RELEASE NOTES

RUCKUS SmartZone (ST-GA) Patch 2 Release Notes, 7.0.0

Supporting SmartZone R7.0.0 Patch 2

Part Number: 800-73688-001 Rev A
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

Document History

Revision Number	Summary of Changes	Publication Date
A	Initial *Release Notes*	28, August 2024

New Features in 7.0.0 Patch2

The following lists software features, modifications, and deprecated features in release 7.0.0 Patch2.

Hardware - New AP Models Supported

This section provides a high-level overview of key hardware models for which SmartZone release 7.0.0 Patch2 introduces support.

RUCKUS T670

This section provides a high-level overview of key features introduced in the AP T670 Firmware Release.

RUCKUS model T670 AP is a high-end outdoor Wi-Fi 7 IEEE (802.11be) tri-band concurrent access point that has the potential to support 6 spatial streams (2x2:2 in 2.4GHz/5GHz/6GHz or, in dual-band mode, 2x2:2 in 2.4GHz and 4x4:4 in 5GHz) with Multi-Link Operation (MLO), Preamble Puncturing, 4K QAM Modulation, and 320 MHz channels. It provides industry-leading performance in various environments with a combined data rate of 9.34 Gbps.

Furthermore, a 1/2.5/5Gbps Ethernet port eliminates the wired backhaul bottleneck, supporting connection to multi-gigabit switches and allowing full utilization of the available Wi-Fi capacity.

The T670 addresses the increasing client demands in transit hubs, stadiums, conference centers, and other high-traffic outdoor spaces. It is the perfect choice for data-intensive streaming multimedia applications like 4K/8K video transmissions, while supporting latency-sensitive voice and data applications with stringent quality-of-service requirements.

The T670, with built-in RUCKUS exclusive technology, dramatically improves network performance through a combination of patented wireless innovations and learning algorithms that includes:

- **Airtime Decongestion:** Increases average network throughput in heavily congested environments.
- **Transient Client management:** Reduces traffic interference from unconnected Wi-Fi devices.
- **BeamFlex® + Adaptive Antennas:** Extends coverage range and optimizes throughput with patented dynamic multi-directional antennas and radio patterns that work with any client.

Limitations

The SmartZone 7.0.0 Patch2 Beta 2 software release imposes the following limitations on the model T670 access point:

- MLO (Multi-Link Operation) is not supported.
- BSS Prioritization is not supported.
- For non-US countries, customers must use 2.4GHz-5GHz mode for the T670. The 2.4GHz-5GHz-6GHz band mode is exclusively for USA due to AFC support on the 6GHz band for the T670.
  - The 6GHz band is not supported.
    - Do not attempt to configure the AP to operate in 2.4GHz-5GHz-6GHz band mode. AP must operate only in 2.4GHz and 5GHz band combination.
    - Do not attempt to enable 6GHz Mesh, Automated Frequency Coordination (AFC), or MLO features on 6GHz.
- BeamFlex is not supported.

NOTE
Refer to the RUCKUS T670 Data Sheet https://www.ruckusnetworks.com/products/wireless-access-points/t670/, for a detailed description and specifications of this AP model.

RUCKUS T670 Power Modes

Refer to the following table for power modes supported.

TABLE 1 RUCKUS T670 Power Modes

Power Mode	PowerSource	2GHz- 5GHz-6GHz chains (Tx/Rx)	2GHz- 5GHz-6GHz Tx Power (dBm) per chain	5GE Ethernet	1GE Ethernet	GPS
Full Power	DC	**2/2/2** **2/4/0**	**22/22/22** **22/22/--**	**Yes** **Yes**	**Yes** **Yes**	**Yes** **Yes**
	4-pairPoE Switch (802.3bt**5**) or 4-pairPoE Injector	**2/2/2** **2/4/0**	**22/22/22** **22/22/--**	**Yes** **Yes**	**Yes** **Yes**	**Yes** **Yes**
PoE 802.3at	2-pairPoE Switch or 2-pairPoE Injector	**2/2/2** **2/4/0**	**19/20/20** **20/21/--**	**Yes** **Yes**	**Yes** **Yes**	**Yes** **Yes**

RUCKUS R670

SmartZone release 7.0.0 Patch2 adds support for AP model T670. This section provides a high-level overview of key features supported on AP model R670.

The RUCKUS model R670 AP is a mid-range Wi-Fi 7, tri-band concurrent indoor AP that has the potential to support 6 spatial streams (2x2:2 in 2.4GHz/5GHz/6GHz or, in dual-band mode, 2x2:2 in 2.4GHz and 4x4:4 in 5GHz) with Multi-Link-Operation (MLO), Preamble Puncturing, 4K QAM Modulation, and 320 MHz channels. It delivers industry-leading performance environments with a combined data rate of 9.34 Gbps.

Furthermore, a 1/2.5/5Gbps Ethernet port eliminates the wired backhaul bottleneck, supporting connection to multi-gigabit switches and allowing full utilization of the available Wi-Fi capacity.

Wireless requirements within enterprises are expanding beyond Wi-Fi. The R670 has one built-in IoT radio offering onboard BLE or Zigbee capabilities. The R670 is a converged access point that allows customers to seamlessly integrate any new wireless technologies with the USB port.

The R670 expands the reach of Wi-Fi 7 and addresses the needs of everyday deployments, in guest rooms, classrooms, hotel rooms, and lobby. It supports data-intensive streaming applications like 4K/8K video transmissions, while supporting latency-sensitive voice and data applications with stringent quality-of-service requirements.

The R670, with built-in RUCKUS exclusive technology, dramatically improves network performance through a combination of patented wireless innovations and learning algorithms that includes:

- **Airtime Decongestion:** Increases average network throughput in heavily congested environments.
- **Transient Client management:** Reduces traffic interference from unconnected Wi-Fi devices.
- **BeamFlex® + Adaptive Antennas:** Extends coverage range and optimizes throughput withpatented dynamic multi-directional antennas and radio patterns that work with any client.

Limitations

The SmartZone 7.0.0 Patch2 software release imposes the following limitations on the model R670 access point:

- MLO (Multi-Link Operation) is not supported.

- BSS Prioritization is not supported.
  - The 6GHz band is not supported.
    - › Do not attempt to configure the AP to operate in 2.4GHz-5GHz-6GHz band mode. AP must operate only in 2.4GHz and 5GHz band combination.
    - › Do not attempt to enable 6G Mesh, Automated Frequency Coordination (AFC), or MLO features on 6GHz.
- BeamFlex is not supported.
- USB port is not working on R670.

NOTE
Refer to the RUCKUS R670 Data Sheet https://www.ruckusnetworks.com/products/wireless-access-points/r670/, for a detailed description and specifications of this AP model.

RUCKUS R670 Power Modes

Refer to the following table for power modes supported.

TABLE 2 R670 Power Modes

Power Mode	PowerSource	2GHz- 5GHz-6GHz chains (Tx/Rx)	2GHz- 5GHz-6GHz Tx Power (dBm) per chain	5GE Ethernet	1GE Ethernet	USB 3.0W	IoT
Full Power	DC	2/2/2 2/4/0	22/22/22 22/22/--	Yes Yes	Yes Yes	Yes Yes	Yes Yes
	4-pairPoE Switch (802.3bt5) or 4-pairPoE Injector	2/2/2 2/4/0	22/22/22 22/22/--	Yes Yes	Yes Yes	Yes Yes	Yes Yes
PoE 802.3at	2-pairPoE Switch or 2-pairPoE Injector	2/2/2 2/4/0	20/20/21 21/21/--	Yes Yes	Yes Yes	No No	Yes Yes

RUCKUS Standard AP LED Description for Wi-Fi 7 Capable APs

The specified LED states for Wi-Fi 7 capable APs are outlined as follows. The LED 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.

TABLE 3 LED Color, Description, and Patterns

LED Color	Description	Light Pattern
Red	AP is in the process of determining its power mode.	Solid Red
	AP is currently operating in IEEE 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 a firmware or configuration update.	Fast Blinking Amber

TABLE 3 LED Color, Description, and Patterns (continued)

LED Color	Description	Light Pattern
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.	
	The WLAN on the AP has at least one client connected, and mesh networking is enabled.	

New Software Features

This section describes the new and enhanced software features introduced in the SmartZone 7.0.0 base release and all subsequent 7.0.0 release updates and patches.

Release SmartZone 7.0.0 Patch 2

Feature	Description
6GHz Outdoor and Indoor Channel Range Separation	The capability to distinguish which channels can be designated for 6GHz outdoor use versus 6GHz indoor use on a per-channel basis.
Cybersecurity Enhancement	New security enhancements in the controller web user interface and CLI now require stronger passwords to prevent unauthorized users from accessing the AP using weak passwords.
Fast Session Transition (FST)	The Fast Session Transition feature reduces the central burden on the controller and enhances roaming performance. It allows access points (APs) to efficiently fetch client session information from the previously connected AP during active Wi-Fi roaming, instead of relying on the controller. This feature is enabled by default and is compatible with all roaming methods, including 802.11r.

Release SmartZone 7.0.0 Patch 1 - AFC Enabled New Feature List

Feature	Description
Automated Frequency Coordination (AFC)	Automated Frequency Coordination (AFC) is a technology enabling Wi-Fi to function within the frequency spectrum shared by licensed users, particularly within the 5.925–6.425 GHz (U-NII-5) and 6.525–6.875 GHz (U-NII-7) frequency ranges. AFC facilitates the dynamic management and allocation of frequencies, enabling Wi-Fi operation in the 6 GHz band while significantly reducing interference with licensed users. Refer to the *Automated Frequency Coordination (AFC) Support on RUCKUS Wi-Fi Network Devices User Guide* [Part number: 800-73572-001 Rev A] for details.

Release SmartZone 7.0.0 New Feature and Enhanced List

Feature	Description
320 MHz Bandwidth Support	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.
AP File System Enhancements	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.

Feature	Description
AP Automatically Calls Home to its Original Cluster in Active-Active Redundancy Configuration	This feature permits an AP to autonomously revert to a designated *Home Cluster* at specified intervals within Active-Active Cluster Redundancy configurations.
RUCKUS AI Branding Change	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.
AP Containerization	Enables dynamic containerization allows for a significant reduction in AP firmware size, decreasing it from 83 MB to 48 MB.
Add iPerf server/client in the AP CLI	The iPerf utility is embedded in the AP Command Line Interface to conveniently run performance tests that help in debugging and serviceability.
Backup and Recovery Events for RNCSS	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.
BSS Priority Tooltip	This feature includes two settings that allow users to configure the priority. • **LOW** - The LOW setting diminishes the WLAN's priority by restricting throughput for all clients linked to this WLAN. • **HIGH** - In contrast, the HIGH setting imposes no limitations on throughput. The default configuration establishes WLAN priority at HIGH.
Client Certificate Supports Certificate Authority Chains	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.
Chatbot Enhancement	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.
ChannelFly and 40 Mhz Channelization as Default	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.
Client roaming with AVC information	Enhancements to better manage traffic between roaming clients and APs.
RUCKUS Dynamic Pre-Shared Key (DPSK3)	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.
Enhancement in AF Power AP Detection	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.
Enhancement to Device Policy OS Vendors	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.

Feature	Description
Enhancement to the upgrade notification	Enhancement of the upgrade notification to clearly inform users that downgrading the SmartZone will result in the removal of the current configuration.
External DPSK Without Proxy Mode	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.
IEEE 802.11mc	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.
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.
Multi-Link Operation (MLO)	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.
Option to Disable Wi-Fi 7	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.
Preamble Puncturing	In Wi-Fi 7, *Preamble Puncturing* 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 *Preamble Puncturing* 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.
Qosmos (Quality of Service) Signature Package support for OpenWRT AP	In SmartZone release 5.1.0, RUCKUS introduced Qosmos as the AP DPI solution to replace Trendmicro. RUCKUS OpenWRT APs are now capable of supporting *Qosmos Signature Package*.
QoS (Quality of Service) Mirroring	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.
Secure Boot Support in Wi-Fi 7	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.

Feature	Description
Single LED requirements	A unified LED model that displays the most pertinent status on operation of the AP.
Support for Certificates with ECDSA-P256 and RSA-3072	This feature provides support for certificates ECDSA-P256 and RSA-3072, catering to customers with elevated security requirements for their certificates.
Switch Management	• **Breakout Port Support** - SmartZone release 7.0.0 introduces the ability edit the settings of existing breakout ports on ICX switches. Enabling breakout mode is not supported and needs to be enabled through CLI configuration. • **Enhancement in Firmware Upgrade Status** - Added additional statuses for better visibility into the firmware upgrade progress. • **SmartZone Usernames in ICX Syslog** - Added support to display SmartZone username in Switch Syslog messages that involve changes made from SmartZone. • **Configuring Separate Authentication and Accounting in AAA Server** - Provides an option to define separate Authentication and Accounting AAA servers under Switch group AAA configuration.
UX Analytics Data Collection Caption	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.
UI/UX Configuration for Client Load Balancing	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 *sticky* 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.
URL Redirect and ACL defined by RADIUS	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 *Ruckus-External-URL* is added for this feature.
WPA3 on SmartMesh	Utilizing WPA3 encryption on RUCKUS Wireless SmartMesh feature.
Deprecated Features	From this release: • The option to toggle back to the legacy version of the SmartZone GUI is discontinued. • 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.

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 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 Patch2 release for users utilizing Wi-Fi7 APs. For those with legacy APs, that are not End-of-Support (EOS), 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.

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 and R7.0.0 Patch1 and Patch2. Refer to the *RUCKUS IoT 2.2.0.0 GA Release Notes* for the hardware and software support details.

SZ300

- Controller Version: **7.0.0.0.956**
- Control Plane Software Version: **7.0.0.0.864**
- Data Plane Software Version: **7.0.0.0.956**
- AP Firmware Version: **7.0.0.0.6365**

SZ144

- Controller Version: **7.0.0.0.956**
- Control Plane Software Version: **7.0.0.0.864**
- Data Plane Software Version: **7.0.0.0.829**
- AP Firmware Version: **7.0.0.0.6365**

vSZ-H and vSZ-E

- Controller Version: **7.0.0.0.956**
- Control Plane Software Version: **7.0.0.0.864**
- AP Firmware Version: **7.0.0.0.6365**

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

- Data plane software version: **7.0.0.0.956**

Upgrade Information

Upgrade to R7.0.0 is available for users currently on SmartZone release versions 6.1, 6.1.1, and 6.1.2. Versions preceding R6.1.0 are not supported for an upgrade to R7.0.0.

Fresh installation is supported.

Following SmartZone upgrade paths are supported

- Release 6.1.2 Patch2 to Release 7.0.0 Patch2
- Release 7.0.0 GA to Release 7.0.0 Patch2

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 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 4 Supported AP Models

11ax	
Indoor	**Outdoor**
R850	T750SE
R770	T750
R760	T670
R750	T350C
R670	T350SE
R650	T350D
R560	
R550	
R350	
R350e	
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 5 Supported AP Models for AP Zones Using Older AP Versions

11ax	11ac-Wave2	
NOTE Supported on R6.1.0, 6.1.1, and 6.1.2.	**Indoor**	**Outdoor**
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 6 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 7 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 8 ICX and SmartZone Release Compatibility Matrix

	SmartZone 5.1[1]	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[1]	No	No	No	No	No	No	No	No
FastIron 08.0.90a	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No
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 9 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

[1] Does not support ICX configuration.

TABLE 9 Switch Management Feature Compatibility Matrix (continued)

Feature	SmartZone Release	ICX FastIron Release
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
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[2]	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[3]
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

[2] To download system logs from SmartZone for a particular ICX switch, TFTP must be enabled.
[3] FastIron 10.0.00 and later releases do not support management VLANs.

TABLE 9 Switch Management Feature Compatibility Matrix (continued)

Feature	SmartZone Release	ICX FastIron Release
Flexible Authentication Configuration	6.1 and later	09.0.10a and later
Network Segmentation	6.1.1 and later	09.0.10d and later[4]
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

Product Documentation

The following product guide is updated for *R7.0.0 Patch2* . Refer to the *New In This Document* section in the publication for detailed changes.

Product Documentation Resources

Along with the guide mentioned below, do refer to the product guides updated for version 7.0.0, available on the RUCKUS support portal https://support.ruckuswireless.com/documents or the CommScope content portal https://docs.commscope.com/. On the support portal 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.

TABLE 10 Updated Product Guides

Category	Name of The Guide
User and Administrator Guides	*RUCKUS SmartZone (ST-GA) Network Administration Guide, 7.0.0* [800-73597-001 Rev B]. This guide has been updated to include 6 GHz outdoor and indoor channel range separation as well as cybersecurity enhancements.

Known Issues

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

Known Issues in R7.0.0 Patch2

Following are the known issues in this release.

Component/s	AP
Issue	SCG-151928
Description	It is recommended to use 802.3bt or DC (direct current) power for the R560, R760, and R770 APs when connecting a wired client to the AP. Using 802.3at power on the R560, R760, or R770 will disable the Ethernet 0 port.

[4] As an exception, FastIron release 10.0.00 does not support this feature.

Component/s	AP
Issue	AP-33568
Description	T670 and R670 APs do not support thermal throttling mechanism.

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	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: • 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). • The default interval in LLDP 1.0.15 is set to 30 seconds. Following are the TTL examples in LLDP 1.0.15. I. • If hold time is set to 10 seconds, TTL is calculated as 30 * 10 = 300 seconds. • If hold time is set to 200 seconds, TTL is calculated as 30 * 200 = 6,000 seconds. • If hold time is set to 500 seconds, TTL is calculated as 30 * 500 = 15,000 seconds. • If hold time is set to 1000 seconds, TTL is calculated as 30 * 1000 = 30,000 seconds.

Component/s	AP
Issue	AP-26728
Description	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. 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. 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.

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	SCG-141990
Description	The CLI command **get mode wlanx** does not accurately reflect the current operating mode of the WLAN.

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 *IGMP_MEMBERSHIP_REPORT* and *IGMP_HOST_LEAVE*, are recognized as known multicast traffic, leading to potential rate limitations.

Component/s	AP
Issue	AP-19942
Description	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.
Workaround	It is recommended to deploy multiple WLANs or VAPs.

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

Component/s	AP
Issue	SCG-146726
Description	**BSI Compliance Mode Limitations** - The ECDSA (Elliptic Curve Digital Signature Algorithm) certificate issued by SmartZone has the following limitation: • The communication between Access Points (APs) does not adhere to BSI compliance standards.

Component/s	AP
Issue	AP-32827, AP-34197
Description	Downlink performance with RUCKUS GRE and SoftGRE may be slightly lower compared to uplink performance for APs R670 or T670.

Component/s	AP
Issue	AP-33444
Description	Under heavy load conditions with Intel BE200 clients on the network, performance is lower compared to Wi-Fi 6E clients.

Component/s	AP
Issue	AP-34372
Description	Repeated speed tests on Wi-Fi 7 APs may result in inconsistent uplink and downlink performance.

Component/s	AP
Issue	SCG-143239
Description	The performance of the 6GHz radio on the AP R560 or R760 decreases under heavy load conditions, particularly when Wi-Fi 6E clients are connected.

Component/s	AP
Issue	AP-32531
Description	Performance may drop in certain conditions when a mix of scaled 802.11ac and 802.11ax clients connect to a Wi-Fi 7 AP.

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

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

Component/s	AP
Issue	AP-33930
Description	Bidirectional performance with LBO (Low Bandwidth Operation) may be slightly lower compared to uplink or downlink performance for the R670.

Component/s	AP
Issue	AP-31501
Description	When applying back-to-back channel or channel bandwidth configurations from the controller web interface, some blacklisted channels, such as 149 - 161, are enabled on the AP. This issue is specific to APs configured for 80MHz channelization and the upper band of 5GHz.
Workaround	Reapply the configuration from the web interface to ensure that only the channels enabled in the UI are applied to the AP.

Component/s	AP
Issue	AP-32474, AP-32965
Description	The available channel list on the AP operating in Norway does not include Channel 157 for Wi-Fi 6E.

Component/s	AP
Issue	AP-34081, AP-34080, AP-34078
Description	In the controller web interface, there is a minor cosmetic issue where UNII-3 channels are marked as non-DFS for the following countries: AR (Argentina), NZ (New Zealand), and AU (Australia).

Component/s	AP
Issue	AP-32736
Description	In the controller web interface, there is a minor cosmetic issue where Channels 52–64 are marked as DFS for Hong Kong, but the AP considers them to be non-DFS.

Component/s	AP
Issue	AP-32811
Description	Channel 165 is accessible in the controller web interface when the AP Zone is configured with Israel as the country and CW (Channel Width) as 40/80MHz. Channel 165 should only be used with 20MHz channelization.

Component/s	AP
Issue	AP-32876, AP-33066, AP-33108, and AP-30095, AP-32161, AP-32939
Description	In the controller web user interface, the following countries have unsupported channels. Attempting to configure these channels on the controller UI will result in AP configuration failures for APs. • **Mexico:** Channels 124-128 are unsupported in the Web UI **[AP-32876]**. • **UAE:** Channels 36-64 are unsupported for the Outdoor T750 AP, even though *Allow Indoor channels* is disabled. **[AP-33066]**. • **Zimbabwe and France:** Channels 149-161 are unsupported in the Web UI. **[AP-33108]** • **Germany:** Channel 149 is unsupported for 802.11ax APs, including Wi-Fi 6E and Wi-Fi 7. **[AP-30095, AP-32161, AP-32939]**.

Component/s	AP
Issue	AP-34218
Description	Channels 100-140 are blocked for Nepal (NP), and channels 149-165 are blocked for Egypt (EG). This issue is specific to the R670 AP model.

Component/s	AP
Issue	AP-34348
Description	Channels 149-161 are blocked for Iceland. This issue is specific to APs R670 and T670 configured in 2GHz-5GHz mode.

Component/s	AP
Issue	SCG-157756
Description	Channels 169 and 173 at 20MHz cannot be enabled by the user in the controller web user interface for Germany. This issue is specific to the T670 AP.

Component/s	AP
Issue	AP-31384
Description	The BSS Priority feature does not function correctly with Wi-Fi 6E and Wi-Fi 7 APs. Due to this bug, all clients will receive the same airtime and performance, regardless of the configured BSS Priority.

Component/s	AP
Issue	AP-33056
Description	This is an issue specific to channel 52 where an AP operating on this channel fails to switch to a new channel when radar is detected. This problem affects both Wi-Fi 6E and Wi-Fi 7 APs.

Component/s	AP
Issue	AP-33145

Component/s	AP
Description	The AeroScout Wi-Fi 6E and Wi-Fi 7 APs are unable to send Tag reports.

Component/s	AP
Issue	AP-33800
Description	In high-density environments, an AP can store up to 20 neighbor entries in the NBRD (Neighbor Discovery) peer list. This limitation has been consistent across all APs and is considered a legacy behavior.

Component/s	AP
Issue	SCG-159467
Description	Rate limiting fails to occur when sending traffic from a wired client connected to a RAP (Remote Access Point) to a wireless client on a Mesh AP. This issue is specific to Wi-Fi 7 AP models.

Component/s	AP
Issue	AP-32006
Description	Apple devices are experiencing random client authentication failures with reason code 3 and unspecified reason when connected to WPA2/WPA3 mixed mode. This behavior is not observed with all Apple devices and does not occur with WPA2-only or WPA3-only configurations..

Component/s	AP
Issue	AP-33344
Description	Random client disconnects with reason code 4 (Client inactivity) are observed and specific to Wi-Fi 7 APs.

Component/s	AP
Issue	AP-32542, ACX-48775
Description	Random client roaming failures due to *Invalid FTIE*(Fast Transition Information Element) are observed when the AP is configured with WPA2/WPA3 mixed mode and 802.11r enabled. This behavior is not observed with WPA2 or WPA3 configurations.

Component/s	AP
Issue	AP-33958
Description	Random client roaming failures are observed after roaming to the target AP, with clients being de-authenticated by the source AP with reason code 8.

Component/s	AP
Issue	AP-32729
Description	When radar is detected on a Mesh AP, the MAP (Mesh AP) switches to a new available channel, but the root AP does not follow the same channel as the MAP. During this process, the AP may experience a kernel panic. This limitation is specific to Wi-Fi 7 APs.

Component/s	AP
Issue	AP-31597, AP-30539

Component/s	AP
Description	The Location Based Service (LBS) functionality will not work on T670 and R670 AP models.

Component/s	AP
Issue	SCG-159180
Description	RTS (Request to Send) data rates in 5GHz WLAN fails to adhere to to the configured BSS minimum rate when the minimum rate is set from the unsupported rate (5.5 Mbps) to supported rates (12/24 Mbps) with *OFDM_ONLY* disabled.

Component/s	AP
Issue	AP-33380
Description	Under certain environmental conditions, the Tx power of R670 for the following countries shows discrepancies for 5GHz and 6GHz: • AE: United Arab Emirates • AU: Australia • CA: Canada • CO: Colombia • CL: Chile • CR: Costa Rica • GB: United Kingdom • HK: Hong Kong • LI: Liechtenstein • MY: Malaysia • PE: Peru • SA: Saudi Arabia

Component/s	AP
Issue	AP-34259
Description	Random kernel panics are observed in high-density environments when a large number of clients roam across Wi-Fi 7 APs.

Component/s	AP
Issue	AP-31322
Description	The AP may encounter a target assert error when collecting Wi-Fi statistics frequently from AP CLI. During the debugging process, it is recommended to provide adequate delay between each iteration for statistics collection.
Workaround	It is recommended to provide adequate delay between each iteration for statistics collection.

Component/s	AP
Issue	AP-32049
Description	The AP may randomly encounter a target assert error under heavy load conditions.

Component/s	AP
Issue	SCG-151928
Description	Using 802.3at power on R560, R760, and R770 APs disables the Ethernet 0 port.

Component/s	AP
Workaround	It is recommended to use 802.3bt Type 5 or DC power for the R560, R760, and R770 APs when connecting a wired client to the Ethernet port of the AP.

Component/s	AP
Issue	AP-33920
Description	During bootup, the R670 requests 25.5W of power from the Switch, and after bootup, it requests 25W. This change in power consumption can cause a reset in power mode, potentially leading to connectivity loss for connected clients. This issue occurs randomly and is not specific to any particular switch model.

Component/s	AP
Issue	SCG-157670
Description	Zero Touch Mesh discovery does not work with the default AP T670 or R670 solo build.

Component/s	AP
Issue	AP-32419
Description	The downlink performance of R670 with 320MHz is slightly lower compared to the R770 performance.

Component/s	AFC
Description	When using AFC (Automated Frequency Coordination), the APs transmit power is capped by both Power Spectral Density (PSD) and Maximum EIRP (Effective Isotropic Radiated Power), using the lower of the two values. In some cases, the AP may assign Low Power (LP) in the U-NII-5 and U-NII-7 bands due to the Maximum EIRP returned in the AFC response. The Web UI displays LP instead of Standard Power (SP), which is normal under these conditions.

Component/s	AFC
Issue	AP-32419
Description	AP R670 operates in low power indoor mode on channel 53, while AP R770 operates at standard power on the same channel. Make sure to collect the support log before rebooting the AP.

Component/s	AFC
Issue	AP-34738
Description	During the upgrade process, the AP may go offline and recover within two hours. The recovery time depends on the *Reboot AP if it cannot reach the controller after* setting in the AP Zone configuration. This issue is inconsistent and occurs randomly.
Workaround	Reboot the AP if the AP stays offline for a longer duration.

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

Component/s	Switches
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.

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
Issue	SCG-146645
Description	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
Issue	SCG-146331
Description	*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
Issue	SCG-146672
Description	The **Stats** 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.

Component/s	AP
Issue	SCG-146685
Description	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
Issue	AP-33486
Description	Clients may randomly fail to reconnect to the AP when using MLO (Multi-Link Operation) in 5GHz with 6G mode.

Component/s	AP
Issue	AP-33853, AP-33854
Description	A random target assert was observed when a MLO client disconnects from an OWE WLAN and connects to a new SSID with WPA3-SAE.

Component/s	AP
Issue	AP-31726
Description	MLO is not supported on mesh-enabled APs in this release.

Component/s	UI/UX
Issue	SCG-159070
Description	In the controller web interface, there is a cosmetic issue where the Tx MCS (Modulation and Coding Scheme) and Rx MCS for Clients appear the same for both 2.4GHz and 5GHz links. This is a UI issue and does not affect performance.

Limitations

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

Component/s	SmartCast
Issue	SCG-145743
Description	• It is advised not to use iPerf 3 for Access Point (AP) 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. • 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.

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.

The following are the Client Interoperability issues.

Component/s	AP
Issue	AP-34359
Description	A device equipped with the Qualcomm FastConnect 7800 Wi-Fi 7 chip and running driver version 3.1.0.1238 is unable to associate with the 6GHz radio on the R770 AP. This issue occurs specifically when the AP is configured for Australia.

Component/s	AP
Issue	AP-33390, SCG-146331
Description	Enabling MLO (Multi-Link Operation) with 802.11x is not recommended until all client vendors officially support 802.11x with MLO, due to limitations and inconsistent behavior across various vendors, such as Samsung S24, Pixel, and Windows. This limitation does not apply to WPA3-SAE WLAN.

Component/s	AP
Issue	AP-27747
Description	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.

Resolved Issues

This section details the issues that have been resolved for this release.

The tables below list the resolved issues in SmartZone Release 7.0.0 Patch 2.

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

Component/s	AP
Issue	AP-27922
Description	Beacon protection was not enabled in MLO WLAN.

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

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

Component/s	**AP**
Issue	ER-13286
Description	An unexpected Client inactivity timeout issue on the 802.11ax driver.

Component/s	AP
Issue	ER-13301
Description	The AP device name was set from DHCP Option 12, even though it was disabled when connected to the controller.

Resolved Issues

Issues Resolved in SmartZone Release 7.0.0 Patch 2

Component/s	AP
Issue	ER-13350
Description	Client connection failure in MAC authentication and PSK (Pre-Shared Key) WLAN caused by an additional WPA 4-way handshake which occurred after a successful authentication.

Component/s	AP
Issue	ER-13478
Description	AP configuration generation could fail if the WLAN group contained non-existing WLAN members.

Component/s	AP
Issue	ER-13501
Description	APs R350 or H350 or H550 sent training packets on 2.4GHz, causing a high TX airtime.

Component/s	AP
Issue	ER-13517
Description	SmartRoam failures were incorrectly reported as TCM failures. The reason code is updated to **Drop by SmartRoam**.

Component/s	AP
Issue	ER-13571
Description	AP SSH tunnel failure when changing the SSH port number.

Component/s	AP
Issue	ER-13806
Description	802.11be AP kernel panic and reboot was caused by an invalid AP neighbor report.

Component/s	Control Plane
Issue	ER-13188
Description	Firmware version validation was added when configuring the encrypted type through public IP addressess.

Component/s	Data Plane
Issue	ER-13386
Description	Increased the pool usage threshold to prevent data plane from dropping multicast packets.

Component/s	Data Plane
Issue	ER-13593
Description	Data plane IP address changed after a reboot.

Component/s	Data Plane
Issue	ER-13565

Component/s	Data Plane
Description	Continuous IP address and routing table refreshes in data plane.

Component/s	RUCKUS One
Issue	ER-13484
Description	Resolved an issue of incorrect SSID name on the *Incident* page.

Component/s	RUCKUS One
Issue	ER-13430
Description	Resolved a high CPU issue caused by CPD (Control Plane Daemon) being stuck in the run state.

Component/s	RUCKUS One
Issue	ER-13611
Description	Incorrect RADIUS server failurs were reported on RUCKUS One.

Component/s	RUCKUS One
Issue	ER-13634
Description	2.4GHz channel seen on RUCKUS One web user interface though the 2.4GHz radio channel was disabled.

Component/s	RUCKUS One
Issue	ER-13701
Description	AP CLI command **get mcsrate** failed to display the current TX MCS (Transmit Modulation and Coding Scheme).

Component/s	RUCKUS One
Issue	ER-13703
Description	AP Tx bandwidth was stuck at 20MHz, even when the AP bandwidth was assigned as 40MHz.

Component/s	RUCKUS One
Issue	ER-13712
Description	AP could not recover to the previous channel width after radar detection and clearing on DFS channels.

Component/s	RUCKUS One
Issue	ER-13734
Description	It is recommended to apply FCC rules for radar detection with Hong Kong country code, so that UNI-III channels will not be treated as DFS channels.

Component/s	RUCKUS One
Issue	ER-13740
Description	Resolved a kernel panic issue in 802.11ax monitor function.

Component/s	RUCKUS One
Issue	ER-13741
Description	Resolved a kernel panic issue caused by a malformed *mDNS* packet.

Component/s	RUCKUS One
Issue	ER-13744
Description	Resolved a kernel panic issue occurred during Wi-Fi target recovery.

Component/s	System
Issue	ER-13286
Description	Resolved race condition issue in the NAT (Network Address Translation) table.

Component/s	System
Issue	ER-13302
Description	In the customer-uploaded Guest Pass HTML template, added a new variable, *GP_LOGO_BASE64*, to include the base64 string of the customer-uploaded Guest Portal logo.

Component/s	System
Issue	ER-13400
Description	The domain name in the query in AP API was incorrect.

Component/s	System
Issue	ER-13403
Description	Resolved an issue where saving the variable *ueMac* for Group DPSK resulted in an error.

Component/s	System
Issue	ER-13432
Description	Upgrade failed due to an odd-numbered serial.

Component/s	System
Issue	ER-13492
Description	Dynamic VLAN (AAA override) setting for Hotspot WLANs with MAC address authentication was consistently disabled when using the controller patch WLAN API.

Component/s	System
Issue	ER-13574
Description	Resolved an issue where when updating AP configuration through the Public API could cause erase the AP name.

R770 Resolved Issues for SmartZone Release 7.0.0 Patch 2

The tables below lists the resolved issues in SmartZone Release 7.0.0 Patch 2.

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

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

Component/s	AP
Issue	ACX-48543
Description	When a client was connected to an R770 Mesh AP, it experienced failed to receive multicast traffic.

Component/s	AP
Issue	SCG-146638
Description	*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	UI/UX
Issue	SCG-151651
Description	The controller web user interface intermittently failed to display an accurate client count and omitted entries for connected clients. This was specific to R770 AP.

Other Generic Issues

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

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**	**vSZ-E**
Latency	68ms	42ms	93ms	229ms
Jitter	10ms	10ms	10ms	10ms

	Model			
	SZ300	**vSZ-H**	**SZ144**	**vSZ-E**
Bandwidth	115Mbps	92Mbps	40.25Mbps	23Mbps

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