RELEASE NOTES

RUCKUS SmartZone (ST-GA) Patch 6 Release Notes, 7.0.0

Supporting SmartZone R7.0.0 Patch 6

Part Number: 800-73623-001 Rev A
Publication Date: November 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*	November 27, 2024

New Feature

This section describes the new and enhanced features.

Feature	Description
AP R760	AP R760 is now Federal Communications Commission (FCC) certified for operation with Automated Frequency Coordination (AFC).

Countries Supported on 6GHz

Wi-Fi 7 APs and the 320MHz channel is supported in controller version R7.0.0 and its subsequent patches for the following country codes.

The following country codes are included in this patch release:

- IE (Ireland)
- KE (Kenya)
- MO (Macau)
- MA (Morocco)
- TW (Taiwan)
- TR (Turkey)

1. Countries supported on 6Ghz U-NII frequency bands 5, 6, 7, and 8 supporting channels: 1, 5, ..., 233:
    - BR: Brazil
    - CA: Canada
    - CL: Chile
    - CO: Colombia
    - DO: Dominican Republic
    - HN: Honduras
    - KR: South Korea
    - PE: Peru
    - PG: Papua New Guinea
    - SA: Saudi Arabia
    - SV: El Salvador
    - US: United States
2. Countries supported on 6Ghz U-NII frequency band 5 supporting channels: 1, 5, ..., 93:
    - AE: United Arab Emirates
    - AL: Albania

- AT: Austria
- AU: Australia
- AZ: Azerbaijan
- BE: Belgium
- BH: Bahrain
- BG: Bulgaria
- BN: Brunei
- BZ: Belize
- BY: Belarus
- CH: Switzerland
- CY: Cyprus
- CZ: Czech Republic
- DE: Germany
- DK: Denmark
- EE: Estonia
- EH: Western Sahara
- ES: Spain
- FI: Finland
- FR: France
- GB: United Kingdom
- GR: Greece
- HK: Hong Kong
- HR: Croatia
- HU: Hungary
- IE: Ireland
- IL: Israel
- IS: Iceland
- IT: Italy
- JO: Jordan
- JP: Japan
- KE: Kenya
- KW: Kuwait
- LI: Liechtenstein
- LT: Lithuania
- LU: Luxembourg
- LV: Latvia
- MA: Morocco
- MC: Monaco
- MN: Mongolia

- MO: Macau
- MT: Malta
- MU: Mauritius
- MX: Mexico
- MY: Malaysia
- NL: Netherlands
- NO: Norway
- PL: Poland
- PT: Portugal
- QA: Qatar
- RO: Romania
- RU: Russia
- SE: Sweden
- SG: Singapore
- SI: Slovenia
- SK: Slovakia
- TH: Thailand
- TR: Turkey
- TW: Taiwan
- ZM: Zambia
- ZA: South Africa
- 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 Providers 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 Virtual SmartZone (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 an 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 the SmartZone R7.0.0 Patch 6 release for users of Wi-Fi 7 APs. For users with legacy APs that are not End-of-Support (EOS), RUCKUS suggests using the SmartZone R6.1.2 release along with its patch updates.

ATTENTION
It is recommended to upgrade the vSZ controller before updating the vSZ-D version. If the data plane version exceeds the vSZ controller version, the data plane cannot be managed by the vSZ platform.

CAUTION
SmartZone users upgrading from R6.1.2.0 Patch 3 should be aware that applying this patch restricts the upgrade path to the upcoming release of R7.1.1 and above only. Directly upgrading to R7.0.0 Patch 6 or the upcoming release of R7.1.0 is strongly discouraged, as it may result in the loss of certain functionalities.

NOTE
RUCKUS IoT version R2.2.0 is not compatible with controller version R7.0.0 or its subsequent patch releases.

SZ300

- Controller Version: **7.0.0.0.1026**
- Control Plane Software Version: **7.0.0.0.875**
- Data Plane Software Version: **7.0.0.0.1029**
- AP Firmware Version: **7.0.0.0.6536**

SZ144

- Controller Version: **7.0.0.0.1026**
- Control Plane Software Version: **7.0.0.0.875**
- Data Plane Software Version: **7.0.0.0.830**
- AP Firmware Version: **7.0.0.0.6536**

vSZ-H and vSZ-E

- Controller Version: **7.0.0.0.1026**
- Control Plane Software Version: **7.0.0.0.875**
- AP Firmware Version: **7.0.0.0.6536**

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

- Data plane software version: **7.0.0.0.1026**

Upgrade Information

- Users on SmartZone R6.1.0, 6.1.1, and 6.1.2 can upgrade to GA base release R7.0.0. However, versions prior to R6.1.0 are not eligible for this upgrade.
- Fresh installations are supported.
- The following SmartZone upgrade paths to R7.0.0 Patch 6 are supported:
  - Upgrade from R6.1.2 Patch 2 to R7.0.0 Patch 6.
  - Upgrade from R7.0.0 to patch update R7.0.0 Patch 6.

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 later 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. All RUCKUS APs support IEEE 802.11 standards.

TABLE 1 Supported AP Models

Wi-Fi 6 (802.11ax)		Wi-Fi 6E (802.11ax)	Wi-Fi 7 (802.11be)	
Indoor	**Outdoor**	**Indoor**	**Indoor**	**Outdoor**
R850	T750SE	R760	R770	T670
R750	T750	R560	R670	
R650	T350C			
R550	T350SE			
R350	T350D			
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 2 Supported AP Models for AP Zones Using Older AP Versions

Wi-Fi 6 (802.11ax)	Wi-Fi 5 (802.11ac Wave 2)	
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 IEEE 802.11ac Wave 2 or IEEE 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 08.0.95 patches or 09.0.10 patches 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.

NOTE
ICX switches must be running FastIron 08.0.95 patches or 09.0.10 patches 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 5.1.1	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 08.0.90a	Yes	Yes	Yes	Yes	Yes	No	No	No	No
FastIron 08.0.91	Yes	Yes	Yes	No	No	No	No	No	No
FastIron 08.0.92	No	Yes	Yes	Yes	Yes	Yes	No	No	No
FastIron 08.0.95 and subsequent patches	No	No	No	No	Yes	Yes	Yes	Yes	No

TABLE 5 ICX and SmartZone Release Compatibility Matrix (continued)

	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 09.0.10a and subsequent patches	No	No	No	No	No	Yes	Yes	Yes	Yes
FastIron 10.0.00 and subsequent patches	No	No	No	No	No	No	Yes	Yes	Yes
FastIron 10.0.10 and subsequent patches	No	No	No	No	No	Yes	Yes	Yes	Yes
FastIron 10.0.20 and subsequent patches	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
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	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
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

TABLE 6 Switch Management Feature Compatibility Matrix (continued)

Feature	SmartZone Release	ICX FastIron Release
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
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

Known Issues

This section outlines known behaviors and provides recommended workarounds, if available.

AP Limitations

Component/s	AP
Issue	AP-37778
Description	The Multi-Link Operation (MLO) tag is included in the beacon on a Dynamic Pre-Shared Key 3 (DPSK3) Wireless Local Area Network (WLAN), even though MLO is disabled by default.

Component/s	AP
Issue	AP-37777
Description	The downlink performance may be slightly reduced when using SoftGRE on the AP R670.

Component/s	AP
Issue	AP-37234

Component/s	AP
Description	AP channel recovery is not working as expected. APs remain limited in a 20MHz channel width after DFS radar signal disappears.

Component/s	AP
Issue	AP-37253
Description	Location-Based Services (LBS) is not supported on the 6GHz radio.

Component/s	AP
Issue	AP-35718, AP-32531, AP-35075
Description	An intermittent drop in Modulation and Coding Scheme (MCS) has been observed during longevity testing.

Component/s	AP
Issue	AP-35910
Description	During longevity tests, clients may disconnect, and the AP may not accept new client connections under certain conditions.
Workaround	Reboot the AP to restore normal operation.

Component/s	AP
Issue	SCG-151928
Description	It is recommended to use 802.3bt or direct current (DC) 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.

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

Component/s	AP
Issue	SCG-142998
Description	For 802.11ax or later AP models: When the user selects the PoE Operating Mode as 802.3at, by design, the USB Port option is forcibly turned off (the toggle is grayed out and cannot be enabled). Subsequently, when the user changes the PoE Operating Mode to Auto, the USB Port toggle changes to edit mode; however, the controller web user interface does not automatically enable the USB Port option. If USB functionality is desired, you must manually enable the USB Port option.
Workaround	If USB functionality is desired, manually enable the USB Port option.

Component/s	AP
Issue	SCG-142102

Component/s	AP
Description	There is a disparity in the Time To Live (TTL) definition between Link Layer Discovery Protocol (LLDP) 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. • 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 Fast Transition (FT) framework mechanism does not support Pairwise Master Key - R1 (PMKR1) 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 Internet Group Management Protocol (IGMP) (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-26297
Description	AP R560 does not support IEEE 802.3az Energy Efficient Ethernet (EEE).

Component/s	AP
Issue	SCG-146726

Component/s	AP
Description	BSI Compliance Mode Limitations - The Elliptic Curve Digital Signature Algorithm (ECDSA) 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-33444
Description	Under heavy load conditions, Wi-Fi 7 clients experience reduced throughput performance compared to Wi-Fi 6E clients on the same network.

Component/s	AP
Issue	SCG-143239
Description	The throughput 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	Throughput 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	AP-33145
Description	The AeroScout Wi-Fi 6E and Wi-Fi 7 APs are unable to send Tag reports.

Component/s	AP
Issue	AP-32542, AP-34774
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-32419
Description	The downlink performance of R670 with 320MHz is slightly lower compared to the R770 performance.

Component/s	AP
Issue	AP-32827
Description	Downlink performance with RUCKUS GRE might be slightly lower than uplink performance for APs R670 or T670.

Component/s	AP
Description	When using Automated Frequency Coordination (AFC), the APs transmit power is capped by both Power Spectral Density (PSD) and Maximum Effective Isotropic Radiated Power (EIRP), 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	AP
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	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.

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	AP-36456
Description	The Samsung S24 device disconnects from the MLO WLAN, showing an error that the *Previous authentication is no longer valid* when attempting to connect using 802.11ax APs.

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	AP-34776
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	AP-31726
Description	MLO is not supported on mesh-enabled APs in this release.

Component/s	AP
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 RUCKUS APs use standard protocols to interoperate with third-party Wi-Fi devices. RUCKUS qualifies its functionality on the most common clients.

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 Austria.

Component/s	AP
Issue	AP-33390, SCG-146331
Description	Enabling Multi-Link Operation (MLO) 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. 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

Component/s	AP
Issue	ER-14193
Description	The Electronic Shelf Label (ESL) module failed to enable on AP R670.

Resolved Issues

Component/s	AP
Issue	ER-14190
Description	No client **Connection Events** are displayed on the **Troubleshooting** page due to an exception caused by the presence of an @ symbol in the Account, Venue, or AP name.

Component/s	AP
Issue	ER-13721
Description	The U-NII-1 and U-NII-2A bands were unavailable on 802.11ax APs configured with the Indonesia country code.

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

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

Component/s	AP
Issue	AP-36960
Description	Downlink performance was slightly slower when using SoftGRE on the R770 AP.

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	ER-14009
Description	Resolved an issue where the IP address of the user equipment was inaccurately reported as 0.0.0.0 via SNMP.

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

Component/s	AP
Issue	SCG-146540

Component/s	AP
Description	Clients connected to the non-mesh interface of R560 or R760 Mesh APs experienced performance degradation.

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

Component/s	AP
Issue	AP-31501
Description	When back-to-back channel or channel bandwidth configurations were applied from the controller web interface, some blacklisted channels, such as 149-161, were enabled on the AP. This issue was specific to APs configured for 80MHz channelization on the upper band of 5GHz.

Component/s	AP
Issue	ER-13703
Description	The channelization of Wi-Fi 7 APs remained fixed at 20 MHz under certain conditions.

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

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

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

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

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

Component/s	AP
Issue	AP-34197, AP-35311
Description	Resolved an issue where downlink performance with SoftGRE was slightly lower than uplink for APs R670 or T670.

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

Component/s	AP
Issue	AP-34836
Description	Resolved an issue where the AP could go offline during the upgrade process.

Component/s	AP
Issue	AP-33920
Description	During bootup, the AP R670 requested 25.5W of power from the switch, and after bootup, it requested 25W. This change in power consumption could cause a reset in power mode, potentially resulting in connectivity loss for connected clients. This issue occurred randomly and was not limited to any specific switch model.

Component/s	AP
Issue	AP-33873
Description	The **crashdump upload** command failed to copy both *q6dumps* files from the */tmp* (temporary) folder.

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

Component/s	AP
Issue	AP-32876, AP-33066, AP-33108, AP-30095, AP-32161, AP-32939
Description	The issue where channels 149-161 could not be configured arose because the AP CLI indicated that these channels were blocked, while the AP configuration through the controller's Web UI showed support for them. This inconsistency between the CLI and Web UI resulted in the channels being unavailable for configuration despite appearing functional in the UI.

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

Component/s	AP
Issue	AP-32736

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

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

Component/s	AP
Issue	AP-31322
Description	The AP at times encountered a target assert error when collecting Wi-Fi statistics frequently from AP CLI.

Component/s	AP
Issue	AP-19942
Description	When SSID Radio Load (RL) was enabled on R560 or R760 or R770 APs with only one WLAN or Virtual Access Point (VAP) deployed, users at times experienced packet loss and reduced throughput in the uplink direction.

Component/s	AP
Issue	SCG-159402
Description	After executing multiple test cases, no logs were generated through *log read*.

Component/s	AP
Issue	SCG-159180
Description	Request to Send (RTS) frames will not comply with the BSS Minimum Rate Configuration in WLAN.

Component/s	AP
Issue	SCG-158601
Description	Target assert was observed at WLAN (wlan_buf_internal.c:915), causing the test automation to terminate in 2-5-6/2-5 mode.

Component/s	AP
Issue	AP-34348
Description	The issue of channels 149-161 being blocked for Iceland, specific to APs R670 and T670 configured in 2.4GHz-5GHz mode, is resolved.

Component/s	AP
Issue	AP-34259, AP-34258
Description	Resolved random kernel panics observed in high-density environments with a large number of clients roaming across Wi-Fi 7 APs.

Resolved Issues

Component/s	AP
Issue	AP-34081, AP-34080, AP-34078
Description	A cosmetic issue where U-NII-3 channels were incorrectly marked as non-DFS for the countries of Argentina (AR), New Zealand (NZ), and Australia (AU) is resolved.

Component/s	AP
Issue	AP-33764
Description	Resolved target assertion issues encountered in a high-scale environment.

Component/s	AP
Issue	AP-33461
Description	The issue involving Multi-Link Operation (MLO) formation inconsistencies with 2.4GHz and 6GHz bands on *Google Pixel 8* is resolved.

Component/s	AP
Issue	AP-32729
Description	The kernel panic issue caused during a Dynamic Frequency Selection (DFS) channel change event is resolved.

Component/s	AP
Issue	AP-30718
Description	The log level for the monitor interface has been updated, with the default setting changed from debug to error to improve log management and reduce unnecessary debug output.

Component/s	AP
Issue	AP-31597, AP-30539
Description	The issue with Location Based Service (LBS) functionality on APs T670 and R670 is resolved.

Component/s	AP
Issue	SCG-157670
Description	The issue with *Zero Touch Mesh* discovery in standalone builds of APs T670 and R670 is resolved.

Component/s	AP
Issue	AP-34022
Description	A target assert was reported on R750 Density APs.

Component/s	AP
Issue	AP-33380
Description	Resolved discrepancies related to Tx Power support for countries in the 2-5-6 GHz mode, specifically affecting AP R670.

Component/s	AP
Issue	SCG-159467

Component/s	AP
Description	Rate limiting failed to occur when traffic was sent from a wired client connected to a Remote Access Point (RAP) to a wireless client on a Mesh AP. This issue was specific to Wi-Fi 7 AP models.

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

Component/s	UI/UX
Issue	SCG-159070
Description	In the controller web interface, there was a cosmetic issue where the Tx Modulation and Coding Scheme (MCS) and Rx MCS for clients appeared the same for both 2.4GHz and 5GHz links.

Adding the AP Patch to the Controller

Before you begin this procedure, copy the AP patch file that you want to apply to a location that you can access from your computer.

> **IMPORTANT**
> This patch only needs to be applied to a single node. After you apply this patch to a node, it will be propagated automatically to other nodes in the cluster.

Follow these steps to apply an AP patch:

1. Download the patch file `ap-scg_7.0.0.0_patch_pkg-7.0.0.0-6536.noarch.patch` and move the patch file to a location that you can access from the computer that you are using to access the controller's web interface.
2. Log on to the SmartZone web interface.
3. Go to the page for uploading AP patches.
   - On the 7.0.0 web interface, go to **Administration** > **Upload AP Patch** > **and then click the AP Patch** tab.
4. In **Patch File Upload**, click **Browse** go to the location where you saved the AP patch file (`ap-scg_7.0.0.0_patch_pkg-7.0.0.0-6536.noarch.patch`).
5. Click **Open**.
6. On the **AP Patch** tab, click **Upload**. After the patch file is uploaded, the section is populated with the Start time, AP firmware version number and AP model number.
7. Click **Apply Patch**.
8. After the firmware file is applied, the AP firmware information is populated with the following information in the *AP Patch History*:
   - Start Time
   - AP firmware version number
   - AP model number
9. After the firmware file is applied, the AP firmware information is populated with the following information:
10. Go to **Configuration** > **AP Zone** > **Select a Zone.**
11. Click **Change AP Firmware**.

12. In the **Change AP Firmware** manually change the AP firmware to the latest AP image (`7.0.0.0.6536`) in the selected Zone.
13. Click **Yes**
14. When the controller completes updating the AP firmware of the zone, a message appears and notifies you that the zone's AP firmware was updated successfully.
15. Verify that all APs in selected zone are upgraded to `7.0.0.0.6536`.
16. Repeat the steps from 10 to 15 for other Zones that need to be updated.

You have completed adding a new AP patch to the controller.

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