COMMSCOPE®
RUCKUS®

RUCKUS SmartZone 5.2.1 Release Notes

Supporting SmartZone 5.2.1

Copyright, Trademark and Proprietary Rights Information

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

Limitation of Liability

Trademarks

Contents

Document History

Revision Number	Summary of changes	Publication date
D	• Added T750SE AP to New Access Points on page 4, Table 1 on page 14 and IoT Suite on page 16 • Added Know Issue SCG-125341	29, September 2020
C	Added the following to Known Issues: 1. SCG-118945 2. SCG-118998	10, September 2020
B	Added SCG-122545 to Known Issues	17, August 2020
A	Initial release notes	31, July 2020

New in This Release

This section provides a high-level overview of several key features that are introduced in the SmartZone (SZ) software release 5.2.1. The release 5.2.1 is applicable to the RUCKUS SmartZone 300, SmartZone 100, SmartZone 144, vSZ-H, vSZ-E, vSZ-D and controller platforms.

AP Features

Release 5.2.1 supports the following 802.11ax APs (R550 and R850).

New Access Points

- **R550**: Wi-Fi 6 2x2 (5G) + 2x2 (2.4G) dual band dual concurrent Access Point with a single switchable integrated IoT radio
- **R850**: Wi-Fi 6 8x8 (5G) + 2x2 (2.4G) dual band dual concurrent Access Point with a single switchable integrated IoT radio
- **T750SE**: Wi-Fi 6 4x4 (5G) + 4x4 (2.4G) dual-band outdoor concurrent Access Point with external antenna connectors that supports eight spatial streams.

> **NOTE**
> DFS channels are diabled on AP T750SE.

Autonomous Cell Sizing on Wi-Fi 6 APs

The primary objective of ACS is to reduce the co-channel interference in the OBSS. Co-channel interference is the interference caused by the Neighbor APs on the same channel. Co-channel interference is a calculated by measuring the amount of time AP spends in Rx of packets not destined to it. In co-channel interference condition, substantial gain in throughput is observed when we bring the tx power of the interference source down to a level where Rx sensitivity adjustment can completely cut off the interference without sacrificing the SNR to the client by a lot. ACS achieves by coordinating the reduction in tx power between the neighboring APs in order to improve spectral reuse.

Legacy Safe Implementation

Some legacy devices like Intel drivers 18 and below cannot recognize valid Wi-Fi 6 APs. Some Mac OSs have problems with Wi-Fi 6 APs because of their large beacons. A customer that does not have control of their clients might want to provide a WLAN that they know that these buggy devices can connect to. Our system currently allows for an AP CLI command that downgrades all WLANs on the entire radio. This current interface is not easy enough nor flexible enough for our customers. This feature adds the ability to downgrade a WLAN from Wi-Fi 6 to Wi-Fi 5 on a per WLAN basis

through the GUI. With this new implementation a customer could have on the same AP one WLAN that supports Wi-Fi 6 and another WLAN that only supports Wi-Fi 5.

Multicast Rate Limit for Wi-Fi 6 APs

This feature allows multicast rate limit configuration for uplink and downlink direction (separately configurable) from SZ GUI. Users are now able to configure multicast rate limit in terms of absolute number instead of percentage of traffic. Rate limit configuration is per WLAN.

L2 ACL Wired Support

This feature supports non-user port profile for L2 ACL on wired side. This feature also introduces customized Ether Types field along with the pre-defined Ether Types field in the configuration screen of L2 ACL profile.

Mesh on 2.4GHz and 5GHz

RUCKUS SmartMesh technology is now available on Wi-Fi 6 APs for both bands, 2.4GHz and 5GHz.

160MHz support on Wi-Fi 6 APs

GUI and CLI support to enable 160MHz on applicable Wi-Fi 6 APs which include T750, R650, R750, R850 and T750SE.

Limitations:

1. Mesh mode in 160Mhz is not supported. There is no explicit disabling of Mesh when radio is configured for 160Mhz mode.

2. No support for MU/OFDMA in beacons IE's when 160Mhz is enabled.

3. 80+80 modes operates radio on 80Mhz mode.

4. 160Mhz is not supported when AP is operating in 802.3af power mode.

Save HiMem Log in to AP File System in Rotating Log

It is quite common to require enabling HiMem log for troubleshooting AP issues. HiMem is an area of RAM reserved for the purpose of troubleshooting and debugging, data written to HiMem are preserved through reboot cycle. With this feature, when AP reboots, HiMem content is copied to AP filesystem. Any existing file is rotated and new content is copied into recent file. The

HiMem is cleared and AP starts copying new log messages again into HiMem memory.

Channelfly Enhancements

The existing Channelfly algorithm has been enhanced to incorporate (off-channel) background scanning data to deliver network-level spectrum utilization. Channelfly now can optimally assign APs to non-overlapping channels even in the absence of active Wi-Fi traffic. An added benefit is that Channel assignments also deliver between airtime utilization during receive. GUI enhancements allow users to control when channel changes occur based on their specific network utilization patterns

Limitations

SCG-119237

1. Clients connected on 2.4GHz radio on MAP are not accounted in count threshold on RAP during a channel change decision.

2. Clients connected on tunnel WLAN on both 2.4 GHz and 5 GHz are not accounted in client count threshold on RAP during a channel change decision.

SCG-121670

1. 2.4GHz lacks logic that considers 20 MHz channel overlaps. Example, consider a situation where the AP is on Ch 1, and Ch 2 and 6 are available with no neighbors. Ch 6 is more ideal because of non-overlap, but chanflybg does not take that into consideration. For now, the user is recommended to enable ONLY 1, 6, 11, or 1, 4, 7, 11.

Legacy Limitations

Assuming that user has configured Legacy ChannelFly (using RKSCLI):

1. After this configuration , if any configuration moves from the controller, channel selection method changes based on the controller configuration. In other words, *Legacy ChannelFly* configuration is not persistent across controller configuration move.

2. Legacy ChannelFly configuration using RKSCLI is not persistent across AP reboot.

802.11ax AP Airtime Statistics

To provide an easy way for our customers to understand Airtime Utilization for 802.11ax APs, RUCKUs extends the airtime statistics (airtime utilization details) for 802.11ax APs - Free Airtime, Tx/Rx (Multicast/Broadcast), interference, non-Wi-Fi interference, management traffic, etc. When seen through the controller GUI, these statistics provide meaningful insights into various aspects of the wireless network.

- **Network Overhead**: Allows the administrator to view the ratio of transmitted and received data vs management, which tells the administrator how much overhead is on the network.
- **Impact of Neighbors**: Allows the administrator to view the airtime impact of managed neighbors that are operating on the same or overlapping channels. This also allows the administrator to evaluate the channel selection system.
- **Impact of Rogues**: Allows the administrator to view the airtime impact from non-managed rogue APs.
- **Uplink / Downlink Ratios**: Allows the administrator to easily visualize the uplink and downlink airtime ratios, which can be cross-referenced with traffic ratios to evaluate efficiency of up/down links.
- **Impact of Non-Wi-Fi Interference**: Allows the administrator to view the airtime impact of non-Wi-Fi interference sources.

My.ruckus Configuration Knob

In release 5.0, we introduced the *my.ruckus* web diagnostics page feature, which is available for LBO and if the AP's management VLAN is in default VLAN(1). However, the same would not work for tunneled-WLAN and non-default management VLAN use-cases.

In release 5.2 we introduced the support for tunneled-WLAN and non-default management VLAN use-cases by adding ACLs. However, we noticed throughput impact due to the introduction of ACLs. Hence in 5.2.1, we are adding this configuration knob to let our users turn on/off this support.
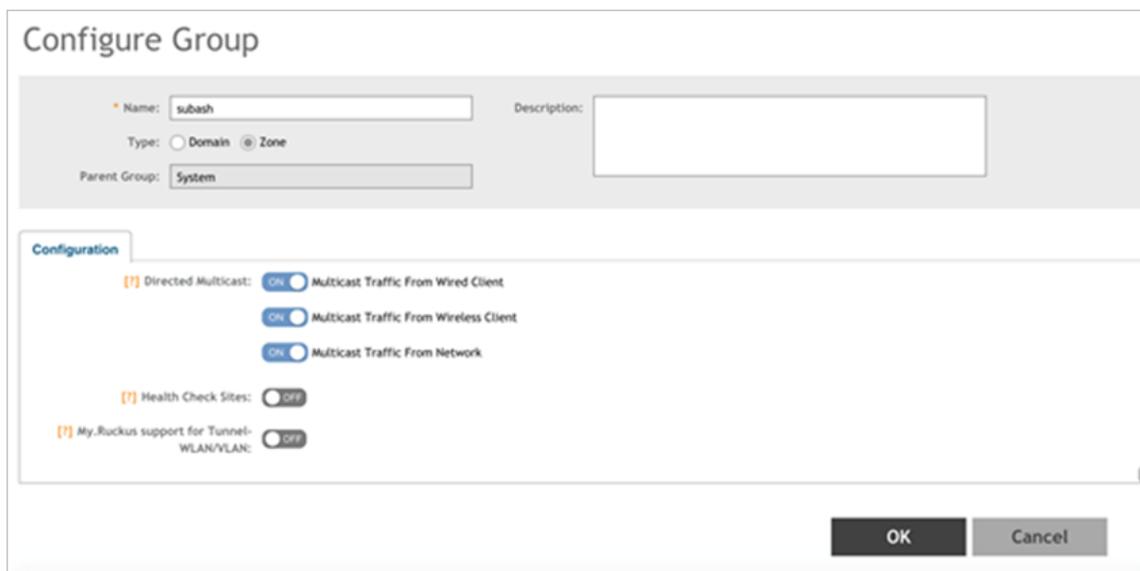
OS Fingerprint Enhancement

In order to leverage OS detection for more functionality than just visibility, it is important to have more granularity over OS type and version. OS fingerprint enhancement is requirement from most customers that use the OS Fingerprint feature. RUCKUS AP has Fingerbank as OS detection solution.

The goal of this feature is to enhance our client OS fingerprinting such that we can identify more granular levels of device OS. There are two components of this: More granular device identification and OS version identification. In this release, RUCKUS made the enhancements on the AP's existing Fingerbank database and HTTP user-agent based device detection to meet these requirements.

Simplify GUI Option for Power Source in AP Configuration

The Power over Ethernet (PoE) mode as per industry standards have the following options.

Selection	Power @ PSE	Power @ AP (100m Cable)
802.3af	15.4W	12.95W
802.3at	30W	25.5W
802.3bt/Class 5	45W	35W to 40W **NOTE** The standard specification for 802.3bt/class5 is 40W. However to maintain backward compatibility with AT+ power mode, we are going continue to set this to 35W.
802.3bt/Class 6	60W	51W
802.3bt/Class 7	75W	62W
PoH	90W	71.3W

However the APs that RUCKUS currently use have use the convention AF, AT, AT+ modes. The objective is to standardize our convention going forward. The standardization will apply when we want to force the AP to a certain POE power mode. If the AP is set to AUTO POE mode, the feedback will also display the POE mode the AP is currently configured in.

Here is the mapping of the Old and New POE configuration:

Current POE Mode Output	New POE Mode Output
AC/DC Power supply	AC/DC Power supply
802.3af	802.3af
802.3at	802.3at
802.3at+	802.3bt/Class 5
POE/Injector	POE/Injector
	802.3bt/Class 6
	802.3bt/Class 7

GUI Enhancement for AP Configuration

With this feature, AP specific configuration functions will now be displayed on the AP Info pane on the Controller GUI. The Info pane is enhanced to show the number of active radios chains, the interfaces enabled or disabled (Downstream Ethernet, USB, PoE_Out, SFP vs Ethernet for backhaul on outdoor APs). The Info pane also details the source of power to each AP, i.e. AC/DC power or POE input power in terms of 802.3af, 802.3at, 802.3bt, etc.

Prior to this feature, the only way to query the physical configuration of the AP was via CLI commands; and the lack of real-time feedback from the AP on these configuration options often led to incorrect diagnoses of observed Wi-Fi connectivity issues.

Report Average MCS Metrics

AP has the ability to get the latest MCS matrix data from driver report so far. Its internal module takes the responsibility to calculate delta value for each category of MCS level, so that we can recognize the most traffic data rate performed in bin period of time. With this release, we will calculate the mean or median Tx and Rx MCS rate on a per client and per AP basis.

The calculated metrics will be reported on the controller web user interface well as via GPB interface to external data collectors.

Switch Management

SmartZone 5.2.1 introduces the following switch management features.

- **Remote CLI:** Enables users to access the CLI session of the selected ICX switch directly from the SmartZone WEB UI. Users will be able to run monitoring/configuration commands.

    ATTENTION
    This feature can be accessed only by the System Super-Administrator in 5.2.1 release.

- **Configuration:** The following configuration options are added to enable more features on ICX switches.

    - Protected ports
    - Granular PoE budget limit at switch port level
    - Ability to change default VLAN
    - Ability to set management VLAN
    - Ability to configure ports across multiple switches in a Switch Group

- – QoS (Quality of Service)

  - › Additional ACL options to remark and/or prioritize traffic
  - › Port level QoS configuration including Voice VLAN and LLDP-MED setting

- **Monitoring**

  - – Ability to search for a client at global level (entire system as opposed to a single switch group).
  - – Group level firmware upgrade:

    - › Users can now upgrade all the switches within a group instead of manually selecting switches one at a time.
  - – Ability to download syslog files of a selected Switch.
  - – Group level firmware enforcement:

    - › Users can now set a minimum ICX firmware release against a group. Switches joining the group with a lower version will automatically get upgraded.

ZAPd Enhancement

RUCKUS Speedflex throughput test tool, historically and prior to this release(R5.2.1), keeps the port 18301 open for both TCP and UDP protocol in Access Point and the controller. It leaves attack surface open and the listener of this port is ZAPd (daemon).

To eliminate this security vulnerability, a UI switch is introduced to enable or disable speed test and hence ZAPd runs or stops accordingly. When ZAPd is not running, AP or controller is not listening to that port.

ZAPd is disabled by default on both controller and AP. ZAPd on AP can be enabled by configuring test speed option in **AP Advance Settings** in the controller web user interface. On the controller ZAPd starts automatically on triggering a speed test and stops and when the test is completed.

RKS CLI commands **get/set zapd enable/disable** is introduced in this release to start or stop ZAPd, but we recommended that you use these commands with caution since the user interface and CLI mode configuration could go out of synchronization. In such cases, toggling the testspeed option in the controller web user interface will synchronize the configuration between the user interface and CLI mode.

Additional Enhancements

The following additional enhancements have been made in the 5.2.1 release:

- ACLB for 802.11ax APs.
- IPSec support is now available on 802.11ax APs
- Spectrum analysis for 802.11ax APs.
- Rogue AP aggressive de-authentication for 802.11ax APs.
- MBO for 802.11ax APs
- Add client latency measurement for 802.11ax APs.
- URL filtering license enhancement for Ethernet ports.
- Change of Authority (COA) for Wired clients allows the user to change the role assigned for dot-1x enabled wired clients using COA messages from Radius server.
- Uboot Ctrl-C is disabled on selected AP for security consideration.

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 Plan 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: **5.2.1.0.515**
- Control Plane Software Version: **5.2.1.0.383**
- Data Plane Software Version: **5.2.1.0.515**
- AP Firmware Version: **5.2.1.0.698**

SZ100

- Controller Version: **5.2.1.0.515**

- Control Plane Software Version: **5.2.1.0.383**
- Data Plane Software Version: **5.2.1.0.101**
- AP Firmware Version:**5.2.1.0.698**

SZ144

- Controller Version: **5.2.1.0.515**
- Control Plane Software Version: **5.2.1.0.383**
- Data Plane Software Version: **5.2.1.0.101**
- AP Firmware Version:**5.2.1.0.698**

vSZ-H and vSZ-E

- Controller Version: **5.2.1.0.515**
- Control Plane Software Version: **5.2.1.0.383**
- AP Firmware Version:**5.2.1.0.698**

vSZ-D

- Data plane software version: **5.2.1.0.515**

   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 at: 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-100: **5.2.1.0.515**
- Control plane software version in the WLAN Controller : **5.2.1.0.383**
- AP firmware version in the WLAN Controller:**5.2.1.0.698**

RUCKUS IoT Controller

- RUCKUS IoT Controller version: 1.6* (* Scheduled for release in August 2020).

- VMWare ESXi version: 5.5 and later

- VMWare VM Player version: 12 and later

- Oracle VirtualBox version: 5.1.20 and later

- Google Chrome version: 61 and later

- Mozilla Firefox version: 56 and later

   NOTE
   Refer to RUCKUS IoT 1.6* Release Notes for Release Build Compatibility and IoT Upgrade Support Matrix

Public API

Click on the following links to view:

- SmartZone 5.2.0 Public API Reference Guide (ICX Management), visit http://docs.ruckuswireless.com/smartzone/5.2.1/switch-management-public-api-reference-guide-521.html

- SZ100 Public API Reference Guide, visit http://docs.ruckuswireless.com/smartzone/5.2.1/sz100-public-api-reference-guide-521.html

   NOTE
   SZ100 Public API link is for SZ144 as well.

- SZ300 Public API Reference Guide, visit http://docs.ruckuswireless.com/smartzone/5.2.1/sz300-public-api-reference-guide-521.html

- vSZ-E Public API Reference Guide, visit http://docs.ruckuswireless.com/smartzone/5.2.1/vsze-public-api-reference-guide-521.html

- vSZ-H Public API Reference Guide, visit http://docs.ruckuswireless.com/smartzone/5.2.1/vszh-public-api-reference-guide-521.html

Application Signature Package

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.
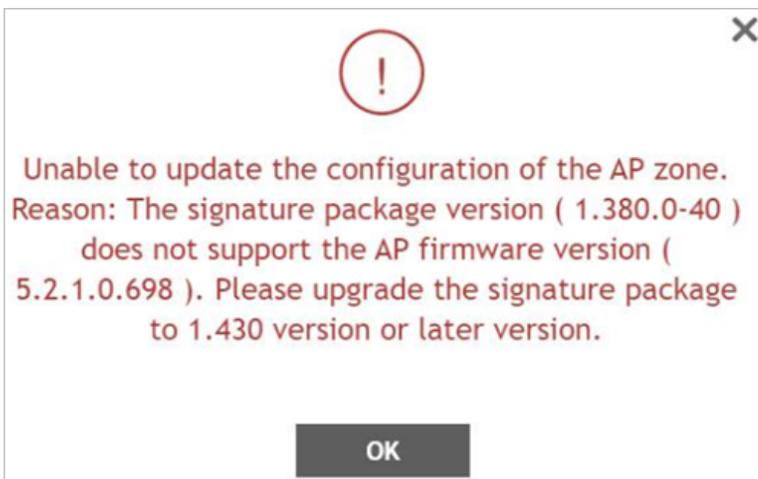
Do follow this mandatory process before upgrading AP zone firmware:

1. Download Signature package by visiting the RUCKUS support site.

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]**

Upgrade Guide

- Do refer to the *RUCKUS SmartZone Upgrade Guide, 5.2.1* for upgrade details. This section is removed from the release notes.

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

LWAPP2SCG must be disabled on 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 > 5.2.1	5.2 , 5.2.1
5.1.x > 5.2.1	5.1.x, 5.2.1
3.6.x > 5.0 > 5.1.x > 5.2.1	3.6.x, 5.0, 5.1.x, 5.2.1
3.6.x > 5.1.x > 5.2.1	3.6.x, 5.1.x, 5.2.1
3.6.x > 5.2.1	3.6.x, 5.2.1

> **NOTE**
> For further details refer to the section *Multiple AP Firmware Support in the SZ100/vSZ-E/SZ300/vSZ-H* in SmartZone Upgrade Guide, 5.2.1

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 diabled on AP T750SE.

Important Note About the PoE Power Modes of the R730, R720, R710, T610, and R610 APs

> **NOTE**
>
> When the R720, R710, T610 series AP is connected to an 802.3af PoE power source, the USB interface and the second Ethernet port are disabled, and the AP radios do not operate in maximum capacity. For more information, refer to the latest Outdoor Access Point User Guide or Indoor Access Point User Guide.

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		

> **NOTE**
> ICX 7550 support also has a dependency on FastIron 08.0.95.

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
FastIron 08.0.80	Y	Y	N	N	N
FastIron 08.0.90a	N	Y	Y	Y	Y
FastIron 08.0.91	N	Y	Y	Y	N
FastIron 08.0.92	N	N	Y	Y	Y
FastIron 08.0.95	N	N	N	N	Y

Following is the matrix for switch management feature compatibility:

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 1.6* and is compatible with the following controller and access point hardware and software.

* Scheduled for release in October 2020.

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)

- R850 Access Point (R850)

- 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 (SZ-100)

- RUCKUS IoT Controller (RIoT)

The below table lists the supported IoT end devices.

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	
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	LIGHTFY 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 Valeto (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
Revogi Lamp	Bulb	BLE	Revogi	Revogi	
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

Known Issues

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

> **NOTE**
> Known issues stated in the 5.2 release notes are also applicable to this release.

Component/s	AP
Issue	SCG-125341
Description	1. By default external antenna is enabled in T750SE. In order to enable sector antenna, user must disable external antenna on both 2.4 and 5 GHz radios together and apply the configuration. 2. To enable or disable external antenna, user must select both the radios together and apply the configuration.
Workaround	**For AP Zones** navigate to: **AP model specific configuration** > **select T750SE > Enable/Disable radio button** together for external antenna (2.4 GHz or 5 GHz) **For APs** navigate to: **AP model specific option** > **Enable/Disable radio button** together for external antenna (2.4 GHz or 5 GHz) ⚠️ **CAUTION** **Enabling external antenna on 2.4 GHz and disabling it on 5 GHz (or vice versa) and applying the configuration can create unexpected situation and AP may not be useable.**

Component/s	AP
Issue	SCG-118945
Description	Single client TCP Downlink and Uplink throughput are reduced 8% and 18% in presence of 39 associated clients. For single client peak performance demos, please try avoid associating multiple clients. If its not possible, use below workaround to address issue by disabling ATF, UL scheduler and UL OFDMA.
Workaround	In RKS CLI mode: 1. Set *atf wifi1* mode to disable 2. Reboot the AP 3. Send the below two commands to disable UL scheduler, *UL OFDMA* ``` iwpriv wlan32 he_ulofdma wifitool wlan32 setUnitTestCmd 0x47 2 92 ```

Component/s	AP
Issue	SCG-118998
Description	MU performance with two S10 clients is lower when ATF is enabled. In 40 MHz mode, MU-MUMO throughput gain is reduced from 25% to 4%. For performance demos, the workaround for this issue is to disable ATF feature.

Component/s	AP
Workaround	In RKS CLI mode: 1. Set *atf wifi1* mode to disable 2. Reboot the AP

Component/s	AP
Issue	ER-7951
Description	Packets larger than 1582 bytes are dropped by all Wave-2 AP models

Component/s	AP
Issue	ER-7746
Description	Multiple **Symbol (model:MC-9060G)** handheld devices fail to connect to **WPA-TKIP** SSID

Component/s	AP
Issue	ER-8298
Description	For AP M510 with DWPD (Dynamic Wan Port Detection) is enabled and when *cellular only* option is enabled (LTE only backhaul) and if Ethernet cable is not connected to the WAN uplink switch, then DHCP/NAT will not work for wired clients connected to the AP. **NOTE** Wireless clients are not impacted.
Workaround	Connect one of the WAN uplink ports to a switch via an Ethernet cable. Once its connected, br0 interface of AP should get IP address, and DHCP/NAT will start working for wired clients as well

Component/s	AP
Issue	SCG-107270
Description	2.4Ghz air time utilization exceeds 75% due to new reporting mechanisms, but this does impact the performance

Component/s	AP
Issue	AP-11670
Description	Outbound L3 ACL works with split tunnel but inbound L3 ACL does not work with split tunnel

Component/s	AP
Issue	AP-12811
Description	Multicast iPerf traffic exceeds the configured rate limit value in the downlink process

Component/s	AP
Issue	AP-13005
Description	L2 ACL rules does not apply for RGRE tunneled traffic on AP WAN link

Component/s	AP
Issue	AP-13027

Component/s	AP
Description	Ethernet types configured as Stream reservation protocol, RARP (Reverse Address Resolution Protocol), VLAN frames, Short Path Bridging, Jumbo frames, Fiber channel over Ethernet and Double Tagging in release 5.2 will not be seen on the AP after the controller (vSZ) is upgraded to release 5.2.1
Workaround	The AP Zone has to be upgraded to reflect the configuration

Component/s	AP
Issue	SCG-118683
Description	Median MCS (Modulation and Coding Scheme) rates are the same when SGI (Short Guard Interval) is enabled and disabled

Component/s	AP
Issue	SCG-118122
Description	Incorrect non Wi-Fi interference values in airtime utilization when 802.11ax AP reboots

Component/s	AP
Issue	SCG-116615
Description	Median Tx MCS metrics is incorrect for the 802.11ax AP when an 802.11ac AP client is connected

Component/s	AP
Issue	SCG-115887
Description	Wired client does not update information, client needs to disconnect/reconnect to upgrade info in 5.2.1 **NOTE** Will be fixed post 5.2.1 release

Component/s	AP
Issue	SCG-112888
Description	802.11ax AP airtime utilization values are not correct when compared with 802.11ac APs

Component/s	AP
Issue	AP-12728
Description	The page *my.ruckus* does not show the device type information in IPv6 mode

Component/s	AP
Issue	AP-12738
Description	The page *my.ruckus* takes approximately 10 to 11 minutes to update after the client roams to other APs

Component/s	AP
Issue	SCG-119669
Description	Changing AP name takes longer than expected

Component/s	AP
Issue	SCG-120551
Description	The rate limit value is less than 30Mbps though the rate limit is configured for 40, 60 and 100Mbps **NOTE** This limitation is specific only to 802.11ax APs.

Component/s	AP
Issue	SCG-119742
Description	Instagram and YouTube traffic sometimes will show as N/A (not applicable), when traffic from client is IPv6

Component/s	AP
Issue	SCG-119641
Description	802.11ax APs marks BK traffic as BE traffic as per latency histogram

Component/s	AP
Issue	SCG-120394
Description	Data loss after channel change in 802.11ax/802.11ac AP

Component/s	AP
Issue	SCG-114343
Description	802.11ax channel switch time is higher causing MAC/IoS clients to disconnect

Component/s	AP
Issue	SCG-120061
Description	According to MLISA PCAP functional design, once HCCD failure occurs, RCCD will notify driver module to stop monitor and update the capture file to controller. Therefore, AP's only ability is monitoring one connection failure at one time then send capture result to controller for reference. In the words, multiple captured file for multiple connection failure session is not supported in current design.

Component/s	AP
Issue	SCG-121156
Description	Design limitation as Radius PKS do not include STA MAC address and we may capture other STA's Radius PKS while doing the capture. Will be fixed in future release.

Component/s	AP
Issue	SCG-118295
Description	Mesh operations with bandwidth set to 160MHz is not supported. AP in 160Mhz radio mode does not exclusively inhibit if a MAP tries to connect in MESH mode
Workaround	Make sure mesh is disabled manually if 160MHz is enabled.

Component/s	AP
Issue	SCG-121601
Description	Expected behavior as change in channelfly mode, from new channelfly mechanism to legacy channelfly, there needs to be clients connected to AP for process to start. It might take seven minutes to find new channel with legacy channelfly after change

Component/s	AP
Issue	SCG-119000
Description	R600 continuously reboot issue seen only when upgrading from release SmartZone software 5.2.0.0.699 to 5.2.1 but not when upgrading from 5.2.0.0.5527

Component/s	AP
Issue	SCG-120946
Description	MacBook not changing channel issue only seen with Catalina 10.15.5 and not with Big Sur, El Capitan and Mojave.
Workaround	Disable CSA for that particular iOS having the issue

Component/s	AP
Issue	SCG-117506
Description	If CA chain is uploaded and OCSP is configured for IPSec then the controller fails to initiate the OCSP status request towards OCS responder
Workaround	Upload all intermediate certificates individually in the controller

Component/s	AP
Issue	AP-10347
Description	On changing RAP channel from Static to Auto, the downlink MAP disconnects and reconnects **NOTE** Expected behavior to be fixed in future release.

Component/s	AP
Issue	SCG-122381
Description	After authorized Guest Access local database WLAN, user equipment (Chrome 84.0.4147.89) failed to redirect to the controller web server page

Component/s	AP
Issue	SCG-56994
Description	AP SNMPv3 displays INFORM when the notification type is set to TRAP

Component/s	AP
Issue	SCG-120210

Component/s	AP
Description	AP does not apply Portal Certificate success if the user uploads: • A single certificate rather a certificate chain • Certificate that terminates with \n • Certificate that do not start with the "---*BEGIN CERTIFICATE*---" keyword

Component/s	AP
Issue	SCG-117912
Description	The downlink rate of APs R650 and R550 is too high through Speedflex

Component/s	AP
Issue	SCG-121571
Description	AP R500 takes more than five minutes to apply the configuration when channelfly configuration is changed on both the radios at the same time

Component/s	AP
Issue	AP-13622
Description	Large number of Rogue APs can affect channelfly's background scan mechanism and affect the channelfly readings resulting in more channel changes

Component/s	AP
Issue	ER-8691
Description	Controller and AP receives 404 reject from cloudpath for health check HEAD request when secondary cloudpath server is configured

Component/s	AP
Issue	ER-8660
Description	R750 AP's do not populate real time data on SPoT analytics

Component/s	AP
Issue	ER-8648
Description	After upgrading controller (vSZ-H) release 3.6.2.0.222 to 5.2.0.0.699, controller does not publish MGR message to LBS

Component/s	AP
Issue	ER-8555
Description	In DPSK WLAN, UE reverts to the default VLAN when AP 802.11r is enabled

Component/s	AP
Issue	ER-8520
Description	Flagged APs are not seen in the exported CSV file when the view mode is set to Zone

Component/s	AP
Issue	ER-8159
Description	Guest portal stops working when upgrading a zone from release 5.1.2 to 5.2
Workaround	Set *lighttpd* as disable to avoid the issue

Component/s	AP
Issue	ER-7979
Description	Controller SZ300 (1) node of (3) node cluster stops placing CPU usage historical data in GUI

Component/s	AP
Issue	ER-6886
Description	APs communicate with vSZ controller over site to site VPN can have a session manager delayed response between controller and APs, which could result in timeout errors during DPSK authentication

Component/s	Control Plane
Issue	SCG-118090
Description	AP network settings will set as *Keep the APs Settings* after migrate from ZD3K **NOTE** AP configuration from migration is not affected

Component/s	CLI
Issue	SCG-121037
Description	Resetting *channelfly_bg* on 2GHz CLI also resets 5GHz **NOTE** Process to be changed to separate both 2GHz and 5GHz in future release

Component/s	Data Plane
Issue	ER-8265
Description	In controller SZ300 three node cluster, GRE tunnels seen in logs do not match the logs from UI/CLI

Component/s	Data Plane
Issue	ER-8539
Description	SZ124D data IP address changed to 0.0.0.0 after grid power loss but management IP address is the same

Component/s	Switch
Issue	SCG-121306
Description	If there are no PDs (Power Device) connected to the port, even though the PoE (Power over Ethernet) budget of a port is set, the value is shown as zero. The configured value is shown when a PD is plugged in

Component/s	Switch
Issue	SCG-121194
Description	In 5.2.1 release, users cannot set a PoE (Power over Ethernet) budget great than 30,000 mW (30W)
Workaround	If a client wants to use a higher value, you would need to configure it from the Switch

Component/s	System
Issue	SCG-90797
Description	IOS, MAC OS and Windows mobile clients may not connect with TCM enabled WLAN if the join wait time is more than 10 seconds as the clients send limited number of probe requests

Component/s	System
Issue	SCG-115436
Description	Upgrade ZoneDirector (ZD) to its supported version or above as listed below before migrating to controller platform release 5.2.1. • 9.13.3.0.164 • 10.0.0.0.1424 • 10.0.1.0.93 • 10.1.0.0.1515 • 10.1.2.0.277 • 10.2.0.0.189 • 10.2.1.0.159 • 10.3.0.0.398 • 10.3.1.0.24 • 10.4.0.0.70 If your ZD login URL ends with (*/admin10) or release after 2019/11, it cannot migrate to SmartZone release 5.2 and previous versions.

	9.13.3.0.164	10.0.0.0.1424	10.0.1.0.93	10.1.0.0.1515	10.1.2.0.277	10.2.0.0.189	10.2.1.0.159	10.3.0.0.398	10.3.1.0.24	10.4.0.0.70
ZD1200	v	v	v	v	v	v	v	v	v	v
ZD3000	v	v	v	v	v	v	v			
ZD5000	v	v	v							

Component/s	System
Issue	ER-8608
Description	In controller SZ-300 : msgdist keeps recording ERR in both of Leader/Follower nodes

Component/s	System
Issue	ER-8454, SCG-121213
Description	Two node cluster w/ single interface, event log reporting Foreign SmartZone IP 128.165.54.205

Component/s	System
Issue	SCG-122545
Description	SNMP walk of RUCKUS-SCG-WLAN-MIB displays erroneous string for *ruckusSCGWLANZone* value

Component/s	UI/UX
Issue	SCG-115978
Description	Device policy summary page does not display number of bytes consumed by wired clients in *hostname-bytes* table

Component/s	UI/UX
Issue	SCG-115977
Description	Device policy summary page displays wired clients information when WLANs filter is selected

Component/s	UI/UX
Issue	SCG-117660
Description	Controller does not persist and shows on web user interface Cassandra 3001 internal database error

Component/s	UI/UX
Issue	SCG-76181
Description	If a zone that has been added to a report is deleted, the corresponding report will fail to be completed because the zone is missing

Component/s	UI/UX
Issue	SCG-115901
Description	Clients should not reuse the same session to send different CCD request to the identical node of the controller. From the controller's point of view, it can only send back CCD notification base on user session. If the client uses the same session for multiple CCD client request, the controller is confused and could cause an error. Clients must use different session to send different client MAC addresses for CCD.
Workaround	Clients can use different browsers to login to the controller. They can use the same login account. In addition, clients can also use Google chrome's incognito window to login to the controller in a different tab under the mode of incognito window.

Component/s	UI/UX
Issue	SCG-117702
Description	The web user interface does not show the last schedule synchronization trigger time. Instead it shows it as *N/A*

Component/s	UI/UX
Issue	ER-8568
Description	On a customized guest portal logo, it shows the right logo when entering the guest pass, terms and conditions page but when the client gets authenticated it shows the default RUCKUS logo

Changed Behavior

The following are the changed behavior issues.

Component/s	AP
Description	By default, *my.ruckus support* for LBO, tunneled-WLAN and non-default management VLAN is **disabled** from this release. In the controller web user interface navigate to **AP Zone Advance Setting** to enable *My.Ruckus support for Tunnel-WLAN/VLAN* .

Component/s	AP
Issue	SCG-110761
Description	AP events 303/312/314 will be seen when ever discontinuous event is generated with > 15 minutes time difference with the controller

Component/s	System
Issue	SCG-118221
Description	RUCKUS does not support user equipment - SpeedFlex application to run speed test against the controller due to security reason. The speed test is not reliable, and serves only as E2E connectivity
Workaround	A simple ping from **User Equipment** > **Controller** can be the replacement of this option within SpeedFlex feature

Component/s	CLI
Issue	ER-8103
Description	1. Enhanced the performance and memory usage for the command: `(config)# domain <domainName>`

Component/s	Data Plane
Issue	ER-8282
Description	Controllers vSZ-D and SZ100-D CLI now has the capability to support restore feature

Component/s	Public API
Issue	ER-7957
Description	Public API now allows clients to disable WLAN by using the parameter *probeRssiTHr*

Component/s	Public API
Issue	ER-7969
Description	Enhanced error message when calling create or update Zone Public API with nonexistent *Tunnel Profile ID*

Component/s	Switch Management
Issue	ER-8244

Component/s	Switch Management
Description	If the switch is running firmware version 08.0.90 and above, VLAN 4093 is no longer a reserved VLAN

Component/s	System
Issue	ER-8232
Description	*SCG-Universal-Exportor* lowers the CPU usage when the LBS (Location Based Services) is activated

Component/s	System
Issue	ER-8145
Description	Resolved an issue where it failed to download snapshot file > 1GB on the web user interface with slow download speed. Buffer is now enhanced to 2GB which is guarantee file size

Component/s	System
Issue	ER-8234
Description	Enhanced the Tomcat memory usage when the controller is enabled for SCI

Resolved Issues

The following are the resolved issues related to this release.

Component/s	AP
Issue	ER-8428
Description	Resolved an issue of APs being stuck in a new configuration or update process state

Component/s	AP
Issue	ER-8211
Description	Resolved an issue where AP model specific interface over-ride reverted after moving from one AP Group to another within the same Zone

Component/s	AP
Issue	ER-7954
Description	Resolved an issue where the AP was not able to be move to a Zone which had more than 1500 APs

Component/s	AP
Issue	ER-7922
Description	Resolved an issue where *Rough-AP* event could not be triggered in time

Component/s	AP
Issue	ER-7877
Description	Resolved an issue where the controller failed to check VLAN pooling profile when deleting it

Resolved Issues

Component/s	AP
Issue	ER-7899
Description	Resolved an issue where AP re-balance and tunnel flapping did not work well

Component/s	AP
Issue	ER-7924
Description	Resolved an issue where AP br0 interface showed MTU size as 850 after ZoneDirector migration

Component/s	AP
Issue	ER-8170
Description	Resolved an issue where the AP failed to establish the SSH tunnel to controller when the AP is configured in dual mode (static IPv4 address and auto IPv6 address)

Component/s	AP
Issue	ER-8269
Description	Resolved an issue where the controller failed to generate AP by *null profile identifier* of the zone's multiple tunnel configuration

Component/s	AP
Issue	ER-7997
Description	Resolved an issue where 5G channel range for AP Group was not applicable

Component/s	AP
Issue	ER-8241
Description	Resolved an issue where root AP failed to beacon mesh VAP interface after migrating from ZoneDirector in release 3.6.2

Component/s	AP
Issue	ER-8167
Description	Resolved an issue where the AP configuration update failed because the time zone buffer was too small for updating the AP RPM key

Component/s	AP
Issue	ER-7920
Description	Resolved an issue where the connection failure increased drastically in a fast roaming scenario

Component/s	AP
Issue	ER-8116
Description	Resolved an issue where WLAN inactivity timeout limit for 802.11ax AP failed to update when the original value exceed the limit

Component/s	AP
Issue	ER-8011

Component/s	AP
Description	Resolved a packet flood at NSS*rflow offload* when a packet with same RX address and TX address hit the module

Component/s	AP
Issue	ER-7870
Description	Resolved AP R730 watchdog timeout issue

Component/s	AP
Issue	ER-7204
Description	Resolved an issue with mesh APs establishing a connection to an uplink AP when smart uplink selection is enabled

Component/s	AP
Issue	ER-6748
Description	Resolved an issue where multicast group caused multicast/broadcast packets to drop

Component/s	AP
Issue	ER-6780
Description	Resolved an issue where fast roaming caused multicast/broadcast packets to drop

Component/s	AP
Issue	ER-8085
Description	Resolved an issue where clients in sleep mode were unable to receive multicast/broadcast packets

Component/s	AP
Issue	ER-8161; ER-7937
Description	Resolved an issue where erroneous AeroScout packets were sent to AeroScout engine server

Component/s	AP
Issue	ER-8299
Description	Resolved an issue where roaming client assigned the IP address from local VLAN and not from the RADIUS server

Component/s	AP
Issue	ER-8007; SCG-112364
Description	Resolved an issue where TX average MCS rate was higher than the actual rate

Component/s	AP
Issue	ER-8340
Description	Resolved an issue where Mesh stopped working on changing to static channel configuration

Resolved Issues

Component/s	AP
Issue	ER-8318
Description	Resolved an issue where airtime statistics showed incorrect values in the support information file

Component/s	AP
Issue	ER-8278
Description	Resolved an issue where obfuscating private key was seen in the AP support log

Component/s	AP
Issue	ER-8189
Description	Resolved an issue where AP failed to upgrade to SmartZone release 5.2

Component/s	AP
Issue	ER-8171
Description	Resolved an issue where the support log file failed to download

Component/s	AP
Issue	ER-8121
Description	Resolved an issue where the client failed to obtain the IP address when device policy was configured

Component/s	AP
Issue	ER-8108
Description	Resolved an issue where the captive portal URL was incorrect when redirecting in WISPr network

Component/s	AP
Issue	ER-7896
Description	Resolved an issue of AP reboot due to kernel panic caused by memory leak

Component/s	AP
Issue	ER-7689
Description	Resolved an issue of high CPU utilization due to collected processes

Component/s	AP
Issue	ER-8455
Description	Resolved an issue where event code 306 (event type : AP channel updated) was not displayed for 2.4GHz channels in 802.11ax AP models

Component/s	AP
Issue	ER-8025; ER-7874
Description	Resolved an issue caused AP R710 (WAVE2) APs to reboot due to target fail detected error

Component/s	AP
Issue	ER-7956
Description	Resolved an issue of decreased throughput performance in WPA/WAP2 WLANs

Component/s	AP
Issue	ER-7636
Description	Resolved an issue of AP reboot caused by kernel panic

Component/s	AP
Issue	ER-7800; ER-7986
Description	Resolved an issue where the controller created multiple APs and the data plane heartbeat was lost, which caused a disconnection with false alarms and a Cassandra connection problem. Resolved an issue of AP configuration update failure caused by Cassandra connection problem

Component/s	AP
Issue	SCG-115354
Description	This is expected as per design and this is a new daemon which gets restarted every 30 minutes and hence the console message is inevitable

Component/s	AP
Issue	SCG-117371, ER-8324
Description	Resolved an issue where the controller displayed the *dBr* value instead of the extrapolated *dBm* value

Component/s	Analytics
Issue	ER-8257
Description	Resolved an issue of customer onboarding and file open error

Component/s	CLI
Issue	ER-8127
Description	Resolved an issue where the controller failed to create the domain using CLI mode

Component/s	CLI
Issue	ER-8068
Description	Resolved an issue where the CLI command output for **show cluster-node** shows the number of APs as zero

Component/s	CLI
Issue	ER-8103
Description	Enhanced the performance and memory usage for the command: `(config)# domain <domainName>`

Resolved Issues

Component/s	Control Plane
Issue	ER-8218
Description	Resolved an issue where the RADIUS process failed when the boundary condition was violated

Component/s	Control Plane
Issue	ER-7861
Description	Resolved an issue where controller upgrade failed when a client uploaded a private key with password

Component/s	Control Plane
Issue	ER-8024
Description	Resolved an issue where controller failed to set up the data plane IP address with different NAT IP address

Component/s	Data Plane
Issue	ER-7833
Description	Resolved an issue where data plane dropped huge packets from the core network and sent a notification to *nordVPN* server to adjust the packet size

Component/s	Data Plane
Issue	ER-8097
Description	Resolved an issue where the data plane tunnel manager caused a memory overflow

Component/s	Data Plane
Issue	ER-8107
Description	Resolved an issue where the data plane failed to create a host entry when receiving broadcast packet

Component/s	Switch Management
Issue	ER-7859
Description	Resolved an issue where some redundant memory usage in the current Switch Management design on endpoints of Spring Boot Actuator caused out of memory situations

Component/s	Switch Management
Issue	ER-8050
Description	Resolved an issue where Switches manual backup failed due to time limit exceed

Component/s	System
Issue	ER-8105
Description	Resolved an issue where *snmpwalk* shows incorrect WLAN status when WLAN schedule is set to **Always Off**

Component/s	System
Issue	ER-8008
Description	Resolved an issue where RADIUS memory leak was seen when UTP profiles were used through **User Role Mapping** under **Authentication Services**

Component/s	System
Issue	ER-7637
Description	Resolved an issue where editing any existing Ethernet profile from system domain level allowed creating new Ethernet profiles at a domain level

Component/s	System
Issue	ER-8004
Description	Resolved an issue where administrator login was successful though AD user was mapped to a user group with incorrect format

Component/s	System
Issue	ER-8183
Description	Resolved an issue of controller SZ100 buffer being stuck during an AP firmware upgrade. This issue occurred in SZ100 port group one setup

Component/s	System
Issue	ER-8148
Description	Resolved an issue where ACL limitation failed to synchronize from the controller web user interface to CLI mode

Component/s	System
Issue	ER-8220
Description	Resolved an issue where the controller administrator login failed against TACACS+ server

Component/s	System
Issue	ER-8313
Description	Resolved an issue where *out-of-service time* extended for a longer duration when a node connected back to a two node cluster setup

Component/s	System
Issue	ER-8438
Description	Resolved an issue where the CSR (Certificate Signing Request) file had invalid certificate attributes

Component/s	UI/UX
Issue	ER-8061
Description	Resolved an issue where controller web user interface was not able to move or delete the Switch when the language was set as German

Resolved Issues

Component/s	UI/UX
Issue	ER-8057
Description	Resolved an issue where duplicate walledgarden entries were allowed on the web user interface

Component/s	UI/UX
Issue	ER-7841
Description	Resolved an issue where the controller failed to display the VLAN/Static route configuration of the Switch router code

Component/s	UI/UX
Issue	ER-8087
Description	Resolved an issue where in the controller web user interface WLAN Group drop-down list selected the wrong data from the WLAN form

Component/s	UI/UX
Issue	SCG-111636
Description	Resolved an issue where if a Zone was upgraded to 5.2 and later downgraded to its original version, then duplicate device policy entries were created when it is upgraded again to 5.2.

Component/s	Virtual SmartZone
Issue	ER-8497
Description	Resolved an issue with migration scripts for all ZoneDirector version

Component/s	Virtual SmartZone
Issue	ER-8317
Description	Resolved an issue where the client was unable to reset the expired administrator account password while logged in with an expired administrator account

Component/s	Virtual SmartZone
Issue	ER-8261
Description	Resolved an issue where in the imported Zone Template WLAN the firewall was not mapped with the correct profile

Component/s	Virtual SmartZone
Issue	ER-8146
Description	Resolved an issue where the controller failed to send emails when Switch is offline

Component/s	Virtual SmartZone
Issue	ER-7950
Description	Resolved an issue where default certificates serial number on the controller instances of different clusters was created from the same AMI (Amazon Machine Image)

Component/s	Virtual SmartZone
Issue	ER-7882
Description	Use Chrome Browser on a MAC OS 10.15 client and access the controller web user interface. ⚠️ **CAUTION** **Client may see the error, *NET::ERR_CERT_REVOKED*. Do contact customer support.**

Interoperability Information

Cluster Network Requirements

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

TABLE 6 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 interoperate with third party Wi-Fi devices. RUCKUS qualifies its functionality on the most common clients.

Component/s	AP
Issue	SCG-116773
Description	Intel Wi-Fi driver version *Wireless-AC 7265 version:19.51.8.3* fails to detect the open SSIDs on 802.11ax APs
Workaround	Update the Dell laptop Wi-Fi driver to *Wireless-AC 7265 version:19.51.18.1* or higher Wi-Fi driver version to connect the open SSID.

Component/s	AP
Issue	SCG-110129
Description	Samsung S10 client is not skipping 802.11x authentication process while roaming with OKC enabled WLAN connect.
Workaround	For successful roaming, connect Samsung S10 client to 11r enabled WLAN.

Component/s	AP
Issue	SCG-110318
Description	HP printer client fails to connect to WPA3 mixed WLAN profile. HP Printer does not support SAE.
Workaround	Connect the HP printer client to WEP, WPA2 WLAN profile.

Component/s	AP
Issue	SCG-115570
Description	Chrome OS device does not send the hostname in the DHCP packet, which results in an empty string as the hostname in the controller web user interface

Component/s	AP
Issue	SCG-115319
Description	MacBook with Catalina version and all iOS devices are able to use Airplay services when client isolation is enabled for bonjour fencing policy
Workaround	Apple system limitation for Catalina OS (10.15.2 and 10.15.3) as Airplay only works with Bluetooth and WLAN interfaces

Component/s	AP
Issue	SCG-109406
Description	Surface Pro Window client fail to connect to WPA3 mixed mode.

Component/s	AP
Issue	SCG-106735
Description	Samsung S10 only connects to WPA2-PSK/WPA3-SAE mixed WLAN with WPA3 SAE passphrase (but not with WPA2-PSK).
Workaround	Samsung S10 can only connect to WPA2-PSK/WPA3-SAE mixed WLAN by WPA3 SAE passphrase. By the packet capture, Samsung S10 uses the passphrase to perform the WPA3-SAE dragonfly handshake. It does not try to use WPA2-PSK. This could be the current behavior of S10's.

Component/s	AP
Issue	SCG-110128
Description	One Plus 5 client does not connect to WPA3 mixed mode and WPA3 SAE mode WLAN profile.
Workaround	One Plus 5 client connects to WEP and WPA2 WLAN profile.

Component/s	AP
Issue	SCG-108843
Description	Hostname for the below devices are not displayed due to missing Option 12 information in DHCP frames from the client. • Lumia 950 • Pixel 1,2 and 3 • Nexus 5, 5x and 6 • PlayStation-I • PlayStation-II • Samsung Chromebook • HP Chromebook • Asus Chromebook • Dell Chromebook

Component/s	AP
Issue	SCG-94006

Component/s	AP
Description	Using EAP-SIM profile Sony Xperia Z5, Sony Xperia Z3, LG G3 Stylus do not connect to AP R730 successfully. This is due to client limitation.

Component/s	AP
Issue	SCG-93051

Description	If clients encounter any interoperability issue with the AP operating in 11ax (default mode) the AP can be re-configured through RKS CLI to operate in 11ac mode including 5g and 2.4g commands. This mode can stay persistent across reboots.
	
	To configure 5G radio to 11ac mode, use the following command on AP:
	
	`set mode wifi1 11ac`
	
	To configure 2.4G radio to 11ng mode, use the following command on AP:
	
	`set mode wifi0 11ng`

Component/s	AP
Issue	SCG-104650
Description	802.11r Fast BSS Transition association fails with Windows 10 and Intel adapter 7265 (driver: 19.51.18.1) and Windows 10 and Intel 11ac 8260.

Component/s	AP
Issue	SCG-115983
Description	MAC OS client device type, OS vendor and model name is unknown after a certain period of connectivity and client initiates connection without initiating DHCP.
Workaround	For MAC OS client force the client to initiate the DHCP for updating the device information.

Component/s	AP
Issue	SCG-114519
Description	iPhone 11 Pro Max supports WPA3-SAE (IOS Version:13.1.1) but does not work with OWE

Component/s	AP
Issue	SCG-119789
Description	By the Apple Forum, the macOS 10.15.4 has a GTK (Group Key Handshake) re-key issue. It may cause the Wi-Fi disconnection when the GTK is re-keyed Visit for details https://discussions.apple.com/thread/251311254

Component/s	AP
Issue	SCG-115566
Description	PS4 device fails to send the hostname in DHCP packet resulting in the hostname as an empty string in the controller web user interface
Workaround	Client needs to provide hostname explicitly when connecting the PS4 to Wi-Fi

Component/s	AP
Issue	SCG-117204

Component/s	AP
Description	Following devices send *Deauthentication frame* with reason code: *STA is leaving BSS* to the AP when performing *Forget WLAN* within client:- 1. A8+ (2018) : (Model= SM-A730F), (OS= Android 9) 2. A9 (2018) : (Model= SM-A920F), (OS= Android 9) 3. Microsoft Surface Pro : (Model= Surface Pro),(OS= Windows 10 Pro- 10.0.18363 Build 18363) 4. Nexus 5X : (Model= LG-H791), (OS= Android 8.1) 5. OnePlus 5 : (Model= A5000), (OS= Android 9)
Workaround	Client should send *disassociation frame*. Client design fault.

Component/s	AP
Issue	SCG-114507
Description	iPhone 11 Pro Max supports with IOS version13.1.1 sometimes goes for open system authentication instead of SAE Authentication for WPA3 profile. **NOTE** Issue is sourced to iPhone 11 Pro and not seen with other iOS like 13.1.3.

Component/s	AP
Issue	SCG-113080
Description	Google Home and Google Home Mini reported as Chrome OS.

Component/s	AP
Issue	SCG-116507
Description	Client limitations observed with WPA3 security type for the below user equipment. 1. IPhone 6s with OS version 13.3.1 failed to perform WPA3-SAE authentication and instead does an open authentication in both WPA3 and WPA3/WPA2 mixed WLANS. 2. Redmi Note 5 and 7 with respective OS versions 9PKQ1.180904.001 and 9PKQ1.181203.001 fail to connect to WPA3 mixed mode with PSK passphrase.

Component/s	AP
Issue	SCG-115318
Description	Browsing is possible for short duration when WLAN is open authentication though the device policy is configured to block Windows phones.
Workaround	Client limitation as *http user-agent/device info* is checked and blocked, gets to Internet but is blocked. Disconnect/reconnect cyclic process for client.

Component/s	System
Issue	SCG-85552
Description	Users will not be redirected to WISPr Internal Logon URL with Chrome browser 65. This is the behavior of Chrome browser version starting from 63

Component/s	System
Workaround	Add the following URLs in Walled Garden list for WISPr redirection to work. • connectivitycheck.gstatic.com • clients3.google.com • connectivitycheck.android.com • play.googleapis.com • gstatic.com For details refer to https://www.chromium.org/chromium-os/chromiumos-design-docs/network-portal-detection

Component/s	System
Issue	SCG-105741
Description	Nexus 5x clients may not be able to connect using SIM authentication profile if the EAP SIM attributes are *AT_VERSION_LIST* and *AT_FULLAUTH_ID_REQ.*

Component/s	System
Issue	SCG-108889
Description	The OS type is displayed as *Nest Learning Thermostat* for Samsung Gear Smartwatch, which is incorrect.
Solution	Client OS issue of fingerprint type *SamsungGear Watch* and *Nest Thermostat* are the same.

COMMSCOPE®
RUCKUS®