

# RUCKUS SmartZone (ST-GA) Release Notes, 7.0.0

## Supporting SmartZone 7.0.0

© 2024 CommScope, Inc. All rights reserved.

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

## Export Restrictions

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

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

## Disclaimer

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

## Limitation of Liability

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

## Trademarks

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

## Patent Marking Notice

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

# Contents

---

<b>Document History</b> .....	<b>4</b>
<b>New Features in R7.0.0</b> .....	<b>4</b>
Hardware .....	4
New Software Features in R7.0.0.....	6
Countries Supported on 6Ghz .....	9
<b>Hardware and Software Support</b> .....	<b>11</b>
Overview.....	11
Release Information.....	11
Supported Matrix and Unsupported Models.....	14
Supported ICX Models.....	16
Product Documentation.....	19
<b>Known Issues</b> .....	<b>19</b>
Known Issues in R7.0.0.....	20
Limitations.....	24
R770 Known Issues and Limitations.....	25
<b>Changed Behavior</b> .....	<b>27</b>
<b>Interoperability Information</b> .....	<b>28</b>
Cluster Network Requirements.....	28
Client Interoperability.....	28

# Document History

Revision Number	Summary of Changes	Publication Date
A	Initial <i>Release Notes</i>	23, February 2024

## New Features in R7.0.0

The following lists hardware and software features, modifications, and deprecated features in release R7.0.0.

### Hardware

This section provides a high-level overview of key hardware features introduced in R 7.0.0. .

#### RUCKUS AP R770

This section provides a high-level overview of key features introduced in the AP R770 Firmware Release.

- **320 MHZ Channelization:** 320 MHz-radio frequency is available for the R770 AP 6 GHz radio frequency which is the first WiFi7 Enterprise AP.
- **R7.0.0-Single LED requirements:** A unified LED model that displays the most pertinent status on operation of the AP.
- **TPM2 in Wi-Fi 7 board:** Updated cryptographic chip which is TPM2.0 TSG specification compliant to better secure hardware from unauthorized use and tampering.
- **Secure Boot support in RUCKUS APs:** Protections placed in R770 AP is to ensure only software (bootloader images) which are properly signed and authorized by RUCKUS Wireless can run on the AP to avoid any unauthorized hacking or tampering of the device.
- **Add iPerf server/client in the AP CLI:** The iPerf utility is embedded in the AP's Command Line Interface to conveniently run performance tests which will help in debugging and serviceability.
- **WPA3 on SmartMesh:** Utilizing WPA3 encryption on RUCKUS Wireless SmartMesh feature.
- **Increase per AP scalability of Dynamic VLANs:** Increased the number of Dynamic VLANs to 128 to provide better support of ease of administration, confinement of broadcast domains, reduced network traffic, and enforcement of security policies. This feature is compatible with 802.11ax or 802.11be models.
- **Client roaming with AVC information:** Enhancements to better manage traffic between roaming clients and APs.
- **QoS Mirroring Improvement:** Allows an AP to give certain applications (For example, Zoom and FaceTime) higher priority when it comes to Quality of Service.
- **Wi-Fi 7 Preamble Puncturing:** Ability to break a frequency channel into discontinuous pieces when there is interference in the frequency. You can access Preamble Puncturing only through CLI mode.

#### Multi-Link Operation (MLO) Support for Wi-Fi7 APs

MLO capable Wi-Fi7 Wireless clients can now associate on multiple radio bands and dynamically switch between multiple bands leading to increased throughput and reduced latency as supported via 802.11BE/Wi-Fi7 standard.

#### NOTE

The Wi-Fi 7 feature Multi-Link Operation (MLO) is available, pending the client OS and driver support. It would be mandated to use WPA3 encryption with MLO to secure your Wi-Fi network in OS.

The following features are supported with MLO and/or non-MLO clients on the same MLO WLAN:

- **AVC and AVC Policies**

- Client Isolation
- Wi-Fi Calling
- Rate Limit Support at WLAN, Firewall, per Client
- Layer 3 ACL feature
- PPE+MLO Offload support
- Dynamic VLAN Support for MLO Clients
- DNS Spoofing
- Synchronization of AVC metadata for client flows during roam
- Thermal Throttling for R770 for 7.0.0
- Failsafe Phase-1 in R7.0.0
- Wi-Fi7 Preamble Puncturing

MLO clients connections are supported on all standard wireless authentication and encryption configurations, including:

- WPA3-SAE
- WPA3-802.1X
- Open-OWE
- MAC-Authentication
- Captive Portal Network

### **RUCKUS Standard AP LED Description for Wi-Fi7 and APs**

The specified LED states for Wi-Fi7 and APs are outlined as follows. The base light of the LED state is designed to transition from *Red* to *Amber* to *Green*. Additionally, there are exception states listed, which will only be activated if the AP is engaged in specific functions as defined below.

State Base Light	Description	Light Pattern
Red	AP is in the process of determining its power mode.	Solid Red
	AP is currently operating in 802.3af power mode.	Slow Blinking Red
	AP is currently undergoing a factory reset.	Blinking between Red and Green
Amber	AP has an adequate power supply and is currently in the process of booting up.	Solid Amber
	AP is currently in setup mode.	Blinking Amber
	AP has lost connectivity to the system controller interface	Slow Blinking Amber
	AP is currently undergoing the loading process for a firmware or configuration update.	Fast Blinking Amber
Green	WLAN services and controller management on the AP are currently operational.	Solid Green
	The WLAN on the AP has at least one client connected.	Blinking Green
	The WLAN on the AP has at least one client connected, and mesh networking is enabled.	Slow Blinking Green

## New Software Features in R7.0.0

The following section lists new, modified, and deprecated software features in release R7.0.0.

Feature	Description
<b>320Mhz Bandwidth Support</b>	In Wi-Fi 7, the adoption of a 320 MHz channel width expands the spectrum bandwidth allocated to a single Wi-Fi channel, resulting in a notable enhancement of data speeds.
<b>AP File System Enhancements</b>	In light of identified issues with the existing file system and to address evolving demands for containers, it is necessary to devise approaches for Wi-Fi 7 APs that effectively address and fulfill these requirements.
<b>AP Automatically Calls Home to its Original Cluster in Active-Active Redundancy Configuration</b>	This feature permits an AP to autonomously revert to a designated <i>Home Cluster</i> at specified intervals within Active-Active Cluster Redundancy configurations.
<b>RUCKUS AI Branding Change</b>	The rebranding initiative from RUCKUS Analytics to RUCKUS AI signifies a strategic shift towards a more advanced and intelligent approach in leveraging data analytics within the RUCKUS ecosystem.
<b>AP Containerization</b>	Enables dynamic containerization allows for a significant reduction in AP firmware size, decreasing it from 83 MB to 48 MB.
<b>Add iPerf server/client in the AP CLI</b>	The iPerf utility is embedded in the AP's Command Line Interface to conveniently run performance tests which will help in debugging and serviceability.
<b>Backup and Recovery Events for RNCSS</b>	Backup and Recovery events have been introduced in this release. These events occur when the RNCSS (Radio Network Controller Subsystem) detects that the NAND copy of the device certificate or key is either corrupted or missing, it initiates a recovery process. This recovery is facilitated using the NOR copy, either during a system reboot or through a manual recovery command.
<b>BSS Priority Tooltip</b>	In this release, a new feature has been introduced called the <i>BSS Priority tooltip</i> . This feature includes two settings that allow users to configure the priority. <ul style="list-style-type: none"> <li>• <b>LOW</b> - The LOW setting diminishes the WLAN's priority by restricting throughput for all clients linked to this WLAN.</li> <li>• <b>HIGH</b> - In contrast, the HIGH setting imposes no limitations on throughput. The default configuration establishes WLAN priority at HIGH.</li> </ul>
<b>Client Certificate Supports Certificate Authority Chains</b>	SmartZone now has the capability to facilitate the uploading of client certificate chains, enabling the utilization of a trusted hierarchy of Certificate Authority (CA) certificates for authenticating client devices. This approach strengthens communication security by validating the legitimacy and trustworthiness of client certificates at multiple levels through the CA chain. The primary advantage is heightened network security, as this multilayer verification process ensures that only authorized devices with duly validated certificates gain access to the network. Consequently, this reduces the risk of unauthorized access and potential security breaches.
<b>Chatbot Enhancement</b>	This functionality enables SmartZone to directly gather AP support logs, snapshot logs, and configuration backups through chatbots. Subsequently, this collected data can be efficiently transmitted to the customer support team and documented within the customer support ticket for comprehensive and streamlined issue resolution.
<b>Channelfly and 40 Mhz Channelization as Default</b>	Sets the default configuration for all radios to use Channelfly. It also sets the default Channel width on 5GHz radio to 40 MHz instead of 80 MHz.
<b>Client roaming with AVC information</b>	Enhancements to better manage traffic between roaming clients and APs.

Feature	Description
<b>RUCKUS Dynamic Pre-Shared Key (DPSK3)</b>	RUCKUS Dynamic Pre-Shared Key (DPSK3) stands out as a distinctive security measure that allocates a unique Wi-Fi password to every device within a network, employing WPA3 security. This method not only bolsters network security by minimizing the potential risks linked to password sharing but also streamlines user administration. This is achieved by granting control over individual device access without necessitating a modification of the network password for all users.
<b>Enhancement in AF Power AP Detection</b>	APs equipped with two radios demand high power (802.3at and above) to fully support their functionality. In cases where 802.3af power is detected on such APs, certain functions may not operate as expected. To address this, SmartZone now incorporates a detection mechanism for APs with three radios experiencing lower-than-required power. The system notifies administrators through events, ensuring awareness and enabling timely corrective actions.
<b>Enhancement to Device Policy OS Vendors</b>	This feature involves updating the OS Vendor Name and ID for Gaming Device Types, introducing a new name and ID while removing the deprecated OS Vendor from the display on the SmartZone GUI. Importantly, it maintains compatibility by supporting the AP-reported former OS Vendor Name and ID.
<b>Enhancement to the upgrade notification</b>	Enhancement of the upgrade notification to clearly inform users that downgrading the SmartZone will result in the removal of the current configuration.
<b>External DPSK Without Proxy Mode</b>	This feature offers support for SmartZone External Dynamic Pre-Shared Key (PSK) without the necessity of employing a proxy RADIUS in Wireless LAN configuration settings.
<b>IEEE 802.11mc</b>	IEEE 802.11mc, commonly referred to as Wi-Fi Fine Time Measurement (FTM), is a protocol enhancement designed to facilitate precise location measurements within Wi-Fi networks. This capability is achieved by gauging the time taken for signals to traverse between a Wi-Fi device and access points, allowing for highly accurate device positioning, typically within a range of one to two meters.
<b>Increase per AP scalability of Dynamic VLANs</b>	Increased the number of Dynamic VLANs to 128 to provide better support of ease of administration, confinement of broadcast domains, reduced network traffic, and enforcement of security policies. This feature is compatible with 802.11ax or 802.11be models.
<b>Multi-Link Operation (MLO)</b>	Wi-Fi7 incorporates Multi-Link Operation (MLO), a technology enabling devices to concurrently transmit data across various radio frequencies or channels. This innovative approach substantially boosts data throughput and reliability by amalgamating the bandwidth from different frequency bands such as 2.4 GHz, 5 GHz, and 6 GHz. MLO is supported for two channel Radio's (2.4+5GHz, or 5+6GHz, or 2.4+6GHz,). MLO enhances resilience against interference by leveraging multiple paths. The key advantage of MLO lies in its capacity to deliver elevated data rates and optimize wireless spectrum utilization, resulting in enhanced network performance. This is particularly beneficial in environments with high data demands or susceptibility to interference.
<b>Option to Disable Wi-Fi 7</b>	The SmartZone web user interface provides users with the capability to disable Wi-Fi 7, particularly useful in cases where client devices may experience issues with SSIDs broadcasting Wi-Fi 7 compatibility. This feature allows for the adjustment of network settings to accommodate specific client device requirements or resolve compatibility issues related to Wi-Fi 7.
<b>Preamble Puncturing</b>	In Wi-Fi 7, <i>Preamble Puncturing</i> is a feature designed to enhance the flexibility and efficiency of wireless spectrum utilization. This capability enables access points to intentionally "puncture" or skip specific subchannels during transmission. This becomes especially valuable in environments where certain portions of the spectrum experience congestion or interference, as it allows the Wi-Fi system to bypass these problematic subchannels. The key advantage of <i>Preamble Puncturing</i> lies in its ability to improve overall network performance and reliability by dynamically adapting to and mitigating interference, resulting in more stable and efficient wireless communications.

**New Features in R7.0.0**  
 New Software Features in R7.0.0

Feature	Description
<b>Qosmos (Quality of Service) Signature Package support for OpenWRT AP</b>	In R5.1.0, RUCKUS introduced Qosmos as the AP DPI solution to replace Trendmicro. RUCKUS OpenWRT APs are now capable of supporting <i>Qosmos Signature Package</i> .
<b>QoS (Quality of Service) Mirroring</b>	QoS Mirroring serves as a method to enhance the prioritization of packets from the AP to its associated Client Device. Going beyond the improvements offered by DSCP values in Quality of Service (QoS), QoS Mirroring addresses a potential limitation. In situations where DSCP to UP mapping is applied and there are 10 users with higher priority traffic, conventional settings may lead to all users transmitting with the same priority. QoS Mirroring, however, prevents this scenario. Even in the presence of numerous high-priority traffic users, QoS Mirroring ensures that only packets conforming to the specified flow are allowed to transmit with higher priority.
<b>Secure Boot Support in Wi-Fi 7</b>	Secure Boot for access points serves as a security measure, ensuring that only authenticated firmware, verified by the manufacturer, is permitted to run on the device during the startup process. The SmartZone (SZ) Graphical User Interface (GUI) provides information about Secure Boot status on the Access Point (AP) page, indicating whether this security feature is enabled or disabled.
<b>Single LED requirements</b>	A unified LED model that displays the most pertinent status on operation of the AP. Refer to <a href="#">RUCKUS Standard AP LED Description for Wi-Fi7 and APs</a> on page 5
<b>Support for Certificates with ECDSA-P256 and RSA-3072</b>	This feature provides support for certificates ECDSA-P256 and RSA-3072, catering to customers with elevated security requirements for their certificates.
<b>Switch Management</b>	<ul style="list-style-type: none"> <li>• <b>Breakout Port Support</b> - SmartZone R7.0.0 introduces the ability edit the settings of existing breakout ports on ICX switches*..</li> <li>• <b>Enhancement in Firmware Upgrade Status</b> - Added additional statuses for better visibility into the firmware upgrade progress.</li> <li>• <b>SmartZone Usernames in ICX Syslog</b> - Added support to display SmartZone username in Switch Syslog messages that involve changes made from SmartZone.</li> <li>• <b>Configuring Separate Authentication and Accounting in AAA Server</b> - Provides an option to define separate Authentication and Accounting AAA servers under Switch group AAA configuration.</li> </ul> <p><i>*Enabling breakout mode is not supported and needs to be enabled through CLI configuration.</i></p>
<b>UX Analytics Data Collection Caption</b>	Enhancement to the text on the SmartZone web user interface to optimize data collection with a more persuasive message. This release introduces a link to the privacy page under the data collection tab, offering users additional information.
<b>UI/UX Configuration for Client Load Balancing</b>	Client Load Balancing (CLB) with sticky client detection or steering in Wi-Fi networks tackles the challenge of devices persistently connected to suboptimal APs. This functionality actively monitors signal quality and guides these <i>sticky</i> clients towards a higher-performing AP. This can be achieved through the use of BSS Transition Management frames for compatible devices or by compelling a disconnect for others, prompting them to reconnect to a more suitable AP. This proactive approach elevates both network performance and user experience by ensuring that devices are consistently connected to the most optimal AP available.
<b>URL Redirect and ACL defined by RADIUS</b>	This feature enables you to set up a WLAN to send users to a specific web page only after 802.1X or MAC authentication has been successfully completed. You can configure this web redirect to allow access to the network completely or partially. The redirect page and the conditions under which the redirection occurs can be configured in the RADIUS server. A new VSA <i>Ruckus-External-URL</i> is added for this feature.
<b>WPA3 on SmartMesh</b>	Utilizing WPA3 encryption on RUCKUS Wireless SmartMesh feature.



Feature	Description
<b>Deprecated Features</b>	<p>From this release:</p> <ul style="list-style-type: none"><li>• The option to toggle back to the legacy version of the SmartZone GUI is discontinued.</li><li>• Eliminate cellular options from SmartZone - Due to the exclusive support for cellular backhaul in the AP M510 and the absence of such support in other models and upcoming APs, combined with SZ R7.0.0's sole compatibility with 11ax APs, it is rational to remove cellular options from the SmartZone web user interface.</li></ul>

## Countries Supported on 6Ghz

Wi-Fi7 APs and 320MHz channel in the R7.0.0 SmartZone release support the following country codes.

1. Countries supported on 6Ghz U-NII frequency bands 5, 6, 7 and 8 supporting channels: 1, 5, ..., 233:

- US: United States
- BR: Brazil
- CA: Canada
- CL: Chile
- SA: Saudi Arabia
- HN: Honduras
- DO: Dominican Republic
- SV: El Salvador
- PG: Papua New Guinea
- KR: South Korea
- CO: Colombia
- PE: Peru

2. Countries supported on 6Ghz U-NII frequency band 5 supporting channels: 1, 5, ..., 93:

- GB: United Kingdom
- AT: Austria
- BE: Belgium
- BG: Bulgaria
- HR: Croatia
- CY: Cyprus
- CZ: Czech Republic
- DK: Denmark
- EE: Estonia
- FI: Finland
- FR: France
- DE: Germany
- GR: Greece
- HU: Hungary
- IS: Iceland

## New Features in R7.0.0

### Countries Supported on 6Ghz

- IT: Italy
- LV: Latvia
- LU: Luxembourg
- MT: Malta
- NL: Netherlands
- NO: Norway
- PL: Poland
- PT: Portugal
- RO: Romania
- SK: Slovakia
- SI: Slovenia
- ES: Spain
- SE: Sweden
- CH: Switzerland
- AU: Australia
- HK: Hong Kong
- JP: Japan
- LT: Lithuania
- MY: Malaysia
- NZ: New Zealand
- IE: Ireland
- LI: Liechtenstein
- AE: United Arab Emirates
- SG: Singapore
- QA: Qatar
- MA: Morocco
- MN: Mongolia
- MU: Mauritius
- TH: Thailand
- ZM: Zambia
- EH: Western Sahara
- RU: Russia
- ZA: South Africa
- MC: Monaco
- BY: Belarus
- JO: Jordan
- BZ: Belize
- AL: Albania
- IL: Israel

- AZ: Azerbaijan
- KW: Kuwait
- BN: Brunei
- BH: Bahrain
- KE: Kenya
- MX: Mexico
- TR: Turkey
- ZW: Zimbabwe

## Hardware and Software Support

### Overview

This section provides release information about SmartZone controllers and Access Point features.

- The SZ300 RUCKUS Networks flagship, large-scale WLAN controller is designed for Service Provider and large Enterprises which prefer to use appliances. The carrier grade platform supports N+1 Active/Active clustering, comprehensive integrated management functionality, high-performance operations and flexibility to address many different implementation scenarios.
- The SZ144 is the second-generation mid-range rack-mountable WLAN controller platform developed for the Enterprise and Service Provider markets. The SZ144 is functionally equivalent to the vSZ-E virtual controller product.
- The vSZ, which is available in *High Scale* and *Essentials* versions, is a Network Functions Virtualization (NFV)-based WLAN controller for Service Providers and Enterprises that desire a carrier-class solution that runs in the cloud. It supports all of the WLAN controller features of the industry, while also enabling the rollout of highly scalable and resilient wireless LAN cloud services.
- The vSZ-D is a Virtual Data Plane aggregation appliance that is managed by the vSZ that offers organizations more flexibility in deploying a NFV aligned architecture. Deploying vSZ-D offers secured tunneling of wireless client data traffic that encrypts payload traffic, POS data traffic for PCI compliance, voice applications while enabling flat network topology, mobility across L2 subnets, and add-on services like L3 Roaming, Flexi-VPN, DHCP Server/NAT as well as CALEA/Lawful Intercept.
- The SZ100-D is a Data Plane hardware appliance, which is functionally equivalent to the vSZ-D virtual data plane product. The appliance provides turnkey deployment capabilities for customers who need a hardware appliance. The SZ100-D is managed by a vSZ Controller only and cannot work in a standalone mode.
- The SZ144-D is the second-generation Data Plane hardware appliance which is functionally equivalent to the vSZ-D virtual Data Plane. The appliance provides turnkey deployment capabilities for customers who need a hardware appliance. The SZ144-D is managed by a vSZ Controller only and cannot work in a standalone mode.

### Release Information

This SmartZone release is a Short Term (ST) release. This section lists the version of each component in this release.

RUCKUS recommends SmartZone R7.0.0 release for users utilizing Wi-Fi7 APs. For those with legacy APs, RUCKUS suggests using SmartZone R6.1.2 release.

#### ATTENTION

It is recommended to upgrade the vSZ before updating the data plane version because if the data plane version is higher than the controller vSZ version, then data plane cannot be managed by the vSZ platform.

## Hardware and Software Support

### Release Information

#### ATTENTION

For Network Segmentation:

- Ensure that all ICX switches are upgraded to firmware version 09.0.10d (or any 09.0.10 patches that may become available after 09.0.10d) or version 10.0.10b (or any 10.0.10 patches that may become available after 10.0.10b).

#### NOTE

RUCKUS IoT R2.2.0 is not supported on SmartZone R7.0.0. Refer to the *RUCKUS IoT 2.2.0.0 GA Release Notes* for the hardware and software support details.

### SZ300

- Controller Version: **7.0.0.0.726**
- Control Plane Software Version: **7.0.0.0.465**
- Data Plane Software Version: **7.0.0.0.726**
- AP Firmware Version: **7.0.0.0.1240**

### SZ100/SZ124/SZ104

- Controller Version: **7.0.0.0.726**
- Control Plane Software Version: **7.0.0.0.465**
- Data Plane Software Version: **7.0.0.0.77**
- AP Firmware Version: **7.0.0.0.1240**

### SZ144

- Controller Version: **7.0.0.0.726**
- Control Plane Software Version: **7.0.0.0.465**
- Data Plane Software Version: **7.0.0.0.77**
- AP Firmware Version: **7.0.0.0.1240**

### vSZ-H and vSZ-E

- Controller Version: **7.0.0.0.726**
- Control Plane Software Version: **7.0.0.0.465**
- AP Firmware Version: **7.0.0.0.1240**

### vSZ-D/104D/124D/144D

- Data plane software version: **7.0.0.0.726**

### Cloudpath

- Cloudpath Version: **5.12 R6 (5.12.5584)**.

## Upgrade Information

Upgrade to R7.0.0 is available for users currently on versions R6.1, 6.1.1, and 6.1.2. Versions preceding R6.1.0 are not supported for an upgrade to R7.0.0.

## Dynamic Signature Package Update

Administrators or users can dynamically upgrade the Signature Package from the RUCKUS support site.

Complete the following steps to perform a manual upgrade:

1. Download the Signature package from the RUCKUS support site:
  - SmartZone R7.0.0 Signature Package version 1.670.2: <https://support.ruckuswireless.com/admin/software/3961-smartzone-7-0-ga-sigpack-1-670-2-application-signature-package>.
  - SmartZone R7.0.0 Signature Package version 1.670.2-regular: <https://support.ruckuswireless.com/admin/software/3960-smartzone-7-0-ga-sigpack-1-670-2-regular-application-signature-package>
2. Manually upgrade the Signature package by navigating to **Security > Application Signature Package**.

### NOTE

For more information, refer to the **Working with Application Signature Package** in *RUCKUS SmartZone Security Guide (ST-GA), 7.0.0*

### NOTE

Upgrade to R7.0.0 from versions prior to R6.1.0 is not supported. It's important to note that RUCKUS does not impose any signature-package upgrade restrictions during the Zone upgrade process.

## SZ Google Protobuf (GPB) Binding Class

Refer to *RUCKUS SmartZone Getting Started on SZ GPB/MQTT Interface* and download the latest SmartZone (SZ) GPB .proto files from the RUCKUS support site:

1. SmartZone **7.0.0.0.726** (GA) GPB.proto (Google ProtoBuf) image for GPB/MQTT [DNP] - <https://support.ruckuswireless.com/software/3962-smartzone-7-0-0-ga-gpb-proto-google-protobuf-image-for-gpb-mqtt>.
2. SmartZone **7.0.0.0.726** MockSCI-TLS (SZ to SCI MQTT subscriber software) for CentOS/Ubuntu - <https://support.ruckuswireless.com/software/3963-smartzone-7-0-0-ga-mocksci-tls-sz-to-sci-mqtt-subscriber-software-for-centos-ubuntu-dnp>.

## Public API

Click on the following links to view Public API documents:

- *SmartZone 7.0.0 Public API Reference Guide (ICX Management)*  
<https://support.ruckuswireless.com/documents/4733>
- *SmartZone 7.0.0 Public API Reference Guide (SZ100)*  
<https://support.ruckuswireless.com/documents/4734>

### NOTE

SZ100 Public API link is for SZ144 as well.

- *SmartZone 7.0.0 Public API Reference Guide (SZ300)*  
<https://support.ruckuswireless.com/documents/4735>

## Hardware and Software Support

### Supported Matrix and Unsupported Models

- *SmartZone 7.0.0 Public API Reference Guide (vSZ-E)*  
<https://support.ruckuswireless.com/documents/4736>
- *SmartZone 7.0.0 Public API Reference Guide (vSZ-H)*  
<https://support.ruckuswireless.com/documents/4737>

## Supported Matrix and Unsupported Models

Before upgrading to this release, check if the controller is currently managing APs, Switches or IoT devices.

APs preconfigured with the SmartZone AP firmware may be used with SZ300, SZ100, or vSZ in their native default configuration. APs factory-configured with the ZoneFlex-AP firmware may be used with the controller when LWAPP discovery services are enabled.

LWAPP2SCG must be disabled on the controller if Solo APs running 104.x are being moved under controller management. To disable the LWAPP2SCG service on the controller, log on to the CLI, and then go to **enable > mode > config > lwapp2scg > policy deny-all**. Enter **Yes** to save your changes.

### NOTE

Solo APs running releases 104.x or higher are capable of connecting to both Zone Director and SmartZone platforms. If an AP is running release 104.x or later and the LWAPP2SCG service is enabled on the controller, a race condition will occur.

### IMPORTANT

**AP PoE power modes:** AP features may be limited depending on power provided via PoE. Refer to AP datasheets for more information.

## Supported AP Models

This release supports the following RUCKUS AP models.

**TABLE 1** Supported AP Models

11ax	
Indoor	Outdoor
R850	T750SE
R770	T750
R760	T350SE
R750	T350D
R650	T350C
R560	
R550	
R350	
H550	
H350	

The following lists the supported AP models in this SmartZone release when placed in an AP Zone that uses an older AP version.

### ATTENTION

The R730 AP must be removed from the AP Zone before upgrading the AP Zone to the AP firmware version 6.1.1 or later.

**ATTENTION**

For APs that are not compatible with R7.0.0, it is essential to maintain them with AP firmware versions of R6.1, 6.1.1, and 6.1.2. The upgrade of the Zone for APs that are not supported in R6.1, 6.1.1, and 6.1.2 is not feasible.

**TABLE 2** Supported AP Models for AP Zones using older AP versions

11ax	11ac-Wave2	
<b>NOTE</b> Supported on R6.1.0, 6.1.1, and 6.1.2.	<b>Indoor</b>	<b>Outdoor</b>
T750SE	R720	T811CM
T750	R710	T710S
T350SE	R610	T710
T350D	R510	T610S
T350C	R320	T610
R850	M510	T310S
R760 (not supported on R6.1.0)	H510	T310N
R750	H320	T310D
R730	C110	T310C
R650		T305I
R560 (not supported on R6.1.0)		T305E
R550		E510
R350		
H550		
H350		

**ATTENTION**

AP R310 is Wave 1 and supports WPA3 - this is the one exception, the rest of the APs that support WPA3 are 802.11ac Wave2 or 802.11ax.

**Unsupported AP Models**

The following lists the AP models have reached end-of-life (EoL) status and, therefore, are no longer supported in this release.

**TABLE 3** Unsupported AP Models

Unsupported AP Models				
SC8800-S	SC8800-S-AC	ZF2741	ZF2741-EXT	ZF2942
ZF7025	ZF7321	ZF7321-U	ZF7341	ZF7343
ZF7343-U	ZF7351	ZF7351-U	ZF7363	ZF7363-U
ZF7441	ZF7761-CM	ZF7762	ZF7762-AC	ZF7762-S
ZF7762-S-AC	ZF7762-T	ZF7962	ZF7781CM	ZF7982
ZF7782-S	ZF7782-E	ZF7782	ZF7372-E	ZF7372
ZF7352	ZF7055	R300	R310	R700
C500	H500	R600	R500	R310
R500E	T504	T300	T300E	T301N
T301S	FZM300	FZP300		

## Supported ICX Models

The following ICX switch models can be managed from SmartZone:

**TABLE 4** ICX Firmware Versions Compatible with SmartZone

ICX Model	First Supported FastIron Release	Last Supported FastIron Release
ICX 7150	08.0.80a	09.0.10a and subsequent patches
ICX 7150-C08P, -C08PT, -24F, -10ZP	08.0.92	09.0.10a and subsequent patches
ICX 7250	08.0.80a	09.0.10a and subsequent patches
ICX 7450	08.0.80a	09.0.10a and subsequent patches
ICX 7550	08.0.95a	-
ICX 7650	08.0.80a	-
ICX 7750	08.0.80a	08.0.95 and subsequent patches
ICX 7850	08.0.90	-
ICX 7850-48C	09.0.10a	-
ICX 8200	10.0.00	-
ICX 8200-24ZP, -48ZP2, -24FX, -24F, -48F, -C08ZP	10.0.10	-

The following table defines ICX and SmartZone release compatibility.

**NOTE**

ICX switches must be running FastIron 08.0.80a at a minimum to connect to SmartZone. An ICX switch running unsupported firmware can still connect to the SmartZone controller. After the switch is connected, you must upgrade it to a firmware version that is compatible with the SmartZone controller version. This can be achieved using the switch firmware upgrade option in the Switch Group or by selecting one or more switches and performing the upgrade.

**NOTE**

FastIron 09.0.10a and later releases support management by SmartZone 6.1 and later.

**NOTE**

ICX switches with FIPS mode enabled do not support management by SmartZone.

**TABLE 5** ICX and SmartZone Release Compatibility Matrix

	SmartZone 5.1 <sup>1</sup>	SmartZone 5.1.1	SmartZone 5.1.2	SmartZone 5.2	SmartZone 5.2.1 / 5.2.2	SmartZone 6.0	SmartZone 6.1	SmartZone 6.1.1	SmartZone 6.1.2	SmartZone 7.0.0
FastIron 08.0.80	Yes	Yes <sup>1</sup>	No	No	No	No	No	No	No	No
FastIron 08.0.90a	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No

<sup>1</sup> Does not support ICX configuration.



**TABLE 5** ICX and SmartZone Release Compatibility Matrix (continued)

	SmartZone 5.1 <sup>1</sup>	SmartZone 5.1.1	SmartZone 5.1.2	SmartZone 5.2	SmartZone 5.2.1 / 5.2.2	SmartZone 6.0	SmartZone 6.1	SmartZone 6.1.1	SmartZone 6.1.2	SmartZone 7.0.0
FastIron 08.0.91	No	Yes	Yes	Yes	No	No	No	No	No	No
FastIron 08.0.92	No	No	Yes	Yes	Yes	Yes	Yes	No	No	No
FastIron 08.0.95 and subsequent patches	No	No	No	No	No	Yes	Yes	Yes	Yes	No
FastIron 09.0.10a and subsequent patches	No	No	No	No	No	No	Yes	Yes	Yes	Yes
FastIron 10.0.00 and subsequent patches	No	No	No	No	No	No	No	Yes	Yes	Yes
FastIron 10.0.10 and subsequent patches	No	No	No	No	No	No	Yes	Yes	Yes	Yes

The following table provides details on switch management feature compatibility between ICX and SmartZone releases.

**TABLE 6** Switch Management Feature Compatibility Matrix

Feature	SmartZone Release	ICX FastIron Release
Switch Registration	5.0 and later	08.0.80 and later
Switch Inventory	5.0 and later	08.0.80 and later
Switch Health and Performance Monitoring	5.0 and later	08.0.80 and later
Switch Firmware Upgrade	5.0 and later	08.0.80 and later
Switch Configuration File Backup and Restore	5.0 and later	08.0.80 and later
Client Troubleshooting: Search by Client MAC Address	5.1 and later	08.0.80 and later
Remote Ping and Traceroute	5.1 and later	08.0.80 and later
Switch Custom Events	5.1 and later	08.0.80 and later
Remote CLI Change	5.2.1 and later	08.0.90 and later
Switch Configuration: Zero-Touch Provisioning	5.1.1 and later	08.0.90a and later
Switch-specific Settings: Hostname, Jumbo Mode, IGMP Snooping, and DHCP Server	5.1.1 and later	08.0.90a and later
Switch Port Configuration	5.1.1 and later	08.0.90a and later
Switch AAA Configuration	5.1.1 and later	08.0.90a and later
Switch Client Visibility	5.1.2 and later	08.0.90a and later

<sup>1</sup> Does not support ICX configuration.

**Hardware and Software Support**  
Supported ICX Models

**TABLE 6** Switch Management Feature Compatibility Matrix (continued)

Feature	SmartZone Release	ICX FastIron Release
Manage Switches from Default Group in SZ-100 / vSZ-E	5.1.2 and later	08.0.90a and later
DNS-based SmartZone Discovery	5.1.2 and later	08.0.95c and later
Download Syslogs for a Selected Switch <sup>2</sup>	5.2.1 and later	08.0.92 and later
Switch Topology	5.2 and later	08.0.92 and later
Designate a VLAN as Management VLAN	5.2.1 and later	08.0.92 and later <sup>3</sup>
Change Default VLAN	5.2.1 and later	08.0.95 and later
Configure the PoE Budget per Port on ICX through the Controller GUI with 1W Granularity	5.2.1 and later	08.0.95 and later
Configuring Protected Ports	5.2.1 and later	08.0.95 and later
Configuring QoS	5.2.1 and later	08.0.95 and later
Configuring Syslog	5.2.1 and later	08.0.95 and later
Geo Redundancy Active-Standby Mode	6.0 and later	08.0.95b and later
Generic CLI Configuration	6.0 and later	08.0.95b and later
Port-Level Override	6.0 and later	08.0.95b and later
Port-Level Storm Control Configuration	6.1 and later	08.0.95 and later
IPv6 Support (connection through static configuration only)	6.1 and later	09.0.10a and later
Save Boot Preference	6.1 and later	09.0.10a and later
Virtual Cable Testing	6.1 and later	09.0.10a and later
Blink LEDs	6.1 and later	09.0.10a and later
Send Event Email Notifications at Tenant Level	6.1 and later	09.0.10a and later
Update the status of a Switch	6.1 and later	09.0.10a and later
Convert Standalone Switch	6.1 and later	09.0.10a and later
Flexible Authentication Configuration	6.1 and later	09.0.10a and later
Network Segmentation	6.1.1 and later	09.0.10d and later <sup>4</sup>
Breakout Port Support	7.0.0 and later	09.0.10h and later
Enhancement in Firmware Upgrade Status	7.0.0 and later	09.0.10h and later
SmartZone Usernames in ICX Syslogs	7.0.0 and later	09.0.10h and later, 10.0.10c and later
Configuring Separate Authentication and Accounting in AAA server	7.0.0 and later	09.0.10h and later

<sup>2</sup> To download system logs from SmartZone for a particular ICX switch, TFTP must be enabled.

<sup>3</sup> FastIron 10.0.00 and later releases do not support management VLANs.

<sup>4</sup> As an exception, FastIron release 10.0.00 does not support this feature.

## Product Documentation

The product guides for R7.0.0 have been updated. Refer to the *New in this Document* section in each publication for detailed changes.

**TABLE 7** Product Guides

Category	Name of The Guide
<b>User and Administrator Guides</b>	<ul style="list-style-type: none"> <li>● RUCKUS SmartZone (ST-GA) SmartZone Upgrade Guide, 7.0.0</li> <li>● RUCKUS SmartZone (ST-GA) AP Management Guide, 7.0.0</li> <li>● RUCKUS SmartZone (ST-GA) Basic Controller Settings, 7.0.0</li> <li>● RUCKUS SmartZone (ST-GA) Client Management Guide, 7.0.0</li> <li>● RUCKUS SmartZone (ST-GA) Guest Access Guide, 7.0.0</li> <li>● RUCKUS SmartZone (ST-GA) Monitoring Guide, 7.0.0</li> <li>● RUCKUS SmartZone (ST-GA) Management Guide, 7.0.0</li> <li>● RUCKUS SmartZone (ST-GA) Security Guide, 7.0.0</li> <li>● RUCKUS SmartZone (ST-GA) Switch Management Guide, 7.0.0</li> <li>● RUCKUS SmartZone (ST-GA) Traffic Management Guide, 7.0.0</li> <li>● RUCKUS SmartZone (ST-GA) User Management Guide, 7.0.0</li> <li>● RUCKUS SmartZone (ST-GA) WLAN Management Guide, 7.0.0</li> </ul>
<b>Interface Guides</b>	<ul style="list-style-type: none"> <li>● RUCKUS SmartZone (ST-GA) Supported RFCs and Standard Compliance Report, 7.0.0</li> <li>● RUCKUS SmartZone (ST-GA) Tunnelling Interface Reference Guide, 7.0.0</li> <li>● RUCKUS SmartZone (ST-GA) Alarm and Event Reference Guide, 7.0.0</li> <li>● RUCKUS SmartZone (ST-GA) AAA Interface Reference Guide, 7.0.0</li> <li>● RUCKUS SmartZone (ST-GA) Hotspot WISPr Interface Reference Guide, 7.0.0</li> <li>● RUCKUS SmartZone (ST-GA) Hotspot 2.0 Reference Guide, 7.0.0</li> <li>● RUCKUS SmartZone (ST-GA) SNMP Reference Guide (SZ300/vSZ-H), 7.0.0</li> <li>● RUCKUS SmartZone (ST-GA) SNMP Reference Guide (SZ100/vSZ-E), 7.0.0</li> <li>● RUCKUS SmartZone (ST-GA) Hanshow Dongle User Guide, 7.0.0</li> <li>● RUCKUS SmartZone (ST-GA) Command Reference Guide, 7.0.0</li> <li>● RUCKUS SmartZone (ST-GA) Network Segmentation Configuration Guide, 7.0.0</li> <li>● RUCKUS SmartZone (ST-GA) Getting Started on SZ GPB/MQTT Interface, 7.0.0</li> </ul>

### Online Help Rendition

A number enhancements are introduced for Online Help (OLH) rendering for R7.0.0. Previous renditions navigated to the *RUCKUS SmartZone Administrator Guide* (consisting of 700+ pages). From R6.1.1, we have split the existing *RUCKUS SmartZone Administrator Guide* into 11 separate guides (Rev B of R6.1.1). This split is based on Taxonomy, and one of the main purposes for this change was for easy reading and keyword search. This enhancement caused a change in the way OLH renders.

The OLH now renders with all of the product guides listed under the relevant firmware release number. A short description appears for each guide. Select the relevant guide for reference.

## Known Issues

This section describes known behaviors and recommended workarounds where they exist.

## Known Issues

Known Issues in R7.0.0

### Known Issues in R7.0.0

Following are the known issues in this release.

Component/s	AP
Issue	SCG-145121
Description	The results of SpeedFlex tests on a multihop mesh setup are not accessible through the <i>Public API</i> . This limitation only when PMTU (Path MTU (Maximum Transmission Unit)) is set to 1500.

Component/s	AP
Issue	SCG-142998
Description	When the user selects the PoE operation mode to AT mode, 11AX or later AP models it is forcibly turned off, and the USB toggle is grayed. Subsequently, when the user changes the PoE operation mode to Auto, the USB toggle changes to edit mode. However, the controller web user interface does not automatically enable the USB toggle.

Component/s	AP
Issue	SCG-142102
Description	<p>There is a disparity in the TTL (Time To Live) definition between LLDP (Link Layer Discovery Protocol) version 0.7.1 and version 1.0.15 as outlined below:</p> <ul style="list-style-type: none"><li>• LLDP 1.0.15 defines TTL as hold time multiplied by the interval (TTL = hold time * interval). In contrast, LLDP 0.7.1 defines TTL as equal to the hold time (TTL = hold time).</li><li>• The default interval in LLDP 1.0.15 is set to 30 seconds.</li></ul> <p>Following are the TTL examples in LLDP 1.0.15. I.</p> <ul style="list-style-type: none"><li>• If hold time is set to 10 seconds, TTL is calculated as <math>30 * 10 = 300</math> seconds.</li><li>• If hold time is set to 200 seconds, TTL is calculated as <math>30 * 200 = 6,000</math> seconds.</li><li>• If hold time is set to 500 seconds, TTL is calculated as <math>30 * 500 = 15,000</math> seconds.</li><li>• If hold time is set to 1000 seconds, TTL is calculated as <math>30 * 1000 = 30,000</math> seconds.</li></ul>

Component/s	AP
Issue	AP-26728
Description	<p>In scenarios where a wireless client transitions from one access point (AP-1) to another (AP-2), the Deep Packet Inspection (DPI) engine on AP-2 may face challenges in accurately identifying and classifying certain applications.</p> <p>This issue is particularly evident for applications characterized by distinct control flows and data flows, such as FTP and YouTube. The difficulty arises because control flows may be initiated on AP-1, and by the time data flows commence, the client has already roamed to AP-2.</p> <p>Consequently, the DPI engine on AP-2 lacks the contextual information of the initial control flows, potentially resulting in a failure to detect or classify the ongoing traffic.</p>

Component/s	AP
Issue	AP-25573
Description	The FT (Fast Transition) framework mechanism does not support PMKR1 (Pairwise Master Key - R1) key re-dispatch to the Access Point (AP) that has newly joined the mobility domain.

Component/s	AP
Issue	AP-25953

Component/s	AP
Description	Logs and events may not be visible in the external syslog server because syslog is sent to the server once the Access Point (AP) obtains an IP address. In the case of RNCSS (RUCKUS NOR Certificate Safe Storage) logs during bootup, occur before the AP acquires an IP address, resulting in the absence of events in the external syslog server.

Component/s	AP
Issue	SCG-141990
Description	The CLI command <b>get mode wlanx</b> does not accurately reflect the current operating mode of the WLAN.

Component/s	AP
Issue	SCG-141611
Description	The NSP (Network Services Platform) failed to configure the tunnel profile in the NSP Ethernet profile.
Workaround	Users are required to choose an AP group with a tunnel WLAN. If the selected AP group does not have a tunnel WLAN configured, the MDU (Multi-Dwelling Unit) wired client functionality will not operate as intended.

Component/s	AP
Issue	AP-27714
Description	The WLAN AP directs the client to transmit to the Service WLAN on the same radio after the client passes through the intermediate WLAN. This behavior is regarded as a design limitation.
Workaround	For a client to connect to the 6GHz Service WLAN, the client needs to disconnect and reconnect after passing through the Service WLAN of 2.4 or 5GHz.

Component/s	AP
Issue	AP-25371
Description	The RUDB (RUCKUS User Database) updates information for wired clients by analyzing the initial packet of the spoofed DHCP request or response, where the source and destination MAC addresses have been altered.

Component/s	AP
Issue	AP-24758
Description	Uplink traffic associated with multicast, including protocols like IGMP (Internet Group Management Protocol) (224.0.0.22), may experience rate limiting. This restriction occurs because only certain IGMP control packets, such as <i>IGMP_MEMBERSHIP_REPORT</i> and <i>IGMP_HOST_LEAVE</i> , are recognized as known multicast traffic, leading to potential rate limitations.

Component/s	AP
Issue	SCG-151847
Description	When the user unplugs the AP PoE interface cable, reconnects it to the ICX switch port, and manually adjusts the power setting to 802.3at through the controller web user interface or AP CLI, the power consumption status on the AP indicates it as <i>802.3bt5 Switch/Injector</i> . This problem specifically affects the R560, R760, and R770 models.
Workaround	Reboot the AP/ Upgrade firmware.

## Known Issues

### Known Issues in R7.0.0

<b>Component/s</b>	AP
<b>Issue</b>	SCG-146391
<b>Description</b>	Flow creation does not take into account fragmented packets, hence SmartCast rules are not applied.

<b>Component/s</b>	AP
<b>Issue</b>	AP-27922
<b>Description</b>	Beacon protection is not enabled in MLO WLAN. This is specific to Wi-Fi7 configuration and does not affect the association of MLO clients.

<b>Component/s</b>	AP
<b>Issue</b>	AP-28024
<b>Description</b>	<p>The <code>docker-24.0.7.tgz</code> for Wi-Fi7 APs is downloaded and installed in the <code>/ruckuswireless</code> directory which resides in a permanent storage (flash memory). In contrast, for non Wi-Fi7 APs, docker binaries are downloaded and installed in the <code>/tmp</code> directory which is a <code>tmpfs</code> (RAM). As a result, the download and installation process takes longer for Wi-Fi7 APs compared to non Wi-Fi7 APs.</p> <p>When downloading a tar file in the <code>/ruckuswireless</code> directory, the extraction process also takes longer compared to downloading and extracting in the <code>/tmp</code> directory. This is because accessing and processing data from permanent storage involves higher latency when compared to data stored in RAM.</p>

<b>Component/s</b>	AP
<b>Issue</b>	AP-27817
<b>Description</b>	Kernel panics occurring randomly on MAPs, particularly when there is a channel change on the RAP due to radar detection. Consequently, deploying a mix of Wi-Fi 6E and Wi-Fi 6 APs in such conditions is not recommended for mesh deployments.

<b>Component/s</b>	AP
<b>Issue</b>	SCG-151853
<b>Description</b>	The client inactivity timeout feature is not functioning as expected on the R550 AP model. Despite the expiration of the inactivity timer values, clients are disconnected, and continue to connect to the R550 AP. This issue is specific to R550 AP.

<b>Component/s</b>	AP
<b>Issue</b>	SCG-151717
<b>Description</b>	The rate limit specified through the user-role from AAA (Authentication, Authorization, and Accounting) server is not enforced on clients connected through 802.1x authentication with WISPr Express Wi-Fi proxy.

<b>Component/s</b>	AP
<b>Issue</b>	SCG-146540, AP-28381
<b>Description</b>	Clients connected to the non-mesh interface of R560 or R760 Mesh APs may experience performance degradation. This issue is particularly noticeable when the client is connected to the 2nd radio of R760 while a mesh link is established on the 5Ghz 3rd radio of the R760.

<b>Component/s</b>	AP
<b>Issue</b>	AP-19942
<b>Description</b>	When SSID Radio Load (RL) is enabled on R560 or R760 or R770 APs with only one WLAN or VAP (Virtual Access Points) deployed, users might experience packet loss and reduced throughput in the uplink direction.
<b>Workaround</b>	It is recommended to deploy multiple WLANs or VAPs.

<b>Component/s</b>	AP
<b>Issue</b>	SCG-143239
<b>Description</b>	The performance of the 6E radio on the AP R560 or R760 decreases when 60 or more WiFi 6E clients are connected.

<b>Component/s</b>	AP
<b>Issue</b>	AP-28388
<b>Description</b>	802.11ax APs may experience kernel panics when transmitting multicast traffic, particularly when the Multicast threshold is set to zero, directed multicast is disabled, and RGRE (Remote GRE) is enabled.

<b>Component/s</b>	AP
<b>Issue</b>	SCG-146177
<b>Description</b>	The uplink performance of the AP R560 decreases when more than 40 WiFi 6/6E clients are connected and actively transmitting data.

<b>Component/s</b>	AP
<b>Issue</b>	AP-27944
<b>Description</b>	In RUCKUS AI, AP rogue data for 2.4GHz band may include channels that belong to 5GHz band.

<b>Component/s</b>	AP
<b>Issue</b>	AP-28481
<b>Description</b>	DFS (Dynamic Frequency Selection) channels 52-65 are not available on R760 or R560 APs for NZ (New Zealand) country code.

<b>Component/s</b>	AP
<b>Issue</b>	SCG-146150
<b>Description</b>	AP R760 6Ghz radio supports up to 30 <i>Microsoft Teams</i> calls, encompassing both voice and video, without any lag.

<b>Component/s</b>	AP
<b>Issue</b>	AP-26297
<b>Description</b>	AP R560 AP does not support 802.3az Energy Efficient Ethernet (EEE).

<b>Component/s</b>	AP
<b>Issue</b>	AP-28178

## Known Issues

### Limitations

Component/s	AP
Description	Dynamic PCAP functionality occasionally fails to generate PCAP files for client failure incidents on RUCKUS AI platform.

Component/s	AP
Issue	SCG-146726
Description	<b>BSI Compliance Mode Limitations</b> - The ECDSA (Elliptic Curve Digital Signature Algorithm) certificate issued by SmartZone has the following limitation: <ul style="list-style-type: none"><li>The communication between Access Points (APs) does not adhere to BSI compliance standards.</li></ul>

Component/s	AP
Issue	AP-26794
Description	The AP directs the client to transmit to the Service WLAN on the same radio when the client successfully passes through the intermediate WLAN, This behavior is a design limitation.
Workaround	To connect to the 6Ghz Service WLAN, the client needs to disconnect and reconnect after passing through the Service WLAN of the 2.4 or 5Ghz frequency bands.

Component/s	Switches
Issue	FI-280394
Description	In the event that SmartZone users add, modify, or delete a static route for an ICX Switch, the ICX Switch will not display the SmartZone username in its syslog entries.

Component/s	Switches
Issue	FI-273372
Description	If the ICX Switch platform 7750 has already been configured with port 1/2/1 set to breakout mode, the breakout port 1/2/1:1 might still retain its stack port configuration.

Component/s	UI/UX
Issue	SCG-151884
Description	Overall percentage of Airtime utilization pie-chart displays utilization more than 100% in some instances.

## Limitations

There are currently no immediate plans to address these issues in the short term.

Component/s	SmartCast
Issue	SCG-145743
Description	<ul style="list-style-type: none"><li>It is advised not to use iPerf 3 for AP (Access Point) QoS testing. Instead, it is recommended to utilize iPerf 2 for this purpose. The reason for avoiding iPerf 3 in AP QoS testing is that the initial packets transacted before the actual traffic starts are treated with best effort QoS. This leads to the fastpath being configured with an incorrect value, impacting subsequent QoS values. Using iPerf 2 is recommended to avoid this issue.</li><li>When a non-default AP management VLAN (VLAN greater than 1) is assigned to a WLAN, it may result in all traffic on that WLAN egressing with video priority.</li></ul>



## R770 Known Issues and Limitations

The following tables provides information on the known issues and limitation in the current release.

### Multi-Link Operation (MLO)

Component/s	AP
<b>Issue</b>	AP-27786, ACX-49444, SCG-146572
<b>Description</b>	Ping between wireless MLO to wired/wireless client including MLO may fails depending the primary link on which MLO client is associated. However, this does not impact the MLO wireless clients to browse the network or access the Internet.

Component/s	AP
<b>Issue</b>	SCG-146645
<b>Description</b>	The MQ Statistics API CLI provides insights into various metrics related to messaging queues. When querying MQ Statistics for an MLO Client, the counters may display as 0, indicating no impact on the MLO client's connectivity.

Component/s	AP
<b>Issue</b>	SCG-146759
<b>Description</b>	Occasionally, an issue arises where an AP utilizes a non-configured static channel after modifying the MLO Radio configuration on a WLAN from one radio combination to another.

Component/s	AP
<b>Issue</b>	SCG-146331
<b>Description</b>	Google Pixel 8 phone experiences connection failures when attempting to connect as an MLO client with a partner link on an MLO WLAN configured with Open+OWE security and utilizing both 2.4GHz and 5GHz frequencies for MLO.

Component/s	AP
<b>Issue</b>	SCG-146685
<b>Description</b>	When R770 MLO-2 2.4GHz and 5GHz active link is employed on both 2.4GHz and 5GHz bands, the single client OTA (Over-The-Air) downlink throughput on 5GHz is observed to be lower compared to the non-MLO 5GHz configuration.

Component/s	AP
<b>Issue</b>	SCG-146638
<b>Description</b>	Google Pixel 8 devices revert to connecting as non-MLO clients after a channel change on an MLO enabled WLAN which is configured to operate on both 2.4GHz and 5GHz frequencies.

Component/s	AP
<b>Issue</b>	SCG-146672
<b>Description</b>	The <b>Stats</b> command does not provide specific information regarding data transfer per link for MLO clients. Instead, it displays the overall data transfer for the client session, which is also reported in the controller user interface.

## Known Issues

### R770 Known Issues and Limitations

Component/s	AP
Issue	ACX-48543
Description	When a client is connected to an R770 Mesh AP, it may experience an inability to receive multicast traffic. This occurs when the R770 MAP (Mesh Access Point) is linked to an R770 RAP (Remote Access Point). However, this limitation is exclusive where the RAP is an R770 model. It does not occur when the RAP is a non Wi-Fi7 AP.

### Other Generic Issues

Component/s	AP
Issue	SCG-146513
Description	When there are over 50 MS Teams calls, users may encounter poor voice quality or Video lag with AP R770.

Component/s	AP
Issue	SCG-146070
Description	Uplink Multi-User MIMO (MU-MIMO) is enabled by default on R770 APs.  However, for an improved user experience with voice and video applications, it is recommended to disable UL MU-MIMO. Disable this feature through AP CLI by executing the command <code>set ul_mu_mimo wlanx 0</code> (where x in <code>wlanx</code> represents the WLAN ID).

Component/s	AP
Issue	ACX-49222
Description	The AP may randomly encounter target assert or reboot, when a large number of clients roam between two R770 APs.

Component/s	AP
Issue	AP-25334, SCG-146151, AP-26815
Description	Latency on R770 APs can spike when handling multiple clients, especially with <i>Best Effort</i> traffic. Latency may be randomly high on connecting Draeger M300 devices.

Component/s	AP
Issue	SCG-145095
Description	vRUE: Service validation is not supported.

Component/s	AP
Issue	AP-26421
Description	An association request is not triggered randomly by client.

Component/s	UI/UX
Issue	SCG-151651
Description	The controller web user interface intermittently fails to display an accurate client count and may also omit entries for connected clients. This is specific to R770 AP.

## Changed Behavior


The following are the changed behavior issues in this release.

The changes for this release include:

- Controller web user interface legacy menu is not supported.
- Wave-2 APs are not supported.
- Cellular configuration at the Zone Level is unavailable.
- WPA3 (Wi-Fi Protected Access 3) is the default encryption method for Wi-Fi7 APs.
- Channelfly is the default for all radios in R7.0.0, with channelization changing from 80MHz to 40MHz for auto mode.
- Wi-Fi7 APs do not support NSS (Network Subsystem) Offload.

Component/s	AP
Issue	SCG-146502
Description	In the SmartZone R7.0.0, L3ACL (Layer 3 Access Control List) takes precedence over Split Tunnel as part of the configuration.

Component/s	AP
Issue	SCG-151928
Description	For optimal performance when connecting a wired client to R560 or R760 or R770 APs, it is advisable to utilize either 802.3bt 5 or DC power. The usage of 802.3at power on these AP models results in the Eth0 port to disable.

Component/s	UI/UX
Issue	SCG-151881
Description	<p>In the controller web user interface, the following European Union (EU) countries indicate unsupported channels 149-161 (Ull-3 band) for 802.11ax APs, including models R560 and R760. Only the AP model R770 supports these channels.</p> <p> <b>WARNING</b> Attempting to configure these channels on the controller UI will result in AP configuration failures for all 11ax APs except R770.</p> <ul style="list-style-type: none"> <li>• Austria</li> <li>• Belgium, Bulgaria</li> <li>• Croatia, Cyprus, Czech Republic</li> <li>• Denmark</li> <li>• Estonia</li> <li>• Finland, France</li> <li>• Germany, Greece</li> <li>• Hungary</li> <li>• Iceland, Italy</li> <li>• Latvia, Luxembourg</li> <li>• Malta</li> <li>• Netherlands</li> <li>• Poland</li> <li>• Romania</li> <li>• Slovakia, Slovenia, Spain, Sweden, Switzerland</li> </ul>

## Interoperability Information

Component/s	UI/UX
Workaround	It is recommended to deploy R770 in a separate AP Zone if there are legacy 802.11ax APs coexisting in the same network.

# Interoperability Information

## Cluster Network Requirements

The following table lists the minimum network requirement for the controller's cluster interface.

### Minimum Cluster Network Requirement

Model	SZ300	vSZ-H	SZ144	SZ100	vSZ-E
Latency	68ms	42ms	93ms	229ms	229ms
Jitter	10ms	10ms	10ms	10ms	10ms
Bandwidth	115Mbps	92Mbps	40.25Mbps	23Mbps	23Mbps

## Client Interoperability

### NOTE

SmartZone controllers and ZoneFlex APs use standard protocols to interoperate with third-party Wi-Fi devices. RUCKUS qualifies its functionality on the most common clients.

### Access Points (APs)

The following are the Client Interoperability issues for APs.

Component/s	AP
Issue	AP-25118
Description	The client, aiming to execute Simultaneous Authentication of Equals (SAE) with Pairwise Master Key (PMK) caching, initiates the process by transmitting an authentication frame with the authentication algorithm set to open. The APs responds with an authentication response. Following this, the client submits a re-association request with the Authentication and Key Management (AKM) set to SAE, and it includes the previously derived PMKID.

Component/s	AP
Issue	SCG-145513
Description	Apple iPhone 15 using 17.0 through 17.3 iOS is not discovering 6Ghz networks as advertised in the co-located RnR (Reduced Neighbor Report) on the R560, R760 and R770 Access Points.

Component/s	AP
Issue	AP-26722
Description	Samsung Galaxy S23 <i>Ultra</i> is experiencing disconnection from the Access Point (AP) after roaming to AP2, and this issue is attributed to an EAPOL (Extensible Authentication Protocol over LAN) timeout.

<b>Component/s</b>	AP
<b>Issue</b>	AP-24759
<b>Description</b>	Windows 11 clients encounter difficulties in completing their 802.1x association with FreeRADIUS versions, specifically 3.0.15 and 3.0.16. However, this issue is resolved, and successful associations are observed when using FreeRADIUS versions 3.0.19 and 3.0.23.

<b>Component/s</b>	AP
<b>Issue</b>	AP-24727
<b>Description</b>	A known issue with Windows 11 involves PMK roaming using the 802.1x+WPA3 WLAN. The problem lies in the incorrect calculation of the PMKID provided during re-association, resulting in OKC (Opportunistic Key Caching) failure and necessitating a complete re-authentication.

<b>Component/s</b>	AP
<b>Issue</b>	AP-26796
<b>Description</b>	Clients that do not support WPA3 and send an Open authentication with SAE (Simultaneous Authentication of Equals) in the association request fail to connect to a WLAN in WPA2/WPA3 mixed mode.

<b>Component/s</b>	AP
<b>Issue</b>	SCG-146308
<b>Description</b>	Some Wi-Fi7 clients do not support 320Mhz and still connect with the AP as 160Mhz. Check the client capability before trying 320Mhz channel width.

<b>Component/s</b>	AP
<b>Issue</b>	AP-26727
<b>Description</b>	When WPA2-PSK (Wi-Fi Protected Access 2 - Pre-Shared Key) and 802.11r are enabled, the iPhone 11 device processes a full authentication during roaming. However, there are known issues where the iPhone 11 fails to send a reassociate request with FTIE (Fast Transition Information Element).

<b>Component/s</b>	AP
<b>Issue</b>	AP-26725
<b>Description</b>	<i>Samsung S23</i> device might not seamlessly transition (roam) to an R770 AP, even if the AP has a strong Received Signal Strength Indicator (RSSI) and sticky client feature enabled.
<b>Workaround</b>	It is recommended to enable sticky client steering to proactively force the roaming.

<b>Component/s</b>	AP
<b>Issue</b>	AP-26145
<b>Description</b>	<i>Samsung S24</i> devices experience connectivity issues when connecting to the networks using WPA3-AES encryption and often displays a password error prompt.
<b>Workaround</b>	Update the client driver.

<b>Component/s</b>	AP
<b>Issue</b>	AP-24355

**Interoperability Information**  
Client Interoperability

Component/s	AP
Description	Samsung Galaxy S21, does not support Fast Transition (FT) roaming with WPA3-SAE. It utilizes the Pairwise Master Key Security Association (PMKSA) when roaming back to a previously configured AP with WPA3-Personal.

Component/s	AP
Issue	SCG-140280
Description	The following devices fail to connect to WPA3-Enterprise networks with GCMP-256 bit encryption. <ul style="list-style-type: none"> <li>• Samsung Galaxy S21</li> <li>• Samsung Galaxy Z Fold4</li> <li>• Google Pixel 5</li> <li>• ASUS ROG</li> <li>• Mi 11 Ultra</li> </ul>

Component/s	AP
Issue	AP-24923
Description	Apple iPad 1 lacks support for mixed mode profiles, such as WPA2/WPA3 mixed and WPA/WPA2 mixed, resulting in connection failures when connecting to networks with these profiles.
Workaround	Avoid configuring mixed mode profile on Apple iPad 1.

Component/s	AP
Issue	AP-25255
Description	Chromebook devices experience random disconnections with reason code 4. This is a behavior observed most frequently during roaming.

Component/s	AP
Issue	SCG-141709
Description	Microsoft <i>Surface Pro 4</i> fails to roam to the target AP and instead performs a full authentication process.

Component/s	AP
Issue	AP-26791
Description	This issue occurs when the client fails to maintain DHCP, resulting in DSAE (Dynamic Simultaneous Authentication of Equals) being unable to set the binding entry at the DSAE module. This is a limitation from the client device.

Component/s	AP
Issue	SCG-140231

<b>Component/s</b>	AP
<b>Description</b>	<p>The following clients fail to connect to the profile with WPA2/WPA3 mixed mode and 802.11r is enabled.</p> <p>By default, PMF (Protected Management Frames) is enabled. When PMF is set to <i>capable</i>, the mentioned clients fail to connect. However, when PMF is set to <i>required</i>, the clients establish connections.</p> <ul style="list-style-type: none"> <li>• macOS Ventura (22D7750270d)</li> <li>• MacBook Air</li> <li>• macOS Catalina (19H2026)</li> </ul>

<b>Component/s</b>	AP
<b>Issue</b>	AP-24513
<b>Description</b>	Microsoft <i>Surface Pro 8</i> devices experience frequent disconnections from the AP, often with reason codes 1 (unspecified failure) or 7 (Class 3 frame received from nonassociated STA).

<b>Component/s</b>	AP
<b>Issue</b>	AP-27747
<b>Description</b>	When tested on 802.11ax APs, the device type for a OnePlus running Android 14 and an iPhone 13 is incorrectly identified as a tablet instead of a smartphone.

<b>Component/s</b>	AP
<b>Issue</b>	ACX-40890
<b>Description</b>	MacBooks running Big Sur 11.7.7 and macOS Monterey 12.6 see packet or ping loss when the 6GHz radio of the AP is active, and MacBooks are connected to the 5GHz radio of the AP. However, this issue is not observed with MacBooks running Monterey version 12.6.8 or Yosemite version 10.10.5.

### Dynamic Pre-Shared Key (DPSK3)

The following are the Client Interoperability issues for DPSK3.

<b>Component/s</b>	AP
<b>Issue</b>	AP-25946
<b>Description</b>	Due to the deployment limitations for 6GHz, it is necessary for the client to complete the binding process at the DPSK (Dynamic Pre-Shared Key) service first.

<b>Component/s</b>	AP
<b>Issue</b>	AP-25940, AP-25537
<b>Description</b>	In DPSK3 (DSAE), it is necessary for the client to establish connections with peer WLANs sequentially, starting from intermediate and then progressing to Service WLAN (designated workflow). If the client attempts to connect to the Service WLAN without following the designated workflow, they may encounter connection issues and may need to manually retry the connection.

<b>Component/s</b>	AP
<b>Issue</b>	AP-25897

**Interoperability Information**  
Client Interoperability

<b>Component/s</b>	AP
<b>Description</b>	Despite the caching of each PMK (Pairwise Master Keys) query result in the AP for 60 seconds, clients are still unable to connect even after changing to the correct password within that time frame.

<b>Component/s</b>	AP
<b>Issue</b>	AP-25372
<b>Description</b>	This is a limitation in the deployment of DPSK3. It is essential for the client to <b>follow the appropriate steps</b> to revert to the intermediate WLAN to initiate a reconnection.

<b>Component/s</b>	AP
<b>Issue</b>	AP-25292
<b>Description</b>	This is a design limitation inherent to DPSK3 (DSAE), particularly in relation to the behavior of Windows clients using Intel AX210 wireless cards. In the DPSK3 (DSAE) feature, the AP attempts to transition the client to the target WLAN, but there is no corresponding action from the client to initiate the connection flow.

<b>Component/s</b>	AP
<b>Issue</b>	AP-25194
<b>Description</b>	In the DPSK3 (DSAE) feature, the AP attempt to guide the client to transmit to the Service WLAN. However, the client's behavior does not correspond as expected.

<b>Component/s</b>	AP
<b>Issue</b>	AP-25075
<b>Description</b>	When a station (STA) utilizes the new password after the original binding is complete, the STA connects using WPA2-PSK (Wi-Fi Protected Access Pre-Shared Key) (Service WLAN) due to key rematching on the DPSK server.

<b>Component/s</b>	AP
<b>Issue</b>	AP-25007
<b>Description</b>	Due to deployment restrictions in the 6GHz spectrum, it is necessary for clients to initially complete the binding process at the DPSK Service on 2.4GHz or 5GHz.

<b>Component/s</b>	AP
<b>Issue</b>	AP-24958, AP-24637, AP-24329
<b>Description</b>	In the DPSK3 (DSAE) feature, the AP attempts to guide the client to transmit to the Service WLAN. However, the client's behavior does not correspond as expected, requiring a manual retry to connect to the SSID again.





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