

RUCKUS SmartZone 5.2.2 Release Notes

Supporting SmartZone 5.2.2

Copyright, Trademark and Proprietary Rights Information

© 2021 CommScope, Inc. All rights reserved.

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

Export Restrictions

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

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

Disclaimer

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

Limitation of Liability

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

Trademarks

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Document History	4
Hardware and Software Support	4
Overview.....	4
Release Information.....	4
Supported Matrix and Unsupported Models.....	7
Known Issues	14
Changed Behavior	15
Resolved Issues	16
Interoperability Information	31
Cluster Network Requirements.....	31
Client Interoperability.....	31

Document History

Revision number	Summary of changes	Publication date
A	Initial release notes	22, February 2021

Hardware and Software Support

Overview

This section provides release information about SmartZone 300 (SZ300), SmartZone 100 (SZ100), Virtual SmartZone (vSZ), Virtual SmartZone Data Plane (vSZ-D), SmartZone Data Plane appliance (SZ100-D), SmartZone 144 (SZ-144), SmartZone 144 Data Plane appliance (SZ144-D) and Access Point features.

- The SZ300 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 SZ100, developed for the enterprise market, is the next generation midrange, rack-mountable WLAN controller platform for the enterprise and service provider markets. There are two SZ100 models: the SZ104 and the SZ124.
- 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 architecture-aligned architecture. Deploying vSZ-D offers secured tunneling of wireless client data traffic that encrypts payload traffic; POS data traffic for PCI compliance, voice applications while enabling flat network topology, mobility across L2 subnets and add-on services like L3 Roaming, Flexi-VPN, DHCP Server/NAT as well as CALEA/Lawful Intercept.
- The SZ100-D, is the Data Plane hardware appliance, which is functionally equal to the vSZ-D virtual data plane product. The appliance provides turnkey deployment capabilities for customers that need a hardware appliance. The SZ100-D is managed by a vSZ Controller only and cannot work in a standalone mode.
- 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. SZ144 is first introduced in the software release 5.2.1. It cannot run any software prior to this release. It does not support any AP zones which run the AP firmware prior to 5.2.1.
- The SZ144-D is the second generation Data Plane hardware appliance which is functionally equivalent to the vSZ-D virtual Data Plane product. The appliance provides turnkey deployment capabilities for customers that need a hardware appliance. The SZ144-D is managed by a vSZ Controller only and cannot work in a standalone mode.
- Access Point (AP): Controllers support 1000 APs per zone.

Release Information

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

SZ300

- Controller Version: **5.2.2.0.317**
- Control Plane Software Version: **5.2.2.0.126**

- Data Plane Software Version: **5.2.2.0.317**
- AP Firmware Version: **5.2.2.0.301**

SZ124

- Controller Version: **5.2.2.0.317**
- Control Plane Software Version: **5.2.2.0.126**
- Data Plane Software Version: **5.2.2.0.21**
- AP Firmware Version: **5.2.2.0.301**

SZ144

- Controller Version: **5.2.2.0.317**
- Control Plane Software Version: **5.2.2.0.126**
- Data Plane Software Version: **5.2.2.0.21**
- AP Firmware Version: **5.2.2.0.301**

vSZ-H and vSZ-E

- Controller Version: **5.2.2.0.317**
- Control Plane Software Version: **5.2.2.0.126**
- AP Firmware Version: **5.2.2.0.301**

vSZ-D

- Data plane software version: **5.2.2.0.317**

NOTE

By downloading this software and subsequently upgrading the controller and/or the AP to release 2.5.1.0.177 (or later), you understand and agree that:

- The AP may send a query to RUCKUS containing the AP's serial number. The purpose of this is to enable your AP to autonomously connect with a wireless LAN controller operated by your choice of cloud service provider. RUCKUS may transmit back to the AP the Fully Qualified Domain Name (FQDN) or IP address of the controller that the AP will subsequently attempt to join.
- You also understand and agree that this information may be transferred and stored outside of your country of residence where data protection standards may be different.

ATTENTION

It is strongly recommended to reboot the controller after restoring the configuration backup.

SZ Google Protobuf (GPB) Binding Class

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

1. SmartZone GPB / MQTT Interface Test Subscriber Software [DNP] – <https://support.ruckuswireless.com/software/2805>
2. SmartZone 5.2.2.0.xxx (GA) GPB.proto (Google ProtoBuf) image for GPB/MQTT [DNP] – <https://support.ruckuswireless.com/software/2804>

<https://support.ruckuswireless.com/software/2581>

IoT Suite

This section lists the version of each component in this release.

- vSCG (vSZ-H and vSZ-E), and SZ-124: **5.2.2.0.317**
- Control plane software version in the WLAN Controller : **5.2.2.0.126**
- AP firmware version in the WLAN Controller:**5.2.2.0.301**

RUCKUS IoT Controller

- RUCKUS IoT Controller version: 1.7.1
- VMWare ESXi version: 6.0 and later
- Google Chrome version: 78 and later
- Mozilla Firefox version: 71 and later

Public API

Click on the following links to view:

- SmartZone 5.2.1 Public API Reference Guide (ICX Management), visit <https://support.ruckuswireless.com/documents/3570>
- SmartZone 5.2.1 Public API Reference Guide (SZ100), visit <https://support.ruckuswireless.com/documents/3569>

NOTE

SZ100 Public API link is for SZ144 as well.

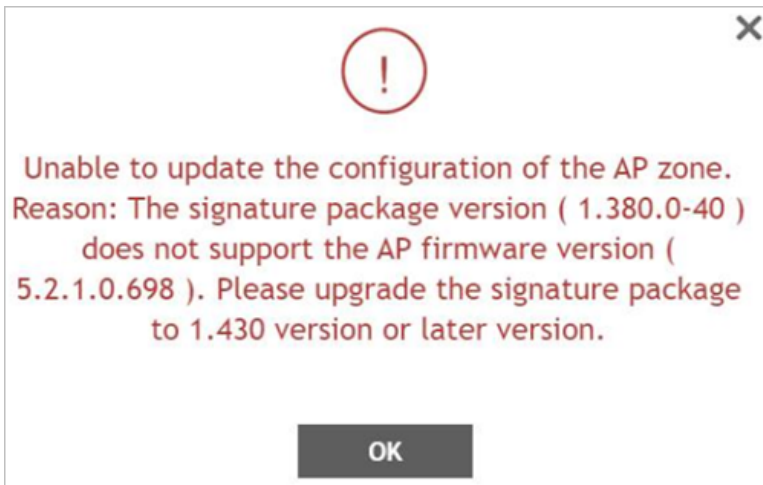
- SmartZone 5.2.1 Public API Reference Guide (SZ300), visit <https://support.ruckuswireless.com/documents/3568>
- SmartZone 5.2.1 Public API Reference Guide (vSZ-E), visit <https://support.ruckuswireless.com/documents/3567>
- SmartZone 5.2.1 Public API Reference Guide (vSZ-H), visit <https://support.ruckuswireless.com/documents/3566>

Application Signature Package

ATTENTION

The signature package is the same for releases 5.2.1 and 5.2.2.

AP DPI feature uses an Application Signature Package that in general it can be optionally updated when a new version is available. But in this case, previous packages are not compatible with 5.2 AP firmware, and upgrading zone firmware is blocked until the corresponding signature package (**RuckusSigPack-v2-1.470.1.tar.gz?**) is installed.



Do follow this mandatory process before upgrading AP zone firmware:

1. Download Signature package by visiting the RUCKUS support site, <https://support.ruckuswireless.com/software/2566-smartzone-5-2-1-0-515-ga-sigpack-1-470-1-application-signature-package>
2. Manually upgrade the signature package by navigating to **Services & Profiles > Application Control > Signature Package**. (more details can be found in Administrator Guide, in section *Working with Application Signature Package*)

Once this is done, AP zones can be upgraded. **[SCG-108730]**

IMPORTANT

SigPack versions 1.430.1 and 1.470.1 are supported on build **5.2.2.0.317**. Version 1.380.0.40 is not supported.

Product Documentation Upgrade Guide

The following product guides, have been updated for this release. Do refer to the *What's New in this Document* section.

1. SmartZone 5.2.2 Administrator Guide (SZ300/vSZ-H)
2. SmartZone 5.2.2 Administrator Guide (SZ100/vSZ-E)
3. SmartZone 5.2.2 Upgrade Guide
4. SmartZone 5.2.2 Command Reference Guide (SZ300/vSZ-H)
5. SmartZone 5.2.2 Command Reference Guide (SZ-100/vSZ-E)
6. SmartZone 5.2.2 Getting Started Guide on GPB/MQTT Interface (SZ300/SZ-100/vSZ)

NOTE

The rest of the SmartZone guides remain the same for this release. Refer to the SmartZone release 5.2.1 set of documents by visiting the RUCKUS website available at support.ruckuswireless.com or [Tech Content Portal](#).

Supported Matrix and Unsupported Models

Before upgrading to this release, check if the controller is currently managing AP models, IoT and Switch feature matrix.

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

Hardware and Software Support

Supported Matrix and Unsupported Models

LWAPP2SCG must be disabled on controller if Solo AP's running 104.x being moved under SZ 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 and higher are capable of connecting to both ZD and SZ controllers. If an AP is running releases 104.x and higher and the LWAPP2SCG service is enabled on the SZ controller, a race condition will occur.

AP Firmware Releases

The AP firmware releases that the controller will retain depends on the controller release version from which you are upgrading:

Upgrade path	AP firmware releases in controller
5.2.x > 5.2.2	5.2.x, 5.2.2
5.1.x > 5.2.2	5.1.x, 5.2.2
3.6.x > 5.0 > 5.1.x > 5.2.x > 5.2.2	3.6.x, 5.1.x, 5.2.x, 5.2.2
3.6.x > 5.1.x > 5.2.x > 5.2.2	3.6.x, 5.1.x, 5.2.x, 5.2.2
3.6.x > 5.2.2	3.6.x, 5.2.2

NOTE

For further details refer to the section *Multiple AP Firmware Support in the SZ100/vSZ-E/SZ300/vSZ-H* in SmartZone Upgrade Guide, 5.2.2

Supported AP Models

This release supports the following RUCKUS AP models.

TABLE 1 Supported AP Models

11ax		11ac-Wave2		11ac-Wave1	
Indoor	Outdoor	Indoor	Outdoor	Indoor	Outdoor
R730	T750	R720	T710	R600	T504
R750	T750SE	R710	T710S	R500	T300
R650		R610	T610	R310	T300E
R550		R510	T310C	R500E	T301N
R850		H510	T310S		T301S
		C110	T310N		FZM300
		H320	T310D		FZP300
		M510	T811CM		
		R320	T610S		
			E510		
			T305e		
			T305i		

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.

NOTE

DFS channels are disabled on AP T750SE.

IMPORTANT

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

Unsupported AP Models

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

TABLE 2 Unsupported AP Models

Unsupported AP Models				
SC8800-S	ZF7762-S-AC	ZF2741	ZF7762-AC	ZF7351
ZF7321	ZF7343	ZF7962	ZF7762-S	ZF2942
ZF7441	ZF7363-U	SC8800-S-AC	ZF7363	ZF2741-EXT
ZF7762	ZF7025	ZF7321-U	ZF7341	ZF7352
ZF7762-T	ZF7351-U	ZF7761-CM	ZF7343-U	ZF7781CM
R300	ZF7782	ZF7982	ZF7782-E	ZF7055
ZF7372	ZF7782-N	ZF7372-E	ZF7782-S	C500
H500	R700			

Switch Management Feature Support Matrix

Following are the supported ICX models:

TABLE 3 Supported ICX Models

Supported ICX Models		
ICX 7150	ICX 7450	ICX 7750
ICX 7250	ICX 7650	ICX 7850
ICX 7550		

Following is the matrix for ICX and controller release compatibility:

TABLE 4 ICX and SZ Release Compatibility Matrix

	SZ 5.1	SZ 5.1.1	SZ 5.1.2	SZ 5.2	SZ 5.2.1	SZ 5.2.2
FastIron 08.0.80	Y	Y	N	N	N	N
FastIron 08.0.90a	N	Y	Y	Y	Y	Y
FastIron 08.0.91	N	Y	Y	Y	N	N
FastIron 08.0.92	N	N	Y	Y	Y	Y
FastIron 08.0.95	N	N	N	N	Y	Y
FastIron 08.0.95a	N	N	N	N	Y	Y
FastIron 08.0.95b	N	N	N	N	Y	Y

NOTE

FastIron 08.0.95b is required for managing ICX7550 switches.

Following is the matrix for switch management feature compatibility:

Hardware and Software Support

Supported Matrix and Unsupported Models

TABLE 5 Switch Management Feature Compatibility Matrix

Feature	SZ 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
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
Switch Topology	5.2 and later	08.0.92 and later
Designate a VLAN as Management VLAN	5.2.1 and later	08.0.95 and later
Change default VLAN	5.2.1 and later	08.0.95 and later
Configuring 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
Download syslogs for a selected switch	5.2.1 and later	08.0.91 and later
Remote CLI	5.2.1 and later	08.0.95 and later

IoT Suite

This release supports IoT Controller release 1.7.1 and is compatible with the following controller and access point hardware and software.

Compatible Hardware

- C110 Access Point (C110)
- E510 Access Point (E510)
- H510 Access Point (H510)
- M510 Access Point (M510)
- R510 Access Point (R510)
- R550 Access Point (R550)
- R610 Access Point (R610)
- R650 Access Point (R650)
- R710 Access Point (R710)
- R720 Access Point (R720)
- R730 Access Point (R730)

- R750 Access Point (R750)
- T310 Access Point (T310)
- T610 Access Point (T610)
- T750 Access Point (T750)
- T750SE Access Point (T750SE)
- I100 IoT Module (I100)

Compatible Software

- Virtual SmartZone – High Scale (vSZ-H)
- Virtual SmartZone – Essentials (vSZ-E)
- SmartZone 100 (SZ100)
- RUCKUS IoT Controller (RIoT)

The below table lists the supported IoT end devices.

Hardware and Software Support

Supported Matrix and Unsupported Models

NOTE

Multiple other devices may work with this release but they have not been validated.

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Vingcard Signature	Lock	ZigBee	Assa-Abloy	AA_LOCK	
Vingcard Essence	Lock	ZigBee	Assa-Abloy	AA_LOCK	
RT+	Lock	ZigBee	Dormakaba	Dormakaba	79PS01011ER-626
Yale YRD220/240 TSDB Display Lock	Lock	ZigBee	Assa-Abloy	Yale	YRD220/240 TSDB
Yale YRD210 Push Button Lock	Lock	ZigBee	Assa-Abloy	Yale	YRD210 Push
Smartcode 916	Lock	ZigBee	Kwikset	Kwikset	SMARTCODE_DEADBOLT_10T
Smartcode 910 (450201)	Lock	ZigBee	Kwikset	Kwikset	
Lightify (RGB) Model 73674	Bulb	ZigBee	Osram	Osram	LIGHTIFY A19 RGBW
Lightify Model 73693	Bulb	ZigBee	Osram	Osram	LIGHTIFY A19 Tunable White45856
Lightify Model 73824	Bulb	ZigBee	Osram	Osram	
Element Color Plus	Bulb	ZigBee	Sengled	Sengled	E11-N1EA
Bulb - LED	Bulb	ZigBee	Sengled	Sengled	Z01-A19NAE26
E11-G13	Bulb	ZigBee	Sengled	Sengled	E11-G13
Lux	Bulb	ZigBee	Philips	Philips	LWB004
SLV E27 Lamp Valetto (ZigBee 3.0)	Bulb	ZigBee 3.0	SLV		
GE Smart Dimmer	Switch	ZigBee	GE	Jasco Products	45857
GE Smart Switch	Switch	ZigBee	GE	Jasco Products	45856
Smart Plug	Plug	ZigBee	Centralite	Centralite	4257050-ZHAC
Zen Thermostat	Thermostat	ZigBee	Zen Within	Zen Within	Zen-01
ZBALRM	Alarm	ZigBee	Smartenit		Model #1021 A
Temp, Humidity Sensor	Sensor	ZigBee	Heiman	Heiman	HT-N
Gas detector	Sensor	ZigBee	Heiman	Heiman	GASSensor-N
Contact Sensor/Door Sensor	Sensor	ZigBee	Centralite	Centralite	3300-G
3-Series Motion Sensor	Sensor	ZigBee	Centralite	Centralite	3305-G
Temperature Sensor	Sensor	ZigBee	Centralite	Centralite	3310-G
Multipurpose Sensor	Sensor	ZigBee	SmartThings	Samjin	
Button	Sensor	ZigBee	SmartThings	Samjin	
Motion Sensor	Sensor	ZigBee	SmartThings	Samjin	
Water Leak Sensor	Sensor	ZigBee	SmartThings	Samjin	
Motion Sensor	Sensor	ZigBee	AduroSmart ERIA	Adurolight	
Smart Plug	Plug	ZigBee	SmartThings	Samjin	
Bulb	Bulb	ZigBee	AduroSmart ERIA		
Bulb	Bulb	ZigBee	Cree		BA19-08027OMF-12CE26-1C100
Smart Plug	Plug	ZigBee	INNR		

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Zen Thermostat	Thermostat	ZigBee	Zen Within	Zen Within	Zen-01
ZBALRM	Alarm	ZigBee	Smartenit		Model #1021 A
Temp, Humidity Sensor	Sensor	ZigBee	Heiman	Heiman	HT-N
Gas detector	Sensor	ZigBee	Heiman	Heiman	GASsensor-N
Contact Sensor/Door Sensor	Sensor	ZigBee	Centralite	Centralite	3300-G
3-Series Motion Sensor	Sensor	ZigBee	Centralite	Centralite	3305-G
Temperature Sensor	Sensor	ZigBee	Centralite	Centralite	3310-G
Multipurpose Sensor	Sensor	ZigBee	SmartThings	Samjin	
Button	Sensor	ZigBee	SmartThings	Samjin	
Motion Sensor	Sensor	ZigBee	SmartThings	Samjin	
Water Leak Sensor	Sensor	ZigBee	SmartThings	Samjin	
Motion Sensor	Sensor	ZigBee	AduroSmart ERIA	Adurolight	
Smart Plug	Plug	ZigBee	SmartThings	Samjin	
Bulb	Bulb	ZigBee	AduroSmart ERIA		
Bulb	Bulb	ZigBee	Cree		BA19-08027OMF-12CE26-1C100
Smart Plug	Plug	ZigBee	INNR		
Smart Blinds	Blinds	ZigBee	Axis Gear		
Occupancy Sensor	Sensor	ZigBee	Telkonet		
Door Sensor	Sensor	ZigBee	Telkonet		
Thermostat	Thermostat	ZigBee	Telkonet		
Picocell	Gateway	LoRa	Semtech		
Mini Hub/ Basic station	Gateway	LoRa	TABS		
Door Sensor	Sensor	LoRa	TABS		
Occupancy Sensor	Sensor	LoRa	TABS		
Panic Button	Beacon	BLE	TraknProtect		
Tray Beacon	Beacon	BLE	TraknProtect		
Asset Beacon	Beacon	BLE	TraknProtect		
Card Beacon	Beacon	BLE	TraknProtect		
Card Tag	Beacon	BLE	Kontakt.io		CT18-3
Beacon Pro	Beacon	BLE	Kontakt.io		BP16-3
Asset Tag	Beacon	BLE	Kontakt.io		S18-3
Vape/Sound Sensor	Sensor	Wired	Soter		FlySense

TABLE 6 Supported Devices tested with SmartThings

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Yale YRD220/240 TSDB Display	Lock	ZigBee	Assa-Abloy	Yale	YRD220/240 TSDB
Lightify (RGB) Model 73674	Bulb	ZigBee	Osram	Osram	LIGHTFY A19 RGBW
Multipurpose Sensor	Sensor	ZigBee	SmartThings	Samjin	
Button	Sensor	ZigBee	SmartThings	Samjin	
Motion	Sensor	ZigBee	SmartThings	Samjin	
Water Leak Sensor	Sensor	ZigBee	SmartThings	Samjin	
Smart Plug	Sensor	ZigBee	SmartThings	Samjin	
Bulb	Bulb	ZigBee	AduroSmart ERIA		

Known Issues

The following are the Caveats, Limitations, and Known issues in this release.

NOTE

Known issues stated in the 5.2.1 release notes are also applicable to this release.

Component/s	Upgrade
Issue	ER-9597
Description	<p>When the controller meets the following conditions before upgrading:</p> <ul style="list-style-type: none"> • Access and core separation feature is enabled. • UDI interface exists. • There are static routes for UDI interface. <p>Then, after upgrading to release 5.2.2, static routes for the UDI interface will be placed in an incorrect routing table so these destinations will not be reachable.</p> <p>For assistance, contact RUCKUS support team using https://support.ruckuswireless.com.</p>

Component/s	AP
Issue	ER-8577
Description	Statistical information provided to SCI may result in discrepancies between total traffic sessions summary and binned sessions reports available in SCI.

Component/s	AP
Issue	SCG-121365
Description	Sometimes when AP Tx power country limits are low, the Tx power settings in the controller web user interface do not decrease the actual AP transmit power.

Component/s	AP
Issue	ER-9622
Description	APs located in same subnet as controller SZ144 will fail to auto discover the controller.
Workaround	Use other available controller discovery options (DHCP option 43, DNS, manual).

Component/s	Control Plane
Issue	ER-9376, SCG-124193
Description	Proxy LDAP/AD over TLS do not support using a certificate with fully qualified domain name (FQDN) for CN.
Workaround	Use IP address for CN field.

Component/s	System
Issue	ER-9476
Description	Configuration details for <i>Authentication Service</i> inside <i>Real Based Authentication Service</i> will not be shown in controller web user interface when editing this value.

Component/s	System
Issue	ER-9529
Description	WLANs may fail to be removed from WLAN group when similar simultaneous operations like this are done using Public API.

Component/s	System
Issue	ER-9556
Description	Controller web user interface will fail to download the alarms log file when the alarm count is over 50000.

Component/s	System
Issue	ER-9423
Description	SNMP traps are not sent by the controller for Switch related alarms and events.

Component/s	System
Issue	ER-9633
Description	Unable to apply WLAN templates extracted from the Zones under Partner Domain .

Component/s	Virtual SmartZone
Issue	ER-9658
Description	SoftGRE profiles containing similar server IP address will fail to be created in controller web user interface with error: <i>Duplicate gateway address found in AP tunnel profile</i> .

Changed Behavior

The following are the changed behavior issues in this release.

Component/s	Control Plane
Issue	SCG-124654
Description	Number of manual controller configuration backups kept in the cluster is now limited to 50. If a user tries to create an additional backup from web user interface, it will be asked to allow removing the older configuration file in system.

Resolved Issues

Component/s	Control Plane
Issue	SCG-126838
Description	Better control is introduced for AP firmware download from the controller when AP zones are upgraded. Default settings will limit to 300 the number of simultaneous connections to download AP firmware (without bandwidth limit per connection). A new SmartZone CLI command is also available to modify number of concurrent connections and download speed per connection: <pre>> enable # config (config) # firmware-download-limit</pre>

Component/s	System
Issue	ER-9028
Description	Removed information related to internal-only interfaces when SZ is queried using SNMP IF-MIB OIDs.

Component/s	System
Issue	SCG-127010, ER-9404
Description	Maximum number of Location Service profiles per regular domains has increased from 128 to 1000 (maximum number per partner domain remains at 128).

Component/s	System
Issue	SCG-127642, SCG-127443, SCG-127833
Description	Several enhancements related to Admin Activity messages are included in this release: <ul style="list-style-type: none"> Administrator Activity messages reported when administrator users are moved between groups or permissions are modified now contain more information. Administrator Activity message reported when there is a user login failure to controller web user interface now contains more details.

Component/s	UI/UX
Issue	SCG-128034, ER-9615
Description	Controller web user interface page available in System > Switch Settings > Switch Registration is now hidden to Partner Domain level users since it contains system level information.

Resolved Issues

The following are the resolved issues related to this release.

Component/s	Analytics
Issue	SCG-124328, SCG-121667, SCG-122357, SCG-125004, SCG-120553, SCG-123478, SCG-123830, SCG-123839, SCG-123929, SCG-124041, SCG-124695, SCG-123746
Description	Enhancements and several fixes for connection to RUCKUS Analytics and Service Validation feature in that platform are included in this release.

Component/s	AP
Issue	ER-8416

Component/s	AP
Description	Resolved an issue where client throughput may decrease for a short period after off-channel scan.

Component/s	AP
Issue	ER-9568
Description	Resolved an issue where AP channel changed even though the <i>Auto Channel</i> selection option was <i>OFF</i> .

Component/s	AP
Issue	ER-9378
Description	Resolved an issue where AP R730 that causes client throughput degradation.

Component/s	AP
Issue	ER-9627
Description	Resolved an issue where AP zone could not be deleted by flush counter reaches the maximum.

Component/s	AP
Issue	ER-9573
Description	Resolved an issue where upon roaming client traffic is dropped or it is disconnected if Force DHCP feature is enabled in WLAN.

Component/s	AP
Issue	ER-9577
Description	Resolved an issue in R730 that could cause client connectivity issues or disconnections.

Component/s	AP
Issue	SCG-124955
Description	Resolved an issue where APs did not correctly balance after one controller node goes down.

Component/s	AP
Issue	SCG-126113, SCG-126862, SCG-125071
Description	Several improvements in zone templates handling are introduced in this release.

Component/s	AP
Issue	SCG-124213, SCG-125601, SCG-126421
Description	Enhancements and several fixes in AP memory utilization are included in this release.

Component/s	AP
Issue	SCG-125120, AP-13953, SCG-121644
Description	Enhancements for AP and controller management initial connection and fail over are included in this release.

Resolved Issues

Component/s	Data Plane
Issue	SCG-125817, SCG-125093, SCG-125553, SCG-125581, SCG-125093, SCG-125059
Description	Enhancements and several fixes in data plane stability during and after an upgrade are introduced in this release.

Component/s	AP
Issue	ER-8490
Description	Resolved an issue where the AP was randomly unable to reach the RADIUS server if packets required fragmentation.

Component/s	AP
Issue	ER-9244
Description	Resolved an issue specific to 802.11ax AP models where some SSIDs may not be broadcasted correctly.

Component/s	AP
Issue	ER-9261
Description	Resolved an issue where client disconnected by the administrator from 802.11x WLAN with PMK/OKC enabled was allowed to reconnect without full re-authentication.

Component/s	AP
Issue	ER-8417
Description	Adjusted MU-MIMO functionality for better distributed throughput in environments with large number of MU capable clients.

Component/s	AP
Issue	ER-8555
Description	Resolved an issue where in DPSK WLAN the roaming client reverted to the default VLAN when 802.11r is enabled.

Component/s	AP
Issue	AP-13662, ER-8660, ER-9393
Description	Resolved an issue in 802.11ax APs where incorrect client RSSI values were reported.

Component/s	AP
Issue	ER-9031, ER-9130
Description	Resolved an issue specific to 802.11ax AP models where channel width may change unexpectedly.

Component/s	AP
Issue	ER-9189
Description	Resolved an issue where some log lines in AP were truncated if remote Syslog was enabled.

Component/s	AP
Issue	ER-8946, ER-9039
Description	Resolved a client connectivity issue specific to 802.11ax AP models where client count was calculated incorrectly for MU-MIMO beamforming to operate correctly.

Component/s	AP
Issue	ER-9112, SCG-125773
Description	Resolved an issue where WISPr client authorization failed on DHCP NAT enabled APs.

Component/s	AP
Issue	ER-8647
Description	Resolved an issue where long GPS coordinates were triggering a frequent error log in AP.

Component/s	AP
Issue	ER-9222
Description	Resolved an issue where AP Ethernet ports using tunneled QinQ were not tagging the traffic correctly.

Component/s	AP
Issue	ER-8397
Description	Resolved an issue where the client may fail to complete DHCP process on roaming.

Component	AP
Issue	ER-8931, ER-8917
Description	Resolved an issue where client using Dynamic VLAN roaming between radios in same AP goes back to default SSID VLAN when using PMK/OKC.

Component/s	AP
Issue	ER-8298
Description	Resolved an issue where NAT/DHCP option failed on LAN2 port of M510 AP.

Component/s	AP
Issue	ER-9202
Description	Resolved an issue where an AP process related to Mesh was enabled although this feature was disabled.

Component	AP
Issue	ER-8568
Description	Resolved an issue where customized guest portal logo was not loaded in authenticated page.

Component/s	AP
Issue	ER-9089

Resolved Issues

Component/s	AP
Description	Resolved an issue where the parameter <i>Tx Power Backoff</i> failed to show the correct value in the controller web user interface.

Component/s	AP
Issue	ER-9215
Description	Resolved an issue specific to 802.11ax AP models where clients may be unable to connect.

Component/s	AP
Issue	ER-9359
Description	Resolved an issue where incorrect MAC addresses were being sent to Ekahau application.

Component/s	AP
Issue	ER-6886
Description	When there is a latency higher than 200ms between controller and remote APs, there can be timeout errors during DPSK authentication. NOTE Contact RUCKUS technical support if your latency is higher than that.

Component	AP
Issue	ER-8968
Description	Resolved an issue where inactivity timeout occurred prematurely and client disconnected with <i>Reason Code 4</i> .

Component/s	AP
Issue	ER-7746
Description	In WLAN configuration, if TKIP is selected, BTM feature will [now] be disabled by default.

Component/s	AP
Issue	ER-9114, ER-9099
Description	Resolved some issues where WLAN stayed or changed to <i>ON</i> though it was provisioned as <i>OFF</i> through the WLAN scheduler specific option.

Component/s	AP
Issue	ER-8985, ER-8876
Description	Enhancements where some frequent non meaningful AP syslog entry are removed.

Component/s	AP
Issue	ER-8691
Description	Resolved an issue where client connected to WISPr WLAN was redirected to secondary redirect URL even when primary redirect URL was active.

Component/s	AP
Issue	ER-9025
Description	Resolved an issue where the controller web user interface failed to show the correct channelization for 2.4GHz and 5GHz radios of 802.11ax AP models.

Component/s	AP
Issue	ER-9251
Description	Resolved an issue specific to 802.11ax AP models where 2.4GHz radio mode was incorrectly set.

Component/s	AP
Issue	ER-9248
Description	Resolved an AP reboot issue caused by kernel panic.

Component/s	AP
Issue	ER-8359
Description	An algorithm improvement is introduced with the AP latency number calculation.

Component/s	AP
Issue	ER-8330
Description	Resolved an issue where R710 acting as RAP was failing to properly pass traffic between other 802.11ac Wave 2 APs acting as MAPs.

Component/s	AP
Issue	ER-8747
Description	Resolved an issue in 802.11ax APs that could cause intermittent packet loss and latency spike.

Component/s	AP
Issue	ER-8674
Description	Resolved an AP reboot issue specific to 802.11ax AP models caused by target assert.

Component	AP
Issue	ER-8761
Description	Resolved an issue where SNMP AP Tx/Rx bytes from <i>RUCKUS-SCG-WLAN-MIB</i> provided delta information instead of cumulative.

Component/s	AP
Issue	ER-8532
Description	Resolved an issue where controller public API Query/AP failed when using the term <i>CONTROLBLADE</i> in the filter.

Component/s	AP
Issue	ER-8634

Resolved Issues

Component/s	AP
Description	Resolved an issue where joining a new controller to an existing cluster would fail if the cluster already had an SZ100-D data plane.

Component/s	AP
Issue	ER-9386
Description	Resolved an issue where disabling the DHCP service on AP for the zones configured with DHCP configuration (enable on multiple AP's) resets the AP model specific setting.

Component/s	AP
Issue	ER-8228
Description	Resolved an issue where AP tunnel statistics showed the wrong data plane name and MAC address.

Component/s	AP
Issue	ER-8754
Description	Resolved an issue where RADIUS <i>Accounting User Name</i> attribute was incorrectly set to client MAC address.

Component/s	AP
Issue	ER-8758
Description	Resolved an issue where WISPr redirection in a tunneled WLAN was not working when client isolation multicast was enabled.

Component/s	AP
Issue	ER-8852, ER-8817
Description	Resolved an issue where radio latency for 802.11ax AP models was not displayed/reported with accurate information in controller GUI.

Component/s	AP
Issue	ER-8538, ER-9379
Description	Resolved an issue in 802.11ac Wave 2 APs of reporting incorrect number of Tx management frames.

Component	AP
Issue	ER-9042
Description	Resolved an issue where the client gets disconnected after inter SSID roaming on the same AP.

Component/s	AP
Issue	ER-8653
Description	Resolved an issue where controller web user interface showed inconsistent AP count between nodes after some cluster member is disconnected for some time and connected back.

Component	AP
Issue	ER-7652, ER-8621
Description	Enhancement in AP locating the correct DPSK key that resolves a client association issue.

Component	AP
Issue	ER-8188
Description	Resolved an issue where after target assert on the AP, UTP rate limiting failed.

Component/s	AP
Issue	ER-8759
Description	Resolved an issue where the AP 5G channel was configured to 48 and the CLI command, show running-config ap wrongly displayed it as AUTO.

Component	AP
Issue	ER-9015
Description	Resolved an issue where clients may fail to authenticate due to a communication issue between AP and controller due to incorrect closure of file descriptor.

Component/s	AP
Issue	ER-9169
Description	Resolved an issue where APs were failing to update the configuration due to an incorrect data validation in controller web user interface for location field when using Unicode characters.

Component/s	AP
Issue	ER-9272
Description	Resolved an issue where the portal redirection did not work when the APs are on a standby cluster in Geo Redundancy deployment.

Component/s	AP
Issue	SCG-126965
Description	Resolved an issue where URL filtering would fail on a DHCP NAT enabled AP.

Component/s	AP
Issue	SCG-120551, ER-8600
Description	Resolved an issue where data traffic was not correctly shaped according to SSID rate limiting value if higher than 30Mbps.

Component/s	AP
Issue	SCG-113164
Description	Resolved an issue where channel 144 may be available in AP even if it is disabled in per AP settings.

Resolved Issues

Component/s	AP
Issue	ER-8328
Description	Resolved an issue where R610 AP may fail to successfully connect to a 2.5Gbps switch port.

Component/s	AP
Issue	ER-8863
Description	Resolved an AP reboot issue specific to 802.11ax AP models caused by kernel panic.

Component/s	AP
Issue	ER-9170
Description	Resolved a random AP reboot issue when creating or deleting a WLAN

Component/s	AP
Issue	ER-9492
Description	Resolved an issue where SSIDs are not broadcasted correctly if Load Balancing with proactive steering mode is enabled.

Component/s	AP
Issue	ER-9516 , ER-9517
Description	Resolved an issue which limited MU-MIMO performance on APs R750 and R650.

Component	Control Plane
Issue	ER-9548
Description	Resolved LBS venue name limitation issue to allow uppercase, lowercase, and some special characters for 3rd Party LBS support.

Component	Control Plane
Issue	ER-8628
Description	Resolved an issue where a controller may be unable to accept any AP because an internal process failed to restart properly.

Component	Control Plane
Issue	ER-8608
Description	Resolved an issue where controller <i>MsgDist</i> log contained frequent lines incorrectly classified at ERROR level.

Component	Control Plane
Issue	ER-8973
Description	Resolved an issue where rate limiting was not applied when <i>Framed-Protocol</i> attribute was received in <i>Access Accept</i> message from AAA server.

Component/s	Data Plane
Issue	ER-8992, ER-9470

Component/s	Data Plane
Description	Resolved a data plane core dump issue caused by log download.

Component/s	Data Plane
Issue	ER-9214
Description	Resolved an issue where the data plane failed to connect to the controller.

Component/s	Data Plane
Issue	ER-8539
Description	Resolved an issue where data plane may lose data IP address due to file corruption.

Component/s	SPoT
Issue	ER-8581
Description	Resolved an issue where the SPoT API to query client did not work.

Component/s	SPoT
Issue	ER-8173
Description	Resolved an issue where AP failed to report to SPoT when WLAN service was down.

Component	Switch Management
Issue	ER-8804
Description	Resolved an issue where remote CLI access to managed switch through the controller failed when the controller management ACL is enabled.

Component	System
Issue	ER-9160
Description	Resolved a controller (SZ300) Power Supply Unit LED issue.

Component/s	System
Issue	SCG-124714, SCG-126657, SCG-127039, ER-9312
Description	<p>Several fixes related to UE roaming are introduced in this release:</p> <p>Resolved an issue when roaming using 802.11r in a tunneled WLAN using DVLAN. [SCG-124714]</p> <p>Resolved an issue when roaming in a WLAN with force DHCP enabled. [SCG-126657]</p> <p>Resolved an issue where Radius Accounting-Stop was missing some attribute when roaming between radios in the same AP. [SCG-127039]</p> <p>Resolved an issue where Single Radius Session Accounting is not done correctly when roaming between radios in the same AP. [ER-9312]</p>

Component	System
Issue	ER-9066
Description	Resolved an issue where switch VLAN deleted through the controller is added back into switch configuration with <i>multicast passive</i> option enabled.

Resolved Issues

Component/s	System
Issue	ER-8910
Description	Resolved a memory leak issue in controller process <i>LWAPP2SCG</i> .

Component/s	System
Issue	ER-9307
Description	Resolved an issue where admin test AAA server could return false result.

Component/s	System
Issue	ER-9310
Description	Resolved an issue where columns were not sorted correctly in Diagnostics > RADIUS controller web user interface.

Component/s	System
Issue	ER-8454
Description	Resolved an issue where certain events showed incorrect Management IP address of the controller.

Component/s	System
Issue	ER-8749
Description	Resolved an issue where proxy ARP feature could not be checked or configured in controller CLI for Tunneled WLAN.

Component/s	System
Issue	SCG-126121, ER-9127
Description	Resolved an issue where VLAN assignment to clients via User Role mapping or WISPr Radius attributes resulted in Radius proxy SZ process memory leak.

Component/s	System
Issue	ER-9233
Description	Resolved an issue where the AP and Clients list CSV file contained Chinese characters after changing the logo.

Component/s	System
Issue	ER-8791
Description	Resolved an issue where the controller SNMP MIB <i>ruckusSCGWLANZone</i> returned a wrong value.

Component	System
Issue	ER-7979
Description	Resolved an issue where the controller stopped showing traffic and health data of the control plane nodes.

Component/s	System
Issue	ER-8827
Description	Enhancement by adding a validation to block creating a zone from the Zone template whose Ethernet port profile refers to a nonexistent firewall profile.

Component/s	System
Issue	ER-9211
Description	Resolved an issue where licenses assigned to a controller node deleted from a cluster were removed immediately. Licenses are kept for 45 days for the node to be replaced with a new one.

Component	System
Issue	ER-8530
Description	Resolved an issue where client authentication and accounting fails when using RADIUS proxy due to an issue in controller RADIUS proxy service.

Component	System
Issue	ER-8957
Description	Resolved an issue where controller WLAN template containing external DPSK WLANs was failing to apply.

Component/s	System
Issue	ER-8942
Description	Resolved an issue where the <i>copy backup</i> CLI command failed to work through TFTP (Trivial File Transfer Protocol).

Component	System
Issue	ER-8810
Description	Resolved an issue where generating a CSR failed due to a blank space in the CSR name.

Component	System
Issue	ER-8520
Description	Resolved an issue where flagged AP number did not count in <i>Connected AP #</i> in the controller exported zone CSV.

Component/s	System
Issue	ER-9054
Description	Resolved an issue where the remote CLI access to Switch through the controller did not provide a prompt.

Component	System
Issue	ER-8836, ER-8795
Description	Resolved an issue where the controller through CLI was unable to move a domain to another parent domain.

Resolved Issues

Component/s	System
Issue	ER-8797
Description	Resolved an issue where event 2102 was wrongly asserted for WLANs with authentication or accounting proxy enabled.

Component	System
Issue	ER-8639
Description	Resolved an issue where flagged Switches were not coming back to online status.

Component	System
Issue	ER-8466
Description	Resolved an issue where the IP address value was seen in controller web user interface as <i>N/A</i> in Switch DHCP pool options when configured through Switch CLI with two IP addresses.

Component	System
Issue	ER-8790
Description	Resolved an issue where users cannot unmark Rogue AP's with the user permission <i>Modify</i> .

Component/s	System
Issue	ER-9421
Description	Enhancement in response time for SNMP queries related to AP data.

Component/s	System
Issue	ER-8159, ER-8278, SCG-120210
Description	Enhancements and several fixes for user uploaded certificates to be used in Guest WLAN are introduced in this release.

Component/s	System
Issue	ER-9351
Description	Resolved an issue where controller CLI show running-config zone command did not display the secondary WISPr redirect URL.

Component/s	System
Issue	ER-8648
Description	Resolved an issue where the controller did not publish MGR message to SPoT.

Component/s	System
Issue	SCG-127645
Description	Resolved an issue where event code 8016 <i>Admin account lockout after failed attempts</i> failed to generate.

Component/s	System
Issue	SCG-127644

Component/s	System
Description	Resolved an issue where SNMP and email notifications were not sent for event code 811 <i>Admin account lockout</i> .

Component/s	System
Issue	SCG-127643
Description	Resolved an issue where failed login administrative activities were not captured for all failed login attempts when <i>Account Security</i> was enabled.

Component/s	System
Issue	SCG-127319
Description	Resolved an issue where the system failed to clear insufficient license capacity alarm status.

Component/s	System
Issue	SCG-125653
Description	Resolved an issue where the country code in the controller Zone fails to inherit the default value from system AP settings during ZD migration.

Component/s	System
Issue	SCG-125497
Description	Resolved an issue where <i>SNMP walk</i> on the <i>ruckusSCGConfigWLANEntry</i> MIB returned an empty value.

Component/s	System
Issue	ER-9124
Description	Enhancements related to switch upgrade are included in this release.

Component/s	UI/UX
Issue	SCG-76181
Description	Resolved an issue where if a zone that has been added to a report is deleted, the corresponding report failed because of the missing Zone.

Component/s	UI/UX
Issue	ER-9398
Description	Resolved an issue where the web user interface was unable to filter access points by keyword once the column was sorted.

Component/s	UI/UX
Issue	ER-9425
Description	Resolved an issue where client are not shown on the controller web user interface.

Component/s	UI/UX
Issue	ER-8854

Resolved Issues

Component/s	UI/UX
Description	Resolved an issue where clients connected to tunneled SSID could not access controller SZ100 (configured as one port group) web user interface.

Component/s	UI/UX
Issue	ER-9301
Description	Resolved an issue where the controller did not support import EC (Elliptic Curve Cryptography) keys.

Component	Virtual SmartZone Data Plane
Issue	ER-8265
Description	Resolved an issue where data plane failed to report the tunnel statistics.

Component	Virtual SmartZone Data Plane
Issue	ER-9199
Description	Resolved an issue where virtual data plane failed to reach the controller after upgrading it.

Component	Virtual SmartZone Data Plane
Issue	ER-8601
Description	Enhanced the tunnel maintenance mechanism to reduce connectivity issues between the controller and data plane (SZ104-D/SZ124-D/SZ144-D and vSZ-D).

Component/s	Virtual SmartZone Data Plane
Issue	ER-7433
Description	Resolved an issue in tunneled WLAN where client traffic was sent to an incorrect default gateway destination.

Component/s	Virtual SmartZone Data Plane
Issue	ER-9058
Description	Resolved an issue of vSZ-D upgrade failure if it was initially created in 3.4.x/3.5.x releases.

Component/s	Virtual SmartZone
Issue	ER-9018
Description	Resolved an issue where controller CLI command failed to disable AP 2.4 GHz Tx power.

Component/s	Virtual SmartZone
Issue	ER-8214
Description	Resolved an issue where the controller was unable to configure the switch ports whose stack identity was larger than nine (Stack ID is the first part of switch port number, for example, Switch ID is 11 for Port Number "11/1/40").

Component/s	Virtual SmartZone
Issue	ER-9064

Component/s	Virtual SmartZone
Description	Enhancements related to controller CLI response time are included in this release.

Interoperability Information

Cluster Network Requirements

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

TABLE 7 Minimum Cluster Network Requirement

Model	SZ300	vSZ-H	SZ144	SZ100	vSZ-E
Latency	77ms	68ms	85ms	119ms	119ms
Jitter	10ms	10ms	10ms	10ms	10ms
Bandwidth	69Mbps	69Mbps	46Mbps	23Mbps	23Mbps

Client Interoperability

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

NOTE

Client Interoperability issues stated in the 5.2.1 release notes are also applicable to this release.

Component/s	AP
Issue	SCG-128368
Description	Samsung Galaxy M51(Android-10) version M515FXXU1AT11 is not able to detect OWE encryption WLAN.
Workaround	For connecting Samsung Galaxy M51(Android-10) version M515FXXU1AT11, set any encryption (WPA2,WPA3,Open,etc) other than OWE.

Component/s	AP
Issue	SCG-127109, SCG-112546
Description	iPad running iOS 13 and above will be detected as MAC or MAC OS when browsing using Safari. Client detection will be normal when using non native browsers like Chrome.

Component/s	AP
Issue	SCG-127709

Interoperability Information
Client Interoperability

Component/s	AP
Description	<p>The following Intel client cards do not connect to a WLAN which have enabled 802.11w as required along with 802.11r.</p> <ul style="list-style-type: none"> Intel(R) Dual Band Wireless-AC 8260 version: 20.70.19.1 date: 9/15/2020 -- Windows 10. Intel(R) Dual Band Wireless-AC 7265 - version: 19.51.31.1 date: 9/15/2020 Windows 10. <p>NOTE Issue is not seen with Intel(R) Dual Band Wireless-AC 8265 Windows 10 pro 20.70.18.2.</p>

Component/s	AP
Issue	SCG-115805
Description	Google Pixel 1 devices running Android version 9 may fail to connect to a WLAN that has enabled <i>Transient Client Management (TCM)</i> feature.
Workaround	With a different TCM values, Google Pixel 1 will able to connect to the TCM WLAN profile.

Component/s	AP
Issue	SCG-112981
Description	iPad (running OS version 9.3.5) and iPhone 4s (running OS version 6.1.3) devices do not connect to WLAN with encryption method as WPA2/WPA3-mixed profile.
Workaround	Configure WLAN with encryption method as WPA2 profile only.

Component/s	AP
Issue	SCG-123157
Description	Android 10 and 11 versions which has MAC address randomization features as <i>Default</i> affects the Wi-Fi experience.
Workaround	For MAC related authentication, disable Wi-Fi MAC randomization and select the option <i>Use Device MAC</i> while connecting to SSID.

Component/s	AP
Issue	SCG-123018
Description	iPhone release iOS 14 version which has MAC address randomization features can affect the Wi-Fi experience.
Workaround	For MAC related authentication, disable features in <i>iPhone, iPad and iWATCH iOS14</i> Wi-Fi configuration.

COMMScope®
RUCKUS®

© 2021 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
<https://www.commscope.com>