RELEASE NOTES

RUCKUS SmartZone (LT-GD) Release Notes, 6.1.2

Supporting SmartZone 6.1.2

Part Number: 800-73529-001 Rev A
Publication Date: November 2023

Export Restrictions

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

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

Disclaimer

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

Limitation of Liability

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

Trademarks

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

Patent Marking Notice

For applicable patents, see www.cs-pat.com.

Contents

Document History

Revision Number	Summary of Changes	Publication Date
A	Initial *Release Notes*	11, November 2023

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 RUCKUS Networks flagship, large-scale WLAN controller is designed for Service Provider and large Enterprises which prefer to use appliances. The carrier grade platform supports N+1 Active/Active clustering, comprehensive integrated management functionality, high-performance operations and flexibility to address many different implementation scenarios.
- The SZ100, Enterprise, 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 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 was first introduced in software release 5.2.1. Release 5.2.1 is the minimum firmware that can be run on the SZ144.
- The vSZ, which is available in *High Scale* and *Essentials* versions, is a Network Functions Virtualization (NFV)-based WLAN controller for Service Providers and Enterprises that desire a carrier-class solution that runs in the cloud. It supports all of the WLAN controller features of the industry, while also enabling the rollout of highly scalable and resilient wireless LAN cloud services.
- The vSZ-D is a Virtual Data Plane aggregation appliance that is managed by the vSZ that offers organizations more flexibility in deploying a NFV aligned architecture. Deploying vSZ-D offers secured tunneling of wireless client data traffic that encrypts payload traffic, POS data traffic for PCI compliance, voice applications while enabling flat network topology, mobility across L2 subnets, and add-on services like L3 Roaming, Flexi-VPN, DHCP Server/NAT as well as CALEA/Lawful Intercept.
- The SZ100-D is a Data Plane hardware appliance, which is functionally equivalent to the vSZ-D virtual data plane product. The appliance provides turnkey deployment capabilities for customers who need a hardware appliance. The SZ100-D is managed by a vSZ Controller only and cannot work in a standalone mode.
- The SZ144-D is the second-generation Data Plane hardware appliance which is functionally equivalent to the vSZ-D virtual Data Plane. The appliance provides turnkey deployment capabilities for customers who need a hardware appliance. The SZ144-D is managed by a vSZ Controller only and cannot work in a standalone mode.

Release Information

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

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

ATTENTION
Upgrade from release 5.2.2.0.1562 to 6.1.2.0.354 requires a patch to be installed first. Please refer to https://support.ruckuswireless.com/documents/4223 for details.

ATTENTION
For Network Segmentation:

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

SZ300

- Controller Version: **6.1.2.0.354**
- Control Plane Software Version: **6.1.2.0.187**
- Data Plane Software Version: **6.1.2.0.354**
- AP Firmware Version: **6.1.2.0.850**

SZ100/SZ124/SZ104

- Controller Version: **6.1.2.0.354**
- Control Plane Software Version: **6.1.2.0.187**
- Data Plane Software Version: **6.1.2.0.19**
- AP Firmware Version:**6.1.2.0.850**

SZ144

- Controller Version: **6.1.2.0.354**
- Control Plane Software Version: **6.1.2.0.187**
- Data Plane Software Version: **6.1.2.0.19**
- AP Firmware Version:**6.1.2.0.850**

vSZ-H and vSZ-E

- Controller Version: **6.1.2.0.354**
- Control Plane Software Version: **6.1.2.0.187**
- AP Firmware Version:**6.1.2.0.850**

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

- Data plane software version: **6.1.2.0.850**

Cloudpath

- Cloudpath Version: **5.1.2**

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

1. SmartZone **6.1.2.0.354** (GA) GPB.proto (Google ProtoBuf) image for GPB/MQTT [DNP] - https://support.ruckuswireless.com/software/3705-smartzone-6-1-2-lt-gd-gpb-proto-google-protobuf-image-for-gpb-mqtt.
2. SmartZone **6.1.2.0.354** MockSCI-TLS (SZ to SCI MQTT subscriber software) for CentOS/Ubuntu - https://support.ruckuswireless.com/software/3706-smartzone-6-1-2-lt-gd-mocksci-tls-sz-to-sci-mqtt-subscriber-software-for-centos-ubuntu.

IoT Suite

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

- vSCG (vSZ-H and vSZ-E), and SZ-124: **6.1.2.0.354**
- Control plane software version in the WLAN Controller: **6.1.2.0.187**
- AP firmware version in the WLAN Controller: **6.1.2.0.850**

RUCKUS IoT Controller

- RUCKUS IoT Controller version: **2.1.0.0**
- VMWare ESXi version: 6.5 and later
- KVM Linux Virtualizer version: 1:2.5+dfsg-5ubuntu 10.42 and later
- Hyper-Version: 6.5 and later
- Google Chrome version: 78 and later
- Mozilla Firefox version: 71 and later

Public API

Click on the following links to view Public API documents:

- *SmartZone 6.1.2 Public API Reference Guide (ICX Management)*

  SmartZone 6.1.2 (LT-GD) Public API Reference Guide (ICX Management)
- *SmartZone 6.1.2 Public API Reference Guide (SZ100)*

  SmartZone 6.1.2 (LT-GD) Public API Reference Guide (SZ100)

  NOTE
  SZ100 Public API link is for SZ144 as well.

- *SmartZone 6.1.2 Public API Reference Guide (SZ300)*

  SmartZone 6.1.2 (LT-GD) Public API Reference Guide (SZ300)
- *SmartZone 6.1.2 Public API Reference Guide (vSZ-E)*

  SmartZone 6.1.2 (LT-GD) Public API Reference Guide (vSZ-E)
- *SmartZone 6.1.2 Public API Reference Guide (vSZ-H)*

  SmartZone 6.1.2 (LT-GD) Public API Reference Guide (vSZ-H)

Dynamic Signature Package Update

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

Complete the following steps to perform a manual upgrade:

1. Download the Signature package from the RUCKUS support site:
   - Regular Signature package for controller release 6.1.2 only: https://support.ruckuswireless.com/software/3799-smartzone-6-1-2-lt-gd-sigpack-1-650-0-regular-application-signature-package.
   - Non-Regular Signature package for 6.1.2 and earlier releases: https://support.ruckuswireless.com/software/3810-smartzone-6-1-2-lt-gd-sigpack-1-650-0-application-signature-package.
2. Manually upgrade the Signature package by navigating to **Security** > **Application Signature Package**.

   NOTE
   For more information, refer to the **Working with Application Signature Package** in *RUCKUS SmartZone Security Guide (LT-GD), 6.1.2*

If 802.11ac Wave 1 APs are configured on legacy firmware (AP firmware R6.1.1.1 or earlier), you cannot download the regular Signature package 1-650-0. Download the non-regular Signature Package. If 802.11ac Wave 1 APs are configured with R6.1.2 firmware, you can download both versions 1-650-0 regular and non-regular signature packs. **[SCG-123375]**

NOTE
As R5.1.x to R6.1.2 release upgrade is not supported, RUCKUS does not have any signature-package upgrade restrictions during the Zone upgrade process.

Supported Matrix and Unsupported Models

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

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

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

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

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

Supported AP Models

This release supports the following RUCKUS AP models.

TABLE 1 Supported AP Models

11ax		11ac-Wave2		11ac-Wave1
Indoor	**Outdoor**	**Indoor**	**Outdoor**	**Indoor**
R850	T750SE	R720	T811CM	R310
R760	T750	R710	T710S	
R750	T350SE	R610	T710	
R650	T350D	R510	T610S	
R560	T350C	R320	T610	
R550		M510	T310S	
R350		H510	T310N	
H550		H320	T310D	
H350		C110	T310C	
			T305I	
			T305E	
			E510	

ATTENTION

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

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

11ax	11n	11ac-Wave1
R730	ZF7982	T504
	ZF7782-S	T300 or T301
	ZF7782-E	R700
	ZF7782	R600
	ZF7781CM	R500
	ZF7372-E	H500
	ZF7372	C500
	ZF7352	
	ZF7055	
	R300	

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

Unsupported AP Models

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

TABLE 3 Unsupported AP Models

Unsupported AP Models				
SC8800-S	SC8800-S-AC	ZF2741	ZF2741-EXT	ZF2942
ZF7025	ZF7321	ZF7321-U	ZF7341	ZF7343
ZF7343-U	ZF7351	ZF7351-U	ZF7363	ZF7363-U
ZF7441	ZF7761-CM	ZF7762	ZF7762-AC	ZF7762-S
ZF7762-S-AC	ZF7762-T	ZF7962		

Supported ICX Models

The following ICX switch models can be managed from SmartZone:

TABLE 4 ICX Firmware Versions Compatible with SmartZone

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

The following table defines ICX and SmartZone release compatibility.

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

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

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

TABLE 5 ICX and SmartZone Release Compatibility Matrix

	SmartZone 5.1[1]	SmartZone 5.1.1	SmartZone 5.1.2	SmartZone 5.2	SmartZone 5.2.1 / 5.2.2	SmartZone 6.0	SmartZone 6.1	SmartZone 6.1.1	SmartZone 6.1.2
FastIron 08.0.80	Yes	Yes[1]	No	No	No	No	No	No	No
FastIron 08.0.90a	No	Yes	Yes	Yes	Yes	Yes	No	No	No
FastIron 08.0.91	No	Yes	Yes	Yes	No	No	No	No	No
FastIron 08.0.92	No	No	Yes	Yes	Yes	Yes	Yes	No	No
FastIron 08.0.95 and subsequent patches	No	No	No	No	No	Yes	Yes	Yes	Yes
FastIron 09.0.10a and subsequent patches	No	No	No	No	No	No	Yes	Yes	Yes
FastIron 10.0.00 and subsequent patches	No	No	No	No	No	No	No	Yes	Yes
FastIron 10.0.10 and subsequent patches	No	No	No	No	No	No	Yes	Yes	Yes

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

TABLE 6 Switch Management Feature Compatibility Matrix

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

[1] Does not support ICX configuration.

TABLE 6 Switch Management Feature Compatibility Matrix (continued)

Feature	SmartZone Release	ICX FastIron Release
Switch Port Configuration	5.1.1 and later	08.0.90a and later
Switch AAA Configuration	5.1.1 and later	08.0.90a and later
Switch Client Visibility	5.1.2 and later	08.0.90a and later
Manage Switches from Default Group in SZ-100 / vSZ-E	5.1.2 and later	08.0.90a and later
DNS-based SmartZone Discovery	5.1.2 and later	08.0.95c and later
Download Syslogs for a Selected Switch[2]	5.2.1 and later	08.0.92 and later
Switch Topology	5.2 and later	08.0.92 and later
Designate a VLAN as Management VLAN	5.2.1 and later	08.0.92 and later[3]
Change Default VLAN	5.2.1 and later	08.0.95 and later
Configure the PoE Budget per Port on ICX through the Controller GUI with 1W Granularity	5.2.1 and later	08.0.95 and later
Configuring Protected Ports	5.2.1 and later	08.0.95 and later
Configuring QoS	5.2.1 and later	08.0.95 and later
Configuring Syslog	5.2.1 and later	08.0.95 and later
Geo Redundancy Active-Standby Mode	6.0 and later	08.0.95b and later
Generic CLI Configuration	6.0 and later	08.0.95b and later
Port-Level Override	6.0 and later	08.0.95b and later
Port-Level Storm Control Configuration	6.1 and later	08.0.95 and later
IPv6 Support (connection through static configuration only)	6.1 and later	09.0.10a and later
Save Boot Preference	6.1 and later	09.0.10a and later
Virtual Cable Testing	6.1 and later	09.0.10a and later
Blink LEDs	6.1 and later	09.0.10a and later
Send Event Email Notifications at Tenant Level	6.1 and later	09.0.10a and later
Update the status of a Switch	6.1 and later	09.0.10a and later
Convert Standalone Switch	6.1 and later	09.0.10a and later
Flexible Authentication Configuration	6.1 and later	09.0.10a and later
Network Segmentation	6.1.1 and later	09.0.10d and later[4]

Supported IoT Release

This release supports IoT Controller release 2.1.0.0.

This release is compatible with the following controller and access point hardware and software.

[2] To download system logs from SmartZone for a particular ICX switch, TFTP must be enabled.
[3] FastIron 10.0.00 and later releases do not support management VLANs.
[4] As an exception, FastIron release 10.0.00 does not support this feature.

Compatible Hardware

The following lists the Access Points modules compatible with IoT.

- T310D or R510 or H510 and i100 IoT module
- T350D or R350 or H350
- R850
- R760
- R750 or T750 or T750SE
- R720 and i100 IoT module
- R650
- R610 or R710 and i100 IoT module
- R560
- R550 or H550
- R550 and i100 IoT module
- Access Points H510 or R510 or T310D and i100 IoT Module
- Access Points H350 or R350 or T350D
- Access Point R550 and i100 IoT Module
- Access Points H550 or R550
- Access Point R560
- Access Points R610 or R710 and i100 IoT Module
- Access Point R650
- Access Point R720 and i100 IoT Module
- Access Point R750 or T750 or T750SE
- Access Point R760
- Access Point R850

Compatible Software

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

The following table lists the supported IoT end devices.

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

Bulbs Devices

TABLE 7 List of Bulbs Devices

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Lightify (RGB) Model 73674	Bulb	Zigbee	Osram	OSRAM	LIGHTFY A19 RGBW

TABLE 7 List of Bulbs Devices (continued)

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
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		
Bulb	Bulb	Zigbee	Aduro SMART ERIA		
Bulb	Bulb	Zigbee	Cree		BA19-08027OMF-12CE26-1C100
Hue	Bulb	Zigbee	Philips	Hue White	840 Lumens

Locks Devices

TABLE 8 List of Locks Devices

Device	Type	Model	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	Zigbee	Assa-Abloy	Yale	Yale YRD220/240 TSDB
Yale YRD210 Push Button	Lock	Zigbee	Assa-Abloy	Yale	YRD210 Push
Smartcode 916	Lock	Zigbee	Kwikset	Kwikset	SMARTCODE_DEADBOLT_10T
Smartcode 910 (450201)	Lock	Zigbee	Kwikset	Kwikset	

Switches/Plugs/Thermostat/Alarm/Blinds Devices

TABLE 9 List of Switches/Plugs/Thermostat/Alarm/Blinds Devices

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
GE Smart Dimmer	Switch	Zigbee	GE	Jasco Products	45857
GE Smart Dimmer	Switch	Zigbee	GE	Jasco Products	45856
Smart Plug	Plug	Zigbee	CentraLite	CentraLite	
Smart Plug	Plug	Zigbee	Smart things	Samjin	
Smart Plug	Plug	Zigbee	INNR		
Zen Thermostat	Thermostat	Zigbee	Zen Within	Zen Within	Zen-01
EcoInsight Plus	Thermostat	Zigbee	Telkonet	Telkonet	
ZBALRM	Alarm	Zigbee	Smartenit		Model #1021 A
Smart Blinds	Blinds	Zigbee	Axis Gear		
UEI Thermostat	Thermostat	Zigbee	UEI		TBH300ZBSN

Sensors Devices

TABLE 10 List of Sensor Devices

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Garage Door Tilt Sensor	Sensor	Zigbee	NYCE	NYCE	NCZ-3014-HA
Curtain Motion Sensor	Sensor	Zigbee	NYCE	NYCE	NCZ-3045-HA
Door / Window Sensor	Sensor	Zigbee	NYCE	NYCE	NCZ-3011-HA
Temperature and Humidity Sensor	Sensor	Zigbee	Aqara	LUMI	WSDCGQ11LM
Motion Sensor	Sensor	Zigbee	Aqara	LUMI	RTCGQ11LM
ERIA Smart Door/ Window Sensor	Sensor	Zigbee	AduroSMART ERIA	ADUROLIGHT	81822
ERIA Smart Motion Sensor	Sensor	Zigbee	AduroSMART ERIA	ADUROLIGHT	81823
Multipurpose Sensor	Sensor	Zigbee	Smart things	Samjin	IM6001-MPP01
Button	Sensor	Zigbee	Smart things	Samjin	IM6001-WLP01
Motion Sensor	Sensor	Zigbee	Smart things	Samjin	IM6001-MTP01
Water Leak Sensor	Sensor	Zigbee	Smart things	Samjin	IM6001-BTP01
EcoSense Plus	Sensor	Zigbee	Telkonet	Telkonet	SS6205-W
EcoContact Plus	Sensor	Zigbee	Telkonet		SS6255-W
Temp, Humidity Sensor	Sensor	Zigbee	Heiman	HEIMAN	HS1HT-N
Gas detector	Sensor	Zigbee	Heiman	HEIMAN	HS3CG
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
3-Series Micro Door Sensor	Sensor	Zigbee	CentraLite	CentraLite	3323-G
Door Sensor	Sensor	Zigbee	Ecolink	Ecolink	4655BC0-R
Temp & Humidity Sensor	Sensor	Zigbee	Sonoff	Sonoff	SNZB-02
Celling Motion Sensor	Sensor	Zigbee	NYCE	NYCE	NCZ-3043-HA
Ecolink Flood Detection Sensor	Sensor	Zigbee	Ecolink	Ecolink	FLZB1-ECO

BLE Devices

TABLE 11 List of BLE Devices

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
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

Wired Devices

TABLE 12 List of Wired Devices

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Vape/Sound Sensor	Sensor	Wired	Soter	-	FlySense

Device not Tested but Supported

TABLE 13 List of Devices not Tested but Supported

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Vingcard	Sigma	Lock	Zigbee	Assa-Abloy	AA_LOCK
Vingcard	Alpha	Lock	Zigbee	Assa-Abloy	AA_LOCK
Vingcard	Classic		Zigbee	Assa-Abloy	AA_LOCK
Vingcard	Allure		Zigbee	Assa-Abloy	AA_LOCK

Product Documentation

The following product guides are updated for R6.1.2. Refer to the *New in this Document* section in each publication for specific changes.

- *RUCKUS SmartZone (LT-GD) SmartZone Upgrade Guide, 6.1.2*
- *RUCKUS SmartZone (LT-GD) Basic Controller Settings, 6.1.2*
- *RUCKUS SmartZone (LT-GD) Management Guide, 6.1.2*
- *RUCKUS SmartZone (LT-GD) Security Guide, 6.1.2*
- *RUCKUS SmartZone (LT-GD) Switch Management Guide, 6.1.2*
- *RUCKUS SmartZone (LT-GD) WLAN Management Guide, 6.1.2*
- *RUCKUS SmartZone (LT-GD) Command Reference Guide, 6.1.2*
- *RUCKUS SmartZone (LT-GD) Network Segmentation Configuration Guide, 6.1.2*
- *RUCKUS SmartZone (LT-GD) Getting Started on SZ GPB/MQTT Interface, 6.1.2*
- *RUCKUS Virtual SmartZone Data Plane Configuration Guide.*

All product guides that did not require updates for R6.1.2 can be accessed by viewing the R6.1.1 product documents on the RUCKUS Support site http://support.ruckuswireless.com or https://docs.commscope.com/.

Online Help Rendition

A number of enhancements are introduced for Online Help (OLH) rendering for R6.1.2. Previous renditions navigated to the *RUCKUS SmartZone Administrator Guide* (consisting of 700+ pages). From R6.1.1, we have split the existing*RUCKUS SmartZone Administrator Guide* into 11 separate guides (Rev B of R6.1.1). This split is based on Taxonomy, and one of the main purposes for this change was for easy reading and keyword search. This enhancement caused a change in the way OLH renders.

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

Security Upgrade

- Upgraded *jQuery UI* to version 1.13.2. **[ER-12375]**

Known Issues

Following are the known issues in this release.

Component/s	AP
Issue	SCG-128166
Description	When sending TCP UP link traffic like voice, video, best effort and background from wireless to wired client, all packets by default go to the best effort queue instead of voice or video queues. This limitation is seen on tunnel enabled SSID (RUCKUS GRE or SoftGRE).

Component/s	AP
Issue	SCG-132965
Description	In the controller web user interface Airtime utilization (Airtime detail pie chart) in health tab shows inaccurate values for *TxFailed* and *RxDataB* fields.

Component/s	AP
Issue	SCG-140164
Description	ICX switches give out 60W of power for the older model of R350 AP as they are classified as Class4 device. The newer models of R350s are classified correctly as Class 3 and therefore give only 15.4W of power.

Component/s	AP
Issue	SCG-141764
Description	The 6GHz channels are unavailable in the controller web user interface for AP R760. The reason why 6GHz channels may not be enabled could be that a Zone was created using a country code that does not allow 6GHz radio, then after a system upgrade or an AP patch, the country code is allowed on 6GHz radio but fails to fill the 6GHz channel range.
Workaround	Follow these steps for recovery. 1. Check the Zone's 6GHz radio configuration and modify the channel range manually. 2. Change the radio channelization bandwidth from Auto mode to 20MHz and save the changes. Later, configure the channelization back to Auto mode.

Component/s	AP
Issue	SCG-138792
Description	Intermittently, the IPad Pro 6e fails to show *MBSSID non-txvap* in the scan list.

Component/s	AP
Issue	SCG-136054
Description	• Tunneled wired clients are not able to reach any tunneled wired and wireless clients. • Tunneled wireless client are not able to reach any tunneled wired clients. • Tunneled wireless clients are able to reach each others. • Tunneled wireless clients are able to reach non-tunneled wired and wireless clients.

Component/s	AP
Issue	SCG-135129

Component/s	AP
Description	When random target asserts occur, the AP recovers automatically without a reboot. It currently takes around 40 to 60 seconds to recover and be completely operational for R560 and R760 APs.

Component/s	AP
Issue	SCG-135256
Description	When the AP is running in 2-5-5 mode, some conditions MAP's are connected to a lower 5Ghz instead of balancing or being connected to both the radios.

Component/s	AP
Issue	SCG-137705
Description	Service validation with virtual wireless client randomly fails when the SNR (signal-to-noise ratio) between target and station APs is less than 30 decibels.

Component/s	AP
Issue	SCG-127767
Description	DHCP/NAT performance drop is observed, when running back-to-back performance tests with Ixia or any performance benchmark tool. This drop is observed due to the *rflow* age out timer not updating or the entry not being refreshed while running back-to-back test iterations.
Workaround	Allow a five minute gap between each iteration of performance test, for *rflow* entries to clear.

Component/s	AP
Issue	SCG-135845
Description	Radio information field (PHY type, NSS) is decoded incorrectly for the packets captured in the controller UI or AP shell on 11ac APs.
Workaround	To get accurate radio information, use an external sniffer.

Component/s	AP
Issue	AP-18235
Description	Dynamic Packet Captures: Few scenarios are seen where clients can send 802.11 authentication request immediately after 802.11 deauthentication (deauth sent by Client). In these cases, AP cannot filter the packets as they are received in quick succession, which is lower than minimum granularity of time on the AP as a system (microseconds versus milliseconds). In these few scenarios 1-2 packets from the previous session are seen in the current filtered packet capture also.
Workaround	To get accurate radio information, use an external sniffer.

Component/s	AP
Issue	SCG-137133
Description	For tri-band radio APs, when operating in 2-5-5 mode and having Spectrum Analysis enabled, Spectrum Analysis will only work for lower channels on 5Ghz. Spectrum Analysis is not supported on the third radio (upper 5Ghz).

Component/s	AP
Issue	SCG-137219

Component/s	AP
Description	Control frames may not follow the 6Ghz management Tx rates and might send packets in Non-HT basic data rates.

Component/s	AP
Issue	SCG-137236
Description	AP uses rates lower than the configured 6GHz BSS minimum rates.

Component/s	AP
Issue	SCG-137278
Description	APs R760/R560 do not currently support third radio use for Spectrum Analysis, which means that the controller will regard an R760/R560 as a two-radio AP for Spectrum Analysis.

Component/s	AP
Issue	AP-18583
Description	This release does not support enabling reduced neighbor report (RNR) on 6Ghz. RNR field is about 240 bytes per *Non Tx VAP* profile and the maximum size of beacon is 1,500. It corrupts the beacon.

Component/s	AP
Issue	AP-18716
Description	When PMF (Protected Management Frames) is enabled on WLANs and if the client fails to respond to a SA (Security Association) query request, the client is deauthenticated by AP with reason: *Association Request rejected temporarily: try again later* .

Component/s	AP
Issue	SCG-138069
Description	**NOTE** There is a very small possibility of this known issue. Do contact RUCKUS support in case this issue occurs. This issue occurs when cloning a WLAN fails though the WLAN is not displayed on the controller web user interface but a WLAN with the same name is actually present in the database.

Component/s	AP
Issue	AP-19214
Description	Channel selection algorithms options in controller web user interface is not inline with AP RKCLI commands. 1. Background scanning algorithm can be configurable only through vSZ UI. This option is not available on AP RKCLI. 2. Legacy channelfly algorithm can be configurable only through AP RKCLI. This option is not available in vSZ UI. 3. *Chanflybg* algorithm is available as channelfly in vSZ UI where as *Channelfly+* in AP RKCLI.

Component/s	AP
Issue	SCG-138310
Description	Laptop keeps flapping or switching between 2.4Ghz and 5Ghz if the RSSI of both the radios comes closer to each other, which is +/- 2dBM. This could cause disconnections during longer connectivity duration. Impacted clients: ● Windows laptops ● MacBook ● Chromebook
Workaround	Reduce RSSI of 2.4 Ghz at least to +/- 5dBM for controlling UE flapping or switching.

Component/s	AP
Issue	SCG-138763
Description	AP R720 power by AF mode cannot be formed as MAP (802.3AF).
Workaround	Power either through DC (Direct Current) or AT power mode.

Component/s	AP
Issue	AP-19942
Description	User may see packet loss and less throughput while SSID (Service Set Identifier) rate limit (wireless) is enabled on R760 AP in uplink direction.

Component/s	AP
Issue	SCG-138294
Description	Wired client with MAC address based authentication - When a user enters wrong credentials, the AAA server rejects the authentication and the wired client does not get the IP address from the Guest VLAN. This issue is specific to wired client running Linux OS but works with Windows or MAC based laptops.

Component/s	AP
Issue	SCG-132435
Description	Bing FQDN in safe search does not get resolved for IPv6.

Component/s	AP
Issue	AP-18407
Description	1. WLAN configuration of *Inactivity Timeout* is correlated to the GTK (Group Temporal Key) Rekey, which is activated by system default. 2. For 11ac AP, the maximum WLAN *Inactivity Timeout* are 65530 seconds. 3. As configured the huge WLAN *Inactivity Timeout* values (for example, 65530, 86400), a 5 to 10 seconds deviation may occur due to the target timer processing.

Component/s	AP
Issue	SCG-138175
Description	In controller web user interface **Access Points** > **Select AP** > **Clients** *packets dropped per client* is seen as zero.

Component/s	AP
Workaround	To debug low throughput or packet drops, use the following AP CLI command: `wifistats wifi1 11 --mac <mac address> | grep -i dropped_count`

Component/s	AP
Issue	SCG-136304
Description	When 11ax AP is configured for 160MHz channelization, chain mask RSSI values are shown intermittently in *athstats -i wifi1 -a 1*. This is an issue with only the **athstats** command in AP CLI and does not impact client performance.

Component/s	AP
Issue	AP-19666
Description	Number of simultaneous VOIP calls handled by 11ax APs is slightly less in 6.1.1 when compared to release 6.1.0.

Component/s	AP
Issue	SCG-134763
Description	Packet loss is observed and wireless client traffic is impacted when *Multicast Rate Limit* is enabled and users send a burst of multicast traffic from wired to wireless client. This is mainly observed with Multicast hammer tool with high burst value.

Component/s	AP
Issue	SCG-138321
Description	*Failed to send msg to RCCD for mac* messages may appear on AP CLI, when WLAN is configured with 802.1x-EAP and sudden burst of clients connect. Once Clients get the IP address and start browsing the network, these messages are not seen.

Component/s	AP
Issue	SCG-138290
Description	It is allowed to configure non-BSS minimum rate as *Mgmt Tx* rate for specific application scenarios as correlated to SCG-138606.

Component/s	AP
Issue	SCG-136481
Description	In some rare scenarios, where authentication packets are sent after deauthentication within few microseconds or when packet capture (pcaps) is filtered with zero timestamp, dynamic pcaps may be seen with a few extra packets and therefore may not match with the ladder diagram in **Troubleshooting** page on the controller UI. In general, dynamic pcap will be equal or a super set of ladder diagram.

Component/s	AP
Issue	SCG-137263
Description	APs do not check the packet capture file (pcaps) size. In a few scenarios where RADIUS packet exchange occurs during client connect and clients connection fails, which may result in a larger pcap files size based on the number of clients performing 802.1x

Component/s	AP
Issue	SCG-136448
Description	This is a rare condition where clients connect and disconnect back-to-back and packet capture files may generate with timestamp zero.

Component/s	AP
Issue	SCG-132076
Description	Debug message *hostapd: failed to send msg to RCCD, errno:11* is frequently seen on the AP console logs during high client connection/failure rate scenarios.

Component/s	AP
Issue	SCG-137810
Description	AP hostname size is restricted to 24bytes for 6Ghz radio only.

Component/s	AP
Issue	SCG-138297
Description	For dual boot system, Client Finger Printing (CFP) shows the details of the first boot which connects for the first time. When the client switches to the second boot, device information is as per first boot, because CFP's cache is based on hardware MAC address.

Component/s	AP
Issue	AP-24759
Description	Windows 11 clients are unable to connect to 802.1X WLANs on Wi-Fi 6 or Wi-Fi 6E APs with FreeRADIUS versions 3.0.15 and 3.0.16 (works with versions 3.0.19 and 3.0.23).

Component/s	AP
Issue	SCG-138038
Description	R760/R560 running with *af* mode cannot join the controller.
Workaround	In order to identify the state, the following LED pattern has been provided as a workaround. ● LED - af power mode ● POWER - Stable Green ● CTL - OFF ● AIR Stable - Amber ● 2Ghz - OFF ● 5Ghz - OFF ● 6Ghz - OFF

Component/s	Cloudpath
Issue	SCG-137222
Description	Traffic is interrupted for end-users when the controller makes VNI changes (the VNI assigned to the device) because Cloudpath requests the controller to place the Access Switch Ethernet port back to web authentication VLAN.
Workaround	1. Administrator needs to remove the port assignment of Access Switch on the Cloudpath 2. User would need to re-authenticate the Web.

Component/s	Switches
Issue	SCG-138785
Description	The existing mapping VLAN for the uplink port in the Access Switch should update accordingly if the user edits the uplink port settings.
Workaround	User needs to add the existing mapping VLAN on the uplink port/LAG of Access Switch or downlink port/LAG of distribution switch when user changes the network deployment between access/distribution Switch. For example: 1. **Scenario 1** - Change the uplink port from port to LAG on Access Switch. Before updating the uplink port from port to LAG in Network Segmentation profile, user needs to add all the existing mapping VLANs as tagged VLANs and Web authentication VLAN when creating the LAG profile on Access Switch. User also needs to add all existing mapping VLANs as tagged VLANs when creating the LAG profile on Distribution Switch. 2. **Scenario 2** - Change the uplink port from original Ethernet port to another Ethernet port on Access Switch. After updating the uplink port in Network Segmentation profile the user needs to add all existing mapping VLANs as tagged VLANs in another Ethernet port on Access Switch. 3. **Scenario 3** - Change uplink port from original LAG to another LAG on Access Switch. Before updating the uplink port in Network Segmentation profile, user needs to add all existing mapping VLANs as tagged VLANs and Web-authentication VLAN when creating the LAG profile on Access Switch. **NOTE** Do not create LAG and tagged VLAN at the same time on Access Switch due to one known issue in ICX firmware 9010d.

Component/s	Switches
Issue	SCG-138835
Description	When you select ICX Switch mode to upgrade FastIron 10.0.00 from the controller, it will not correspond to the switch firmware upgrade since ICX build FastIron 10.0.00 only supports router firmware version with the following: ● GZR10000ufi.bin ● TNR10000ufi.bin ● RDR10000ufi.bin

Component/s	Switches
Issue	FI-260961
Description	When Switch is offline and the user deletes TACACS+ server profile, the TACACS configuration in the Switch is not deleted when the Switch reconnects to the controller.

Component/s	Switches
Issue	SCG-140569
Description	*Internal Server Error* is displayed on the controller web user interface when trying to access the Switch tab/page.

Component/s	System
Issue	SCG-140358

Component/s	System
Description	When OWE-Transition (Opportunistic Wireless Encryption) transition WLANs are created in the template, only a single WLAN with an encryption of OWE-Transition is created resulting in a configuration failure.

Component/s	System
Issue	ER-12584
Description	L2 ACL does not apply to the Client when it is associated through a user role (RBAC Role Based Access Control).

Component/s	System
Issue	SCG-135740
Description	Controller version 6.1.1 has the capability to support both TLSv1 and TLSv1.2 at the same time, but RUCKUS vSPoT may not support it.
Workaround	It is recommended to the vSPoT server for a different TLS version.

Component/s	System
Issue	SCG-135808, FI-260414
Description	End user device may fail to do a Web authentication with Cloudpath RADIUS server if the Switch has multiple AAA servers when it joins the Network Segmentation group.
Workaround	The network administrator needs to define only Cloudpath as the RADIUS server(s) on the Access Switches.

Component/s	System
Issue	SCG-136964
Description	Controller may not overwrite/update the setting under VXLAN successfully when the distribution Switch has scale VXLAN settings. 1. Controller may fail to overwrite the VXLAN setting when joining a distribution Switch with a large amount of VLAN/VNI mapping. 2. Controller may fail to update the site setting (data plane setting in distribution Switch) when the distribution Switch has a large amount of VLAN/VNI mapping.

Component/s	System
Issue	SCG-135682
Description	Controller does NOT compare the latest configuration similar to Golden configuration or does not pop-up or clear the configuration change alerts when a user deletes the latest configuration sequentially.

Component/s	System
Issue	SCG-136885
Description	The packet cannot forward from Virtual Data Plane to distribution switch in VXLAN environment.
Workaround	The network administrator needs to add the static route in the router with the VXLAN environment.

Component/s	System
Issue	SCG-136387
Description	Controller does not block users from ICX firmware upgrade to unsupported Network Segmentation firmware versions by Switch group level when the Switch joins the Network Segmentation profile.

Component/s	UI/UX
Issue	SCG-137149
Description	White spaces in AP name are truncated.

Component/s	UI/UX
Issue	SCG-138178, SCG-138712
Description	Airtime Utilization (Airtime detail pie chart) shows TxFailed and RxDataB inaccurate statistics on all 11ax, R760 AP. **NOTE** This will be addressed in future release.

Component/s	UI/UX
Issue	SCG-138936
Description	At the current stage, the *OWE-Transition* validation logic does not support the controller template handling. However, the *OWE-Transition* validation logic can support the function of apply and extract on the controller template.

Changed Behavior

The following are the changed behavior issues in this release.

Component/s	AP
Issue	ER-11958
Description	SoftGRE offload is disabled by default.

Component/s	System
Issue	ER-12505
Description	Enhancement to validate that the user can set a maximum of only 128 characters in the **Username** box of the controller's login page.

Component/s	System
Issue	ER-12506
Description	Remove Session IDs from the session termination feature.

Component/s	System
Issue	ER-12523

Component/s	System
Description	Change in the setup wizard where the controller saves the login credentials from the configuration backup when a user uploads the configuration backup. The user must log in to the controller using the *backup password* to log in after backup completion. The controller web site displays a note on this setup wizard change, *The admin/enable credentials will be changed to the uploaded configuration backup's*.

Component/s	UI/UX
Issue	SCG-141571
Description	In the controller web user interface WLAN configuration screen, the Priority option previously located in the **Wireless Client Isolation** section has been moved and renamed, now appearing as **BSS Priority** in the **Advanced Options** section.

Component/s	UI/UX
Issue	SCG-143001
Description	Due to the security fix, when the end user clones or edits a profiles such as AAA authentication/accounting profiles, FTP, SMTP, LDAP, the *Test* operations fail.
Workaround	Manually enter the password every time an edit or a clone operation is carried out.

Component/s	Virtual SmartZone Data Plane (vSZ-D)
Issue	SCG-141666
Description	A new warning message is displayed indicating the need to back up the vSZ-D image when upgrading the system.

Resolved Issues

The following are the resolved issues in this release.

Component/s	AP
Issue	ER-11001
Description	The AP login password with double quote (") was not working.

Component/s	AP
Issue	ER-11309
Description	A kernel panic issue caused by a null pointer access in the ACL component of the Wi-Fi driver.

Component/s	AP
Issue	ER-11338
Description	AP reboot caused by Wi-Fi target core watchdog timeout.

Component/s	AP
Issue	ER-11339
Description	A memory 801.11ac Wi-Fi driver leakage issue.

Component/s	AP
Issue	ER-11377
Description	802.11ac Wave 2 AP's rebooted with target assert.

Component/s	AP
Issue	ER-11432
Description	The client failed to pass traffic on AP when the client exhausted its grace period.

Component/s	AP
Issue	ER-11539
Description	DFS (Dynamic Frequency Selection) channels failed to function properly under certain conditions.

Component/s	AP
Issue	ER-11551
Description	A target assert issue when certain *pdev* resets were hit.

Component/s	AP
Issue	ER-11562
Description	The VLAN tag was removed and the client recognized the failure packet sent by the AP.

Component/s	AP
Issue	ER-11595

Component/s	AP
Description	An error was displayed when changing the AP status configuration.

Component/s	AP
Issue	ER-11605
Description	AP T710/T710s showed incorrect link speed on 1Gigabit SFP (small form-factor pluggable) port.

Component/s	AP
Issue	ER-11659
Description	The firewall profile name with 32 characters failed.

Component/s	AP
Issue	ER-11673
Description	The AP was unable to airplay and screen mirror from wireless to wired interface when *rflow* (Research Flow) offload was enabled.

Component/s	AP
Issue	SCG-137371
Description	When a client with a wrong SAE (Simultaneous Authentication of Equals) connected to WPA3-SAE enabled WLAN, HCCD (Historical Client Connection Diagnostic) in the controller UI it showed a failure for the second and fourth authentication packets.

Component/s	AP
Issue	SCG-138426
Description	The corporate environments (HCCD [Historical Client Connection Diagnostic] and RUCKUS Analytics), observed re-association response failure or client connection failure even though the client roamed successfully.

Component/s	AP
Issue	SCG-127253
Description	The DHCP-NAT hierarchy network when used caused the Non-Gateway AP to disconnect (offline) from the controller.

Component/s	AP
Issue	SCG-131270
Description	The Hotstar application failed detection when the AP or the controller ran on *Signature Package* version 540.1 or 590.1.

Component/s	AP
Issue	SCG-138184
Description	The FaceTime application failed detection.

Component/s	AP
Issue	SCG-138888
Description	The R760 AP Zone (2-5-6 radio mode) with builds 6.1.0.0.9018/6.1.0.0.9020, needed to be mandatorily upgraded to 6.1.0.0.9023 build, before upgrading to 6.1.1 GA.

Component/s	AP
Issue	SCG-136547
Description	The Mesh APs IP address failed to update in RAP APs mesh table.

Component/s	AP
Issue	SCG-138384
Description	MESH on WAP3 now has the PMF (Protected Management Frames).

Component/s	AP
Issue	SCG-138610
Description	The **Mqstats** command in AP CLI could not see traffic identifiers (TID) (A-MSDU, A-MPDU in downlink), airtime and media queue flags.

Component/s	AP
Issue	SCG-138764
Description	During voice calls the ChannelFly was triggered, which interrupted the call for a short duration.

Component/s	AP
Issue	SCG-138946
Description	The split-tunnel configuration failed to update on AP, when the AP moved from the controller default zone to a zone with split-tunnel enabled WLANs.

Component/s	AP
Issue	SCG-128288, SCG-128287
Description	The R550 AP Ethernet ports at time negotiated to 100 Mbps instead of 1000 Mbps speed on the switch ports supporting Multi-Gig.

Component/s	AP
Issue	ER-11775
Description	Resolved an exception, *For input string error: debug data* caused by incorrect or incomplete software version to the controller.

Component/s	AP
Issue	ER-11807
Description	The 802.11ac Wave 2 rebooted with target assert crash.

Component/s	AP
Issue	ER-11838

Component/s	AP
Description	The AP broadcasted ARP (Address Resolution Protocol) all the time to its gateway if the MAC address ended with :00.

Component/s	AP
Issue	ER-11913
Description	The non-wireless station (STA) stale IGMP group member entries were not cleared from table.

Component/s	AP
Issue	ER-11918
Description	Resolved an issue related to IPv6 AP performance.

Component/s	AP
Issue	ER-11959
Description	The firewall profile was not assigned to the client when PMK/OKC (Pairwise Master Key and Opportunistic Key Caching) was enabled.

Component/s	AP
Issue	ER-12005
Description	Resolved an issue by fixing the portal redirection when Restricted AP Access (RAA) is enabled.

Component/s	AP
Issue	ER-12012
Description	Kernel panic caused by some abnormal DNS (Domain Name System) packets.

Component/s	AP
Issue	ER-12016
Description	The 802.11ax AP models broadcasted Lithuanian country code incorrectly.

Component/s	AP
Issue	ER-11962
Description	Resolved an issue of target assert and kernel panic with AP R650.

Component/s	AP
Issue	ER-11978
Description	The generation of the report on disconnected APs failed due to target zone or domain deletion or pre-provision APs in the target zones or domains.

Component/s	AP
Issue	ER-12034
Description	The packet capture function is enhanced to avoid truncating *bootp* (DHCP) frames.

Component/s	AP
Issue	ER-12126
Description	The WLAN could not be configured due to empty 6Ghz fields after upgrading the Zone to release 6.1.0.

Component/s	AP
Issue	ER-12306
Description	The vulnerable scripts can now be saved or executed in APs.

Component/s	AP
Issue	ER-12045
Description	Resolved an issue of memory leakage when IoT service was enabled on the AP's.

Component/s	AP
Issue	ER-12053
Description	The cluster was unable to upgrade with 9000 AP Groups.

Component/s	AP
Issue	ER-12089
Description	Failure to forward PN-DCP (PROFINET Discovery and Basic Configuration Protocol) packets from a few clients.

Component/s	AP
Issue	ER-12115
Description	Resolved an issue of kernel panic in IPv6 user case.

Component/s	AP
Issue	ER-12124
Description	The message was incorrect for AP certification replacement.

Component/s	AP
Issue	ER-12148
Description	The clients could still join the AP even though the client RSSI (Radio Signal Strength Identifier) was less than the *Join RSSI Threshold*.

Component/s	AP
Issue	ER-12151
Description	Resolved an issue of target assert during rate drop.

Component/s	AP
Issue	ER-12160
Description	AP H510 Ethernet interface failed to respond.

Component/s	AP
Issue	ER-12162
Description	The 802.11ac Wave 1 AP kernel panic was caused by reorder buffer corruption.

Component/s	AP
Issue	ER-12173
Description	The IOS devices failed to access the **Guest Self Registration** page.

Component/s	AP
Issue	ER-12241
Description	The AP sent excessive LLDP (Link Layer Discovery Protocol) packets to connected switches.

Component/s	AP
Issue	ER-12264
Description	Extra logs are added to clearly indicate the progress of TCM (Transient Control Management) or JWT (JSON Web Tokens).

Component/s	AP
Issue	ER-12268
Description	Resolved an issue of kernel panic in SmartCast.

Component/s	AP
Issue	ER-12285
Description	The virtual clients failed to associate when the *Service Validation* was run.

Component/s	AP
Issue	ER-12287
Description	Massive reboot was caused by local gateway not being accessible for a long duration.

Component/s	AP
Issue	ER-12299
Description	The Tx (transmit) power failed to apply on the AP.

Component/s	AP
Issue	ER-12334
Description	Resolved an issue of AP error message, *wlan-band-bal-enable value too big*.

Component/s	AP
Issue	ER-12374
Description	Resolved an issue of kernel panic caused by *race condition* when clients disassociated from the AP.

Resolved Issues

Component/s	AP
Issue	ER-12338
Description	Resolved an issue of target assert caused by unexpected watchdog timeout.

Component/s	AP
Issue	ER-12392
Description	The AP CLI command though entered incorrectly **set capture wlan_id dile** was executed without an error.

Component/s	AP
Issue	ER-12496
Description	The AP showed high memory utilization.

Component/s	AP
Issue	ER-12426
Description	Resolved an issue of *Research Flow* (rflow) leak.

Component/s	AP
Issue	ER-12436
Description	The AP failed to join the controller when the server list was manually provisioned.

Component/s	AP
Issue	ER-12449
Description	The random signal dropped and static clients constantly roamed for AP R350.

Component/s	AP
Issue	ER-12465
Description	Virtual Client and Virtual Wireless Clients failed at the DHCP stage while testing with 5Ghz radio on R650 and H550 APs.

Component/s	AP
Issue	ER-12507
Description	The 802.11x authentication using local data base failed when the symbol # was included in certain user passwords.

Component/s	AP
Issue	ER-12560
Description	The RTS (Request to Send) rate was not set correctly.

Component/s	AP
Issue	ER-12570
Description	Resolved an issue of target assert.

Component/s	AP
Issue	ER-12933
Description	Channels failed to change in the *ChannelFly* feature on 20Mhz.

Component/s	AP
Issue	ER-12872
Description	AP down time was caused by DFS channels for India country code.

Component/s	AP
Issue	FR-6138
Description	A factory reset, the AP erased the content of write/data/scripts.

Component/s	AP
Issue	ER-8507
Description	RUCKUS NOR Certificate Safe Storage - certificates are copied to more than one location so that they can be restored if a *NAND* (NOT AND) is erased.

Component/s	AP
Issue	FR-5915
Description	R6.1.2 allows configuration of DHCP Option 82 for SoftGRE tunnels on AP Ethernet ports, mirroring the functionality introduced in R5.2.2. This enhancement offers more granular control over SoftGRE tunnels.

Component/s	AP
Issue	FR-6075
Description	The controller web UI now displays supported AP models for its AP firmware. This eliminates the need for administrators to refer to release notes or contact support to verify AP model compatibility.

Component/s	Control Plane
Issue	ER-12028
Description	Resolved an issue of RADIUS proxy memory leak.

Component/s	Control Plane
Issue	ER-12116
Description	The elasticsearch (ES) re-index failed due to CLI template configuration.

<

Component/s	Control Plane
Issue	ER-12157
Description	Incorrect data plane IP address was sent to the AP after the controller was upgraded.

Component/s	Control Plane
Issue	ER-12297
Description	The MD logs created on the controller were not rotated leading to high disk usage.

Component/s	Control Plane
Issue	ER-12317
Description	The clients failed to connect on WLANs since the AAA server was not reachable.

Component/s	Control Plane
Issue	ER-12356
Description	The RADIUS reject message was missed in the NBI response payload.

Component/s	Control Plane
Issue	ER-12406
Description	The Switches did not receive SNMP trap for *Switch Discovery*.

Component/s	Control Plane
Issue	ER-12411
Description	The Switch moved to the staging Zone unexpectedly.

Component/s	Control Plane
Issue	SCG-138299
Description	Radio Frequency band information for events *RogueAPdetected(186)*, *RogueAPdisappeared(185)* and *RogueClient(194)* was not sent to RUCKUS Analytics from the controller.

Component/s	Control Plane
Issue	ER-12463
Description	The AP always re-established to the tunnel when a configuration change occurred.

Component/s	Control Plane
Issue	ER-12479
Description	An incorrect alarm *Detect unconfirmed program on control plane* was generated when the controller was upgraded.

Component/s	Control Plane
Issue	ER-12600
Description	Resolved an issue of AAA server of FQDN (fully qualified domain name) when using an alias.

Component/s	Data Plane
Issue	ER-11689
Description	The AP failed to connect back to the first data plane in the priority list.

Component/s	Data Plane
Issue	ER-11889
Description	The data plane crashed due to a *race condition* .

Component/s	IoT
Issue	ER-11719
Description	The IoT service failed to start AP C110.

Component/s	Network Segmentation
Issue	FR-6149
Description	Network Segmentation for latest version of ICX firmware is supported.

Component/s	Public API
Issue	ER-12141
Description	Enhancement to improve API performance of WLAN configuration.

Component/s	Public API
Issue	ER-12474
Description	The Rest API queries for APs and Switches using the *extraNotFilters* parameter produced differing results.

Component/s	RUCKUS One
Issue	ER-11939
Description	The AP failed to join RUCKUS One due to registrar being stuck.

Component/s	RUCKUS One
Issue	ER-12135
Description	The AP failed to set the Tx power.

Component/s	SPoT
Issue	ER-11208
Description	A large number of visitor were shown on the vSPoT server.

Component/s	Switches
Issue	FI-266177
Description	The trust port/uplink port CLI was appending as LAG interface when it is was tagged as LAG interface under Web authentication VLAN.

Component/s	Switches
Issue	FI-266896, FI-265881
Description	The DHCP server configuration moved through controller, showing the status as success from Switch, even though DHCP client was enabled on the Switch.

Component/s	Switches
Issue	FI-195837
Description	The ICX switches with firmware 08.0.90 went offline when the controller upgraded from release 6.1 to 6.1.1.

Component/s	Switches
Issue	ER-11711
Description	The ICX port details failed to show on the controller web user interface.

Component/s	System
Issue	ER-11940
Description	One of the nodes showed the status as red for CRT LED.

Component/s	System
Issue	ER-11963
Description	Incorrect report intervals was seen when the system was configured as five minute intervals in *Resource Utilization* report.

Component/s	System
Issue	ER-12330
Description	The CLI command **show service** was null for some applications.

Component/s	System
Issue	ER-11989
Description	Enhanced the performance of *Get APGroup list* and *Query AP* API calls.

Component/s	System
Issue	ER-12382
Description	The data was missing when the configuration was restored.

Component/s	System
Issue	ER-12384
Description	Resolved an Switches offline issue caused by elasticsearch reindexing failure.

Component/s	System
Issue	ER-12388
Description	Resolved an issue of docker memory leak by upgrading to version *docker-1.13.1-209*.

Component/s	System
Issue	ER-11569

Component/s	System
Description	Security concerns for SHA1 are addressed. The SSH communication library is updated, and provides a configurable option to disable **diffie-hellman-group14-sha1**, enhanced security without compromising system functionality.

Component/s	System
Issue	FR-5236
Description	CLI command **(diagnostic)# remote-packet-capture disable/enable** disables or enables the ability for a packet capture through the *Management Interface* of the controller and allows for more detailed troubleshooting.

Component/s	System
Issue	ER-11178
Description	R6.1.2 allows you to enable Passpoint (Hotspot 2.0) version 2 with Onboarding (OSU) for SoftGRE Tunnel WLANs.

Component/s	System
Issue	ER-12401
Description	The UP time of the system was more that 497 days the SNMP traps failed to generate.

Component/s	System
Issue	ER-12486
Description	Enhanced the WLAN performance when: 1. WLAN is deployed to many AP Groups. 2. WLAN does not belong to default WLAN Group.

Component/s	System
Issue	ER-12598
Description	A client could not associate to WPA3 and WPA2/WP3Mixed WLAN after the WLANs was configured using CLI mode.

Component/s	System
Issue	ER-12616
Description	The controller CPU/Memory/IO usages increased after configuring firewall profiles in a high scale environment.

Component/s	UI/UX
Issue	ER-12626
Description	Resolved the issue by adjusting the **Accept** and **Continue** button and text display format in terms and conditions of the Guest Portal.

Component/s	UI/UX
Issue	ER-12311

Component/s	UI/UX
Description	The web user interface combo-box was stuck in a loading state status after moving between pages.

Component/s	UI/UX
Issue	ER-12430
Description	The **OK** button failed to respond for certain country codes in the APs.

Component/s	UI/UX
Issue	ER-12415
Description	Controller web user interface is updated with a note that the *Max Tunnel* unit value is 9018.

Component/s	UI/UX
Issue	FR-5938
Description	Previously, the controller administrators lacked visibility into RUCKUS Analytics' control over RF parameters within the controller web user interface (UI). This led to confusion as changes made by ChannelFly or static configurations were overridden by Cloud RRM (Radio Resource Management). For SZ 6.1.2, clear indicators are introduced on the controller UI that signify when RUCKUS Analytics is managing channels and channel width for a specific zone.

Component/s	Virtual SmartZone
Issue	SCG-138206
Description	The *OWE-Transition* WLAN SSIDs bound to the original Open WLAN SSID with *None* encryption can only be displayed on the MVNO configuration menu in the current implementation. With this resolved issue, the controller shows both the WLANs (OPEN and the corresponding transition WLAN) but the **delete** button is activated only for the OPEN WLAN. When this OPEN WLAN is deleted from under the MVNO configuration tab, the corresponding transition WLAN is deleted as well.

Component/s	Virtual SmartZone
Issue	ER-12021
Description	Importing a controller certificate with CSR (Certificate Signing Request) for a private key caused an error.

Component/s	Virtual SmartZone
Issue	ER-12125
Description	The user role to User Traffic Profile (UTP) mapping failed when the rate-limiting attribute was sent with the *filter-id*.

Component/s	Virtual SmartZone
Issue	ER-12207
Description	Importing a Zone template generated an error.

Component/s	Virtual SmartZone
Issue	ER-12332

Component/s	Virtual SmartZone
Description	Adding more than five UDI (Unique Device Identification) entries in the controller caused an AP connection failure.

Component/s	Virtual SmartZone
Issue	ER-12951
Description	An incorrect Wi-Fi Tx power issue.

Component/s	Virtual SmartZone Data Plane
Issue	SCG-138986
Description	The release 3.6.2 Zones, on default data plane affinity group, were receiving the data plane IP addresses which was not part of the default list.

Interoperability Information

Cluster Network Requirements

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

Minimum Cluster Network Requirement

Model	SZ300	vSZ-H	SZ144	SZ100	vSZ-E
Latency	34ms	34ms	68ms	76.5ms	76.5ms
Jitter	10ms	10ms	10ms	10ms	10ms
Bandwidth	115Mbps	92Mbps	40.25Mbps	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.

NOTE
Client Interoperability issues stated in the 6.1.1 *Release Notes* are also applicable to this release.

Component/s	AP
Issue	SCG-140231
Description	The following client devices fail to connect to the profile with WPA2/WPA3 mixed mode with 802.11r being enabled. ● macOS Ventura (22D7750270d) ● MacBook Air ● macOS Catalina (19H2026) When PMF (Protected Management Frames) bit is set (default setting), the above listed clients cannot connect. When the bit is disabled, the listed clients can connect to the configured WLAN.

Component/s	AP
Issue	SCG-141661
Description	Authentication requests from an iPhone to an AP in order to roam to AP2 are fewer as compared to Android devices. The iPhone fails to roam to the target AP and does not attempt retries.

Component/s	AP
Issue	SCG-141709
Description	Surface Pro 4 fails to roam to the target AP. Instead, the device processes a full authentication, disconnecting from the original AP and connecting to the target AP.

Component/s	AP
Issue	SCG-143120
Description	Samsung S9 does not provide the PMKID (Pairwise Master Key Identifier) when carrying out a PMK with OKC (Opportunistic Key Caching) roam on an 802.11x WLAN with WPA3 encryption enabled.

Component/s	AP
Issue	SCG-145489
Description	The *MacBook Pro (macOS Ventura 13.5)* with an 802.11ac card processes a full authentication when roaming on a WPA3-SAE WLAN which is enabled for 802.11r.

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