RELEASE NOTES

SmartZone 6.1.1 (LT-GA) Release Notes

Supporting SmartZone 6.1.1

Part Number: 800-73141-001 Rev C
Publication Date: January 2023

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

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

Limitation of Liability

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

Trademarks

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

Contents

Document History

Revision Number	Summary of changes	Publication date
C	Added ER-11388/SCG-137191, ER-11519, ER-11594, ER-11682, ER-11729,ER-11793 to Resolved Issues on page 36.	27, January 2023
B	Deleted the note on R760 APs in a different AP Zone in Supported AP Models section	23, January 2023
A	Initial release notes	16, December 2022

New in This Release

This section provides a high-level overview of several key features that are introduced in the SmartZone (SZ) software release 6.1.1. The release 6.1.1 is applicable to the RUCKUS SmartZone 300 (SZ300), SmartZone 144 (SZ144), SmartZone Data Plane virtual (vSZ-D) and physical (SZ100-D), Virtual SmartZone – High Scale (vSZ-H), Virtual SmartZone – Essentials (vSZ-E) and controller platforms.

Wi-Fi 6e Access Points

The RUCKUS R560 is a 2x2:2 Wi-Fi 6E mid tier indoor Access Point (AP) that supports six spatial streams (2x2:2 (6GHz) + 2x2:2 (5GHz) + 2x2:2 (2.4GHz) 802.11ax Indoor AP).

The RUCKUS R760 is our highest capacity tri-band, tri-concurrent Wi-Fi 6GHz Access Point (AP) that supports 12 spatial streams (4x4:4 in 6GHz, 4x4:4 in 5GHz, 4x4:4 in 2.4GHz).

When the AP operates in 6GHz mode, the 6GHz radio:

- Operates in Low Power (Indoor) mode.
- Automatic Frequency Coordination (AFC) is required for standard power support and is not expected to be ratified for approved use at launch.
- Defaults to 160MHz.
- Only Channelfly as the automatic channel selection.
- Background scan default interval is 10 seconds.
- 6GHz radio only supports WPA3 and OWE security protocols.

AP R760 and R560 features not supported for this release

- 2SS downlink/uplink MU-MIMO (Multi-User Multiple Input Multiple Output)
- FILS (fast initial link setup) authentication
- Auto Cell Size*
- BSS Prioritization*
- 6E Spectrum Analysis*
- BeamFlex *
- 6Ghz BSS coloring*
- UNI4 channels

* *Features not supported on 6Ghz radio*

Limitations for this release

- **6GHz MBSS** - Maximum service WLANs on a 6GHz radio is limited to five.
- AP when powered by AF power source is not supported.

Power Modes

The table below depicts the operational state of each interface based on the negotiated/configured PoE Mode between AP (R560) and PSE Switch.

Power Mode	Power Source	2G/5G/6G Radio Chains (Tx/Rx)	6G Radio Chains (Tx/Rx)	2G/5G/6G Tx Power (dBm)	6G Tx Power (dBm)	1GE Ethernet Port	IoT	USB (3W)	Measured Power Consumption	LLDP Power Request
POE 802.3bt5	48V DC, BT POE Switch/ Injector	2x2/2x2	2x2	23/22	22	Yes	Yes	Yes	33.4W	35.0W
POE 802.3at	** 48V DC, AT POE Switch/ Injector	2x2/2x2	2x2	23/22	19	Off	Yes	Off	25.0W	25.5W
POE 802.3af	* AF POE Switch	2x2/2x2	Off	Off	Off	Off	Off	Off	11.4W	12.9W

NOTE
*AF mode - When AP is powered by AF power source cannot discover the controller. It is required that AP be powered by either 802.3at or 802.3bt5 or DC source.
**Whenever a POE injector is used, the AP operates in 802.2at power mode. However, if the administrator knows that POE injector is capable of providing higher wattage, 60 watts for example, then administrator can change the AP's power mode to 802.3bt5 through controller (vSZ) web user interface.

2-5-5 and 2-5-6 Radio Mode at Different Level

Simplifies the controller web user interface for APs points with tri-band radio.

11.5 Regulatory Domains

Update of regulatory domains for new APs.

Countries Supported on 6Ghz

1. Countries supported on 6Ghz U-NII frequency bands 5, 6, 7 and 8 supporting channels: 1, 5, ..., 233:
   - Brazil (BR)
   - Canada (CA)
   - South Korea (KR)
   - USA (US)
2. Countries supported on 6Ghz U-NII frequency band 5 supporting channels: 1, 5, ..., 93:
   - Australia (AU)
   - Austria (AT)

- Belgium (BE)
- Bulgaria (BG)
- Croatia (HR)
- Cyprus (CY)
- Czech Republic (CZ)
- Denmark (DK)
- Estonia (EE)
- Finland (FI)
- France (FR)
- Germany (DE)
- Greece (GR)
- Hong Kong (HK)
- Hungary (HU)
- Iceland (IS)
- Italy (IT)
- Latvia (LV)
- Luxembourg (LU)
- Malta (MT)
- Netherlands (NL)
- Norway (NO)
- Poland (PL)
- Romania (RO)
- Slovakia (SK)
- Slovenia (SI)
- Spain (ES)
- Sweden (SE)
- Switzerland (CH)
- United Kingdom (GB)

AAA Server Configuration Enhancement

This release supports use of Fully Qualified Domain Name (FQDN) for RADIUS server configuration. This allows the user to connect to the RADIUS server with a DNS name in addition to the IP address.

6Ghz BSS Minimum Rate – HE MCS

Adds the High Efficiency (HE) MCS rates to the BSS min rate options.

6Ghz Multicast Rate Limiting

Added support for 6Ghz multicast rate limiting.

CAC and PIV

Gives you the ability to implement Common Access Card (CAC) / Personal Identity Verification (PIV) card and *Two Factor Authentication* from the controller on Switches.

Characterizing Different Traffic Types for Quality of Experience (QoE)

Controller or APs gathers relevant metrics to be able to characterize different traffic types for application QoE.

Controller and Access Points gather relevant metrics to help classify different types of traffic (for example, video streaming, audio streaming, mail, web, file transfer) and sends the information to RUCKUS Analytics.

Change in Default TLS Version

Change in default TLS version from version 1.0 to 1.2 in Access Points (AP).

This increases security by making the AP default to using TLS version 1.2 for communications instead of version 1.0. TLS1.0 and TLS1.1 will no longer work by default. User can allow version TLS1.0 and TLS1.1 if required by configuring it through AP CLI.

> **ATTENTION**
> If LBS is configured in AP Zone, the controller LBS/vSPoT profile and LBS/vSPoT server should do the corresponding adjustment (change to TLSv1.2) after the AP firmware upgrade to release 6.1.1.

Chat Bot Integration

Added Chat Bot to the controller web user interface for customers to open tickets directly from the chat option.

Client Isolation per VLAN

Allows client isolation based on the VLAN. This can be applied to AP wired or wireless clients. It allows for better security and easier configuration of client isolation.

Cloud Radio Resource Management

Ability to use RUCKUS Analytics to manage the Radio Resource Management on the controller. RUCKUS Analytics has visibility into the entire environment and can use that information to plan radio channels more effectively.

Device Fingerprint Enhancement

Enhancement to take care of Client roaming and re-connections scenarios on same/neighboring APs. This enhancement makes device finger printing reporting more accurate and uniform.

Enhance Dynamic Packets Capture on APs

Dynamic packet captures will be collected on an APs per client basis when a client connection fails. This information is provided to RUCKUS Analytics to help troubleshooting.

Hanshow Dongle Support

An electronic shelf label (ESL) system is used by retailers for displaying product pricing on shelves. The product pricing are automatically updated whenever a price is changed from a central control server. Typically, electronic display modules are attached to the front edge of retail shelving. This feature allows support of ESL solutions on the RUCKUS APs. It supports third party USB device that utilize the `cdc_eem driver`. This USB device is used to communicate with the ESL devices with their proprietary protocols.

Hotspot 2.0 Data

Controller sends all the connection information and statistics for Hotspot 2.0 networks to RUCKUS Analytics and SmartCell Insight (SCI).

IPv6 AVC Enhancement

Allows application control and visibility when clients are using IPV6 address.

AVC enhancement aims to provide IPv6 support for AVC features like application recognition and control, URL Filtering and Wi-Fi calling. These features can now be configured and enabled in pure IPv6 network. Feature support provides better policy control and helps to monitor IPv6 traffic better.

Link to RUCKUS Analytics

This feature adds a link to the controller web user interface to make it easier for end users to sign up for RUCKUS Analytics.

Mesh Enhancements

Mesh Basic Service Set (MBSS)

Changes are made to Mesh Basic Service Set (MBSS) feature in this release to support mesh in 6Ghz radios.

5G and 6G Network Differentiation

Provides the ability to choose if wireless mesh uses the 5Ghz radio or 6Ghz radio. AP will compare throughput between 5G radio and 6G radio and choose the better one to be uplink if setting is auto mode.

Mesh User Interface Improvement

Mesh UI now shows the uplink and downlink MCS rates for Mesh APs.

Added MCS Rate to Mesh View

Adds the MCS information to the wireless mesh view to help with configuration and troubleshooting of mesh links.

Multiple Devices Support

Multiple devices support third party Wireless Distribution System (WDS) in Tunnel mode.

Supports third party wireless bridges with multiple Ethernet ports when using tunnel mode. This allows multiple wired devices to be connected to a single wireless bridge.

Network Segmentation

Network Segmentation allows a network administrator to easily on-board thousands of wireless and wired devices.

Data Plane Redundancy

This feature allows redundancy for VNIs, NAT, and DHCP. After implementing this feature, users will not lose these services if there is a failover to a redundant data plane.

AP Changes

AP changes will trigger an event when a Network Segmentation port is down due to non-assignment of VNI. It will also report VNI for wired Network Segmentation clients in the controller.

Data Plane Integration with Switches

VXLAN capable switches will be able to use the same Network Segmentation functionality as access points. This will make it simpler to provide a unified wired and wireless network for customers using network segmentation.

Profile Configuration

Adds the ability to select both Wi-Fi and Switch Zones to participate in network segmentation.

UI/UX Enhancement

Controller web user interface enhancements for setting network segmentation in WLAN section of the controller.

Troubleshooting

Enhanced troubleshooting options for devices using Network Segmentation. Provides troubleshooting with Client Connection Diagnostics (CCD) and Historical Client Connection Diagnostics(HCCD) for network segmentation.

Data Synchronization

Cloudpath will now synchronize the current state of network segmentation with the controller. This makes it so that configuration changes on one system will propagate to the other system.

Performance Tuning

Speed is increased of Cloudpath integration when using large numbers of APs with network segmentation.

Passpoint/HS2.0 v2 Support

Passpoint/HS2.0 v2 support with Onboarding(OSU) and SoftGRE in 5.2.2 code.

Allows to use of Hotspot 2.0 online sign-up when using SoftGRE.

PoE Healing and LLDP Values

PoE Healing

Sends sends information to RUCKUS Analytics for PoE (Power over Ethernet) Healing Network Insight.

PoE LLDP Values (35W to 40W)

Updates LLDP (Link Layer Discovery Protocol) codes to provide proper PoE values in specific situations.

> **NOTE**
> AP R760 request a maximum value of 40W through LLDP packets, whereas AP R560 requests a maximum value of 35W through LLDP packets.

R760 UI/UX Unification

Simplifies the configuration for AP R760 access points tri-band radio.

Removed IoT Radio Status from the Controller UI/UX

The IoT radio status is removed from the controller user interface to prevent confusion for users that are not using IoT radios.

Service Validation for RUCKUS Analytics

Change in default TLS version from version 1.0 to 1.2 in Access Points (AP).

Added the ability to use the R760 for service validation in RUCKUS Analytics.

Support 3.6.2 Zone

This allows you to run older access points that require a 3.6.2 Zone on controller with 6.1.1 firmware. This makes it possible to run different generations of access points on the same controller.

Supports OWE Transition Mode in RUCKUS APs

Supports *Opportunistic Wireless Encryption (OWE)* Wi-Fi standard to ensure that communication between endpoints is protected from other endpoints.

Switch Management

RUCKUS Switch ICX-8200

Supports RUCKUS Switch ICX-8200 on the controller - Future release will allow the controller to manage Switch ICX-8200.

Switch Port Template

Added the ability to create a template for port settings on Switches managed in the controller. This will make it simpler to assign the exact same configuration to multiple ports easily.

Configuration Change Alert

Provides an option to designate a selected switch configuration backup as the Master backup. If the subsequent backup differs from the master, the controller will display an alert informing the user that a configuration change is detected.

Filters Alarms for Specific Switch Interfaces

Added the ability to filter each alarms on Switches by specific text pattern on the controller.

CLI Template Enhancement

Added the ability to re-use (copy) variables across templates and provide an option to apply the configurations to stacks. This feature is for users using the controller for managing switches.

Schedule Switch Configuration Backup

Added the ability to schedule backups of switches that are managed by the controller.

Updates to Switch Synchronization

Lowers the time between switch synchronizations to three minutes and automatically triggers synchronizations after some specific configuration (Port/VLAN/LAG/Specific Setting) change is initiated on the controller and also when the user closes a Switch CLI session. This improvement makes the switch configuration changes appear faster on the controller whenever they are initiated by the controller.

UNII-2 Extended and UNII-3 for Israel Country Code

Israeli Ministry of Communications recently opened up bands 5470 to 5725 and 5.7525 to 5.875 . This update will allow the use of UNII-2 Extended and UNII-3 bands when using the country code for Israel.

> **ATTENTION**
> Israel country code does not support 6Ghz radio on AP R760 and R560 but supports 2.4GHz and 5GHz. This will be addressed in a future release. **[SCG-136558]**.

UI/UX RUCKUS Logo Update

The controller web user interface is updated with the new RUCKUS theme.

Verizon-RFC 5580 for Virtual Zone Phase2 Certification

This feature supports RFC 5580.This will convey access-network ownership and location information based on civic and geospatial location formats in Remote Authentication Dial-In User Service (RADIUS).

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.

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

ATTENTION
Upgrade from release 5.2.2.0.1562 to 6.1.1.0.688 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).

NOTE
The 10.0.00 release branch does not currently support network segmentation.

.

SZ300

- Controller Version: **6.1.1.0.959**
- Control Plane Software Version: **6.1.1.0.446**
- Data Plane Software Version: **6.1.1.0.959**
- AP Firmware Version: **6.1.1.0.1274**

SZ100/SZ124/SZ104

- Controller Version: **6.1.1.0.959**
- Control Plane Software Version: **6.1.1.0.446**
- Data Plane Software Version: **6.1.1.0.85**
- AP Firmware Version:**6.1.1.0.1274**

SZ144

- Controller Version: **6.1.1.0.959**
- Control Plane Software Version: **6.1.1.0.446**
- Data Plane Software Version: **6.1.1.0.85**
- AP Firmware Version:**6.1.1.0.1274**

vSZ-H and vSZ-E

- Controller Version: **6.1.1.0.959**
- Control Plane Software Version: **6.1.1.0.446**
- AP Firmware Version:**6.1.1.0.1274**

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

- Data plane software version: **6.1.1.0.959**

Cloudpath

- Cloudpath Version: **5.11 (5.11.5440)**

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

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

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

SZ Google Protobuf (GPB) Binding Class

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

1. SmartZone **6.1.1.0.xxx** (GA) GPB.proto (Google ProtoBuf) image for GPB/MQTT [DNP] –

   https://support.ruckuswireless.com/software/3502-smartzone-6-1-1-ga-gpb-proto-google-protobuf-image-for-gpb-mqtt

   File: ruckus_sz_6.1.1_protos.tar.gz

   Checksum: f921c13c82a2fb06d74761d0c9bf8ab6

2. SmartZone **6.1.1.0.xxx** MockSCI-TLS (SZ to SCI MQTT subscriber software) for CentOS / Ubuntu

   https://support.ruckuswireless.com/software/3501-smartzone-6-1-1-ga-mocksci-tls-sz-to-sci-mqtt-subscriber-software-for-centos-ubuntu

   File: scg-mock-sci-6.1.1-20221026.065353-56.tar.gz

   Checksum: f959db14fce0579c5da72ec4b4413e6b

IoT Suite

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

- vSCG (vSZ-H and vSZ-E), and SZ-124: **6.1.1.0.959**
- Control plane software version in the WLAN Controller : **6.1.1.0.446**
- AP firmware version in the WLAN Controller:**6.1.1.0.1274**

RUCKUS IoT Controller

- RUCKUS IoT Controller version: 2.0.1.0
- 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:

- SmartZone 6.1.1 Public API Reference Guide (ICX Management), visit

SmartZone 6.1.1 Public API Reference Guide (ICX Management)

- SmartZone 6.1.1 Public API Reference Guide (SZ100), visit

  SmartZone 6.1.1 Public API Reference Guide (SZ100)

  NOTE
  SZ100 Public API link is for SZ144 as well.

- SmartZone 6.1.1 Public API Reference Guide (SZ300), visit

  SmartZone 6.1.1 Public API Reference Guide (SZ300)

- SmartZone 6.1.1 Public API Reference Guide (vSZ-E), visit

  SmartZone 6.1.1 Public API Reference Guide (vSZ-E)

- SmartZone 6.1.1 Public API Reference Guide (vSZ-H), visit

  SmartZone 6.1.1 Public API Reference Guide (vSZ-H)

Dynamic Signature Package (Sigpack) Update

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

For manual upgrade, follow below steps:

1. Download Signature package by visiting the RUCKUS support site:
   - Regular Sigpack only for controller release 6.1.1: https://support.ruckuswireless.com/software/3473-smartzone-6-1-1-0-0-sigpack-1-590-1-regular-application-signature-package
   - Non-Regular Sigpack for 6.1.1 and older releases: https://support.ruckuswireless.com/software/3474-smartzone-6-1-1-0-0-sigpack-1-590-1-application-signature-package
2. Manually upgrade the signature package by navigating to **Security** > **Application Signature package**.

   NOTE
   More details can be found in Administrator Guide, in section *Working with Application Signature Package*

If 802.11ac Wave 1 APs are on legacy firmware (AP firmware prior to R6.1.1 release), you cannot download the current Sigpack version 1-590-1 regular Sigpack but can download the current non-regular Sigpack. If 802.11ac Wave 1 APs are on on R6.1.1 firmware, clients can download both 1-590-1 regular and non regular signature packs. **[SCG-123375]**

NOTE
As R5.1.x to R6.1.1 release upgrade is not supported, RUCKUS does not have any signature-package upgrade restrictions during Zone upgrade.

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.

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

ATTENTION
R730 has to be removed from the AP Zone **before upgrading** the AP Zone to 6.1.1 AP firmware. R730 can be still managed to an AP Zone running firmware older than 6.1.1.

The below table list the supported AP models in this SmartZone release when placed in an AP Zone, which uses an older AP version.

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

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

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.

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

Unsupported AP Models

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

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	
ZF7762-T	ZF7351-U	ZF7761-CM	ZF7343-U	

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	ICX 8200	

NOTE
* ICX 7750 is supported through FastIron 08.0.95 release.

NOTE
** FastIron 08.0.95a or later is required for managing ICX7550 switches.

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

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

The following table defines ICX and SmartZone release compatibility:

TABLE 4 ICX and SmartZone Release Compatibility Matrix

	SmartZone 5.0	SmartZone 5.1	SmartZone 5.1.1	SmartZone 5.1.2	SmartZone 5.2	SmartZone 5.2.1	SmartZone 6.0	SmartZone 6.1	SmartZone 6.1.1
FastIron 08.0.80	Yes	Yes	Yes	No	No	No	No	No	No
FastIron 08.0.90a	No	No	Yes	Yes	Yes	Yes	Yes	No	No
FastIron 08.0.91	No	No	Yes	Yes	Yes	No	No	No	No
FastIron 08.0.92	No	No	No	Yes	Yes	Yes	Yes	Yes	No
FastIron 08.0.95 and subsequent patches	No	No	No	No	No	No	Yes	Yes	Yes
FastIron 09.0.10a	No	No	No	No	No	No	No	Yes	Yes
FastIron 10.0.00	No	No	No	No	No	No	No	No	Yes

NOTE

FastIron 08.0.80 – SmartZone 5.1.1 does not support ICX configuration.

Following is the matrix for switch management feature compatibility:

TABLE 5 Switch Management Feature Compatibility Matrix

Feature	SmartZone Release	ICX FastIron Release
Switch Registration	5.0 and later	08.0.80 and later
Switch Inventory	5.0 and later	08.0.80 and later
Switch Health and Performance Monitoring	5.0 and later	08.0.80 and later
Switch Firmware Upgrade	5.0 and later	08.0.80 and later
Switch Configuration File Backup and Restore	5.0 and later	08.0.80 and later
Client Troubleshooting: Search by Client MAC Address	5.1 and later	08.0.80 and later
Remote Ping and Traceroute	5.1 and later	08.0.80 and later
Switch Custom Events	5.1 and later	08.0.80 and later
Remote CLI Change	5.2.1 and later	08.0.90 and later
Switch Configuration: Zero-Touch Provisioning	5.1.1 and later	08.0.90a and later
Switch-specific Settings: Hostname, Jumbo Mode, IGMP Snooping, and DHCP Server	5.1.1 and later	08.0.90a and later
Switch Port Configuration	5.1.1 and later	08.0.90a and later
Switch AAA Configuration	5.1.1 and later	08.0.90a and later
Switch Client Visibility	5.1.2 and later	08.0.90a and later
Manage Switches from Default Group in SZ-100 / vSZ-E	5.1.2 and later	08.0.90a and later
DNS-based SmartZone Discovery	5.1.2 and later	08.0.95c and later
Download Syslogs for a Selected Switch	5.2.1 and later	08.0.91 and later
Switch Topology	5.2 and later	08.0.92 and later
Designate a VLAN as Management VLAN	5.2.1 and later	08.0.92 and later
Change Default VLAN	5.2.1 and later	08.0.95 and later
Configure the PoE Budget per Port on ICX through the Controller GUI with 1W Granularity	5.2.1 and later	08.0.95 and later
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	08.0.90 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 (MDU)	6.1.1 and later	09.0.10d and later

NOTE

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

IoT Suite

This release supports IoT Controller release 2.0.1.0 and is compatible with the following controller and access point hardware and software.

Compatible Hardware

- H510/R510/T310D and i100 IoT Module
- R610/R710 and i100 IoT Module
- R720 and i100 IoT Module
- R730 Access Point
- R650 Access Point
- R750/T750/T750SE Access Point
- R850 Access Point
- R550/H550 Access Point
- R350/H350/T350D Access Point
- R550 and i100 IoT Module

Compatible Software

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

The below table lists the supported IoT end devices.

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

TABLE 6 Bulbs

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

TABLE 7 Locks

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	

TABLE 8 SWITCHES/PLUGS/THERMOSTAT/ALARM/BLINDS

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

TABLE 9 Sensors

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

TABLE 10 BLE

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

TABLE 11 Wired

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

TABLE 12 Supported Devices tested with SmartThings

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Yale YRD220/240 TSDB Display	Lock	Zigbee	Assa-Abloy	Yale	YRD220/240 TSDB
Lightify (RGB) Model 73674	Bulb	Zigbee	Osram	OSRAM	LIGHTFY A19 RGBW
Multipurpose Sensor	Sensor	Zigbee	SmarThings	Samjin	
Button	Sensor	Zigbee	SmartThings	Samjin	
Motion Sensor	Sensor	Zigbee	SmartThings	Samjin	
Water Leak Sensor	Sensor	Zigbee	SmartThings	Samjin	
Smart Plug	Sensor	Zigbee	SmartThings	Samjin	
Bulb	Bulb	Zigbee	Aduro SMART ERIA		
AEOTEC Multi Sensor	Sensor	Zwave	AEOTEC	AEOTEC	ZW 100-A
Hue Hub	Hub	Wired	Philips	Philips	3241312018A

TABLE 13 Device not QA 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

Known Issues

The following are the known issues in this release.

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-128288, SCG-128287
Description	R550 AP Ethernet ports at time negotiates to 100 Mbps instead of 1000 Mbps speed on the switch ports supporting Multi-Gig.
Workaround	If you see it go into 100Mbps, configure the speed-duplex port on the switch to disable auto-negotiation and set the static to 1000 Mbps(1Gbps).

Component/s	AP
Issue	SCG-138384
Description	Controller 6.1.1 supports 6Ghz mesh link between MAP and RAP. However the PMF (Protected Management Frames) capability is likely to be supported in future release.

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-131270
Description	Hotstar application fails to get detected when AP or the controller runs on Sigpack version 540.1 or 590.1.

Component/s	AP
Issue	SCG-135129
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-138426

Component/s	AP
Description	Corporate environments (HCCD [Historical Client Connection Diagnostic] and RUCKUS Analytics), observed re-association response failures or client connection failures even though client successfully roams. This does not have an impact to client connectivity or performance and it is a false alarm.

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 are less than 30 decibels.

Component/s	AP
Issue	SCG-127253
Description	When DHCP-NAT hierarchy network is used, the Non-Gateway AP remains disconnected (goes offline) from the controller once firmware upgrade is completed. The non-gateway AP becomes operational after it is rebooted

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 *rflow* age out timer not updating or entry not refreshed while running back to back test iterations.
Workaround	Give 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 (micro seconds Vs milli seconds). In these few scenarios it is seen 1-2 packets from previous session is 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 supported APs and when operating in 2-5-5 mode and when Spectrum Analysis is enabled it 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
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 (Ampere Frame) 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-138888
Description	If R760 AP Zone (2-5-6 radio mode) is running with builds 6.1.0.0.9018/6.1.0.0.9020, it needs to be mandatorily upgraded to 6.1.0.0.9023 build, before upgrading to 6.1.1 GA.

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 as mentioned in SCG-128672. 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-138963, SCG-132965
Description	For 11ax APs, **Airtime Utilization Pie Chart** > **Under Health** tab is planned to be released in subsequent releases once all Airtime stats are addressed by the chip vendor.

Component/s	AP
Issue	SCG-136547
Description	Mesh APs IP address fails to updated correctly in RAP APs mesh table but updates it correctly in the controller UI. This case can happen when Mesh AP reboots and connect to RAP or when Mesh link disconnects and reconnects.

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

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. To debug low throughput or packet drops, use below command in AP shell
Workaround	To debug low throughput or packet drops, use the below 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 only issue with **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-138946
Description	Split-tunnel configuration may not get updated on AP, when AP is moved from the controller default zone to a zone with split-tunnel enabled WLANs. This may not happen always but is inconsistent due to a timing issue.
Workaround	1. In the controller web user interface navigate to **AP Group** > **WLAN Group** assign it back to default (which has no WLAN). 2. Wait for AP configuration update and then re-assign the WLANs again. After the update, split tunnel will be enabled.

Component/s	AP
Issue	SCG-137371
Description	When client with wrong SAE (Simultaneous Authentication of Equals) connects to WPA3-SAE enabled WLAN, HCCD (Historical Client Connection Diagnostic) in controller UI shows failures for both second and fourth authentication packets instead of showing failure only for fourth authentication response.

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-138038
Description	R760/R560 AP fails to join the controller under 802.3af power mode.
Workaround	Connect to 802.3at or 802.3bt to PoE Injector or DC power.

Component/s	AP
Issue	SCG-138184
Description	FaceTime application may not get detected, which is known issue with Sigpack version 590.1.

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 starts browsing the network, these messages are not seen.

Component/s	AP
Issue	SCG-138610
Description	**Mqstats** command in AP CLI cannot see traffic identifiers (TID) (A-MSDU, A-MPDU in downlink), airtime and media queue flags.
Workaround	For debugging purpose, use alternate command: `nodestats wifi2 -DP <mac>`

Component/s	AP
Issue	SCG-138290
Description	At the current stage, 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

Component/s	AP
Description	In some rare scenarios, where authentications packets are sent after deauthentication within few micro seconds or when packet capture (pcaps) is filtered with zero timestamp, (SCG-136448) 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	Control Plane
Issue	SCG-138299
Description	Radio Frequency band information for events *RogueAPdetected(186)*, *RogueAPdisappeared(185)* and *RogueClient(194)* is not sent to RUCKUS Analytics from the controller.

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	FI-266177
Description	Trust port/uplink port CLI is appending as LAG interface when it is tagged as LAG interface under Web authentication VLAN.
Workaround	1. Select the **Access Switch** > **Port** > **LAG Setting** to create a LAG profile without Web authentication VLAN and then save the LAG profile. Make sure the LAG configuration is applied in the Switch. (Check **Configuration History** from the controller UI to confirm that the status is successful.) 2. Select the same profile and click **Configure** button to add the VLAN (for example. VLAN 10). 3. Save the LAG profile.

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 FI-266177 in ICX firmware 9010d.

Component/s	Switches
Issue	SCG-138835, SCG-137222
Description	When you select ICX Switch mode to upgrade FI10000 from the controller, it will not correspond to the switch firmware upgrade since ICX build FI10000 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 reconnect to the controller.

Component/s	Switches
Issue	FI-266896, FI-265881
Description	DHCP server configuration is moved through controller, shows the status as success from Switch, even though DHCP client is enabled on the Switch.
Workaround	Disable the DHCP client from Switch CLI and then enable DHCP server through controller.

Component/s	Switches
Issue	FI-195837
Description	ICX switches with firmware 08.0.90 may become offline when the controller upgrades from release 6.1 to 6.1.1.
Workaround	Upgrade the switch to 08.0.95 software before upgrading the controller to release 6.1.1.

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

Component/s	System
Issue	SCG-135808, FI-260414
Description	User 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	User 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 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 distribution Switch with 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	User 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	In AP R760 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.

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.

Component/s	Virtual SmartZone Data Plane
Issue	SCG-138986
Description	In 6.1.1 zone affinity profiles will be migrated to data plane (DP) group profiles. In the previous GD release (5.2.2), when an AP zone does not associate with a user defined DP zone affinity profile, the zone can establish a tunnel to any of available DP. In 6.1.1 the AP zone will be linked to default DP group automatically. When upgrading from 5.2.2 to 6.1.1 the AP only can establish a tunnel to the DPs in the default DP group, and a DP can only be assigned to one DP group profile in 6.1.1.

Changed Behavior

The following are the changed behavior issues in this release.

Component/s	AP
Issue	SCG-136335, ER-11480
Description	MU-MIMO (multi-user, multiple-input, multiple-output) is disabled by default in release 6.1.1 on all 2x2 APs like R560, R550, R350, H550, H350 and T350 series.

Component/s	AP
Issue	SCG-138506
Description	Users upgrading to 6.1.1 GA will observe 16db (approximately) lower RSSI and SNR values for Wi-Fi clients as compared to previous release of 6.1. RSSI/SNR values are corrected in this release and hence these values are as expected.

Resolved Issues

The following issue is resolved in this release.

Component/s	AP
Issue	ER-11665
Description	Resolved an issue where only one of two SoftGRE tunnels were displayed for vSZ AP.

Component/s	AP
Issue	ER-11255
Description	Resolved an issue where Web authentication for UEs reported an error of *System is too busy, please try again*.

Component/s	AP
Issue	ER-11169
Description	Resolved an issue where: • AP configuration preview table showed default values for Band/Spectrum configuration • Zone configuration preview table showed default values for Band/Spectrum configuration. .

Component/s	AP
Issue	SCG-128288, SCG-128287
Description	Resolved an issue where 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-11267
Description	Resolved an issue where WLAN QoS map set table was missing in WLAN form.

Component/s	AP
Issue	ER-11079
Description	Resolved an issue by changing the strategy of AP re-balance on data plane.

Component/s	AP
Issue	ER-11074
Description	Resolved an issue where AP support bundle feature failed to upload the file when AP is behind NAT server.

Component/s	AP
Issue	ER-11231
Description	Resolved an issue where AP T350D was found to be tagging Native VLAN, which was configured on the Ethernet 0 port.

Component/s	AP
Issue	ER-11374, 10837
Description	Modern 802.11ac, 802.11ax including 802.11ax-6E clients support 2by2 streams. As a result the MU-MIMO functionality with 2by2 AP's: R510 etc., is inherently not exercised. As such CLI support to enable MU-MIMO is provided. By default it is disabled.

Component/s	AP
Issue	ER-10674, ER-10760
Description	Modified AP internal logic for client disconnection due to inactivity to adhere to Inactivity Timeout configured in WLAN. In this release this is available in 802.11ax and 802.11ac wave 2 AP models.

Component/s	AP
Issue	ER-10474
Description	Resolved an issue of AP R710 throughput issue with 3 tier client.

Component/s	AP
Issue	ER-10671
Description	Enhancement in WISPr survivability feature allows the use of custom certificate loaded for this service during client authentication using HTTPS.

Component/s	AP
Issue	ER-10892
Description	Resolved an issue where AP name defaulted back to RUCKUS AP after upgrade to 5.2.2.0.1080.

Component/s	AP
Issue	ER-11308
Description	Resolved an issue where the AP CSV file failed to download because of an invalid *fwVersion*.

Component/s	AP
Issue	ER-11449
Description	Resolved an issue of WPA2 decryption on 2.4G radio of 11ac Wave 1 APs.

Component/s	AP
Issue	ER-11497
Description	Resolved an unexpected memory leakage reboot issue on 11ac APs.

Component/s	AP
Issue	ER-11792
Description	Resolved an issue of a looping condition when the network forwarded client packets from a roamed AP to the original AP.

Component/s	AP
Issue	ER-11793
Description	Resolved an issue where API call 'Retrieve AP model' from AP group was not providing expected reply: if AP model configuration is not overwritten, then return payload should be empty (return 1); otherwise, it would provide the configuration.

Component/s	Control Plane
Issue	ER-11005
Description	Resolved an issue of missing *strict transport security* header.

Component/s	Control Plane
Issue	ER-11541
Description	Resolved an issue where by adding the missing attributes in North Bound Interface (NBI) authorizes the API, such that the API call with *UE-Session-Timeout*, including other needed attributes, for example, works.

Component/s	Control Plane
Issue	ER-11458
Description	Resolved an issue where Public API was set to an incorrect default value for AP LAN port.

Component/s	Control Plane
Issue	ER-11627
Description	Resolved an issue where when WISPr UE failed authentication, the URL redirected does not include the full path.

Component/s	Control Plane
Issue	ER-11546
Description	Resolved an issue where data plane snapshot file failed to be transfer from data plane to control plane after it was created.

Component/s	Control Plane
Issue	ER-11720
Description	Resolved an issue where WISPR ZD login failed to redirect URL, which resulted in portal attributes not being passed. This is fixed by adding missing user portal attributes to the redirected URL when ZD login fails and the client gets redirected to the expected URL.

Component/s	Control Plane
Issue	ER-9797
Description	VMware vulnerability was identified in Open VM Tools (*open-vm-tools*) version 10 and has been fixed in version 11, which is included controller release 6.1.1.

Component/s	Data Plane
Issue	ER-11594
Description	Resolved an issue where new clients connected to tunneled WLAN may fail to have connectivity due to a host table leak issue in data plane.

Component/s	Data Plane
Issue	ER-11143
Description	Resolved an issue where the CLI command **Show dhcp** binding for a specific UE MAC address failed in vSZ-D.

Component/s	Data Plane
Issue	ER-11019
Description	Resolved an issue where the data plane upgrade procedure was halted due an internal RPM error.

Component/s	Data Plane
Issue	ER-11425
Description	Disk full is from large size of logs and need to avoid large size of logs by detecting the failure of log rotation function and recovering the log rotation function due to any failure. This issue is resolved in this release of 6.1.1.

Component/s	Data Plane
Issue	ER-11397
Description	Wireless client Mac address was learnt on controller SZ-144-D interface from more than one VLAN. Enhancement is made on data plane to make it wait for the flow to come up fully and then send out the packets. This will make MAC address of one UE be learnt from only one VLAN in core switches, instead of from multiple VLANs.

Component/s	Public API
Issue	ER-11073
Description	Resolved an issue of slower response to *snmpwalk*.

Component/s	SPoT
Issue	ER-11208
Description	Resolved an issue of unique visitor count mismatch.

Component/s	Switches
Issue	ER-11248
Description	Resolved an issue where when downloading a particular Switch port configuration displayed all the connected switches port configuration from the controller (vSZ).

Component/s	Switches
Issue	ER-11223
Description	Resolved an issue of failing to view the configuration back up from the controller and events/alarms by using *getQueryFiltersWithoutGlobalFilter* for switch pages.

Component/s	Switches
Issue	ER-10417
Description	Resolved an issue where Switch stack failed in initialization state on the Cloud GUI.

Component/s	Switches
Issue	SCG-128287, FI-255079
Description	Resolved an issue where R550 AP Ethernet ports at time negotiated to 100 Mbps instead of 1000 Mbps speed on the switch ports supporting Multi-Gig.

Component/s	Switches
Issue	ER-11682
Description	Resolved an issue where port view for switches could be missing when some port has over 1000 VLANs assigned.

Component/s	System
Issue	ER-11388, SCG-137191
Description	Resolved an issue where the correct AAA server fails to display on the troubleshooting page.

Component/s	System
Issue	ER-11519
Description	Resolved an issue where AP radio settings are shown differently on controller UI after upgrading to 6.1.

Component/s	System
Issue	ER-11729
Description	Resolved an issue where the controller version fails to change after upgrade, which causes the controller to be out-of-service after service restart and crash mode after reboot.

Component/s	System
Issue	ER-11040
Description	Resolved an issue of lost Switches and Switch Groups after upgrading to vSZ firmware.

Component/s	System
Issue	ER-11606
Description	Resolved an issue where third party AP broadcasted a hidden SSID to simulate NULL SSID rogue. The AP failed to match the rogue classification policy *Default Policy* with rule *Null SSID*.

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.

Component/s	AP
Issue	AP-18708
Description	Windows laptops will not be able to connect intermittently to FT (Fast BSS Transition) enabled WLANs due to wrong AKM (Authentication and Key Management) type sent by Windows laptops.

Component/s	AP
Issue	SCG-138759
Description	Intel AX210 with driver level 22.160.0.4 is not sending 802.11v BTM (BSS Transition Management) response when queried with BTM request. While not sending BTM response has not affected roaming or latency, the BTM request from the AP will contain the preferred roam candidate, and perhaps. when there's high population of AP's in same BSS (Basic Service Set), the station may not have all the roaming assistance needed to make the correct decision. This behavior is not present in driver version 22.160.0.4.

Component/s	AP
Issue	SCG-138875
Description	With Intel AX210 driver 22.180.0.4 version, 80 milliseconds latency is observed when roaming using WPA3 PSK. This specific driver 22.180 has a malformed roaming behavior, when using WPA3 PSK in all bands and the same is not observed with Enterprise. This behavior may result in slight VoIP degradation during roam.

Component/s	AP
Issue	SCG-136257
Description	iPhone 11 Pro with iOS version-14.8 has a connectivity issue with WPA3-SAE-AES WLAN.

Component/s	AP
Issue	SCG-136468
Description	Model name and OS vendor are shown as Roku streaming stick for Canon printer on the controller web user interface **> Client Information** .

Component/s	AP
Issue	SCG-136473
Description	• As Wi-Fi 6E cannot support Open-Security WLAN, the OWE-Transition mode (Wi-Fi Enhanced Open) is not supported for Wi-Fi 6E. • As stated on the Apple website, Apple devices are not currently supported for OWE-Transition mode. Refer to https://support.apple.com/guide/security/secure-access-to-wireless-networks-sec8a67fa93d/web • To associate WLAN UE to the AP in OWE-Transition mode, the WLAN UE is required to support the OWE-Transition mode feature. It is recommended to consult with the device vendor for relevant product information.

Component/s	AP
Issue	SCG-138747
Description	OS vendor and model name for Wyze camera is displayed as Amazon Kindle as DHCP fingerprint sent by client is similar to Amazon Kindle.

Component/s	AP
Issue	SCG-138463
Description	FT roaming failure is observed on below client-OS version combination: • Samsung S21, Android version: 11 • iPhone XR, iOS version: 15.6.1 • iPhone8, iOS version: 15.6 • iPhone11, iOS version: 15.5
Workaround	Update OS versions to Android 12 and iOS 16 respectively.

Component/s	AP
Issue	SCG-138375
Description	Majority iOS devices display *Reason code 23* during a longer run and frequently fail to connect back automatically. Impacted clients: • IPhone 12 • IPhone 13 • iPad Air Pro Max

Component/s	AP
Issue	SCG-138310
Description	Laptop keeps flapping between 2.4GHz and 5GHz if the RSSI of both the radio comes closer to each other - *+-2DBM*. This can create disconnections during longer connectivity cases. Impacted clients: • Windows laptops • MacBook • Chromebook

Component/s	AP
Workaround	Reduce RSSI of 2.4 Ghz to *+-5DBM* to control UE flapping.

Component/s	AP
Issue	SCG-137240
Description	Mi TV connectivity is not smooth as sometimes client does not respond to EAP messages which results in EAPOL timeout. It was also observed that the UE disconnects when a channel changes.

Component/s	AP
Issue	SCG-133156
Description	After successful UEs iOS, MAC devices connection, if the device moves away from the AP RF coverage and if the client comes within the AP RF coverage and within the inactivity timeout then the device goes for a full authentication instead of skipping the authentication process.

Component/s	AP
Issue	SCG-136634
Description	Intermittently *Sonos* product client information is reported as *unknown* on the controller web user interface as the client fails to go through DHCP process on re-connection.

Component/s	AP
Issue	SCG-136510
Description	Samsung Galaxy Z Fold3 (SM-F926U1, Android 12, Build Number : SP1A. 210812.016.F926U1UES1CVC9) fails to connect on Channel 40 intermittently.

Component/s	AP
Issue	SCG-136839
Description	Mac mini devices with Intel chip sets do not support FT (Fast BSS Transition) roaming. **NOTE** FT roaming is supported on *Mac mini* running on *Apple M1* chip sets.

Component/s	AP
Issue	SCG-136942
Description	Few clients fail to re-associate to SSID after either enabling or disabling WLAN service of radio.
Workaround	Manually attempt connecting to the SSID.

Component/s	AP
Issue	SCG-136946
Description	802.11r roaming fails on iPhone 11 (2019, IOS version 15.4) and iPad Pro (10.5 inch, 2017, IOS version 15.4).

Component/s	AP
Issue	SCG-137196

Component/s	AP
Description	1. Model: Dell 5490 2. Operating System: Windows 11Driver 3. Version and NIC: 22.140.0.3 and AX210 Intel 6E clients with AX210 show a sticky behavior when connected to 6GHz radio and fails to roam to a better signal AP when RSSI is greater than *-70 dBm*.

Component/s	AP
Issue	SCG-137209
Description	Windows client processes full authentication when *OKC (Opportunistic Key Caching) is enabled with WPA3-profile*. This is because Windows does not support OKC for WPA3 but only supports OKC WPA2.
Workaround	For Windows clients use WPA2 as the encryption type if OKC is enabled.

Component/s	AP
Issue	SCG-137239
Description	All Windows 11 clients are reported as *Microsoft Windows/Windows 10.0.0* on the controller web user interface > **Client Information** (*Model Name*).

Component/s	AP
Issue	SCG-137243
Description	Apple MAC devices having macOS *Big Sur* and above (version 11+) reports OS version as *Apple Mac/Mac OS X 10.15.7* on the controller web user > **Client Information** (*Model Name*.

Component/s	AP
Issue	SCG-137244
Description	With MAC randomization enabled, iPhone13 Pro hostname is not displayed on the controller web user **Zone** > **Client Information** (*Model Name*.

Component/s	AP
Issue	SCG-137294
Description	Samsung 6E client is not able to connect to R760 with 6.1.1 on 6Ghz radio.
Workaround	Devices must have capabilities element set to High Efficiency (HE) to associate to Wi-Fi 6E AP's with 6Ghz frequency.

Component/s	AP
Issue	SCG-138535
Description	When QUIC (Quick UDP Internet Connection) session by YouTube resumes without any client-hello/server-hello handshake, flow is not detected by DPI (Deep Packet Inspection) and therefore ARC policy will not be applied if it is configured for YouTube.

Component/s	AP
Issue	SCG-138910

Component/s	AP
Description	Client fails to connect to the WPA3 EAP TLS profile with *AES_GCMP_256* bit encryption. This issue is specific to Android 13 QPR (T1B3.221003.008). It works with the earlier version of Android 13 QPR (T1B2.220916.004).

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