RELEASE NOTES

RUCKUS SmartZone 6.0.0 Release Notes

Supporting AP Patch 6.0.0.0.1640

Part Number: 800-72614-001 Rev C
Publication Date: November 2021

Copyright, Trademark and Proprietary Rights Information

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

Export Restrictions

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

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

Disclaimer

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

Limitation of Liability

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

Trademarks

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

Contents

Document History

Revision Number	Summary of changes	Publication date
C	Changed the Known Issue number from SGC-128308 to SGC-128038	15, November 2021
B	1. Updated the AP firmware version to 6.0.0.0.1640. 2. Moved the below Known Issues to Resolved Issues section: a. SCG-128828 b. SCG-128881 c. SCG-128898 d. SCG-129034 e. ER-9291, ER-9925 3. Added Security consideration section. 4. Added a section on AP Patch to the Controller.	20, May 2021
A	Initial release notes.	06, April 2021

New in This Release

This section provides a high-level overview of several key features that are introduced in the SmartZone (SZ) software release 6.0. The release 6.0 is applicable to the RUCKUS SmartZone 300, SmartZone 100, SmartZone 144, vSZ-H, vSZ-E, vSZ-D and controller platforms.

AP H550

H550 is an 802.11ax Dual-Band Concurrent 2x2:2 802.11ax (5GHz) with 2x2:2 802.11ax (2.4GHz) for wall plate applications with an integrated five 1Gbps Ethernet ports, in a form factor which allows mounting to electrical outlet boxes. H550 is the 802.11ax successor product in the H5x0 series of AP(s) in the Hospitality portfolio.

Power Modes

Power Mode		**802.3af**	**802.3at**			**802.3bt, uPoE, PoH**
Wi-Fi (2.4 GHz)	Configuration	2x2	2x2	2x2	2x2	2x2
	Tx Power (per chain)	16dBm	16dBm	16dBm	16dBm	16dBm
Wi-Fi (5 GHz)	Configuration	2x2	2x2	2x2	2x2	2x2
	Tx Power (per chain)	19dBm	19dBm	19dBm	19dBm	19dBm
IoT	BLE	Enabled	Enabled	Enabled	Enabled	Enabled
Radios	Zigbee	Enabled	Enabled	Enabled	Enabled	Enabled
Ethernet LAN Ports (4x)		Enabled	Enabled	Enabled	Enabled	Enabled
PSE	PoE_Out	Disabled	Disabled	Enabled	Enabled	Enabled
	Power@PD	N/A	N/A	8.4W	12.4W	12.95W
	Maximum Cable Length	N/A	N/A	20m	20m	100m
USB		Disabled	Enabled	Enabled	Disabled	Enabled
Power Consumption		12.54W	15.9W	24.91W	25.48W	32.21W

PoE Injector Model : 902-0180-US00 (740-64284-001 w/o power cord), 60W is rated only for 1Gbps speed. If POE operating mode = Auto, POE injector will power AP in AT mode.

AP Ethernet Port Speed

In this release RUCKUS has added AP Ethernet Port Speed in the controller GUI.

There are several Ethernet ports in some AP models and one of them is the POE port. The actual speed of the Ethernet ports are reported to controller and displayed as *Physical Link* in the LAN ports of the General preview panel (in the controller GUI navigate to **Access Point** > **Click on some AP** > **General** the preview panel > **LAN Ports**). This feature is to make the POE port's Physical Link become a selectable display column in the Access Points grid table.

AP DHCP/NAT Enhancements

The enhancements in this release are to address the functionality of the multi port APs (more than 2 ports) like (H510, H320) and address various different issues in the current design.

Current Design:

1. DHCP/NAT provides 3 topologies of *Enable on Each AP" (EOEA)*, *Enable on Multiple APs* (Flat network or FNT) and *Enable on Hierarchical APs* (Hierarchical Network or HNT). The EOEA and HNT need user to configure the Gateway AP(s) to set one of its LAN1 or LAN2 as WAN. For easy configuration, the wizard provides the Dynamic WAN Port Detection (DWPD) and WAN port selection for the AP LAN1 and LAN2 overridden, all other attributes will set as model default.
2. The LAN1 and LAN2 overridden are set to eth0 and eth1 in the DHCP/NAT configuration. (But H510 and H320 APs do not have the same lan/eth mapping.)
3. If selecting DWPD, the AP can report the WAN/LAN detecting status in the AP preview page.

Problems:

1. M510 may not need the DHCP LAN1/LAN2 overridden.
2. The H510/H320 has different port mapping of LAN1/LAN2 to eth0/eth1.
3. Enabled on DWPD or WAN port selection, for the Gateway AP model override in Zone, AP model specific, the Gateway AP will not be effective but the user is not aware of it.
4. Enabled on DWPD or WAN port selection, for the Gateway AP, modifying the AP model specific LAN1/LAN2 could cause DHCP service to fail.

Enhancements:

1. For problems 1 and 2 the release provides a *Disable* option for not processing the DHCP LAN1/LAN2 override.
2. For problems 3 and 4 the release provides a *dynamic message* showing in the Zone and AP for user awareness.
3. In addition, the preview page displays the WAN/LAN for the relavant LAN port.

AP Hostname Advertisement

This feature is to include AP hostname in beacon and probe response frames. The feature is *disabled by default* for security reason and can be enabled by configuration. When enabled, the AP will take the configured hostname and insert it as a separate vendor specific *Information Element* in beacon and probe response frames.

BSS Coloring

BSS coloring improves spectral efficiency by allowing the AP to assign a color to its SSID and transmit over SSIDs with a different color.

In the current implementation, the APs (802.11ax) will pick a random color on bootup and use that color for all its SSIDs. Not all clients at this time support the BSS Color Switch announcement, so in order to ensure interoperability, the AP will not change colors after bootup. There are 63 colors to choose from, represented by the integers 1 to 63. The user is able to specify a fixed color (1 to 63), disable BSS coloring (0), or auto color selection (64).
BSS coloring is not supported by 802.11ac clients.

Controller Web User Interface

The following are the changes to the UI for this beta release.

1. **New Menu**: A new mega-menu for controller allows users to quickly access various features without taking up valuable screen space. The new menu also improves performance and response time.
2. **Menu Bookmarks**: SmartZone R6.0 introduces capability to bookmark favorite menu items so they can be accessed easily.
3. **Menu Search**: With a rich set of features provided by SmartZone, finding the right configuration knob in the menu can sometimes be challenging. The new search feature allows a user to search for a configuration item, reducing the time and number of clicks needed to get to a given page in the UI.

   IMPORTANT
   The following changes will take place with 6.0 beta refresh.

   1. **Menu re-organization**: R6.0 introduces a new menu with several key enhancements including a new layout and organization. The new organization of menu items makes it easier to navigate the system and allows users to find appropriate items more intuitively.
   2. **Classic/Legacy menu option**: For users who wish to use the pre-R6.0 menu layout as they transition to the new menu, an option to switch to classic menu or legacy menu as termed in the UI will be available. The classic menu option is available to help transition to the new menu system and will be deprecated in the future release.

Dynamic DPI Application Signature Package Update

RUCKUS DPI engine partner periodically provides updates, which is packaged into Application Signature Package (Sigpack) updates. Customers today have to manually upgrade to the AP when a new Sigpack becomes available. From this release on, the SmartZone controller automatically checks for new Sigpack update, downloads the same and updates the APs without manual intervention.

Default Behavior for Upgrade

Below changes are observed when upgrading the controller from previous releases (5.2.x) to 6.0 release:

1. After system upgrade, the controller checks for latest available sigpack version in RUCKUS support site as periodic check toggle button is enabled by default in case upgrade and same is updated in *Latest available from support site* section.
2. On logging in to the controller for the first time login after the upgrade, the administrator is notified through the advice view on the new SigPack being available for download.
3. Users are notified through advice view by the controller on periodic checks on version updates of SigPack being available for download from support site.
4. Periodic check is set to first day of each month.

5. User can set the date for through the controller for periodic checks. Navigate to **Security>** > **Application Signature Package** to set the date.

Default Behavior for Fresh Installation

Below changes are observed with a fresh install a R6.0 controller:

1. After system installation, the controller checks for latest available sigpack version in RUCKUS support site as periodic check toggle button is enabled by default in case upgrade and same is updated in *Latest available from support site* section.
2. On logging in to the controller for the first time, the administrator is notified through the advice view on the new SigPack being available for download.
3. Users are notified through advice view by the controller on periodic checks on version updates of SigPack being available for download from support site.
4. Periodic check is set to first day of each month.
5. User can set the date for through the controller for periodic checks. Navigate to **Security>** > **Application Signature Package** to set the date.

Extract Virtual ID from Social Media and Emails

Some Managed Service Provider (MSP) customers who deploy APs at remote sites need to audit the client/end users required by the government regulations. This release utilizes the integrated DPI (ARC) system to extract the virtual ID of the users who log into certain social media applications and public emails with the successful Wi-Fi connection and send them to the server located in the MSP NOC, thus equiping the MSP to do cloud based auditing.

Express Wi-Fi (XWF)

Facebook has been running the Express Wi-Fi (XWF) program aiming at connecting people via partnership with Service Providers in emerging markets. To date, RUCKUS is XWF Certified for Phase 1 and 2. In this release, RUCKUS implemented the Phase 3 requirements. More specifically, it addresses these two features:

1. **RADIUS over HTTP/2**: This feature removes the need for Facebook (FB) to deploy a RADIUS server in the Service Provider (SP) network by having the by having the AP directly forward and receive RADIUS messages from the FB service logic over HTTP/2.
2. **802.1x WLANs**: To this point XWF was limited to portal based open non secure WLANs (Wispr Hotspot WLAN). From this release onwards, RUCKUS supports XWF over 802.1x WLANs

LACP on 802.11ax APs

Link aggregation is a method of aggregating multiple network interfaces into a single logical interface. By combining multiple interfaces, the network equipment can get more bandwidth/throughput between the connected devices and redundancy. In case of redundancy or HA, the load or traffic will be sent via remaining UP links if one of the link fails. Below are some of the RUCKUS LACP implementation enhancements for this release for all supported APs.

- Increases throughput, create flow between bond slave interface and WLAN interface.
- Disable per port Ethernet settings once LACP enabled on the AP.
- Introduce new option in GUI to configure bond port profile.
- Modify RKSCLI to configure bond setting from CLI.
- Enable LACP on 802.11ax APs.

Default Behavior for Upgrade

1. LACP/LAG is not disabled by default.
2. Enable the LACP on the controller web user interface for APs R720, R710 and R610 in Zone/AP Group/APs.
3. Check the bond status for enabled status.
4. Enable the LACP from using RKSCLI for APs T710 and T710S.
5. Check the bond status for enabled status.
6. Upgrade the controller from R5.2/R5.2.1 to R6.0.
7. On successful upgrade in the controller web user interface navigate to **Zone > AP model list > Select the AP** to view the LACP/LAG status.
   a. For APs R720, R710 and R610 APs, LACP/LAG status is seen as **Enabled** with **Default Bond** profile selected.
   b. For APs T710 and T710S LACP/LAG status in R6.0 is seen as **Keep AP settings**.

Locate UE on Controller Indoor Map

The purpose of this feature is to visually identify the estimated approximate location area of a connected client on a map within the controller (SmartZone) GUI. The feature helps use cases such as identifying location of lost devices and locating users, etc.

Named VLAN Assignment

With named VLAN assignment, user can have a name to a VLAN that maps to different site for site awareness. VLAN name profile is per WLAN level configuration form SZ, which allows user to configure with multiple key-value pair of *vlan-name:vlan-id* format.

In addition, a new VSA named *Ruckus-Vlan-Name* will be applied on AAA server for VLAN assignment whenever RADIUS client is authenticated, AP would assign corresponding VLAN according to the VLAN name profile from SZ.

Quick Disable Button for Any WLAN

This feature is to add capability on the Menu structure to disable a WLAN from the GUI. From the list of WLANs, we introduced a quick way to disable any WLAN. RUCKUS added the ability to see, which WLANs are Disabled/Enabled on the WLAN status window.

RADSEC Support

RADIUS over TLS is supported in this release. On receiving the RADIUS packets for authentication and accounting, the controller first establishes an encrypted TLS channel with external AAA server and then forwards any packet over the TLS channel. Likewise for CoA/DM, external AAA server establishes a TLS channel with the controller and then sends the packets over the encrypted channel.

For authentication and accounting port 2083 will be used for TLS connection. This port is configurable. For CoA/DM messages port 2084 will be used.

> **ATTENTION**
> Shared secret used for RADSEC internally is RADSEC. RADSEC does not support:
>
> - Accounting ON/OFF.
> - Authentication/Accounting/CoA/DM in IPv6 mode.
> - No secondary AAA server support.
> - OCSP stapling not supported but does support OCSP URL to verify certificates.

Role-based Policy Enhancements

The objective of the release is to support the role-based policy as follows:

- Role-based allow or deny per WLAN.
- Role-based time schedule.
- Role-based OS policy WLAN.
- Shortest match group attribute matching.

Separate Configurations for Each MQTT Listener

In prior releases, we did not differentiate configurations for different MQTT listeners. So, a single configuration with same set of subscribed topics is sent to all Northbound MQTT listeners. That is a limitation to our MSP (Managed Service Provider) customers who want to provide the capability for their customers to be able to subscribe to different statistics topics of their choice.

The release addresses this concern by offering separate configurations for each MQTT listener, so that each can receive its own set of statistics data. In doing so, we have also enhanced the GUI layout to facilitate the domain/zone selection.

Session Timer Enhancement

In this release, RUCKUS introduced the Session timer configurations.

- As part of WLAN configuration for 802.11ax and MAC-authorization, RUCKUS has added timeout configuration between 120 and 864,000 seconds if AAA does not send back the session timeout CoA (Change of Authorization)

  NOTE
  APs configured with longer session time may significantly impact its capacity.

Split Tunnel Enhancement

By default, once the RUCKUS GRE tunnel is enabled on a WLAN, all the frames go to or come from the data plane through the tunnel. However, the network can benefit if some traffic remains local and is not tunneled all the way back to the data plane, for example, print documents to a home printer. In this case, there is no benefit to tunneling it to the corporate network and then back to the remote location, needlessly congesting the tunnel. Multiple subnets can be added to the split tunnel profiles to allow for greater segmentation of what traverses the GRE tunnel and what stays on the local network

Social Login Support

Currently RUCKUS supports OAuth authentication together with CloudPath. We have seen many asks from our customers to support this function on controller alone. Therefore in this release, we have implemented the feature to provide Wi-Fi clients a way to use their social media login credentials to authenticate Guest WLAN access on controller platforms.

OAuth 2.0 WLAN allows end-user to access the Internet if its authenticated by the OAuth 2.0 provider (LinkedIn/Google/Microsoft). After the end-user is authenticated by OAuth 2.0 providers, it redirects the user to the original URL. If it fails to get the original URL, it redirects the user to the OAuth 2.0 provider's official URL.

The below popular social media applications are supported:

- Facebook
- Google
- LinkedIn

- Microsoft

Support HS2.0 R3

Passpoint Release 3 adds some more features to the existing Release 2 program to make it easier for Hotspot Operators to deploy Passpoint.

RADIUS Proxy Authentication and Accounting

SZ as controller currently allows to configure only unique IP address in proxy authentication and accounting service. For example - if IP address 1 is configured in authentication service 1, the same IP address cannot be configured in authentication service 2. Similar is the case for accounting service. We have seen requirements to support same IP address/Port/Secret across multiple authentication and accounting services. So, in this release, we made the change to support this configuration accordingly. But, since proxy statistics are inserted/updated based on the AAA IP address and is the key of the table, after this implementation, statistics will be updated against one IP address even though multiple services configured with same IP address.

Support SpeedFlex for Behind NAT APs

In prior releases, when AP was behind NAT, speed test did not work because AP was not reachable from WAN side. The supported topology for this release: AP is connected to its gateway and the other participant of speedtest is reachable via the WAN side of gateway. Similarly for public AP IP address and controller (SmartZone) behind NAT.

Users will not able to run ZAP test behind NAT AP server and the controller when the controller is behind the NAT server. **[SCG-128781]**.

Workaround: For AP behind NAT feature to work, only the AP should be behind NAT server and not the controller.

Switch Management

SmartZone 6.0 introduces the following switch management features.

- **Generic CLI Configuration**: SmartZone 6.0 introduces capability to provision switches using predefined CLI configuration making it extremely easy for users to deploy any feature that ICX supports.
  - **Group level CLI configuration**: Users can predefine configuration for switch groups with the option to define different configurations based on the switch model. Switches will automatically inherit the configuration upon joining the group.
  - **CLI templates**: CLI templates enable users to make incremental configuration changes on the fly to the selected switches
- **Geo-Redundancy**: Geo-Redundancy (Active-Standby mode) is now supported for switches.

  Prior to this release, Switches supported local HA via SZ cluster. From this release, Switch Management supports Geo-Redundancy for active/standby HA. This feature is only available on SZ300 and vSZ-H controller platforms. After failover is triggered and switches failed over to the standby cluster, manual rehome is needed for the switches to join back to the active SZ. Separate HA license is required for this feature.
- **Port Level Configuration Override**: The port level configuration overrides will be preserved. Any modifications at the switch group level will not affect the port level customizations.
- **Ability to add VLANs to LAGs**.

UE Role Visibility

On controller GUI in the release, RUCKUS has added a field of *user role name*, which the UE is authorized to the details area of wireless client page. If the UE associates with the AP with an authorizing method having no user role information, the field will show it as *N/A*.

White Label per Partner Domain

This feature enables MSPs and partners to customize their controller setup by using their own Company logos and texts. So every time they login into the controller, they will be able to see their company related customization. In addition, an administrative user of the partner domain will also be able to customize the controller for their sub-domain users.

This feature is supported on controller platforms vSZ-H and SZ300 only.

Additional Enhancements

The following additional enhancements have been made in the 6.0.0 release:

- Ability to configure IPv6 FTP server.
- Support IoT1.8 Gateway on SmartZone.
- Encrypt MAC on a per-WISPr basis.
- Modernize the existing Guest Captive portal on the controller.
- Unicast support for IPv6 client traffic on data plane northbound S-GRE tunnel.
- Cluster backup download via controller web user interface.
- Ability to download core dump file.

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. Release 6.0 SZ144 supports 5.2.x (5.2.0/5.2.1) AP zone firmware.

- 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 Short Term (ST) 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.

SZ300

- Controller Version: **6.0.0.0.1331**
- Control Plane Software Version: **6.0.0.0.1213**
- Data Plane Software Version: **6.0.0.0.1331**
- AP Firmware Version: **6.0.0.0.1640**

SZ100/SZ124/SZ104

- Controller Version: **6.0.0.0.1331**
- Control Plane Software Version: **6.0.0.0.1213**
- Data Plane Software Version: **6.0.0.0.1044**
- AP Firmware Version:**6.0.0.0.1640**

SZ144

- Controller Version: **6.0.0.0.1331**
- Control Plane Software Version: **6.0.0.0.1213**
- Data Plane Software Version: **6.0.0.0.1044**
- AP Firmware Version:**6.0.0.0.1640**

vSZ-H and vSZ-E

- Controller Version: **6.0.0.0.1331**
- Control Plane Software Version: **6.0.0.0.1213**
- AP Firmware Version:**6.0.0.0.1640**

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

- Data plane software version: **6.0.0.0.1331**

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.

RUCKUS Analytics(MLISA)

This release supports RUCKUS Analytics (MLISA) release 1.3.3.

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 **6.0.0.0.1331** MockSCI-TLS (SZ to SCI MQTT subscriber software) for CentOS / Ubuntu

   https://support.ruckuswireless.com/software/2891

   File: scg-mock-sci-6.1.0-20210322.064140-37.tar.gz

   Checksum: 29868a556b620a30e5e168031ed0da44

2. SmartZone **6.0.0.0.1331** (GA) GPB.proto (Google ProtoBuf) image for GPB/MQTT [DNP] –

   https://support.ruckuswireless.com/software/2890

   File: ruckus_sz_6.0.0_protos.tar.gz

   Checksum: cac9c2746b5263c3058325466a3e9650

IoT Suite

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

- vSCG (vSZ-H and vSZ-E), and SZ-124: **6.0.0.0.1331**
- Control plane software version in the WLAN Controller : **6.0.0.0.1213**
- AP firmware version in the WLAN Controller:**6.0.0.0.1594**

RUCKUS IoT Controller

- RUCKUS IoT Controller version: 1.8
- VMWare ESXi version: 6.5 and later
- KVM Linux Virtualizer version: 1:2.5+dfsg-5ubuntu 10.42 and later
- Google Chrome version: 78 and later
- Mozilla Firefox version: 71 and later

Public API

Click on the following links to view:

- SmartZone 6.0 Public API Reference Guide (ICX Management), visit SmartZone 6.0.0 Public API Reference Guide (ICX Management)
- SmartZone 6.0 Public API Reference Guide (SZ100), visit SmartZone 6.0.0 Public API Reference Guide (SZ100)

  NOTE
  SZ100 Public API link is for SZ144 as well.

- SmartZone 6.0 Public API Reference Guide (SZ300), visit SmartZone 6.0.0 Public API Reference Guide (SZ300)
- SmartZone 6.0 Public API Reference Guide (vSZ-E), visit SmartZone 6.0.0 Public API Reference Guide (vSZ-E)
- SmartZone 6.0 Public API Reference Guide (vSZ-H), visit SmartZone 6.0.0 Public API Reference Guide (vSZ-H)

Dynamic Signature Package Update

In R6.0 release has a new feature enhancement *Dynamic Signature Package Update* where 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 SZ6.0: https://support.ruckuswireless.com/admin/softwares/2746-smartzone-6-0-0-0-1021-ga-sigpack-1-510-1-regular-application-signature-package-dnp
   - Non-Regular Sigpack for SZ6.0 and older releases: https://support.ruckuswireless.com/admin/softwares/2747-smartzone-6-0-0-0-1021-ga-sigpack-1-510-1-application-signature-package-dnp
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 R6.0 release), you cannot download the current Sigpack version 1-510-1 regular Sigpack but can download the current non-regular Sigpack. If 802.11ac Wave 1 APs are on on R6.0 firmware, clients can download both 1-510-1 regular and non regular signature packs. **[SCG-123375]**

> **NOTE**
> As R5.1.x to R6.0 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.

AP Firmware Releases

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

Upgrade path	AP firmware releases in controller
6.0.x	5.2.x > 6.0.x

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

Supported AP Models

This release supports the following RUCKUS AP models.

TABLE 1 Supported AP Models

11ax		11ac-Wave2		11ac-Wave1
Indoor	**Outdoor**	**Indoor**	**Outdoor**	**Indoor**
R730	T750	R720	T710	R310
R750	T750SE	R710	T710S	
R650		R610	T610	
R550		R510	T310C	
R850		H510	T310S	
H550		C110	T310N	
		H320	T310D	
		M510	T811CM	
		R320	T610S	
			E510	
			T305e	
			T305i	

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

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

Unsupported AP Models

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

TABLE 2 Unsupported AP Models

Unsupported AP Models				
SC8800-S	ZF7762-S-AC	ZF2741	ZF7762-AC	ZF7351
ZF7321	ZF7343	ZF7962	ZF7762-S	ZF2942
ZF7441	ZF7363-U	SC8800-S-AC	ZF7363	ZF2741-EXT
ZF7762	ZF7025	ZF7321-U	ZF7341	ZF7352
ZF7762-T	ZF7351-U	ZF7761-CM	ZF7343-U	ZF7781CM
R300	ZF7782	ZF7982	ZF7782-E	ZF7055
ZF7372	ZF7782-N	ZF7372-E	ZF7782-S	C500
H500	R700	T300	T301N	T301S
T300E	R500	R500E	R600	FZM300
FZP300	T504			

Switch Management Feature Support Matrix

Following are the supported ICX models:

TABLE 3 Supported ICX Models

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

Following is the matrix for ICX and controller release compatibility:

TABLE 4 ICX and SZ Release Compatibility Matrix

	SZ 5.1	SZ 5.1.1	SZ 5.1.2	SZ 5.2	SZ 5.2.1	SZ 6.0
FastIron 08.0.80	Y	Y	N	N	N	N
FastIron 08.0.90a	N	Y	Y	Y	Y	Y
FastIron 08.0.91	N	Y	Y	Y	N	N
FastIron 08.0.92	N	N	Y	Y	Y	Y
FastIron 08.0.95	N	N	N	N	Y	Y
FastIron 08.0.95a	N	N	N	N	Y	Y
FastIron 08.0.95b	N	N	N	N	Y	Y

NOTE

FastIron 08.0.95a is required for managing ICX7550 switches.

Following is the matrix for switch management feature compatibility:

TABLE 5 Switch Management Feature Compatibility Matrix

Feature	SZ Release	ICX FastIron Release
Switch Registration	5.0 and later	08.0.80 and later
Switch Inventory	5.0 and later	08.0.80 and later
Switch Health and Performance Monitoring	5.0 and later	08.0.80 and later
Switch Firmware Upgrade	5.0 and later	08.0.80 and later
Switch Configuration File Backup and Restore	5.0 and later	08.0.80 and later
Client Troubleshooting: Search by Client MAC Address	5.1 and later	08.0.80 and later
Remote Ping and Traceroute	5.1 and later	08.0.80 and later
Switch Custom Events	5.1 and later	08.0.80 and later
Switch Configuration: Zero-touch Provisioning	5.1.1 and later	08.0.90a and later
Switch-specific Settings: Hostname, Jumbo Mode, IGMP Snooping, and DHCP Server	5.1.1 and later	08.0.90a and later
Switch Port Configuration	5.1.1 and later	08.0.90a and later
Switch AAA Configuration	5.1.1 and later	08.0.90a and later
Switch Client Visibility	5.1.2 and later	08.0.90a and later
Manage switches from default group in SZ-100/vSZ-E	5.1.2 and later	08.0.90a and later
Switch Topology	5.2 and later	08.0.92 and later
Designate a VLAN as Management VLAN	5.2.1 and later	08.0.92 and later
Change default VLAN	5.2.1 and later	08.0.92 and later
Configuring the PoE budget per port on ICX through the Controller GUI with 1W granularity	5.2.1 and later	08.0.92 and later
Configuring Protected Ports	5.2.1 and later	08.0.92 and later
Configuring QoS	5.2.1 and later	08.0.92 and later
Configuring Syslog	5.2.1 and later	08.0.92 and later
Download syslogs for a selected switch	5.2.1 and later	08.0.92 and later
Remote CLI	5.2.1 and later	08.0.92 and later
Generic CLI Config	6.0 and later	08.0.95b and later
Geo-Redundancy (Active-Passive mode)	6.0 and later	08.0.95b and later
Port level override	6.0 and later	08.0.95b and later

IoT Suite

This release supports IoT Controller release 1.8 and is compatible with the following controller and access point hardware and software.

Compatible Hardware

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

- R710 Access Point (R710)
- R720 Access Point (R720)
- R730 Access Point (R730)
- R750 Access Point (R750)
- T310 Access Point (T310)
- T610 Access Point (T610)
- T750 Access Point (T750)
- T750SE Access Point (T750SE)
- I100 IoT Module (I100)
- H550 Access Point (H550)

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.

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Vingcard Signature	Lock	ZigBee	Assa-Abloy	AA_LOCK	
Vingcard Essence	Lock	ZigBee	Assa-Abloy	AA_LOCK	
RT+	Lock	ZigBee	Dormakaba	Dormakaba	79PS01011ER-626
Yale YRD220/240 TSDB Display Lock	Lock	ZigBee	Assa-Abloy	Yale	YRD220/240 TSDB
Yale YRD210 Push Button Lock	Lock	ZigBee	Assa-Abloy	Yale	YRD210 Push
Smartcode 916	Lock	ZigBee	Kwikset	Kwikset	SMARTCODE_DEADBOLT_10T
Smartcode 910 (450201)	Lock	ZigBee	Kwikset	Kwikset	
Lightify (RGB) Model 73674	Bulb	ZigBee	Osram	Osram	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	SmartThings	Samjin	
Button	Sensor	ZigBee	SmartThings	Samjin	
Motion Sensor	Sensor	ZigBee	SmartThings	Samjin	
Water Leak Sensor	Sensor	ZigBee	SmartThings	Samjin	
Motion Sensor	Sensor	ZigBee	AduroSmart ERIA	Adurolight	
Smart Plug	Plug	ZigBee	SmartThings	Samjin	
Bulb	Bulb	ZigBee	AduroSmart ERIA		
Bulb	Bulb	ZigBee	Cree		BA19-08027OMF-12CE26-1C100
Smart Plug	Plug	ZigBee	INNR		

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

TABLE 6 Supported Devices tested with SmartThings

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

Known Issues

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

Component/s	AP
Issue	SCG-128780
Description	Before running ZAP speed test from AP to the controller and AP to client or vice versa, make sure that the below ports are open. ● 18301 ● 18303 ● 18305 ● 18307

Component/s	AP
Issue	AP-14102
Description	R850/R750 APs WAN Ethernet port fails when Ethernet speed of the Switch, connected to the AP is configured as 100 full. This limitation is observed with ICX7150-C12 10.1.11T225 (mnz10111) and not observed with ICX7150-48Z (SPS08092b.bin).

Component/s	AP
Issue	AP-15115
Description	Event 205 *Client connection timed out* is seen on the controller from the original AP, when client roams from Mesh AP to root AP or vice versa. The client roam is seamless most of time and due to current logic in inactive timer these events are generated on the controller.

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-128166
Description	When sending TCP Uplink traffic like Voice, Video, Best Effort & BK from wireless to wired client, all packets by default goes to Best Effort Queue instead of VO, VI queue. This limitation is applicable for Tunnel enabled SSID (RUCKUS GRE or SoftGRE) and will be enhanced in future releases .

Component/s	AP
Issue	SCG-127791

Component/s	AP
Description	Inconsistent offload traffic observed between two wireless client connecting to two different tunneled WLANs belonging to the same VLAN. This limitation is in case of non-default VLAN only, where first time a flow is created while pumping traffic between two clients is seen offloaded and subsequent flows go through the host path

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	It is recommended to give a five minutes gap between each iteration of performance test, for *rflow* entries to clear.

Component/s	AP
Issue	SCG-127736
Description	WISPr WLAN always sends the RADIUS access-request from the controller even though the non-proxy AAA server is selected in the **Hotspot Portal Authentication Service**.
Workaround	If the client is using the non-proxy AAA server, make sure it is reached from the controller by using the option, **Test AAA** in the controller web user interface to test the user authentication and make sure it is successful.

Component/s	AP
Issue	SCG-127405
Description	Tunnel traffic goes through host path instead of offload path on Mesh AP. This particular case is not applicable to root AP or AP LBO traffic on Mesh AP.

Component/s	AP
Issue	SCG-127253
Description	In DWPD enabled DHCP-NAT HN network, if APs/Clients connected to LAN switch and coming up before DWPD process completes on Gateway APs then Clients/Non-gateway APs may get addressees from WAN network VLANS (default VLAN or non-default VLAN, which is part of WAN network).

Component/s	AP
Issue	SCG-127188
Description	Delay in displaying AP MAC update correctly in the Client monitor page when the client roams. Controllers vSZ-H screen takes approximately six minutes and vSZ-E takes approximately three minutes to reflect the new AP MAC.

Component/s	AP
Issue	SCG-127087
Description	Enabling POE out in AP CLI or on the web user interface does not enable POE out for APH550. This feature is available under certain power modes but is not enabled by default.
Workaround	Requires enabling at POE on the AP or from the controller web user interface.

Component/s	AP
Issue	SCG-125005
Description	T750SE AP model specific configuration **External Antenna Default Setting** is disabled by default.
Workaround	Manually enable the option *Ext-Antenna* again if needed when editing the AP level model specific configuration.

Component/s	AP
Issue	SCG-127995
Description	Second wired client connected to the AP do not receive DHCP address and cannot browse, when Ethernet profile is configured for 802.1x port based MAC bypass and when non-default VLAN is used. This limitation is applicable only for RUCKUS Wi-Fi 6 AP's. This issue is not observed with VLAN 1 used in Ethernet profile.
Workaround	With second wired client plugged, reboot the AP.

Component/s	AP
Issue	SCG-123943
Description	When AP radios are disabled, the **get client-info** from AP CLI shows stale client entries. This does not impact client connectivity.

Component/s	AP
Issue	SCG-123375
Description	If 802.11ac Wave 1 APs are on legacy firmware (AP firmware prior to R6.0 release), you cannot download the current Sigpack version 1-510-1 regular Sigpack but can download the current non-regular Sigpack. If 802.11ac Wave 1 APs are on on R6.0 firmware, clients can download both 1-510-1 regular and non regular signature packs.

Component/s	AP
Issue	SCG-119716
Description	When a CoA-Request is received at the controller with valid XWF VSAs, which is, *RUCKUS-CP-Token* and *RUCKUS-TC-Attrs-Ids-With-Quota*, CoA acknowledgement is sent from the controller regardless of the traffic class configuration in the controller web UI. The AP ignores the traffic class if it is not configured at the controller web UI.

Component/s	AP
Issue	AP-14280
Description	Unable to send the ICMP payload size more than 1620 bytes without fragmenting on AP R730. However, this works fine on AP R710.

Component/s	AP
Issue	SCG-125006
Description	XWF UE is able to browse the blocked IP address when XWF with L3 ACL and DHCP NAT is enabled. L3 ACL with DHCP NAT is not supported.

Component/s	AP
Issue	SGC-128038
Description	The fix in this release 6.0.0 could create/update/delete huge volumes of LBS profiles without errors when the outbound firewall is disabled. But, with outbound firewall enable, create/update/delete huge amount of LBS profiles still has an issue. Consider this as a rare case (Enable Outbound Firewall/Large amount of LBS profiles). Ruckus will provide a fix in future release.

Component/s	AP
Issue	SCG-128145
Description	There is limitation with DPI where *Telegram Application* detection fails during an audio or a video call. This will be addressed in the new Sigpack in later releases.

Component/s	AP
Issue	SCG-128979
Description	Client fails to connect sometimes to 802.11x or 802.11x and MACAuth WLAN when configured with role based policy with the option *Time Schedule Policy - Allow Specific*. This inconsistency is observed often with Windows OS. This issue is not observed with role based policy with the option, *Time Schedule Policy - Allow All*.

Component/s	AP
Issue	SCG-127469
Description	When sending Video, Best Effort and Background traffic from Wired to Wireless Client, if the Client disconnect for some reason and re-associates to AP, it is observed that all traffic goes with Video priority even for Best Effort traffic. This limitation is only for if WLAN VLAN and Management VLAN of AP uses the same VLAN. If AP management VLAN and WLAN VLAN are different then Best Effort traffic goes properly in BE Queue.

Component/s	AP
Issue	SCG-126338
Description	With certain clients EAPOL failures are observed due to *received EAPOL-Key 2/4 Pairwise with unexpected replay counter* and in some conditions AP fails to de-authenticate the client for invalid MIC in Key(2/4). **NOTE** This behavior is same in controller version 5.2.x releases and is not a new behavior in release 6.0.

Component/s	AP
Issue	SCG-123495
Description	AP runs out of memory and page allocation failure is seen, when UDP traffic moves from the client unidirectional. This limitation is not applicable to bidirectional traffic.

Component/s	AP
Issue	SCG-127585

Component/s	AP
Description	R730 AP does not support AP Monitoring mode. The controller web user interface shows an exception while moving R730 to Monitoring Group. Forcing the AP to enable monitoring mode causes a Kernel panic. This limitation is only for R730 AP model and other Wi-Fi 6 APs support Monitoring mode.

Component/s	AP
Issue	SCG-128672
Description	The inactivity value which is configured through the controller web user interface is not applied in the AP, while the AP disconnects the idle STA’s after the inactivity timeout. Currently AP's using the internal Wi-Fi firmware logic to identify the Idle/Inactive STA's irrespective of the configured value. This limitation will be addressed in future releases.

Component/s	Control Plane
Issue	SCG-128059
Description	After modifying the AP mesh setting, user must wait for all the APs to update to view the mesh topology on the controller web user interface.

Component/s	Data Plane
Issue	SCG-126864
Description	When tunnel WLAN is turned ON after the AP establishes RGRE tunnel to data plane, the user equipment connecting tunnel WLAN encounters a TCP traffic failure on the data plane inter-tunnel functions (Flexi-VPN / L3 Roaming).
Workaround	Rebuild or re-establish AP GRE tunnel for Flexi-VPN / L3 Roaming.

Component/s	Data Plane
Issue	SCG-116650
Description	Data plane is unable to reassemble fragmented packets.
Workaround	Make sure L2oGRE gateway forwarded traffic is unfragmented.

Component/s	Switch Management
Issue	SCG-122429
Description	Errors in Group Level CLI configuration are not reported under the configuration history **NOTE** CLI templates are not affected. Users are recommended to ensure accuracy of CLI commands when using them for Switch group level CLI configuration.

Component/s	System
Issue	SCG-126856
Description	Application Signature Package (Sigpack) upgrade will be blocked if the existing rule not be supported on the install Sigpack engine.
Workaround	Remove the conflicting rule and reinstall Sigpack.

Component/s	System
Issue	SCG-118801
Description	Total count is incorrect after importing Guest Pass CSV file including massive Guest Passes.

Component/s	System
Issue	SCG-122346
Description	RADIUS process restarts if CA certificates are modified or deleted.

Component/s	UI/UX
Issue	SCG-128233
Description	When the controller service ticket has expired by a day, could cause the Switch Management UI bootstrap failure.

Component/s	UI/UX
Issue	SCG-126970
Description	On upgrading the controller, user is unable to downgrade the AP since the web UI fails to display older AP firmware versions.
Workaround	Downgrade button will not appear when Zone is applied to a data plane group. Assign the Zone to the default data plane group for downgrading the AP Zone firmware.

Component/s	UI/UX
Issue	SCG-127857
Description	The controller updates the Control Plane IP address as 0.0.0.0 before changing to the new IP address. Customers will now see two IP change events. One is current IP addressed to *0.0.0.0* and the other is *0.0.0.0* to new IP address. It is an expected behavior.

Component/s	UI/UX
Issue	SCG-121459
Description	The status of the switch client only supports local search. It highlights the keywords in the controller web user interface to help users find the record.

Component/s	UI/UX
Issue	SCG-123947
Description	**Time Schedule** and **Quick Disable WLAN** are separate functions. WLANs, which are disabled by **Time Schedule** do not list in the WLAN grid column.

Component/s	UI/UX
Issue	SCG-123871
Description	Historical device fingerprinting chart displays incorrect number of clients for last one hour and 24 hour time frame in device policy summary page since clients can be seen with different device names.

Component/s	UI/UX
Issue	SCG-123609

Component/s	UI/UX
Description	Controller web user interface only show the status from switches managed by the controller directly.

Component/s	UI/UX
Issue	SCG-121780
Description	Cannot find certain guest pass record by search key or name.
Workaround	User can use the **Filter** option to find particular a Guest Pass key .

Component/s	UI/UX
Issue	SCG-122966
Description	Device detection like device name, OS details fails if the client has pure IPv6 address.

Component/s	UI/UX
Issue	SCG-128998
Description	Controller web user interface background is locked and inaccessible while running CLI session.
Workaround	User can open a new browser for accessing other UI menu.

Component/s	Virtual SmartZone (vSZ)
Issue	ER-9540
Description	RUCKUS does not support the vSZ web UI migration tool for Amazon Web Services (AWS) or Google Cloud Platform (GCP) or Microsoft Azure Public Cloud platforms.

Changed Behavior

The following are the changed behavior issues in this release.

Component/s	AP
Issue	SCG-124718

Component/s	AP
Description	Below client IOS connects to only WPA2 profile but fails to connect to WPA2/ WPA3 profile. ● iPhone7 ● iPhoneX ● iPhone XR ● iPhone XS MAX ● iPhone 11 ● iPhone 11 Pro Max ● iPad Air3 Pro (10.5-inc) ● iPad pro ● iOS 13.0.0 ● iOS 13 ● iOS 13.1 ● iOS 13.1.3 ● iOS 13.2.3 ● iOS 13.4.1 ● iOS 13.6 ● iOS 14

Component/s	AP
Issue	SCG-124607
Description	Starting from release 6.0.0 all Wave1 APs except for AP R310 are **NOT** supported. If the user upgrades from 5.x to 6.0, the AP zone firmware will be grayed. Remove the Wave1 AP's from the Zone in order to upgrade AP firmware.

Component/s	AP
Issue	SCG-128939
Description	With LACP enabled on AP there is limitation of rate limiting functionality, where uplink rate limit functionality does not works and downlink rate limit works. This will be enhanced in future releases. **NOTE** This limitation of rate limit is only when LACP enabled and without LACP both uplink and downlink rate limit works.
Workaround	If LACP is enabled, do **NOT** configure uplink rate limit and configure only downlink rate limit for R6.0.0.

Component/s	Control Plane
Issue	SCG-127162
Description	Before deploying vSZ controller on the hypervisor, make sure the system time of the hypervisor is correct. It is recommended to turn ON the network time protocol of the hypervisor (NTP client) if it is supported.

Component/s	Control Plane
Issue	SCG-128016

Component/s	Control Plane
Description	For vSZ-H controllers if the LBS profiles reaches a maximum of 1000, a warning that the number of LBS servers allowed has exceeded the upper limit of 1000 is seen when using the create/clone button. For vSZ-E controllers, the system does not display any warning if the maximum number is reached instead the create/clone button is grayed.

Component/s	Data Plane
Issue	SCG-127226
Description	If a client does not upgrade all data planes to release 6.0.0 the data plane inter tunnel function will fail (Flexi-VPN/ L3 Roaming/ CALEA) between release 5.2.x and 6.0.0 data plane. General tunnel WLAN functions will work such as LBO/ L2oGRE.

Component/s	System
Issue	SCG-117468
Description	Controller vSZ-H Virtual Hard Disk (VHD) format increases the size from 40GB to 150GB, which impacts the upload time for Azure platform.

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

Component/s	System
Issue	SCG-128645
Description	Due to change in EAP supplicant timeout from default 12 seconds to 60 seconds in SmartZone release 6.0.0 [SCG-124967], client fails to get the IP address when RADIUS proxy switches to the secondary server.
Workaround	It is recommended to change the RADIUS option values in WLAN before upgrading the controller or AP to 6.0.0 to: ● NAS request timeout = 5 ● NAS maximum number of retries retry = 6

Component/s	UI/UX
Issue	SCG-124948
Description	Unable to zoom IN or OUT the AP performance and connection failure graphs.

Resolved Issues

The following are the resolved issues related to this release.

Component/s	AP
Issue	ER-9581
Description	Resolved an issue where user equipment was unable to authenticate in WISPr WLAN when the WLAN scheduler is also provisioned.

Component/s	AP
Issue	ER-8577
Description	Resolved an issue where the statistical information provided to SCI could have resulted in discrepancies between total traffic sessions summary and binned sessions reports available in SCI.

Component/s	AP
Issue	ER-9274
Description	Resolved an issue where the AP reboot issue caused by the target assert.

Component/s	AP
Issue	ER-9622
Description	Resolved an issue where APs located in same subnet as controller SZ144 failed to auto discover the controller.

Component/s	AP
Issue	ER-9483
Description	Resolved an issue where it showed excessive message, *FCS err, drop a false ekahaul frame* in syslog from the support file.

Component/s	AP
Issue	SCG-128828
Description	Resolved an issue where AP fragments packets with size greater than tunnel MTU when force fragmentation was disabled and failed to send ICMP packet that was too big (ICMP type = 2).

Component/s	AP
Issue	SCG-128881
Description	Resolved an issue where multicast traffic dropped when disabled multicast and directed threshold was disabled on R720 AP.

Component/s	AP
Issue	SCG-128898
Description	Resolved an issue where in mixed 802.11ac and 802.11ax AP mesh deployment when MAP is 802.11ac AP and RAP is 802.11ax AP, MAP failed to get IPv6 address in dual zone.

Component/s	AP
Issue	ER-9291, ER-9925
Description	Resolved an issue where authentication server was unreachable and fallback events were generated even when the AAA server responded within the zombie time.

Component/s	System
Issue	ER-9476
Description	Resolved an issue where configuration details for *Authentication Service* inside *Realm Based Authentication Service* was not shown in controller web user interface when editing this value.

Component/s	System
Issue	ER-9556
Description	Resolved an issue where the controller web user interface failed to download the alarms log file when the alarm count was over 50000.

Component/s	System
Issue	ER-9633
Description	Resolved an issue where the system was unable to apply WLAN templates extracted from the Zones under **Partner Domain**.

Component/s	System
Issue	ER-9612
Description	Resolved an issue where creating the second management interface caused the current management interface to hang.

Component/s	System
Issue	ER-9529
Description	Resolved an issue where WLANs failed to remove from WLAN group when similar simultaneous operations like this were done using Public API.

Component/s	System
Issue	ER-9522
Description	Resolved an issue which caused invalid characters when configuring AP location parameters in CLI mode.

Component/s	System
Issue	ER-9423
Description	Resolved an issue where SNMP traps were not sent by the controller for Switch related alarms and events.

Component/s	Virtual SmartZone
Issue	ER-9658
Description	Resolved an issue where SoftGRE profiles containing similar server IP address failed to create in controller web user interface.

Component/s	UI/UX
Issue	SCG-129034
Description	Resolved an issue where the controller failed to trigger periodic checks for latest available Sigpack on the default date. For example, 1st of every month.

Interoperability Information

Cluster Network Requirements

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

TABLE 7 Minimum Cluster Network Requirement

Model	SZ300	vSZ-H	SZ144	SZ100	vSZ-E
Latency	34ms	34ms	68ms	76.5ms	76.5ms
Jitter	10ms	10ms	10ms	10ms	10ms
Bandwidth	115Mbps	92Mbps	46Mbps	23Mbps	23Mbps

Client Interoperability

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

Component/s	AP
Issue	SCG-124891
Description	Nokia X2 devices do not accept passphrase if the string length is above 24 characters.
Workaround	Administrator should reduce the password length to less than 24, to allow the client Nokia X2 with dual sim to connect to WEP-64 encryption.

Component/s	AP
Issue	SCG-125696
Description	Samsung S10, Samsung Note 10, Google Pixel 4XL, Samsung S20 running Android 10, 11 with WPA3 11r PSK uses open system authentication instead of FT over SAE while roaming.

Component/s	AP
Issue	SCG-124953
Description	Google *Pixel 2*, *Pixel 3* and OnePlus *6* clients are unable to connect to WPA2/WPA3 mixed and WPA3 profile with 802.11r enabled.
Workaround	With WPA2/WPA3 mixed profile with 802.11r enabled, connect it manually by adding the WLAN network with WPA2 encryption.

Component/s	AP
Issue	SCG-128368
Description	Samsung Galaxy M51 (Android-10) version M515FXXU1ATI1 is not able to detect OWE encryption WLAN.
Workaround	For connecting Samsung Galaxy M51 (Android-10) version M515FXXU1ATI1, set any encryption (WPA2, WPA3, Open) other than OWE.

Component/s	AP
Issue	SCG-128203

Component/s	AP
Description	Samsung-S20, Samsung-Note10 fails to detect WPA3-Enterprise WLAN with encryption AES-GCMP-256.
Workaround	Samsung-S20 and Samsung-Note10 supports WPA3 Enterprise WLAN with AES encryption.

Component/s	AP
Issue	SCG-128254
Description	Following devices do not connect to 802.11x WPA3 AES or 802.11x WPA3 AES-GCMP-256. ● iPhoneX iOS 14.2 ● iPhone XE with iOS 12.3.1 ● iPhone HB with iOS 14.1 ● iPhone 7 plus with iOS 13.5.1 Following devices do not connect to 802.1x WPA3 AES-GCMP-256 but connect to 802.1x WPA3 AES. ● MacBook Pro with 10.15.7 ● Samsung Galaxy S10 with Android 11 ● Samsung Galaxy S20 with Android 11

Component/s	AP
Issue	SCG-125694
Description	iPhone X with OS version iOS version 14.0 does not support WPA3 11r roaming.

Component/s	AP
Issue	SCG-128171
Description	There is limitation with DPI where chat based app flows cannot be detected due to very few intermittent packets that are sent by these apps. Chat messages from WhatsApp, Telegram, Signal applications are not blocked due to this limitation.

Component/s	AP
Issue	SCG-115805
Description	Google Pixel 1 with Android version 9 fails to connect with a Transient Client Management (TCM) based WLAN profile for specific values - *[Join Ignore Timeout: 30seconds; Join Ignore Threshold: 40 seconds, Join Accept Timeout: 4 seconds]*.
Workaround	Use default Transient Client Management values instead of non default values.

Component/s	AP
Issue	SCG-123157
Description	Android 10 and 11 version having MAC address randomization features as *default* affects the Wi-Fi.
Workaround	For MAC address related authentication: 1. Disable Wi-Fi MAC randomization. 2. Select *Use Device MAC* while connecting to SSID.

Component/s	AP
Issue	SCG-123018

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

Component/s	AP
Issue	SCG-126038
Description	iPhone running iOS 14 or 14.0.1 has Wi-Fi connectivity issues.
Workaround	Recommend to upgrade the iOS to 14.4 to avoid connectivity issues.

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

Component/s	AP
Issue	SCG-109406
Description	Surface Pro Window client fail to connect to WPA3 mixed mode.
Workaround	Use WPA2 authentication for Surface Pro clients.

Component/s	AP
Issue	SCG-124854
Description	Android clients (Google Pixel 1 (Android 9), OnePlus 3 (Android 8.1.0), LG Nexus 5X (Android 9) are unable to load WISPr login page by clicking SSID name in Wi-Fi settings.
Workaround	Use a browser (Chrome, etc.) to load the WISPr login page.

Component/s	AP
Issue	SCG-125084
Description	Xiaomi Mi 4W (Android 4.4.4) is intermittently detected as falsely as an iOS device by *Client Fingerprinting* feature.

Component/s	AP
Issue	SCG-126335
Description	User agent for IPad with OS version 14.0 is seen as a MAC device.

Component/s	AP
Issue	SCG-122427
Description	There is limitation with DPI where chat based application flows cannot be detected due to few intermittent packets sent by these applications. Chat messages from QQ and WeChat are not blocked due to this limitation.

Component/s	AP
Issue	SCG-128920

Component/s	AP
Description	Client with Intel AX201 Gig+ NIC fails 802.11r authentication at EAPOL 2 message due to Intel Mobility Domain IE abnormalities which have been isolated to PMKID format malformation.
Recommendation	Upgrade the Intel Driver version to 22.30.0.

Component/s	UI/UX
Issue	SCG-125723
Description	iOS 14 device fails to send the hostname (Option 12) in DHCP resulting in the AP reporting the MAC address provided the hostname is empty from the UE (device).

Component/s	UI/UX
Issue	SCG-123453
Description	Given the limitation with MAC Safari browser, it is recommended to log off from the controller managed account, clear the Safari browser history and then re-login to the controller to view the customized icon.

Security Considerations

Following are the security fixes and third party software upgrade for this release.

- Refer to the Security Advisory for the Aggregation And Fragmentation Attacks Vulnerability (aka “FragAttacks”) https://support.ruckuswireless.com/security_bulletins/310. **[SCG-128883]**

Adding AP Patch to the Controller

Before you begin this procedure, copy the AP patch file that you want to apply to a location that you can access from your computer.

IMPORTANT
This patch only needs to be applied to a single node. After you apply this patch to a node, it will be propagated automatically to other nodes in the cluster.

Follow these steps to apply an AP patch:

1. Download the patch file `scg-ap-6.0.0.0.1640.patch` and move the patch file to a location that you can access from the computer that you are using to access the controller's web interface.
2. Apply this patch to release 6.0.0 (build number `6.0.0.0.1331`).
3. Log on to the SmartZone web interface.
4. Go to the page for uploading AP patches.
   - On the 6.0.0 web interface, go to **Administration** > **Upload AP Patch** > **and then click the AP Patch** tab.
5. In **Patch File Upload**, click **Browse** go to the location where you saved the AP patch file (`scg-ap-6.0.0.0.1640.patch`).
6. Click **Open**.
7. On the **AP Patch** tab, click **Upload**. After the patch file is uploaded, the section is populated with the Start time, AP firmware version number and AP model number.
8. Click **Apply Patch**.

9. After the firmware file is applied, the AP firmware information is populated with the following information:
   - Name of the patch file
   - Size of the patch file
   - AP firmware version number
   - AP model number
10. Go to **Configuration** > **AP Zone** > **Select a Zone.**
11. Click **Change AP Firmware**.
12. In the **Change AP Firmware** manually change the AP firmware to the latest AP image (`6.0.0.0.1640`) in the selected Zone.
13. Click **Yes**
14. When the controller completes updating the AP firmware of the zone, a message appears and notifies you that the zone's AP firmware was updated successfully.
15. Verify that all APs in selected zone are upgraded to `6.0.0.0.1640`.
16. Repeat the steps from 10 to 15 for other Zones that need to be updated.

You have completed adding a new AP patch to the controller.

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