RELEASE NOTES

RUCKUS SmartZone 5.2 Release Notes

Supporting SmartZone 5.2

Part Number: 800-72236-001 Rev G
Publication Date: September 2020

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
G	Added the following to Known issues: 1. SCG-118945 2. SCG-118998	10, September 2020
F	Added a bullet point on APs support in Overview on page 17	16, July 2020
E	Added ***Nutanix Hypervisor Support*** in New in This Release on page 5	19, June 2020
D	Added AP firmware table and modified the sentence on non-supported 802.11ax AP feature in New in This Release on page 5	13, April 2020
C	• Added to resolved issue ER-7642 and ER-8026 • Deleted the line *H510 and T310c APs do not support PoE operating mode* from Supported AP Models section	24, February 2020
B	Added new build numbers Removed SCG-113477 from Known issues. Added the following to Known issues: • SCG-112702 • SCG-103158 • SCG-102179 • SCG-98589 • SCG-91887 • SCG-93034 • SCG-89015 • SCG-84658 • SCG-82509 • SCG-103688 • SCG-103799 • SCG-105847 • SCG-93304 Modified the text for SCG-112702 and SCG-97553 Added to Resolved issues: • ER-8098 • SCG-104362 • SCG-48792 Removed SCG-108451 from Resolved issues Added to Client Interoperability: • SCG-105741 • SCG-104650	11, February 2020
A	Initial release notes	28, January 2020

New in This Release

This section provides a high-level overview of several key features that are introduced in the SmartZone (SZ) software release 5.2

The SZ release 5.2 is applicable to the Ruckus SmartZone 300, SmartZone 100, vSZ-H, and vSZ-E controller platforms. For additional details, do refer to the SmartZone Controller Documentation Suite for Release 5.2.

NOTE
For detailed descriptions of these features and configuration help, refer to the respective 5.2 documentation guides available at https://support.ruckuswireless.com/

AP Features

Release 5.2 supports the following 802.11ax APs (R750, R650 and T750). The table, below, lists the features supported on each 802.11ax AP.

New Access Points

- R650

  The Ruckus R650 is a new mid-range "Wi-Fi 6" (802.11ax) dual-band indoor 4x4: 4 AP with BeamFlex+, one 2.5 Gbps PoE+ port and one 1 Gbps Ethernet port, and onboard support for IoT and BLE/Zigbee.

- T750

  The Ruckus T750 is a new carrier-class "Wi-Fi 6" (802.11ax) dual-band outdoor access point with integrated 2-port Ethernet and SFP/SFP+ fiber interface. The T750 includes onboard BLE/Zigbee support, one 2.5 Gbps PoE+ port and one 1 Gbps Ethernet port in addition to the fiber interface.

TABLE 1 802.11ax AP

New Feature	Supported 802.11ax AP Platforms	Comment
Transmit Beamforming	R750, R650, T750	Digital transmit beamforming to 802.11ac and 802.11ax clients. Improves over the air performance .
Downlink Multiuser-MIMO (Multiple Input Multiple Output)	R750, R650, T750	Transmit downlink traffic to multiple users simultaneously using Multiuser-MIMO technique. Supports both 802.11ac and 802.11ax clients. Improves performance mainly with 1x1 clients.
OFDMA (Orthogonal Frequency Division Multiple Access)	R750, R650, T750	Transmit and receive traffic with multiple users simultaneously using downlink and uplink OFDMA technique. Helps reduce overhead, for small packets and reduces collisions in high density scenario. **NOTE** Supported only for 802.11ax clients.
Target Wake Time	R750, R650, T750	Sets individual wake time intervals with 802.11ax clients that supports target wake time feature.
Airtime Fairness	R750, R650, T750, R730	Ensures equal airtime is allocated to all types of clients .
BSS Prioritization	R750, R650, T750, R730	Allows higher airtime allocation for clients in one BSS over clients in other BSS.
WPA3 (Wi-Fi Protected Access 3)	R750, R650, T750, R730	Supports WPA3 authentication.

TABLE 1 802.11ax AP (continued)

New Feature	Supported 802.11ax AP Platforms	Comment
Optimized Connectivity Experience	R750, R650, T750, R730	Improves connectivity experience for clients supporting 802.11ai.
End to End Rogue Security Enhancement	R750, R650, T750, R730	Enhancement to rogue security to match capability of non 802.11ax APs.

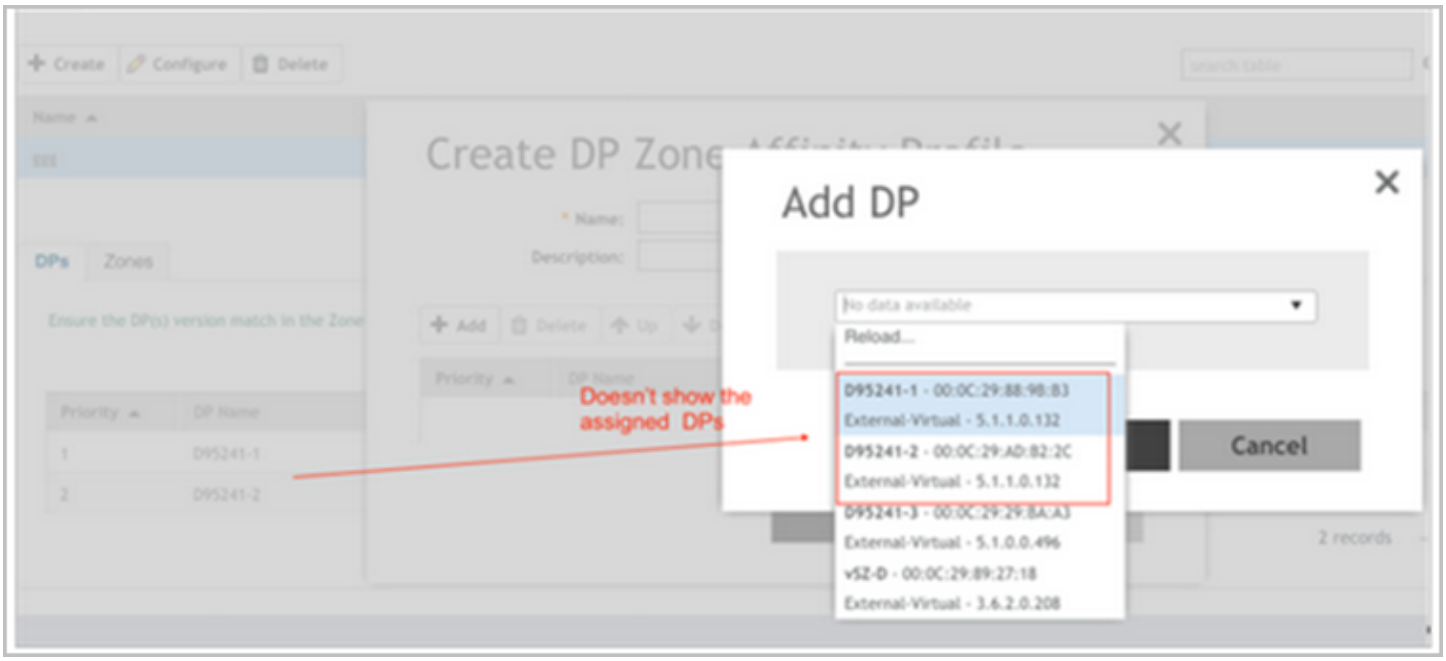
The below list of features is not supported in 5.2 release for the mentioned APs.

Feature	802.11ax AP Platforms
Transmit Beamforming	R730
Downlink Multiuser-MIMO	R730
Uplink Multiuser-MIMO	R750, R650, T750, R730
OFDMA	R730
Target Wake Time	R730
Autonomous Cell Sizing	R750, R650, T750, R730
Agile Multiband or MBO	R750, R650, T750, R730
Agile DFS	R750, R650, T750, R730
160 MHz Bandwidth	R750, R650, T750, R730
Spectrum Analysis	R750, R650, T750, R730
LACP	R750, R650, T750, R730
Mesh	R750, R650, T750, R730
IPSec Tunnel	R750, R650, T750, R730
Rogue Auto/ Aggressive Mode	R750, R650, T750, R730
Multicast Rate Limit	R750, R650, T750, R730
User Agent	R750, R650, T750, R730
Telemetry Statistics	R750, R650, T750, R730

Data Plane Zone Affinity Enhancement

To simplify data plane (DP) zone affinity management and managed DP group, the controller checks profiles on the DP to make sure there is only one profile being assigned to a DP. The original purpose is to prevent a DP from being over-assigned to 1+ Zone Affinity profiles, which means a DP only belongs to a profile at a time.

On the web user interface, when the administrator assigns profile to a DP, it only shows DPs that have not been assigned profile yet.



SZ100 Data Plane Multicast Forwarding for Bonjour Fencing and Bonjour Gateway

Ruckus APs support Bonjour Fencing and Bonjour Gateway, but the data plane prior to R5.2 did not support Bonjour Fencing and Bonjour Gateway but supported *Multicast Forwarding* on SZ100 and this could potentially cause some performance issues. So, in this release, we have added that feature to SZ100 data plane to limit Bonjour traffic by Bonjour Fencing and Gateway feature.

A typical example when multicast forwarding is enabled:

1. SZ100 data plane will provide at most 128 APs to forward Chromecast service for each VLAN
   a. Bonjour Fencing can be used to configure service and range (same AP or one-hop)
      1. If customers set up the service to Chromecast and range is *same- AP* when SZ100 data plane receives *Chromecast mDNS* from AP1. SZ100 data plane forwards only Chromecast mDNS to the core side and not to other APs.
      2. If customers set up the service to Chromecast and range is *one-hop* when SZ100 data plane receive Chromecast mDNS from AP1. SZ100 data plane forwards Chromecast mDNS to core side and to AP1's neighbor APs.
   b. If Bonjour Fencing is not configured when SZ100 data plane receives Chromecast mDNS from AP1, it forwards Chromecast mDNS to the core side and to other 127 APs.
2. If customer wants to increase their supported APs, Bonjour Gateway can be enabled to transfer traffic from VLAN A to VLAN B. Under this configuration, SZ100 data plane can serve Chromecast service up to 256 (128*2) APs.

DNS Spoofing on AP Enhancement

In some cases, customer network needs to be able to override DNS server when client performs DNS queries. This means having the AP respond to the client DNS query on behalf of the server. In short the AP is acting as a proxy for the DNS server.

Today the Ruckus SmartZone APs have that feature built in and can be used through CLI, for instance, the AP CLI commands of **set dns-spoofing** and**get dns-spoofing**. However, the settings are not permanent as they do not survive WLAN configuration updates from SmartZone nor AP reboots.

With this release, we make this configuration available through SmartZone on a per WLAN basis and make such configuration persistent.

Known Limitations:

- There is no mutual intersection on AP when both URL Filtering and DNS spoofing are configured and put to AP simultaneously.
- If DNS spoof and URL filtering with safe search is enabled, URL filtering safe search will take the precedence for Google, YouTube, Bing domain names. If safe search is not enabled, DNS-Spoof will take the precedence. If safe search is not enabled and URL filtering is enabled also DNS-Spoof will take the precedence.
- Allow maximum of **64** unique domain name entries per profile.
- Each domain name entry can have maximum of **Eight** IP addresses (IPv4 or IPv6, based on Zone configuration)

  NOTE
  IPV4 Zone will allow to configure only IPV4 addresses, IPV6 zone will allow only IPV6 addresses and both IPv4 & V6 are allowed to configure in Dual Zone.

- The maximum profiles per Zone is **32**.
- The maximum profiles per System is **10,000**.
- The domain name canot configure**my.ruckus** and **scg.ruckuswireless.com**.
- Added remind wording **Please ensure that the domain name should not be internal domain names and certificate FQDN names**when create / update DNS spoofing profile.

Display Firewall Rules Required for External Firewall Policy Implementation

When SmartZone is installed behind an external firewall secured from the Internet, a number of TCP and UDP ports are required to be opened and permitted for SmartZone to be fully operational. In previous releases, a table with all the firewall rules required are documented in the technical documentation however some of the rules are static and specific to certain processes which may not be applicable to every single installation.

Therefore this feature introduces the dynamic queries to the running services and generate all the firewall rules (inbound and outbound) required to be implemented at the external firewall to allow SmartZone to function fully. An enhancement is also introduced to make the built-in firewall enabled by default across all variants of SmartZone platform. The dynamic firewall rules are available from the admin console and also via the public API query.

Firewall Enhancements

Prior to 5.1.2 release SmartZone already has a number of security related features implemented on the platform but they are located in different web user interface structure and sometimes difficult to associate policy to profile and enforcement. This enhancement is to consolidate all the security features under single umbrella web user interface menu collection, namely firewall profile. Security profiles under the firewall profile includes the following:

- L3 Access Control Policy
- L2 Access Control Policy
- Application Policy
- URL Filtering Policy
- Device Policy

Starting from 5.2, previous UTP (User Traffic Profile) will be replaced with firewall profile. Individual traffic policy profiles will be linked at the firewall profile level or WLAN level. Device policy and L2 ACL are removed from Zone Level to Domain Level to maintain consistency, while both will be included as part of the new firewall profile. Traffic ACLs have been removed from the UTP and incorporated into the new L3 ACL Profile which is now part of the firewall profile as well.

As part of the firewall enhancement, security features such as AVC, URL Filtering and L3 ACL are now also supported on the Wired Port on AP, on top of the support on the WLAN.

A brand new firewall dashboard is introduced which provides enhanced reporting on firewall to allow better stats reporting with hit counts per firewall profile.

Geo-Redundancy Enhancements

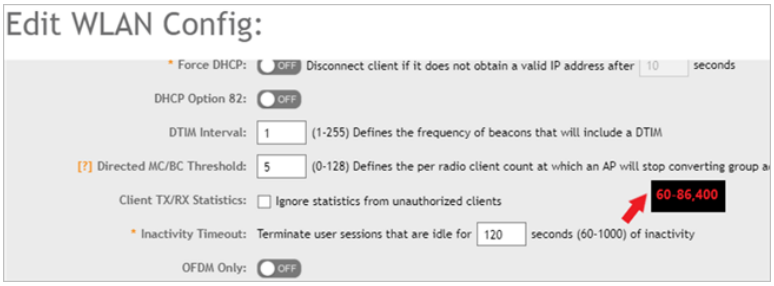
This is the phase four of Ruckus wireless network geo-redundancy feature. In previous release, precondition was to disable Active-Standby cluster redundancy and to have standby cluster in monitor mode. From this release, Geo redundancy is one-to-one deployment where standby cluster is always in backup mode, so the precondition is to disable Active-Standby cluster redundancy in one-to-one deployment is the number AP and external data planes connected to standby cluster.

1. In one-to-one deployment:
   a. Standby cluster restores configuration from active cluster every time after configuration synchronisation is completed, and
   b. Standby cluster is always in backup mode, ready to receive the APs (Access Points) and external-DPs (Data Plane) from out-of-service active cluster.
2. In many-to-one deployment (Two or three active clusters and one standby cluster)

   The time taken by Standby cluster from detecting Active cluster is out-of-service to it's being ready to serve APs and external-DPs is enhanced.
3. Data brokers such as MLISA, ALTO, SCI are all disabled in standby cluster.
4. Geo Redundancy does **not** support ICX switches.
5. Make sure the HA licenses are on standby cluster when the configuration restore is completed on standby cluster.

Increase WLAN Inactivity Timeout

This feature is to increase the maximum user equipment inactivity timeout limit (previously maxed at 1,000 seconds). Typical use case is to timeout after 24 hours so the maximum limit has been increased to 86,000 seconds (24 hours). This is particularly important for the user experience when repetitive portal or authentication request is popping up too frequent during single day access.



M510 Mesh Support

Currently, M510 AP is only allowed to be deployed in a mesh disabled zone. Use either Wired or LTE (Long Term Evolution) as the backhaul. In this 5.2 release, M510 will be allowed to establish mesh uplink as an additional backhaul support. This kind of topology is suggested to be used when M510 is deployed on a moving system, such as Bus.

- **Design enhancements**: In the original Mesh scan design, MAP does full channel scan when it is trying to find an uplink AP to connect. With this, client traffic will be affected due to frequent channel switching. In R5.2, LTE is used as the backhaul when there is no Mesh uplink. In this case, client traffic will not be affected when M510 is searching for uplink AP to connect.
- **Known limitations:**
  - M510 mesh role is fixed to Mesh AP. It cannot be a root AP.
  - Mesh link and LTE link will not be activate simultaneously. When Mesh link is up, LTE link will be disabled.
  - LBO (Ethernet without tunnel) traffic is only routed through Mesh uplink.
  - When deploying M510 in a mesh enabled and DHCP/NAT enabled zone, M510 can only be a non-gateway AP.
  - Administrator should deploy service WLAN and Ethernet with tunnel mode to ensure WLAN/Ethernet traffic can pass through no matter using LTE or mesh link as the backhaul.
  - Non-tunnel WLAN will not be brought up on mesh enabled M510
  - M510 as a MAP allows downlink MAP connection only when using mesh link but not LTE as the backhaul
  - GPS geo-fence is used to decide when M510 will start searching for mesh uplink. The default GPS is updated periodically. It is expected to have delay for M510 to start searching mesh uplink (until M510's GPS data is updated).
  - Zero Touch Mesh is not supported

Management ACL on APs

The significance of ACLs has been recognized in past and continuously increasing rapidly due to the explosive growth of Internet-based applications and malicious attacks. An access control list provides a security to a network by inspecting inbound and outgoing packet traffic. Hence, customers want to deploy the restriction of administrative access from only allowed network, user or IPs, which will protect AP's management interface as well as the clients which are connected to it.

ACL can be divided into two categories for the kind of traffic involved:

1. **Client Traffic:** The traffic originating and terminating from/to the clients and Ruckus AP bridges the traffic from wireless to wired and vice-versa.
2. **Ruckus AP's Management Interface Traffic** : The traffic originating and terminating at the APs management IP address.

Before SmartZone 5.2 release, Ruckus APs supported only Client ACL in the upstream direction (that is from the wireless towards Ethernet backhaul) for the wireless clients only. The main objective is to enhance the present ACL feature for all types and direction for client traffic as well as for the traffic terminating at the Ruckus AP management IP address.

More Granular Device Fingerprinting

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

The goal of this feature is to enhance our client OS fingerprinting such that we can identify more granular levels of device OS. There are two components of this:

- More granular device identification - be able to distinguish between iPhone, iPad, or AppleTV.
- OS version identification - be able to tell difference between XP, Windows 7, Windows 8, Windows 10 or other device versions.

Multicast and Broadcast Filter

Dropping multicast and broadcast traffic from clients helps avoiding multicast and/or broadcast storms from wireless clients which in turn saves wireless bandwidth, AP resources and protects network from unnecessary traffic.

In this SmartZone release, we implemented a new checkbox labeled as *Multicast filter* will be enabled in the *Advanced Options* section of the WLAN configuration page of SmartZone. When this option is enabled, the AP will drop all IPv4 and IPv6 multicast/broadcast from associated wireless clients except for below traffics, which form the *multicast filter bypass* list. The packets in the below list will always be allowed.

- ARP (Address Resolution Protocol) request
- DHCPv4 request
- DHCPv6 request
- IPv6 NS (Neighbor Solicitation) Message
- IPv6 NA (Neighbor Advertisement) Message
- IPv6 RS (Router Solicitation)
- IGMP (Internet Group Management Protocol)
- MLD (Multicast Listener Discovery)
- All unicast packets

Native IoT Support

SmartZone 5.2 introduces native support for the Ruckus IoT eliminating the need for a dedicated IoT version of SmartZone. The IoT controller is still a separate virtual controller with its own user interface for configuration and management of IoT gateways and sensors.

Organizations seeking to deploy IoT solutions face a complex, fragmented ecosystem of standards, devices and services that often slows or stalls enterprise IoT deployments.

The Ruckus IoT Suite, is a collection of network hardware and software infrastructure components that enable organizations to build a secure, scalable IoT access network leveraging the Wi-Fi infrastructure. The Ruckus IoT Suite consolidates multiple physical-layer IoT networks into a single network enabling organizations to more quickly realize benefits from IoT investments.

The IoT Suite consists of four main components:

- **Ruckus IoT-Ready Access Points (APs)**: Accommodates Ruckus IoT modules to establish multi-standards wireless access for Wi-Fi and non-Wi-Fi IoT endpoints.
- **Ruckus IoT Modules**: Radio or radio-and-sensor devices that connect to a Ruckus IoT-ready AP to enable endpoint connectivity based on standards such as Bluetooth Low Energy (BLE), Zigbee and LoRaWAN.

- **Ruckus SmartZone Controller**: A network controller that provides a management interface for the WLAN and allows for delivery of IoT software updates to the APs.
- **Ruckus IoT Controller**: A virtual controller, deployed in tandem with a Ruckus SmartZone based controller, that performs connectivity, device and security management functions for IoT devices, as well as facilitate disparate endpoint management coordination and APIs for northbound integration with analytics software and IoT cloud services.

Features

Ruckus IoT-1.4 Suite provides the following update:

- Multi-Mode Radio Support in R730 (1-Zigbee and 1-BLE only supported)
- Gateway as a Beacon
- BLE Visualization
- AA Operator Key support
- Statistics Push (MQTT Based)
- Connector Gateway Mapping (connector enable/disable on per Gateway basis)
- Connector Gateway Heartbeat
- iBeacon and Eddystone Vendor UUID Filtering
- N+1 Enhancement (Master/Slave replacement and Force Fallback)

Best Practices

- Both IoT Controller and vSZ/AP need to be upgraded to their release versions of 1.4.0/5.2 together and upgrade only from the release versions of 1.3 for IoT controller with vSZ/AP from the supported upgrade paths for 5.2
- Upgrade is supported only on +1. In case of lower version eg. 1.2 then controller needs to be upgraded to 1.3 and then to 1.4
- Time and Timezone should be properly set in Ruckus IoT Controller.
- N+1 works on Virtual IP mode. For successful failover AP MQTT Broker should be configured for Virtual IP.
- N+1 Configuration Sync happens every 5 minutes. If a configuration change and failover happened within the 5 minutes window, new configuration will be lost.
- In N+1 mode make sure Master and Slave have the same admin credentials (password).
- The IoT Controller (4vCPU) at max supports upto 400 packets/second and any load above this could lead to controller instability. Capacity planning needs to be taken care of during deployment so as not to exceed the limit.
- Use the Replace master option in N+1 only after making sure master is not reachable from slave
- For information on clusters, refer to this externally available Zigbee Alliance Zigbee Cluster Library 6 document at http://www.zigbee.org/~zigbeeor/wp-content/uploads/2014/10/07-5123-06-zigbee-cluster-library-specification.pdf.

Limitations

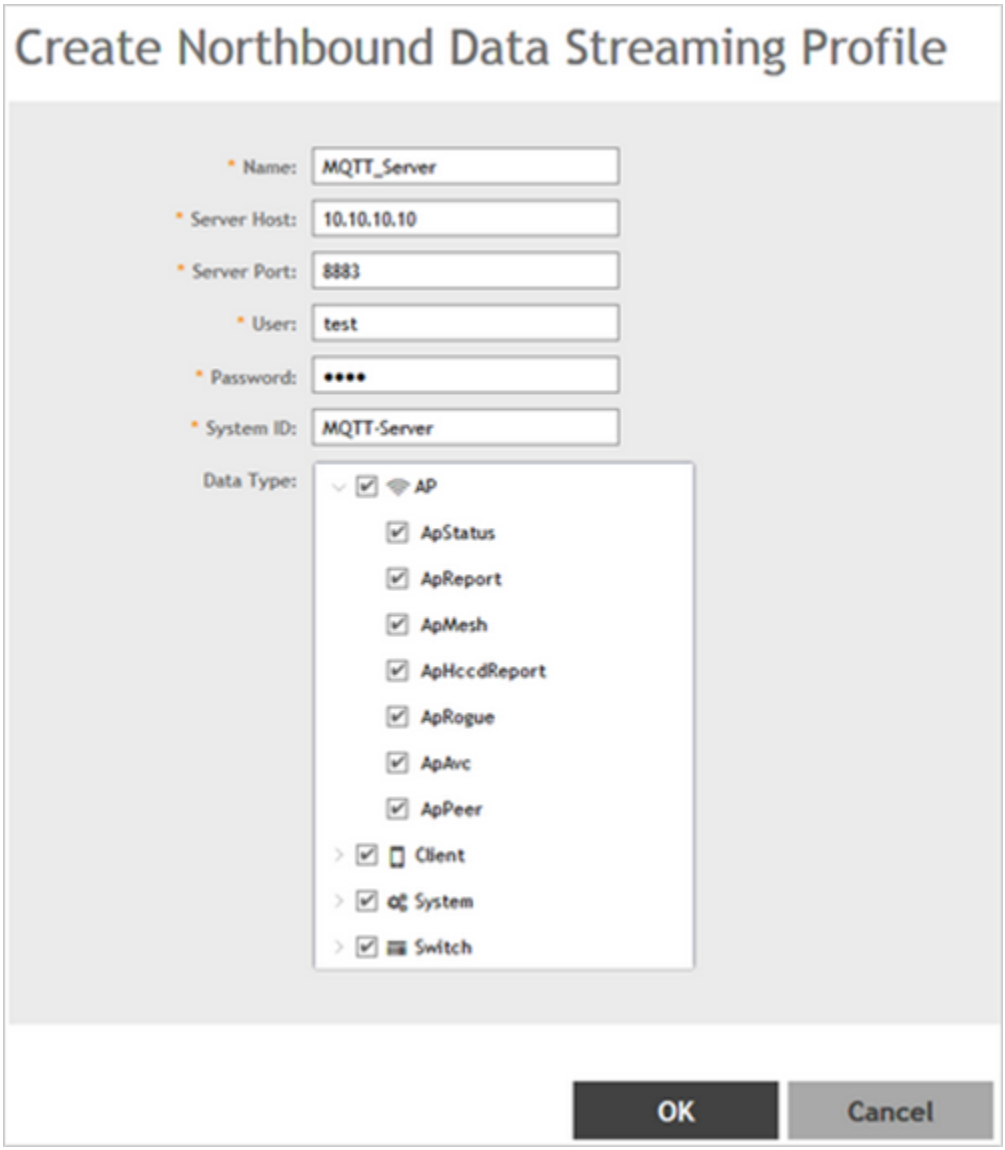
- N+1 can be disabled (from Master) even when Slave is not reachable. When Slave comes back online, need to delete and create a new Slave controller.
- N+1 Auto Fallback is not supported (If Master is back online, Slave will run as Active Slave)
- Database backup and restore is not supported across major releases.
- Gateway supporting multi-mode causes IoT by AP protocol count to go wrong as each mode is considered as a separate AP
- IoT co-ex feature is not supported on multi-mode Gateway (R730)

Northbound MQTT Enhancements

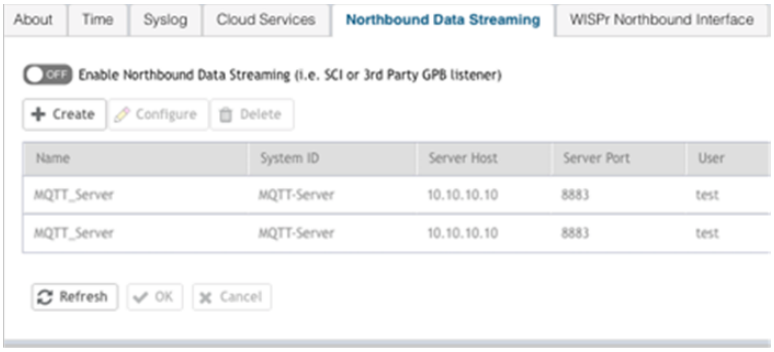
Instead of streaming all data northbound to the subscriber, Ruckus categorized all statistics and status that are being sent northbound into four categories:

1. All
2. AP
3. Client
4. System

User will be able to choose from these categories to send the data.



In addition, the current MQTT interface only allows one GPB listener. In release 5.2, we will now allow a maximum of two listeners to subscribe to the interface. Each subscriber will be able to select its own topics. One issue to note is that user should choose to use either MQTT streaming or FTP data export.

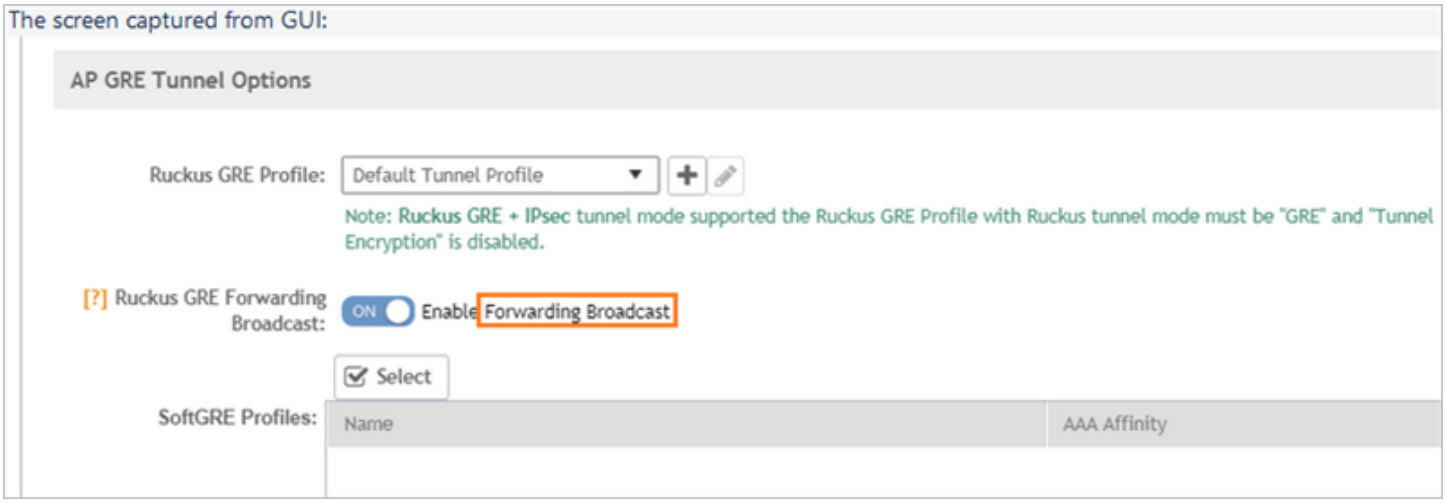


Nutanix Hypervisor Support

Beginning from release 5.1.2, we added Nutanix Hypervisor support for vSZ and vSZ-D. Please refer to Nutanix official site for their hardware resource requirements to run the Hypervisor itself. The resource requirements to run vSZ and vSZ-D will be same as the other Hypervisors we support.

Option to Enable Forwarding Broadcast to AP in RGRE Tunnels

Ruckus current design only allows DHCP and ARP broadcast traffic to be forwarded to APs via the Ruckus GRE tunnels from the core side. With this release, users can enable *Forwarding Broadcast* traffic from network to tunnel except ARP and DHCP in the web user interface. The enablement can be a zone, ap-group or per-ap based to provide enough granularity to mitigate the potential impact from high traffic demand.



There are some limitations to this feature. The below features are not supported.

- DHCP/NAT
- Flex-VPN and L3 roaming
- Core side tunnels (L2oGRE and TTG)
- QinQ

Ruckus IoT Suite

This section provides release information about Ruckus IoT Suite 1.4 a versatile system for managing IoT devices.

The Ruckus IoT Suite is a collection of network hardware and software infrastructure components used to create an IoT access network that is comprised of four elements:

- **Ruckus IoT-ready Access Points (APs)**— in addition to the wall-mount H510, the ceiling-mount R510, the outdoor model T310, the ceiling-mount R610, R710, and R720, the outdoor models E510, and T610 as of this release the following additional AP models are now IoT-ready: Indoor Access Point R730 (802.11 ax) and Indoor Access Point C110.
- **Ruckus IoT Modules**— A new device that attaches to a Ruckus IoT-ready AP and supports standards such as Bluetooth Low Energy (BLE), Zigbee, LoRa and more. Our first IoT Module, the I100, supports BLE or Zigbee within the same enclosure.
- **Ruckus SmartZone Controller**— Existing WLAN controller, which provides basic networking information for both the WLAN and the IoT access network.
- **Ruckus IoT Controller**— A new virtual controller, deployed in tandem with a Ruckus SmartZone Controller, that performs connectivity, device, and security management functions behind the scenes for non-WiFi devices. Our IoT Controller also facilitates cross-solution endpoint communication and provides APIs for northbound integration with IoT cloud services.

Support License Compliance Check Button

In current SZ implementation, when a user tries to perform system upgrade, SZ checks the AP Support License to see if the support license threshold is met for continuing the upgrade process. If not met, a warning message pop ups to notify users to acquire enough AP support licenses. However, there is lack of way to know that beforehand. So, Ruckus has introduced this Compliance Check Button on SZ GUI for user to check such compliance before the actual upgrade is carried out.

Switch Topology

With topology view, SmartZone 5.2 brings in the ability to visualize the connections among Switches and APs at a switch group level. Information shown includes:

- Switch and AP status.
- Switch to Switch link details.
- Switch to AP link details.
- Switch AAA configuration at group level - Switch AAA configuration can now be defined at switch group level to support multi tenancy style deployments.
- New ICX model support - SmartZone 5.2 supports management of ICX7150-C08PT.

Tunneled QinQ Support for Wired Ports

Wired Q-in-Q feature is to support Q-in-Q tagging at the core or data plane for wired clients connected to AP LAN ports configured with RGRE tunnel and 802.1x mac based authentication. With this feature, the end user/service provider can reuse or transport the client VLANs over different service VLANs and terminate the VLAN traffic across different gateways.

Known limitations:

1. On Akronite based APs (R710), this cannot be supported with NSS offload enabled.
2. 11ax APs are not supported.

Upgrade Multiple AP Zones At Same Time

Currently, Ruckus administrator needs to go through the manual process to upgrade each zone one by one. It can be a tedious process when it is a large network with many zones.

In this release, we let our administrators to be able to select multiple zones from the web user interface and with one single upgrade click, the system goes through the firmware upgrade process for all these zones without further user intervention. There is check mechanism in place to ensure successful upgrade: When the process is successfully done, a successful result message is displayed on the web user interface and if errors happen in some zone(s), the user interface pop ups a failure message to let the user download a check list to exam the errors.

WPA3

Ruckus access points supports WPA3 (Wi-Fi Protected Access 3) encryption in this release. WPA3 was announced by WFA as a replacement to WPA2.

The new standard uses 128-bit encryption in WPA3-Personal mode (192-bit in WPA3-Enterprise). WPA3 standard also replaces the Pre-Shared Key exchange with Simultaneous Authentication of Equals (SAE) as defined in IEEE 802.11-2016 resulting in a more secure initial key exchange in personal mode. WFA also claims that WPA3 will mitigate security issues posed by weak passwords and simplify the process of setting up devices with no display interface. Opportunistic Wireless Encryption (OWE) is also introduced in WPA3 to provide a chance to enhance the Open WLAN security. In release 5.2, we support the following main WPA3 function areas:

- WPA3 - SAE
- WPA3 - OWE
- Suite - B

Additional Enhancements

The following additional enhancements have been made in this release:

1. Use UDI to add additional management interface: Use user defined interface to let the controller have second management interface, user can access web user interface of the controller or SSH CLI of the controller through sub management interface.
2. List UE MAC that causes AP health issues**.**
3. Ability to configure the CLI command **roam_macfilt_time**in the controller.
4. Add DHCP latency measurement KPI.
5. Ability to create data plane DHCP/NAT assignment wizard with data plane zone affinity.
6. DHCP Option 82 sub-option customization enhancements.
7. PoE granularity support on R610.

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 100 - Data Plane (SZ 100-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.
- Access Point (AP): Controllers support 1000 APs per zone.

Release Information

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

SZ300

- Controller Version:**5.2.0.0.699**
- Control Plane Software Version:**5.2.0.0.770**
- Data Plane Software Version:**5.2.0.0.699**
- AP Firmware Version:**5.2.0.0.1412**

SZ100

- Controller Version: **5.2.0.0.699**
- Control Plane Software Version:**5.2.0.0.770**
- Data Plane Software Version:**5.2.0.0.261**
- AP Firmware Version:**5.2.0.0.1412**

vSZ-H and vSZ-E

- Controller Version: **5.2.0.0.699**

- Control Plane Software Version:**5.2.0.0.770**
- AP Firmware Version:**5.2.0.0.1412**

vSZ-D

- Data plane software version:**5.2.0.0.699**

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

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

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

SZ Google Protobuf (GPB) Binding Class

Refer to the GPB MQTT Getting Started Guide and download the latest SmartZone (SZ) GPB .proto files from the Ruckus support site at: https://support.ruckuswireless.com/software/2315-smartzone-5-2-ga-gpb-proto-google-protobuf-image-for-gpb-mqtt

IoT Suite

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

vSCG (vSZ-H and vSZ-E), and SZ-100:

- WLAN Controller version: **5.2.0.0.699**
- Control plane software version in the WLAN Controller : **5.2.0.0.770**
- AP firmware version in the WLAN Controller:**5.2.0.0.1412**

Ruckus IoT Controller

- Ruckus IoT Controller version: 1.4.0.0.17
- VMWare ESXi version: 5.5 and later
- VMWare VM Player version: 12 and later
- Oracle VirtualBox version: 5.1.20 and later
- Google Chrome version: 61 and later
- Mozilla Firefox version: 56 and later

  NOTE
  Refer to Ruckus IoT 1.4 Release Notes for Release Build Compatibility and IoT Upgrade Support Matrix

Public API

Click on the following links to view:.

- SmartZone 5.2.0 Public API Reference Guide (Cloud), visit http://docs.ruckuswireless.com/smartzone/5.2.0/cloud-wifi-public-api-reference-guide-520.html
- SmartZone 5.2.0 Public API Reference Guide (ICX Management), visit http://docs.ruckuswireless.com/smartzone/5.2.0/switch-management-public-api-reference-guide-520.html
- SZ100 Public API Reference Guide, visit http://docs.ruckuswireless.com/smartzone/5.2.0/sz100-public-api-reference-guide-520.html
- SZ300 Public API Reference Guide, visit http://docs.ruckuswireless.com/smartzone/5.2.0/sz300-public-api-reference-guide-520.html
- vSZ-E Public API Reference Guide, visit http://docs.ruckuswireless.com/smartzone/5.2.0/vsze-public-api-reference-guide-520.html
- vSZ-H Public API Reference Guide, visit http://docs.ruckuswireless.com/smartzone/5.2.0/vszh-public-api-reference-guide-520.html

Upgrade Guide

- Do refer to the *Ruckus SmartZone Upgrade Guide, 5.2* for upgrade details. This section is removed from the release notes from this release onwards.

Supported Matrix and Unsupported Models

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

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

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

NOTE
Solo APs running releases 104.x and higher are capable of connecting to both ZD and SZ controllers. If an AP is running releases 104.x and higher and the LWAPP2SCG service is enabled on the SZ controller, a race condition will occur.

AP Firmware Releases

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

TABLE 2 AP Firmware

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

NOTE
For further details refer to the section *Multiple AP Firmware Support in the SZ100/vSZ-E/SZ300/vSZ-H* in SmartZone Upgrade Guide, 5.2

Supported AP Models

This release supports the following Ruckus AP models.

TABLE 3 Supported AP Models

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

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

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

Unsupported AP Models

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

TABLE 4 Unsupported AP Models

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

IMPORTANT
Ruckus Networks is announcing an End-of-Sale (EOS) of R700 from this release.

Switch Management Feature Support Matrix

Following are the supported ICX models:

TABLE 5 Supported ICX Models

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

Following is the matrix for ICX and SZ release compatibility:

TABLE 6 ICX and SZ Release Compatibility Matrix

	SZ 5.1	SZ 5.1.1	SZ 5.1.2	SZ 5.2
FastIron 08.0.80	Y	Y	N	N
FastIron 08.0.90a	N	Y	Y	Y
Fastiron 08.0.91	N	Y	Y	Y
Fastiron 08.0.92	N	N	Y	Y

Following is the matrix for switch management feature compatibility:

TABLE 7 Switch Management Feature Compatibility Matrix

	SZ Release	ICX FastIron Release
Switch Registration	5.0 and above	08.0.80 and above
Switch Inventory	5.0 and above	08.0.80 and above
Switch Health and Performance Monitoring	5.0 and above	08.0.80 and above
Switch Firmware Upgrade	5.0 and above	08.0.80 and above
Switch Configuration File Backup and Restore	5.0 and above	08.0.80 and above
Client Troubleshooting - search by Client MAC	5.1 and above	08.0.80 and above
Remote PING and TRACEROUTE	5.1 and above	08.0.80 and above
Switch Custom Events	5.1 and above	08.0.80 and above
Switch Configuration - Zero Touch Provisioning	5.1.1 and above	08.0.90a and above
Switch-specific settings - Hostname, Jumbo Mode, IGMP Snooping, and DHCP Server	5.1.1 and above	08.0.90a and above
Switch Port Configuration	5.1.1 and above	08.0.90a and above
Switch AAA Configuration	5.1.1 and above	08.0.90a and above
Change Default Switch Group Behavior	5.1.2 and above	08.0.92 and above
ICX Wired Client Visibility	5.1.2 and above	08.0.92 and above
Switch AAA Configuration	5.2 and above	08.0.92 and above

IoT Suite

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

Compatible Hardware:

- C110 Access Point (C110)
- H510 Access Point (H510)
- R510 Access Point (R510)
- R610 Access Point (R610)
- R710 Access Point (R710)

- R720 Access Point (R720)
- T310 Access Point (T310)
- E510 Access Point (E510)
- T610 Access Point (T610)
- R730 Access Point (R730)
- I100 IoT Module (I100)

Compatible Software:

- Virtual SmartZone High Scale (vSZ-H)
- Virtual SmartZone Essentials (vSZ-E)
- SmartZone 100 (sz-100)
- Ruckus IoT Controller (RIoT)

This below table documents the supported IoT end devices.

NOTE

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

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Vingcard Signature	Lock	Zigbee	Assa-Abloy	AA_LOCK	
Vingcard Essence	Lock	Zigbee	Assa-Abloy	AA_LOCK	
Yale YRD220/240 TSDB Display Lock	Lock	Zigbee	Assa-Abloy	Yale	YRD220/240 TSDB
Yale YRD210 Push Button Lock	Lock	Zigbee	Assa-Abloy	Yale	YRD210 Push
Smartcode 916	Lock	Zigbee	Kwikset	Kwikset	SMARTCODE_DEADBOLT_10T
Smartcode 910 (450201)	Lock	Zigbee	Kwikset	Kwikset	
Lightify (RGB) Model 73674	Bulb	Zigbee	Osram	OSRAM	LIGHTFY A19 RGBW
Lightify Model 73693	Bulb	Zigbee	Osram	OSRAM	LIGHTIFY A19 Tunable White45856
Lightify Model 73824	Bulb	Zigbee	Osram	OSRAM	
Element Color Plus	Bulb	Zigbee	Sengled	sengled	E11-N1EA
Bulb - LED	Bulb	Zigbee	Sengled	sengled	Z01-A19NAE26
E11-G13	Bulb	Zigbee	Sengled	sengled	E11-G13
Lux	Bulb	Zigbee	Philips	Philips	LWB004
SLV E27 Lamp Valeto (Zigbee 3.0)	Bulb	Zigbee 3.0	SLV		
GE Smart Dimmer	Switch	Zigbee	GE	Jasco Products	45857
GE Smart Switch	Switch	Zigbee	GE	Jasco Products	45856
Smart Plug	Plug	Zigbee	CentraLite	CentraLite	4257050-ZHAC
Zen Thermostat	Thermostat	Zigbee	Zen Within	Zen Within	Zen-01
ZBALRM	Alarm	Zigbee	Smartenit		Model #1021 A
Temp, Humidity Sensor	Sensor	Zigbee	Heiman	HEIMAN	HT-N
Gas detector	Sensor	Zigbee	Heiman	HEIMAN	GASSensor-N
Contact Sensor/Door Sensor	Sensor	Zigbee	CentraLite	CentraLite	3300-G
3-Series Motion Sensor	Sensor	Zigbee	CentraLite	CentraLite	3305-G
Temperature Sensor	Sensor	Zigbee	CentraLite	CentraLite	3310-G
Multipurpose Sensor	Sensor	Zigbee	Smart things	Samjin	
Button	Sensor	Zigbee	Smart things	Samjin	
Motion Sensor	Sensor	Zigbee	Smart things	Samjin	
Water Leak Sensor	Sensor	Zigbee	Smart things	Samjin	
Motion Sensor	Sensor	Zigbee	Aduro SMART ERIA	ADUROLIGHT	
Smart Plug	Plug	Zigbee	Smart Things	Samjin	
Bulb	Bulb	Zigbee	Aduro SMART ERIA		
Bulb	Bulb	Zigbee	Cree		BA19-08027OMF-12CE26-1C100
Smart Plug	Plug	Zigbee	INNR		
Smart Blinds	Blinds	Zigbee	Axis Gear		
Occupancy Sensor	Sensor	Zigbee	Telkonet		
Door Sensor	Sensor	Zigbee	Telkonet		
Thermostat	Thermostat	Zigbee	Telkonet		
Picocell	Gateway	LoRa	Semtech		
Mini Hub/ Basic station	Gateway	LoRa	TABS		
Door Sensor	Sensor	LoRa	TABS		
Occupancy Sensor	Sensor	LoRa	TABS		
Panic Button	Beacon	BLE	TraknProtect		
Tray Beacon	Beacon	BLE	TraknProtect		
Asset Beacon	Beacon	BLE	TraknProtect		
Card Beacon	Beacon	BLE	TraknProtect		
Card Tag	Beacon	BLE	Kontakt.io		CT18-3

Changed Behavior

The following are the changed behavior issues.

Component/s	AP
Issue	SCG-110139
Description	While creating a user role profile, both User Traffic Profile and Firewall Profile are mandatory to maintain compatibility with AP zones using 5.2 or earlier versions

Component/s	Control Plane
Issue	SCG-105136
Description	When Standby cluster monitors only one Active cluster, it allows to disable cluster redundancy when there is no AP or data plane connected to standby in backup mode

Component/s	Control Plane
Issue	SCG-111698
Description	When upgrading from controller release 3.6.x to 5.2 directly, the legacy ARC profile does not migrate to the new firewall profile
Workaround	Create a new ARC profile and add to firewall profile

Component/s	Control Plane
Issue	SCG-111544
Description	Due to Firewall enhancements in this release, zone level OS policy and L2 ACL are no longer available in 5.2 zone for configuration using Web UI or public API.

Component/s	Public API
Issue	SCG-108362
Description	From this release, one of the PoE mode is renamed from 802.3at+ to 802.3bt Class 5

Component/s	SCI
Issue	SCG-105147
Description	Due to Northbound MQTT enhancements, events 4001-4005 are no longer valid and they are replaced by events 4701-4703

Component/s	System
Issue	SCG-111535, SCG-111524
Description	Due to Firewall enhancements in this release, when AP zone firmware is upgraded to 5.2, only the OS policy and L2 ACL objects in use will be migrated to the new domain level device policy and L2 ACL

Component/s	Virtual SmartZone
Issue	SCG-110117
Description	In vSZ-H with 3 interfaces, the administrator should use the same adapter type in VM configuration for all network interfaces. Failure to do so may cause network connectivity issues

Known Issues

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

Component/s	AP
Issue	SCG-118945
Description	Single client TCP Downlink and Uplink throughput are reduced 8% and 18% in presence of 39 associated clients. For single client peak performance demos, please try avoid associating multiple clients. If its not possible, use below workaround to address issue by disabling ATF, UL scheduler and UL OFDMA.

Workaround	In RKS CLI mode:
	1. Set *atf wifi1* mode to disable
	2. Reboot the AP
	3. Send the below two commands to disable UL scheduler, *UL OFDMA*
	`iwpriv wlan32 he_ulofdma`
	`wifitool wlan32 setUnitTestCmd 0x47 2 92`

Component/s	AP
Issue	SCG-118998
Description	MU performance with two S10 clients is lower when ATF is enabled. In 40 MHz mode, MU-MUMO throughput gain is reduced from 25% to 4%. For performance demos, the workaround for this issue is to disable ATF feature.
Workaround	In RKS CLI mode: 1. Set *atf wifi1* mode to disable 2. Reboot the AP

Component/s	AP
Issue	SCG-101470
Description	WPA3 is a new feature introduced in this release. One of the options include 802.1X EAP WPA3 using AES-GCMP-256 (also called WPA3-Enterprise 192-bit mode). This option is not supported in 11ac Wave-1 APs. Configuration is moved to the AP, but the WLAN remains down. A warning message will be displayed when creating the WLAN. Refer to Supported Matrix and Unsupported Models on page 19 section.

Component/s	AP
Issue	SCG-108838
Description	Downlink multicast rate limit feature will not work with 11AC Wave-1 APs like R500, R600, T300, R310 models

Component/s	AP
Issue	SCG-108898, SCG-108896, SCG-112150, SCG-112425, SCG-112546

Component/s	AP
Description	Client fingerprinting feature fails to correctly detect the following devices: • Canon printer (reported as Roku Streaming Stick) • Google Home Mini (reported as Smartphone - Android) • Windows Phone (reported as Laptop-Windows) • Ring Door Bell Client Gaming (reported as Xbox 360) • Samsung gear smart watch (reported as Nest learning thermostat) • Fit Bit Gaming (reported as Xbox 360) • iPAD devices running iOS 13.0 or above versions are detected as smart phone instead of tablet • Chrome OS is not updating properly. Device Info is updated as **(Laptop, Chrome OS, Chrome OS)** instead of **(Laptop, Chrome OS, Google Chrome OS / Chrome OS 10718.88.2)** • iPAD devices running iOS 13.0 or above version are detected as Laptop instead of Tablet. This issue is specific when User browses using iPAD's native Safari browser

Component/s	AP
Issue	SCG-113084
Description	The client device information reported is not consistent for below iOS devices, when client initially connects Vs browsing HTTP traffic Vs when client disconnect and reconnects : • iPad with iOS 9.3.5 • iPad Pro • iPad Air 2 with iOS 13.1/13.1.3 • iPhone 11, XS, XR, iPhone 7, 6 with Safari version 12.1/13

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

Component/s	AP
Issue	SCG-108892
Description	Google Home and Google Home Mini device information is reported as smartphone

Component/s	AP
Issue	SCG-109486
Description	ARC policy does not deny Facebook messenger traffic

Component/s	AP
Issue	AP-11721
Description	L3 ACL rule works for the same VLANS but not on different VLANs when DHCP NAT is enabled on WLAN and Ethernet interface of the AP

Component/s	AP
Issue	SCG-110478

Component/s	AP
Description	AP Ethernet port configuration fails to update when DHCP/NAT is enabled with DWPD (Dynamic WAN Port Detection)

Component/s	AP
Issue	AP-11839
Description	L2 Access Control Policy Ethernet type rules will not apply to between clients connected to the same WLAN on the same AP and radio

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

Component/s	AP
Issue	SCG-102633
Description	A client may be disconnected from WLAN before *inactivity timeout* times out if the AP believes the station is not inactive or tries to contact it and fails to get any response

Component/s	AP
Issue	AP-11971
Description	When the client is connected to AP DHCP/NAT feature, which is not the Gateway AP, RUDB (Ruckus user database) lookup fails when the DNS packet is sent to the client's Gateway AP
Workaround	Add the DNS IP address while configuring the DHCP pool

Component/s	AP
Issue	SCG-102636
Description	The WPA rekey impacts the inactivity timeout if it is set to a long time

Component/s	AP
Issue	AP-11671
Description	L3 Access Control Policies does not block multicast/broadcast traffic

Component/s	AP
Issue	SCG-110982
Description	Rate limit ARC rules may fail to apply to some Webmail applications.

Component/s	AP
Issue	SCG-111052, SCG-105895
Description	Application control summary client table shows model name as N/A for historical clients

Component/s	AP
Issue	SCG-110105

Component/s	AP
Description	Application policy rate limit takes precedence over firewall profile and WLAN specific rate limit for the traffic matching the individual policy rules

Component/s	AP
Issue	SCG-110102
Description	SSID rate limit takes precedence over firewall profile and WLAN specific rate limit

Component/s	AP
Issue	SCG-110098
Description	Device policy rate limit takes precedence over firewall profile and WLAN specific rate limit

Component/s	AP
Issue	SCG-108534
Description	WISPr and Walled garden whitelists take precedence over L3 ACL

Component/s	AP
Issue	SCG-110200, SCG-110202
Description	Device information (hostname and OS type) is not displayed for IPv6 only clients

Component/s	AP
Issue	SCG-111194
Description	For T750 AP, if two uplink ports are connected for redundancy purposes, ensure STP is enabled in the switch to avoid a network loop
Workaround	Enable the STP protocol to detect loop and block the port on the switch

Component/s	AP
Issue	SCG-113164
Description	If channel 144 is disabled at AP level, and then it is disabled and enabled at Zone level, the channel is still blocked per Web UI but it is available for use by the AP

Component/s	AP
Issue	SCG-109677
Description	AP running solo image 110 will not connect by default to SZ controller using LWAPP (Lightweight Access Point Protocol) protocol. Instead, it will use same discovery methods as an AP running SZ firmware

Component/s	AP
Issue	SCG-110522
Description	An AP will reboot when it is moved to a monitoring group

Component/s	AP
Issue	SCG-112888, SCG-112922

Component/s	AP
Description	Airtime detail utilization will not show correct values in 11ax APs

Component/s	AP
Issue	AP-11917
Description	Change of authorization (CoA) fails to work for wired clients

Component/s	AP
Issue	SCG-113727
Description	SWIPE app discovery fails with R650 AP model

Component/s	AP
Issue	SCG-114275
Description	C-band channels (149-161) can still be configured in WebUI for Spain country code, although they will not be used in AP due to regulatory change
Workaround	It is recommended not to enable 5.8 GHz Channels option for Spain/ES country code

Component/s	AP
Issue	SCG-114331
Description	R650/T750 will fail to update the configuration if a DFS channel is manually selected for 5G band
Workaround	Select a non-DFS channel for static configuration, or select Auto option

Component/s	AP R750
Issue	SCG-107270
Description	2.4Ghz air time utilization can go over 75% due to new reporting mechanisms, but this has no performance impact

Component/s	AP R750
Issue	SCG-107013
Description	Speedflex application on Wi-Fi client device when connected to R750 radio inaccurately shows uplink speed is lower than downlink speed

Component/s	AP R750
Issue	SCG-106484
Description	Controller web user interface incorrectly displays radio type as *an/ac/ax* instead of *a/n/ac/ax* for Wi-Fi 6 connected clients

Component/s	AP R750
Issue	SCG-105751
Description	Controller web user interface incorrectly always displays MCS Rate (Tx) as *zero (0)*

Component/s	AP R750
Issue	SCG-93197

Component/s	AP R750
Description	Airtime details tab does not show up for R750 in the controller

Component	AP
Issue	SCG-105318
Description	When only Customer-Premises Equipment (CPE) connects with the AP and if a client behind it is not connected, then CoA/DM for the CPE is still served and fails to be ignored

Component	AP
Issue	SCG-103174
Description	Channel 144 feature does not work on other countries except USA

Component	AP
Issue	SCG-101173
Description	Roaming performance for Samsung S5 or IPhone in tunnel downlink mode shows a drop beyond acceptable values

Component	AP
Issue	SCG-97876
Description	When the Windows Deployment Services (WDS) clients connects behind a Customer-Premises Equipment (CPE) in a series, the accounting stop is sent and No Change of Authorization (CoA) or Disconnect Message (DM) requests can be initiated to that CPE. But, if all WDS clients and CPE are attached to the AP at the same time, accounting stop is not sent for the CPE

Component	AP
Issue	SCG-97465
Description	The GPS history in the web user interface does not always work when *lte-gps-probe*interval is 1

Component/s	AP
Issue	SCG-94547
Description	Latest iOS(Version 12) and Mac OS(10.14) Clients are unable to accept version negotiation fallback during the SSL/TLS session establishment during EAP PEAP/EAP TLS 1.0 profiles with Free Radius Server(which supports only 1.0).

Component/s	AP
Issue	SCG-94545
Description	When APs are moved in a dual zone, the APs use IPv6 address for SSH tunnel formation but for GRE tunnel formation IPv4 address is used. Previous APs used IPv4 address for SSH and GRE tunnel formation in dual zone

Component	AP
Issue	SCG-94143

Component	AP
Description	To support LACP (Link Aggregation Control Protocol) or Link Aggregation Group (LAG) feature on Ruckus APs, the administrator needs to ensure the correct PoE power modes to Bring-Up LAN1 and 2 ports. For example, PoE-at+ for R720, PoE-at for R710, and so on. Refer to the respective AP product guides for details. **NOTE** LACP/LAG uplink throughput is limited to 1Gbps.

Component	AP
Issue	SCG-92652
Description	By default the AP R720 sends a neighbor solicitation to the gateway after every 30 seconds and updates its cache. However, even after receiving a valid response from the controller the AP resends the neighbor solicitation to the gateway at times.

Component	AP
Issue	SCG-84194
Description	The controller web user interface does not have the option to upgrade LTE firmware
Workaround	Use the AP CLI to upgrade LTE firmware

Component	AP
Issue	SCG-84785
Description	802.1x supplicant functionality on Ethernet 0 or Ethernet 1 does not work

Component	AP
Issue	AP-5480
Description	Any change in ARC policy resets the pre-existing policy to null. R710/R610/R510 APs are not affected while other or the rest of the AP models are affected

Component	AP
Issue	AP-7387
Description	When WAN link of one of the GAP (Gateway AP) goes down the clients connected to those APs do not get any service

Component/s	AP
Issue	AP-8909
Description	The default IP address currently used for IPv6 is *fc00::1/7* similar to 192.168.0.1 as IPv4. Changing the default IP address to an unique local address will be fixed in future release

Component	AP
Issue	AP-9311
Description	RA Throttle on DVLAN/VLAN pool enabled WLAN considers RA from all the VLAN's irrespective of client association on those VLAN's. This can impact valid associated clients from receiving RA packets once RA throttle limit is reached

Component	AP
Workaround	• Preferred lifetime for the wireless network VLANs should be at least double the RA throttle duration configured and the periodic RA interval for these VLANs should be less than other VLANs in the network

Component/s	AP
Issue	AP-9319
Description	For the traffic flows where the uplink and downlink ports used are different for example, TFTP, the split tunnel feature does not work

Component/s	AP
Issue	AP-9549
Description	Split tunnel is not supported with portal redirection enabled WLANs, therefore the below combinations will not work. • Split tunnel with WISPr • Split tunnel with Web authentication

Component/s	AP
Issue	AP-9659
Description	Fragmented packets are dropped by AP in the downlink direction with DHCP NAT

Component	AP
Issue	AP-10145
Description	Bonjour fencing does not work if services like SSH, Apple TV and Airdrop are discovered through any other interface other than WLAN interface of the client. It is observed bluetooth is able to discover the services for Apple TV and MAC devices. To effectively make Bonjour Fencing work, had to disable Mac UE bluetooth interface down with below commands:
Workaround	For Bonjour fencing to work on the Airplay devices, below mentioned configurations on Apple TV and MAC OS needs to done. 1. Bluetooth option needs to be disabled on Apple TV device. 2. Disable Apple Wireless Direct Link feature on Mac book devices using: `sudo ifconfig awdl0 down` 3. In Apple TV navigate to Airplay configuration select the option **Anyone on the same network** 4. Disable bluetooth from system setting of Apple Wireless clients **NOTE** If there is no provision to disable bluetooth, Bonjour fencing will not work effectively.

Component/s	AP
Issue	SCG-50883
Description	The WLAN scheduler closes a WLAN one hour ahead of schedule because the AP does not take into consideration daylight saving time (DST).

Component/s	AP
Issue	SCG-51529
Description	Beginning with ZoneFlex standalone AP version 104.0, APs will delay joining a ZoneDirector in favor of joining a SmartZone controller for 30 seconds, if both controllers exist on the same L2 subnet. However, in some situations, the AP can still potentially join the ZD instead of the SZ when both controllers are set to auto approve
Workaround	Do not deploy both ZD and SZ controllers on the same L2 subnet, or there will be potential for APs to join the ZD instead of the SZ

Component/s	AP
Issue	SCG-59255
Description	When the C110 AP is using an Ethernet backhaul (instead the CM), the cable modem serial number cannot be displayed on the access point detail page on the controller's web interface

Component/s	AP
Issue	SCG-60852
Description	In a two-node cluster, Smart Monitor causes APs to lose connection with the controller. When an AP resumes its connection with the controller, the AP sends Accounting-On message to the controller, but the controller never forwards the same Accounting-On message to the AAA server

Component/s	AP
Issue	SCG-67158
Description	Rogue AP detection does not work if the rogue AP's channel is not on the list of Ruckus AP operating channels

Component/s	AP
Issue	SCG-69227
Description	The *Mesh Mode* and *Mesh Role* columns incorrectly display *Auto*, when they should actually display *Not Applicable* as the H320 AP does not support mesh

Component/s	AP
Issue	SCG-78247
Description	The AP E510 will be automatically rebooted when external antenna gain setting is modified

Component/s	AP
Issue	SCG-78457
Description	AP does not auto negotiate with switch ports when the switch is configured with half duplex

Component/s	AP
Issue	SCG-81588
Description	An AP reboot is required when enabling and disabling the non-Beamflex antenna (Part Number: 911-0505-DP01).

Component/s	AP
Issue	SCG-81705

Component/s	AP
Description	AP Tx power is not reverting to default values after applying non-Beamflex antenna (Part Number: 911-0505-DP01) gain and switching back to a Beamflex antenna (Part Number: 902-2101-0000)

Component/s	AP
Issue	SCG-82191
Description	Cellular backhaul connection in M510 has roaming feature enabled by default and this option cannot be changed

Component/s	AP
Issue	SCG-82513
Description	AP-to-AP communication in M510 does not work when the backhaul is LTE (Long Term Evolution). This may impact features like Fast Roaming, Bonjour Fencing and 11r. []

Component/s	AP
Issue	SCG-83730
Description	AP does not advertise 2.5 and 5 Gbps speed capabilities for POE (Ethernet1) interface in LLDP (Link Layer Discovery Protocol) frames. The speed reflected in the LLDP frames does not match actual negotiated link speed

Component/s	AP
Issue	SCG-83734
Description	User will not be able to set speed using RKSCLI for POE (Ethernet1) interface
Workaround	User would need to change the speed on switch side and the AP will automatically come up with that speed

Component/s	AP
Issue	SCG-84002
Description	Configuring SmartCast L2 and L3 IPv6 filters on WLAN interface drops all traffic from the UE

Component/s	AP
Issue	AP-12047
Description	When Restricted AP Access Profile is enabled, wireless clients can still have access to AP HTTP/ HTTPS services when client and AP are in different subnets

Component/s	AP
Issue	SCG-112702
Description	Controller Web UI will not have any client latency data for clients connected to 11ax APs

Component/s	AP
Issue	SCG-105847
Description	AP PoE interface fails to connect when the switch port is set to 100-full duplex speed
Workaround	It is recommended to set the configuration to auto negotiation

Component/s	AP
Issue	IOTC-3039
Description	MQTT Brokerip changes to unconfigured after multiple AP reboots
Workaround	1. Reconfigure the broker IP address from RKSCLI using command: `set iotg-mqtt-brokerip <ip-address>` or 2. Use Option 43 (this will automatically set DHCP lease renew)

Component/s	AP
Issue	IOTC-2815
Description	Controller fails to detect the PAN ID conflict resulting in failure of PAN ID change

Component/s	AP
Issue	IOTC-2787
Description	Blacklist overlap channel (BLE) will not happen when the current IoT channel overlaps with WLAN channel

Component/s	ARC
Issue	AP-4835
Description	ARC does not support clients that are assigned IPv6 addresses

Component/s	Control Plane
Issue	SCG-106454
Description	When Geo redundancy is disabled in Active cluster while Standby is not online, this feature gets disabled only in Active cluster
Workaround	Disable this feature only when all clusters are online and in service

Component/s	Control Plane
Issue	SCG-109530
Description	AP running solo image 100 will fail to connect to SZ 5.2 controller
Workaround	Upgrade the AP to solo image 104 or later

Component/s	Control Plane
Issue	SCG-109040
Description	TACACS and test AAA server connection is successful though it is mapped to an incorrect service

Component/s	Control Plane
Issue	SCG-93304
Description	ACL in UTP policy will not take effect in Express Wi-Fi WLAN whereas ARC policy and URL filtering in UTP policy will work without any issue

Component/s	Data Plane
Issue	SCG-93034
Description	AP does not try to join the data plane within the DP Group after the losing the tunnel, rather fails over to data plane on another data plane group

Component/s	Data Plane
Issue	SCG-103688
Description	Created tunnel WLAN could trigger the alarm of data plane configuration update failed

Component	SPoT
Issue	SCG-93224
Description	LBS server supports open SSL TLSv1.0 and not TLSv1.1 and TLSv1.2

Component/s	SNMP
Issue	SCG-110613
Description	Controller firmware version details are empty in trap *ruckusSCGUpgradeSuccessTrap*

Component/s	Switch Management
Issue	SCG-103158
Description	In the current design, the controller does not support operators other than *equal to* . If the user configures ACL rules on switch using operators like *greater than* , *less than* , it will be transferred to *equal to* in the controller

Component	Switch Management
Issue	SCG-98589
Description	The maximum configurable limit of OSPF areas is four on ICX7150
Workaround	OSPF area needs to deleted by the user if it creates L3 interfaces with different OSPF areas

Component	Switch Management
Issue	SCG-103799 **NOTE** For easy readability non-supported ICX attributes listed below is split in to three tables.
Description	SZ currently supports a subset of attributes for the features that are available for configuration (ACL for example). These non-supported attributes can be configured on ICX directly through CLI or SSH or Telnet or SNMP Example: The controller only supports ACL rule *equal to* option. When a client configures the ACL rule with *less than* option through ICX console directly and tries to modify the same rule from the controller web user interface later the non-support attribute *less than* will be modified to *equal to*.
Workaround	The recommendation is to only use other mechanisms (for example Console, SSH, and so on) if these non-supported attributes need to be configured to avoid potential configuration loss. However, if the user tries to modify the same feature from SmartZone, these non-supported attributes might be overwritten

Component	Switch Management
Non-supported ICX attributes	**Standard** • remark • enable-accounting • mirror • log **Extended** • remark • enable-accounting • mirror • log • gt • lt • neq • established • 802.1p-and-internal-marking • 802.1p-priority-marking • 802.1p-priority-marking • dscp-marking • dscp-matching • internal-priority-marking • precedence • tos • traffic-policy
ICX Switch or Router - VLAN (non-support ICX attributes)	**Spanning Tree (802.1d)** • forward-delay • hello-time • max-age **Spanning Tree (802.1w)** • force-version • forward-delay • hello-time • max-age

Component	Switch Management
Issue	SCG-103799
ICX Switch or Router - Static route (non-support ICX attributes)	**Static route** • name - optional static route name • tag- optional tag value of this route. Default value is zero (0)

Component	Switch Management
ICX Switch or Router - VE Port (non-support ICX attributes)	**VE Port** • access-group • arp-age • bootp-gateway • dhcp-client • directed-broadcast • dscp-remark • encapsulation • follow • forward-protocol • icmp • igmp • irdp • local-proxy-arp • mtu • multicast-boundary • ospf • pcp-remark • pim • pim-sparse • policy • proxy-arp • redirect • rip • tcp • tunnel • use-acl-on-arp • vrrp • vrrp-extended
ICX Switch or Router - VE interface (non-support ICX attributes)	**VE Interface** • acl-logging • bandwidth • clear • delay-notifications • disable • enable • ip-mac • ipv6 • rate-limit • rpf-mode • source-guard • vrf

Component/s	System
Issue	SCG-105356

Component/s	System
Description	The zone view of access points on the controller administrative web page are only applicable for the account privileges with the system administrators due to the current system limitation

Component/s	System
Issue	SCG-108213
Description	Authentication AD server fails to return non Ruckus WSG (Wireless Service Gateway) user information
Workaround	Only one Ruckus WSG user can be set on AAA server. Multiple roles should not be mapped

Component/s	System
Issue	SCG-90479
Description	The order of execution of the scheduled AP CLI script is not guaranteed and the execution might be terminated due to timeout constraints. Clients should be aware this constraint before planning the scheduled execution

Component/s	System
Issue	SCG-89454
Description	When the system boots it does not display the IPv6 address since DHCP IPv6 address in the management IP address is not auto updated. Workaround: Restart the system for it to display the DHCP IPv6 address in the management IP address.

Component/s	System
Issue	SCG-82509
Description	Geo-redundancy feature does not support ICX switches

Component	Syslog
Issue	SCG-88903
Description	AP M510 stops sending LTE related event after disabling LTE when using the below RKSCLI command: `# set lte-state`

Component/s	System
Issue	SCG-91887
Description	This release does not support IPv6 for Radius, TACACS+, AD and LDAP on Admin AAA page. (MVNO neither)

Component/s	UI/UX
Issue	SCG-105153
Description	Due to the specific keyboard definition with Safari browser in MAC OS, the key-combination of **Command + Mouse click** is applied to select multiple APs in zone view on the controller administrative web page

Component/s	UI/UX
Issue	SCG-110136
Description	It is recommended that you do not configure in *Restricted AP Access* profile blocking rules for the ports used for DHCP, DNS or Web services since this may impact AP operation

Component/s	UI/UX
Issue	SCG-109989
Description	When editing WLAN configuration for the first time after a page refresh in controller web user interface, some WLAN groups will be automatically removed when clicking on that option
Workaround	Cancel WLAN edit window and re-open it again

Component/s	UI/UX
Issue	SCG-107474, SCG-107811, SCG-107532
Description	Unable to display destination information in outbound firewall list if that entry is configured in Domain name or IPv6 format

Component/s	UI/UX
Issue	SCG-109906
Description	Troubleshooting page will not display authentication packets if WLAN is using AD/LDAP proxy authentication profile

Component/s	UI/UX
Issue	SCG-109739
Description	ZD auto migrate fails when the controller outbound firewall is enabled

Component/s	UI/UX
Issue	SCG-111636
Description	If a Zone was upgraded to 5.2 and later downgraded to its original version, then duplicate device policy entries will be created when it is upgraded again to 5.2

Component/s	UI/UX
Issue	SCG-105519
Description	On the AP page, some columns that have the option to sort fail to sort

Component/s	UI/UX
Issue	SCG-88854
Description	When URL Filtering policy is created and applied to UTP, which is mapped to a WLAN, the blacklisted sites in the URL policy are not blocked. The URL filtering settings has to be enabled at WLAN level along with UTP. UTP policy will take precedence over WLAN level

Component/s	Virtual SmartZone
Issue	SCG-67593
Description	Application of DiffServ values is not preserved on downlink IPv6 Tunnel header when the inner packet is also IPv6 is not supported

Component/s	Virtual SmartZone Data Plane (vSZ-D)
Issue	SCG-89015
Description	vSZ-D does not assign the IP address when DHCP packets are relayed by another vSZ-D with Option82 and sub options

Component/s	Virtual SmartZone Data Plane (vSZ-D)
Issue	SCG-84658
Description	IPv6 multicast traffic fails for RGRE wireless station

Component/s	Virtual SmartZone Data Plane (vSZ-D)
Issue	SCG-102179
Description	Multicast forwarding feature is only supported on SZ100 for IPv4, and not on any other platforms. However, SZ-100 data plane does not support this feature for IPv6 in SmartZone 5.1.1 due to which MDNS request and response messages will not be exchanged across RGRE tunnel. Therefore, Bonjour, Bonjour Gateway and Bonjour Fencing is not supported for IPv6 Ruckus has extensively tested on the following services, limited to these client devices: **File Sharing, Screen Sharing and Remote Login** - MacBook Pro 10.12.4 MacBook Air 10.14. **Bonjour, Bonjour Gateway and Bonjour Fencing** will not work for SZ-100, SZ100-D with IPv6 clients in tunnel mode **NOTE** If there is change in behavior of the iOS clients / Applications (data traffic is initiated with global IPv6 instead of link-local IPv6), then this limitation becomes irrelevant

Component/s	Visual Connection Diagnostics
Issue	SCG-63193
Description	The connection failure counter does not increment when EAP fails

Component/s	Wired Clients
Issue	SCG-67708
Description	In a wired guest VLAN implementation, the wired client is authorized with a different VLAN even if the client fails wired 802.1X authentication. It can use the Ethernet profile's guest VLAN number to check whether the client is a guest or a normal user

Resolved Issues

The following are the resolved issues related to this release.

Component/s	AP
Issue	ER-8098
Description	Resolved an issue where certain AP models were not accessible after upgrade to 5.2 **ATTENTION** Visit https://support.ruckuswireless.com/articles/000010114 for details.

Component/s	AP
Issue	ER-7642, ER-8026
Description	Resolved an issue where Controller and AP time synchronization with NTP server was not happening regularly

Component/s	AP
Issue	ER-6748
Description	Resolved an issue where some ARPs packets to be transmitted as broadcast were being dropped at the AP

Component/s	AP
Issue	ER-7595
Description	Resolved an issue where clients failed to connect to 2.4GHz AP radio due to some internal resource was not released properly

Component/s	AP
Issue	ER-7643
Description	Resolved an issue where AP CLI scheduled script would still be executed after disabling it

Component/s	AP
Issue	ER-7592
Description	Resolved an issue where model-specific AP settings where not correctly applied to APs in 3.6.x zones

Component/s	AP
Issue	ER-7674
Description	Resolved an AP reboot issue on 11ax AP models

Component/s	AP
Issue	ER-7631
Description	Resolved an issue where real-time SNR value reported in Wireless Clients Health tab was incorrect

Component/s	AP
Issue	ER-7484
Description	Resolved an issue where an offline AP would be reported online during some time in Web UI after moving it to a different zone or group

Component/s	AP
Issue	ER-7541, SCG-108803
Description	Resolved an issue where *Switch Over Clusters* function was failing for APs inside zones that have been upgraded from 3.6.x to a newer version

Component/s	AP
Issue	ER-7529, SCG-108821
Description	Resolved an issue where VLAN pool profile changes were not correctly applied in APs

Component/s	AP
Issue	ER-7783
Description	Resolved an issue where a client was not accepted during some time for an AP that moved it away using 802.11v (BSS Transition Management)

Component/s	AP
Issue	ER-7801
Description	Resolved an issue where RSSI-based Association Rejection Threshold option for Optimized Connectivity Experience (OCE) WLAN configuration setting was not working properly

Component/s	AP
Issue	ER-7849
Description	Resolved an issue with simultaneous processing of DNS packets in different cores resulted in AP Reboot

Component/s	AP
Issue	ER-6780, ER-6748
Description	Resolved an issue where GRP key was not set at FT roam

Component/s	AP
Issue	ER-7327
Description	Several enhancements included into background scanning channel selection algorithm in R730 APs

Component/s	AP R750
Issue	SCG-109216
Description	Resolved an issue where R750 Historical Client Connection Diagnostic (HCCD) failed to create *CCD_REASON_AUTH_FILTERED_BY_ACL* log when L2 ACL was configured

Component/s	AP
Issue	ER-7419
Description	Resolved an issue where T310C/D rebooted with reason of reset button

Component/s	AP
Issue	ER-7630
Description	: Resolved an issue where AP neighbor entries were not up to date when background scanning timer was higher than 256 second

Component/s	AP
Issue	ER-7665
Description	Resolved an issue where clients intermittently failed to pass any traffic when connected to 802.11ax (R750/R730)AP's

Component/s	AP
Issue	SCG-111081
Description	Resolved an issue where R730 AP was sending username attribute in Radius accounting messages as client MAC address instead of the username for WebAuth WLAN

Component/s	AP
Issue	SCG-109262
Description	Resolved an issue where AP initiated accounting on/off message when editing WLAN settings but without saving any modifications if Radius vendor specific attribute profile is associated to the WLAN

Component/s	AP
Issue	IOTC-2838
Description	Resolved an issue where PAN mismatch is detected upon AP reboot leading to stop communication with connected devices

Component/s	AP
Issue	IOTC-2817
Description	Resolved an issue where Zigbee channel did not change after detection of conflict with new WLAN channel

Component/s	AP
Issue	SCG-101365, SCG-99923
Description	Resolved an issue where AP's WLAN couldn't be mapped to VLAN ID of 1 if any AP Ethernet port is configured with untagged VLAN ID different than 1

Component/s	AP
Issue	SCG-97553
Description	Resolved an issue where no latency data or corresponding graph data was populated for 11ax AP radios

Component/s	AP
Issue	SCG-58332
Description	Resolved an issue where LAN port status and mapping for C110 were incorrect on the controller's web interface

Component/s	AP
Issue	SCG-48792
Description	Resolved an issue where wireless clients based on Intel Dual Band Wireless AC-7256 and Intel Centrino N 6300 AGN, and Samsung S5 mobile devices failed to perform Opportunistic Key Caching (OKC) roaming

Component/s	AP
Issue	SCG-104362
Description	Resolved an issue where with 2.4g connected Chrome book running software version 71 and lower caused low throughput issue on the radio

Component/s	ARC
Issue	SCG-65933
Description	Resolved an issue where ARC rate limiting for user-defined applications did not work on fragmented packets

Component/s	CLI
Issue	ER-7753, ER-7905
Description	Resolved an issue where SZ CLI *show running-config all'* command was not working properly

Component/s	Control Plane
Issue	ER-7591
Description	Resolved an issue where newly generated DPSKs could not be used to connect to the network because they were not being correctly shared between cluster nodes

Component/s	Control Plane
Issue	ER-7695
Description	Resolved an issue where Radius process in controller could restart due to a timeout processing CoA/DM messages

Component/s	Control Plane
Issue	ER-7581
Description	Resolved an issue where Zone configuration changes could not be done due to incorrect error handling in the controller

Component/s	Control Plane
Issue	ER-7693, SCG-111020
Description	Resolved an issue where cluster restore pointed to incorrect data plane version in controller SZ300

Component/s	Control Plane
Issue	ER-7861, SCG-112325
Description	Resolved an issue where controller upgrade may fail while migrating internal certificates

Component/s	Control Plane
Issue	SCG-107712
Description	Resolved an issue where R750 may had issues when channelization was to set to Auto or 80Mhz for country codes Bangladesh, Bahrain, Costa Rica, El Salvador

Component/s	Control Plane
Issue	SCG-106322
Description	Resolved an issue where RAC was failing to match UTP identifier when the user role was modified under authentication profile

Component/s	Data Plane
Issue	ER-7471, SCG-105468
Description	Resolved an issue where data plane interfaces were not accepting non 24 prefix subnets

Component/s	Data Plane
Issue	ER-7412, SCG-109643
Description	Resolved an issue where data plane status was flapping between Configuring and Managed due to controller restart

Component/s	Data Plane
Issue	ER-7626, ER-7558
Description	Resolved an issue where data plane may be unstable or disconnect due to excessive amount of internal logs generated for receiving small MTU packets

Component/s	Data Plane
Issue	ER-7973
Description	Resolved an issue where the status LED was blinking red during normal operation in SZ100-D

Component/s	SCI
Issue	AP-11708, ER-7497
Description	Resolved an issue where SCI failed to distinguish correctly between authorized or unauthorized client types

Component/s	SCI
Issue	ER-7523
Description	Resolved an issue where MAC authentication WLAN was reported as OPEN WLAN on SCI

Component/s	Switch Management
Issue	ER-7560
Description	Resolved an issue where the controller incorrectly reported high switch CPU usage

Component/s	Switch Management
Issue	ER-7534
Description	Resolved an issue where Switch traffic ranking was not accurate

Component/s	Switch Management
Issue	ER-7387
Description	Resolved an issue where no SNMP trap was generated when a switch was going offline

Component/s	Switch Management
Issue	ER-7708
Description	Resolved an issue where the response time was too long when fetching the list of domains and sub-domains using public API

Component/s	Switch Management
Issue	SCG-109929
Description	Resolved an issue where the controller were failing to differentiate ICX7150-C12 and ICX7150-C10ZP switch models

Component/s	System
Issue	ER-7645
Description	Resolved an issue where switch traffic graph for last 1 hour could have some gaps

Component/s	System
Issue	ER-7516
Description	Resolved an issue where configuration synching in Geo-Redundancy deployments was failing if clusters had different admin credentials

Component/s	System
Issue	ER-7488
Description	Resolved an issue where disabling client isolation through CLI caused an error

Component/s	System
Issue	ER-7367
Description	Resolved an issue where the Radius attributes are now the same with test Radius function when logging to the controller through Radius server

Component/s	System
Issue	ER-7652
Description	Resolved an issue where random clients failed to connect to DPSK WLAN

Component/s	System
Issue	ER-7550
Description	Resolved an issue where the controller historical client TX and RX data was inaccurate

Component/s	System
Issue	ER-7703
Description	Resolved an issue where the controller Zone Retrieve List Public API failure was caused by data corruption

Component/s	System
Issue	ER-7385
Description	Resolved an issue where the controller can now create SFTP connection successfully to the remote server

Component/s	System
Issue	ER-7590
Description	Resolved an issue where controller configuration restore may fail if the backup contains a Web certificate

Component/s	System
Issue	ER-7808
Description	Resolved an issue where changing indoor radio channels resulted in reset of outdoor radio channels to default setting

Component/s	System
Issue	ER-7627
Description	Resolved an issue where Northbound SZ process was going out of memory

Component/s	System
Issue	SCG-113681, ER-7890, ER-7897
Description	Resolved an issue where with five or more than five UDI's configured and the controller rebooted Radius proxy process would not come up

Component/s	System
Issue	ER-7744, SCG-111337
Description	Resolved an issue where SZ CLI was not handling properly special characters "[ ]"

Component/s	System
Issue	ER-7862
Description	Resolved an issue where static routes could not be created in controller

Component/s	System
Issue	ER-7770, ER-7959
Description	Resolved an issue where Web and SubscriberPortal SZ applications were restarting due to continuous login attempts to public API

Component/s	UI/UX
Issue	ER-7696
Description	Resolved the issue by modifying the controller web user interface by allowing the user to disable 5.8Ghz channels on the AP Zone for UK country code UK

Component/s	UI/UX
Issue	ER-7981, ER-7987
Description	Resolved an issue where controller Web UI login using Radius realms was failing

Component/s	UI/UX
Issue	SCG-100495
Description	Resolved an issue where option button was failing to display when change the Geo-Redundancy mode from active-standby to active-active

Component/s	UI/UX
Issue	SCG-98310
Description	Resolved an issue where Real time latency chart failed to update any value

Component/s	UI/UX
Issue	SCG-68696
Description	Resolved an issue where SZ300's web interface showed inaccurate data plane network usage

Component/s	UI/UX
Issue	SCG-58881
Description	Resolved an issue where the Restart Cable Modem button on the Restart tab were not functional for C110 on the controller's web interface

Component/s	Virtual SmartZone Data Plane
Issue	ER-7502
Description	Resolved the issue where AP failed to establish the tunnel to the vSZ-D when going through CM (Cable Modem) or CMTS (Cable Modem Termination System)

Component/s	Virtual SmartZone
Issue	ER-6917
Description	Resolved an issue where username field may be incorrect in AP client events

Component/s	Virtual SmartZone
Issue	ER-7726, SCG-110277
Description	Resolved the issue where the controller configuration restore failure was caused by Cassandra timeout

Component/s	Virtual SmartZone
Issue	ER-7574
Description	Resolved an issue where top level domain length was limited to six characters in SMTP configuration

Component/s	Virtual SmartZone
Issue	ER-7355
Description	Resolved an issue where clients could discover neighbor MAC addresses when client isolation was enabled in WLAN

Component/s	Virtual SmartZone
Issue	ER-7530
Description	Resolved an issue where zone list in Web UI failed to be retrieved in case of very large configurations

Component/s	Virtual SmartZone
Issue	ER-7647
Description	Resolved an issue of data corruption when deleting controller northbound data streaming enabled domain or zone

Component/s	Virtual SmartZone
Issue	ER-7603, SCG-109777
Description	Resolved an issue where default static route was not showing on the controller web user interface

Component/s	Virtual SmartZone
Issue	ER-7812, ER-7722, SCG-112293, SCG-112195
Description	Resolved a two node cluster AP configuration out-of sync issue

Component/s	Virtual SmartZone
Issue	ER-7948, SCG-113442
Description	Resolved an issue of missing timestamp column in exported statistics files of flow message table

Component/s	Virtual SmartZone Data Plane
Issue	SCG-71118
Description	Resolved an issue where L2oGRE in vSZ-D core side was still configurable when vSZ-D NAT service is enabled

Interoperability Information

Cluster Network Requirements

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

TABLE 8 Minimum Cluster Network Requirement

Model	SZ300	vSZ-H	SZ100	vSZ-E
Latency	85ms	68ms	77ms	77ms
Jitter	10ms	10ms	10ms	10ms

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.

- Users will not be redirected to WISPr Internal Logon URL with Chrome browser 65. This is the behavior of Chrome browser version starting from 63. **[SCG-85552]**

  Workaround: Add the following URLs in Walled Garden list for WISPr redirection to work.

  - connectivitycheck.gstatic.com
  - clients3.google.com
  - connectivitycheck.android.com
  - play.googleapis.com
  - gstatic.com

  For details refer to https://www.chromium.org/chromium-os/chromiumos-design-docs/network-portal-detection

- Samsung S10 client is not skipping 802.1x authentication process while roaming with OKC enabled WLAN connect. **[SCG-110129]**

  Workaround: For successful roaming, connect Samsung S10 client to 11r enabled WLAN.

- HP printer client fails to connect to WPA3 mixed WLAN profile. **[SCG-110318]**

  Workaround: It is recommended to connect the HP printer client to WEP, WPA2 WLAN profile.

- Devices iPad OS version 9.3.5 and iPhone 4s and OS version 6.1.3 do not connect to WLAN with encryption method WPA2/WPA3 mixed profile. **[SCG-112981]**

  Workaround: These devices will connect to WLAN only with encryption method WPA2 profile.

- Surface Pro Window client fail to connect to WPA3 mixed mode. **[SCG-109406]**
- Samsung S10 only connects to WPA2-PSK/WPA3-SAE mixed WLAN with WPA3 SAE passphrase (but not with WPA2-PSK). **[SCG-106735]**

  Workaround: Samsung S10 can only connect to WPA2-PSK/WPA3-SAE mixed WLAN by WPA3 SAE passphrase. By the packet capture, Samsung S10 uses the passphrase to perform the WPA3-SAE dragonfly handshake. It does not try to use WPA2-PSK. This could be the current behavior of S10's.

- One Plus 5 client does not connect to WPA3 mixed mode and WPA3 SAE mode WLAN profile. **[SCG-110128]**
- Hostname for the below devices are not displayed due to missing Option 12 information in DHCP frames from the client. **[SCG-108843]**
  - Lumia 950
  - Pixel 1,2 and 3
  - Nexus 5, 5x and 6
  - PlayStation-I

  - PlayStation-II
  - Samsung Chromebook
  - HP Chromebook
  - Asus Chromebook
  - Dell Chromebook
- Using EAP-SIM profile Sony Xperia Z5, Sony Xperia Z3, LG G3 Stylus do not connect to AP R730 successfully. This is due to client limitation. **[SCG-94006]**
- If clients encounter any interoperability issue with the AP operating in 11ax (default mode) the AP can be re-configured through RKS CLI to operate in 11ac mode including 5g and 2.4g commands. This mode can stay persistent across reboots. **[SCG-93051]**

  To configure 5G radio to 11ac mode, use the following command on AP:

  ```
  set mode wifi1 11ac
  ```

  To configure 2.4G radio to 11ng mode, use the following command on AP:

  ```
  set mode wifi0 11ng
  ```
- Nexus 5x clients may not be able to connect using SIM authentication profile if the EAP SIM attributes are *AT_VERSION_LIST* and *AT_FULLAUTH_ID_REQ*. **[SCG-105741]**
- 802.11r Fast BSS Transition association fails with Windows 10 and Intel adapter 7265 (driver:19.51.18.1) and Windows 10 and Intel 11ac 8260. **[SCG-104650]**

COMMSCOPE®
RUCKUS®

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