxx.xxx"
- "primaryGRE"="xxx,xxx.xxx.xxx"

apSoftGREGatewayReachable
AP [{apname@apMac}] is able to reach [{softgreGW}] [{softgreGWAddress}] successfully.
Code: 613
Severity: Informational
Attributes:

- "apMac"="xx:xx:xx:xx:xx:xx"
- "softgreGW"="primaryGRE"
- "softgreGWAddress" = "xxx.xxx.xxx.xxx"

apSoftGREGatewayNotReachable
AP [{apname@apMac}] is able to reach [{softgreGW}] [{softgreGWAddress}] successfully.
Code: 614
Severity: Critical
Attributes:

- apMac"="xx:xx:xx:xx:xx:xx"
- "softGREGatewayList"="xxx.xxx.xxx.xxx, yyy,yyy.yyy.yyy"

Multi Tunnel Support

Multi-Tunnel Support for Access Points

In prior RUCKUS solutions, APs could only support a single tunnel to a data plane, as well as a local break out. In this release, we're adding support for RUCKUS APs to provide multiple simultaneous tunnels to different data planes.

For 5.0, the AP will support a single RUCKUS GRE tunnel (with our without encryption) while supporting up to three SoftGRE (without encryption) tunnels, in addition to local breakout option. The tunneling will be based on SSID configurations on the AP.

This feature is designed to help in common MSP (Managed Service Provider) use cases, where each of the MSP's customer will have the possibility to get its own tunnel directly to the data center.

Before configuring multiple tunnels, consider the following configuration prerequisites:

- Ensure that there is a reachable SoftGRE gateway and also verify that there is network connectivity.
- Ensure that the zone is configured with correct SoftGRE gateway information.
- Verify that the SSID to SoftGRE tunnel mapping is correct.
- Verify the SoftGRE tunnel configuration and run time status using the command **get softgre***tunnel-index*. The tunnel index can be 1, 2, or 3.

Configuring Multiple Tunnels for Zone Templates

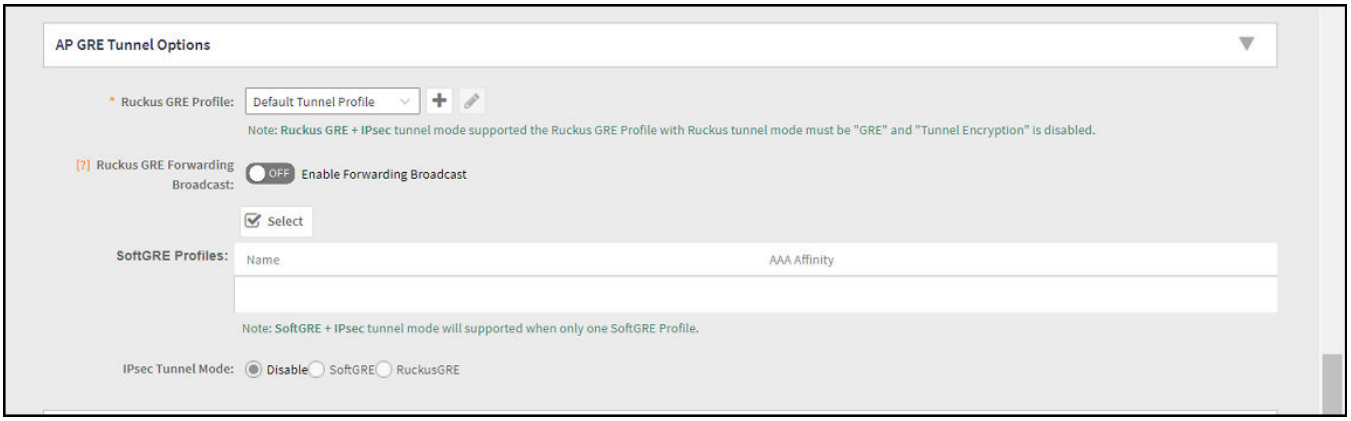
Multiple tunnels can be configured for a zone template.

Perform the following steps to select a tunnel profile for a zone template.

1. From the main menu, go to **Administration** > **System** > **Template** > **Zone Templates**.
2. Click **Create**.

   The **Create Zone Template** form appears.

   FIGURE 13 Configuring a RUCKUS GRE Profile



AP GRE Tunnel Options ▼

* Ruckus GRE Profile: Default Tunnel Profile

Note: Ruckus GRE + IPsec tunnel mode supported the Ruckus GRE Profile with Ruckus tunnel mode must be "GRE" and "Tunnel Encryption" is disabled.

[?] Ruckus GRE Forwarding Broadcast: OFF Enable Forwarding Broadcast

☑ Select

SoftGRE Profiles:

Name	AAA Affinity

Note: SoftGRE + IPsec tunnel mode will supported when only one SoftGRE Profile.

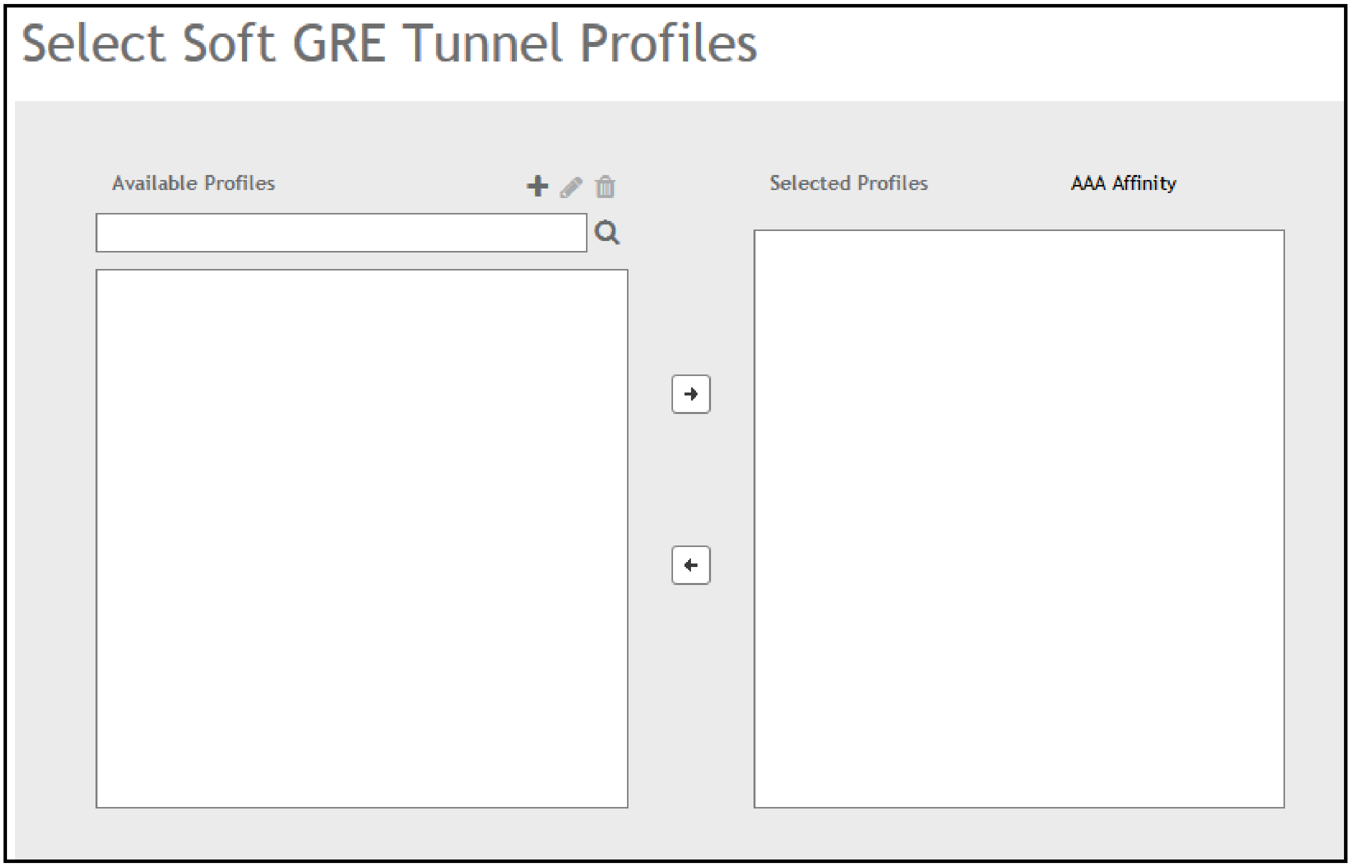
IPsec Tunnel Mode: ● Disable ○ SoftGRE ○ RuckusGRE

3. Navigate to the **AP GRE Tunnel Options** section.
4. For the **Ruckus GRE Profile** select a profile from the drop-down menu.

   Click the **+** icon to create a new Ruckus GRE profile.
5. Click the **Select** checkbox above the SoftGRE Profiles box.

   A form appears from which you can select the SoftGRE profiles that you want to apply to the zone. The profiles you can select are displayed under **Available Profiles**. Select the profile and click the **->** icon to choose it. The profile is now listed under the **Selected Profiles** area.

   FIGURE 14 SoftGRE Profiles Form

   You can also click the **+** icon to create a new SoftGRE profile.

   If you wish to deselect a profile, select it and click the **<-** icon. The profile will be moved back to the **Available Profiles** area and will not be applied to that zone.
6. Click **OK**.

   Your multiple tunnel configuration for the zone template is saved.

Configuring Multiple Tunnels for Zone

Multiple tunnels can be configured for a zone.

To configure the tunnel types for an AP zone, perform the following steps.

1. From the main menu, go to **Network** > **Wireless**, select **Access Points**, the **Access Point** page is displayed, select the AP from the list.
2. From the System tree, select the location where you want to create the zone. For example, System or Domain. Click **+** icon.

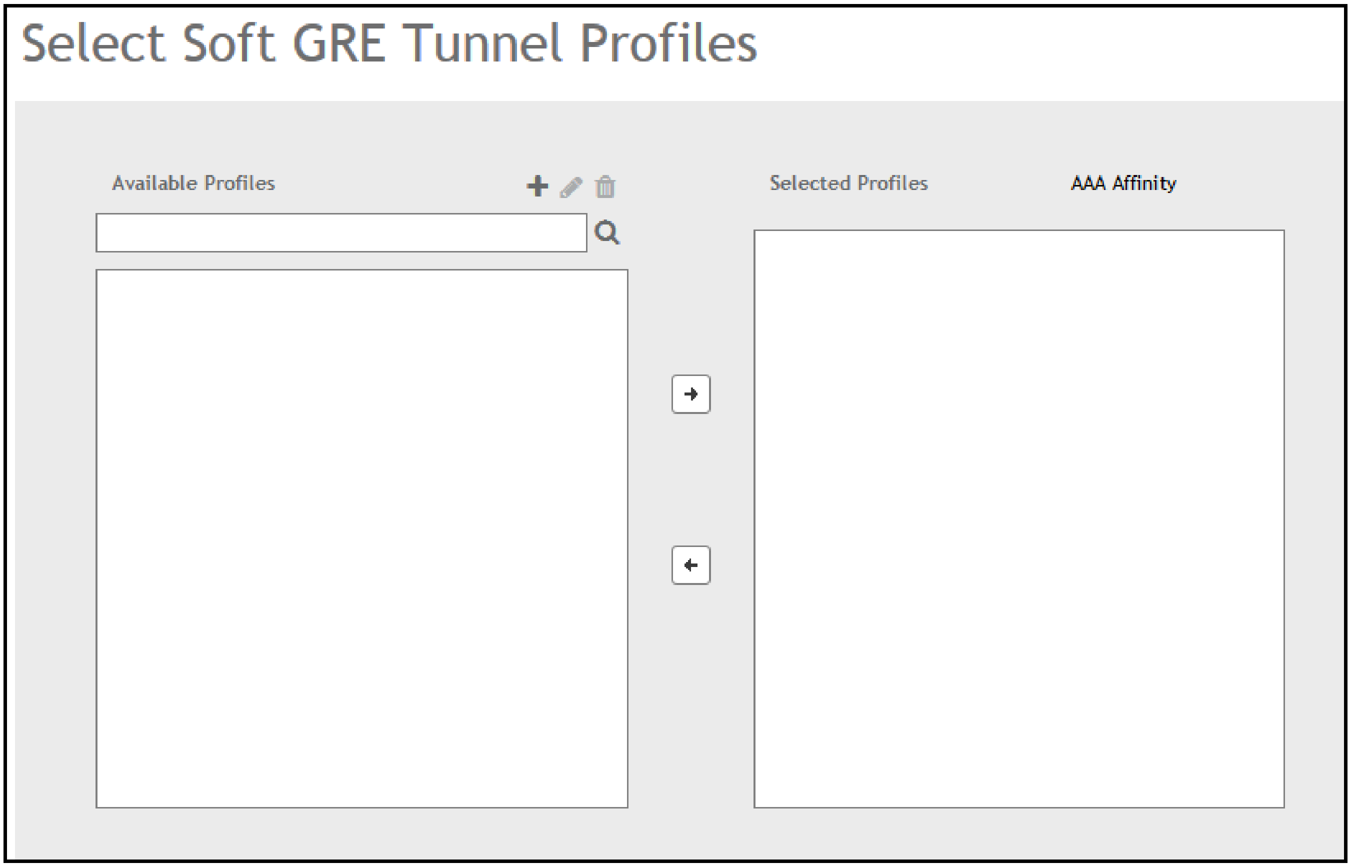
   The **Create Group** page appears.
3. Under **Type**, select **Zone**.
4. Navigate to the **AP GRE Tunnel** section.
5. For the **Ruckus GRE Profile** select a profile from the drop-down menu.

   Click the **+** icon to create a new Ruckus GRE profile.

6. Click the **Select** checkbox above the SoftGRE Profiles box.

   A form appears from which you can select the SoftGRE profiles that you want to apply to the zone. The profiles you can select are displayed under **Available Profiles**. Select the profile and click the **->** icon to choose it. The profile is now listed under the **Selected Profiles** area.

   FIGURE 15 SoftGRE Profiles Form

   Select Soft GRE Tunnel Profiles

   You can also click the **+** icon to create a new SoftGRE profile.

   If you wish to deselect a profile, select it and click the **<-** icon. The profile will be moved back to the **Available Profiles** area and will not be applied to that zone.

7. Click **OK**.

   Your multiple tunnel configuration for the zone is saved.

Configuring Multiple Tunnels in WLANs

In WLANs where there is an option to tunnel the traffic, you can choose the tunneling profile the WLAN can use.

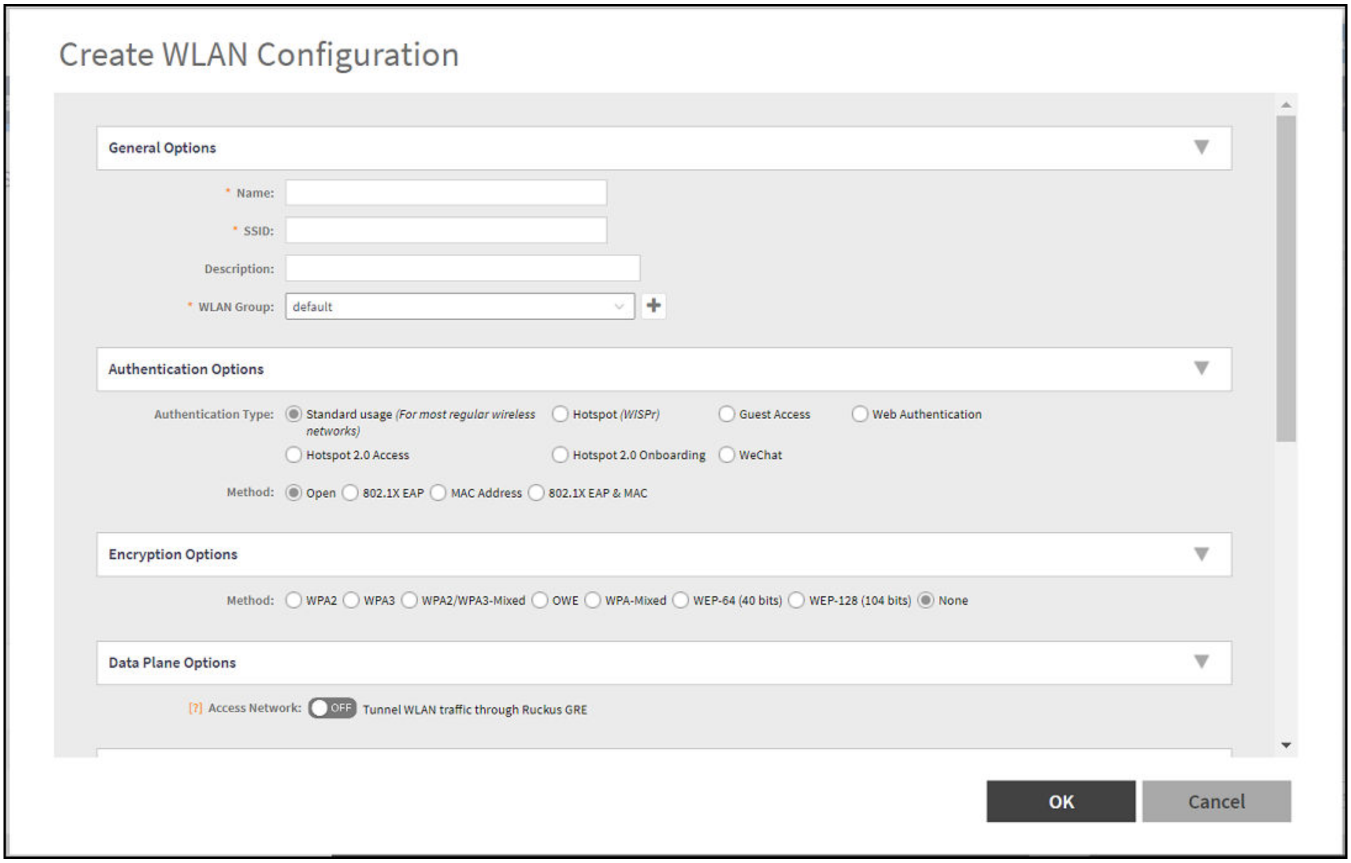
Perform the following steps to enable tunneling in WLANs.

1. Go to **Network** > **Wireless** > **Wireless LANs**, from the **System tree hierarchy**, select the **Zone** where you want to create a WLAN.

2. Click **Create**.

   The **Create WLAN Configuration** page appears.

   FIGURE 16 Tunneling Options while Creating a WLAN Configuration



Create WLAN Configuration

General Options

* Name:

* SSID:

Description:

* WLAN Group: default

Authentication Options

Authentication Type: ● Standard usage *(For most regular wireless networks)* ○ Hotspot *(WISPr)* ○ Guest Access ○ Web Authentication ○ Hotspot 2.0 Access ○ Hotspot 2.0 Onboarding ○ WeChat

Method: ● Open ○ 802.1X EAP ○ MAC Address ○ 802.1X EAP & MAC

Encryption Options

Method: ○ WPA2 ○ WPA3 ○ WPA2/WPA3-Mixed ○ OWE ○ WPA-Mixed ○ WEP-64 (40 bits) ○ WEP-128 (104 bits) ● None

Data Plane Options

[?] Access Network: OFF Tunnel WLAN traffic through Ruckus GRE

3. In the section **Data Plane Options** , enable the **Tunnel WLAN traffic through Ruckus GRE** switch.

You have successfully configured the tunneling option to forward traffic in a WLAN.

Data Plane Upgrade

Upgrading the Data Plane

You can view and upgrade the virtual data plane version using patch files. This feature is applicable only for virtual platforms.

Upgrading vSZ-D

vSZ support APs starting version 3.4. You must first upgrade vSZ before upgrading vSZ-D, because only a new vSZ can handle an old vSZ-D. There is no order in upgrading the AP zone or vSZ-D. During the vSZ upgrade, all tunnels stay up except the main tunnel which moves to the vSZ. Once the upgrade procedure is completed, allow ten minutes for the vSZ-D to settle.

Upgrade to R5.0 does not support data migration (statistics, events, administrator logs). Only the existing system and the network configuration is preserved. For more information, contact Ruckus support.

Upgrading SZ100-D

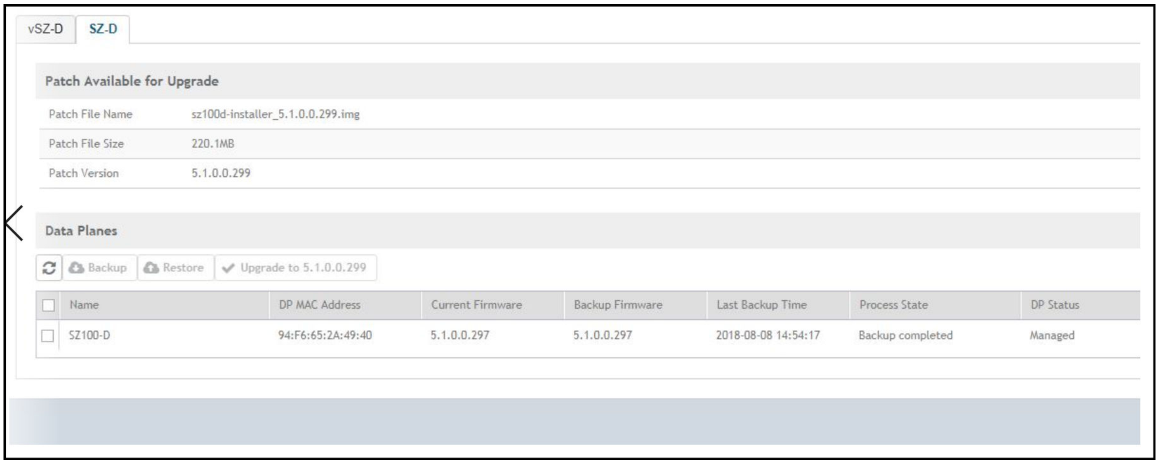
SZ100-D is shipped with 3.6.1 release version and you must upgrade it to 5.1 release version. As vSZ manages SZ100-D, ensure that vSZ has the same or later version than SZ100-D. Otherwise, upgrade vSZ before upgrading SZ100-D. SmartZone release 5.1.1 supports SZ100-D. For more information, refer to the *Ruckus SmartZone100-D Quick Setup Guide*.

To Upgrade the Data Plane:

1. Go to **Administration** > **Administration** > **Upgrade**.
2. Select the **DP Patch** tab.

   The **DP Patch** page appears.

   FIGURE 17 DP Patch - Data Plane Upgrade



Patch Available for Upgrade

Patch File Name	sz100d-installer_5.1.0.0.299.img
Patch File Size	220.1MB
Patch Version	5.1.0.0.299

Data Planes

□	Name	DP MAC Address	Current Firmware	Backup Firmware	Last Backup Time	Process State	DP Status
□	SZ100-D	94:F6:65:2A:49:40	5.1.0.0.297	5.1.0.0.297	2018-08-08 14:54:17	Backup completed	Managed

3. In **Patch File Upload**, click **Browse** to select the patch file (.ximg file).

4. Click **Upload**. The patch files is uploaded.

   The controller automatically identifies the Type of DP (vSZ-D or SZ-D) and switches to the specific Tab page. Uploads the file to its database, and then performs file verification. After the file is verified, the **Patch for Pending Upgrade** section is populated with information about the upgrade file.
   The following details are displayed:

   - Patch File Name: Displays the name of the patch file.
   - Patch File Size: Displays the size of the patch file.
   - Patch Version: Displays the version of the patch file.

5. In **Data Planes**, identify the data plane you want to upgrade, and then choose a patch file version from **Select upgrade version**.
6. Click **Apply** to apply the patch file version to the virtual data plane.

   The following information about the virtual data plane is displayed after the patch file upgrade is completed.

   - Name: Displays the name of the virtual data plane.
   - DP MAC Address: Displays the MAC IP address of the data plane.
   - Current Firmware: Displays the current version of the data plane that has been upgraded.
   - Backup Firmware: Displays the backup version of the data plane.
   - Last Backup Time: Displays the date and time of last backup.
   - Process State: Displays the completion state of the patch file upgrade for the virtual data plane.
   - DP Status: Displays the DP status.

You have successfully upgraded the virtual data plane.

> **NOTE**
> To have a copy of the data plane firmware or move back to the older version, you can select the data plane from the list and click **Backup** or **Restore** respectively.

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