

RUCKUS SmartZone 5.2.2 Release Notes

Supporting SmartZone 5.2.2 Patch 1 (MR1)

Copyright, Trademark and Proprietary Rights Information

© 2021 CommScope, Inc. All rights reserved.

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..... 4**
- Hardware and Software Support..... 4**
 - Overview..... 4
 - Release Information..... 4
 - Supported Matrix and Unsupported Models..... 7
- Known Issues..... 9**
- Changed Behavior..... 10**
- Security Considerations 10**
- Resolved Issues..... 11**
- Interoperability Information.....22**
 - Cluster Network Requirements..... 22
 - Client Interoperability..... 22

Document History

Revision Number	Summary of changes	Publication date
A	Initial release notes	20, October 2021

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 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. While SZ144 can only run controller version 5.2.1 and software, it can also host controller version 3.6.2 AP firmware Zones.
- The SZ144-D is the second generation Data Plane hardware appliance which is functionally equivalent to the vSZ-D virtual Data Plan product. The appliance provides turnkey deployment capabilities for customers that need a hardware appliance. The SZ144-D is managed by a vSZ Controller only and cannot work in a standalone mode.
- Access Point (AP): Controllers support 1000 APs per zone.

Release Information

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

SZ300

- Controller Version: **5.2.2.0.1161**
- Control Plane Software Version: **5.2.2.0.1040**
- Data Plane Software Version: **5.2.2.0.1161**

- AP Firmware Version: **5.2.2.0.1106**

SZ124

- Controller Version: **5.2.2.0.1161**
- Control Plane Software Version: **5.2.2.0.1040**
- Data Plane Software Version: **5.2.2.0.1012**
- AP Firmware Version: **5.2.2.0.1106**

SZ144

- Controller Version: **5.2.2.0.1161**
- Control Plane Software Version: **5.2.2.0.1040**
- Data Plane Software Version: **5.2.2.0.1012**
- AP Firmware Version: **5.2.2.0.1106**

vSZ-H

- Controller Version: **5.2.2.0.1161**
- Control Plane Software Version: **5.2.2.0.1040**
- AP Firmware Version: **5.2.2.0.1106**

vSZ-E

- Controller Version: **5.2.2.0.1161**
- Control Plane Software Version: **5.2.2.0.1040**
- AP Firmware Version: **5.2.2.0.1106**

vSZ-D

- Data plane software version: **5.2.2.0.1161**

NOTE

By downloading this software and subsequently upgrading the controller and/or the AP to release 5.2.1.0.177 (or later), you understand and agree that:

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

ATTENTION

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

SZ Google Protobuf (GPB) Binding Class

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

1. SmartZone GPB / MQTT Interface Test Subscriber Software [DNP] – <https://support.ruckuswireless.com/software/2805>
2. SmartZone 5.2.2.0.317 (GA) GPB.proto (Google ProtoBuf) image for GPB/MQTT [DNP] –
<https://support.ruckuswireless.com/software/2804>
<https://support.ruckuswireless.com/software/2581>

Public API

Click on the following links to view:

- SmartZone 5.2.1 Public API Reference Guide (ICX Management), visit <https://support.ruckuswireless.com/documents/3570>
- SmartZone 5.2.1 Public API Reference Guide (SZ100), visit <https://support.ruckuswireless.com/documents/3569>

NOTE

SZ100 Public API link is for SZ144 as well.

- SmartZone 5.2.1 Public API Reference Guide (SZ300), visit <https://support.ruckuswireless.com/documents/3568>
- SmartZone 5.2.1 Public API Reference Guide (vSZ-E), visit <https://support.ruckuswireless.com/documents/3567>
- SmartZone 5.2.1 Public API Reference Guide (vSZ-H), visit <https://support.ruckuswireless.com/documents/3566>

Application Signature Package (Sigpack)

ATTENTION

The signature package is the same for releases 5.2.1 and 5.2.2.

AP DPI feature uses an Application Signature Package that in general it can be optionally updated when a new version is available. But in this case, previous packages are not compatible with 5.2 AP firmware, and upgrading zone firmware is blocked until the corresponding signature package (**RuckusSigPack-1.510.1 .tar.gz**) is installed.

Do follow this mandatory process before upgrading AP zone firmware:

1. Download Signature package by visiting the RUCKUS support site,
<https://support.ruckuswireless.com/software/2746-smartzone-6-0-0-0-1331-ga-sigpack-1-510-1-regular-application-signature-package>
2. Manually upgrade the signature package by navigating to **Services & Profiles > Application Control > Signature Package**. (more details can be found in Administrator Guide, in section *Working with Application Signature Package*)

Once this is done, AP zones can be upgraded. [**SCG-108730**]

IMPORTANT

Sigpack versions 1.430.1, 1.470.1 and 1.510.1 are supported on build 5.2.2.0.1153. Version 1.380.0.40 is not supported.

Product Documentation Upgrade Guide

The following product guides, have been updated for this release. Do refer to the *What's New in this Document* section.

1. SmartZone 5.2.2 Administrator Guide (SZ300/vSZ-H)
2. SmartZone 5.2.2 Administrator Guide (SZ100/vSZ-E)
3. SmartZone 5.2.2 Upgrade Guide

4. SmartZone 5.2.2 Command Reference Guide (SZ300/vSZ-H)
5. SmartZone 5.2.2 Command Reference Guide (SZ-100/vSZ-E)
6. SmartZone 5.2.2 Getting Started Guide on GPB/MQTT Interface (SZ300/SZ-100/vSZ)

NOTE

The rest of the SmartZone guides remain the same for this release. Refer to the SmartZone release 5.2.1 set of documents by visiting the RUCKUS website available at support.ruckuswireless.com or [Tech Content Portal](#).

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

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

NOTE

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

AP Firmware Releases

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

Upgrade path	AP firmware releases in controller
5.1.x > 5.2.x	5.1.x, 5.2.x
5.0 > 5.1.x > 5.2.x	5.1.x, 5.2.x
3.6.2 > 5.1.x > 5.2.x	3.6.2, 5.1.x, 5.2.x
3.6.2 > 5.2.x	3.6.2, 5.2.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, 5.2.2

Supported AP Models

This release supports the following RUCKUS AP models.

Hardware and Software Support

Supported Matrix and Unsupported Models

TABLE 1 Supported AP Models

11ax		11ac-Wave2		11ac-Wave1	
Indoor	Outdoor	Indoor	Outdoor	Indoor	Outdoor
R730	T750	R720	T710	R600	T504
R750	T750SE	R710	T710S	R500	T300
R650		R610	T610	R310	T300E
R550		R510	T310C	R500E	T301N
R850		H510	T310S		T301S
		C110	T310N		FZM300
		H320	T310D		FZP300
		M510	T811CM		
		R320	T610S		
			E510		
			T305e		
			T305i		

ATTENTION

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

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			

Switch Management Feature Support Matrix

NOTE

Switch Management feature support stated in the 5.2.2 release notes are also applicable to this patch release.

IoT Suite

NOTE

IoT feature support stated in the 5.2.2 release notes are also applicable to this patch release.

Known Issues

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

NOTE

Known issues stated in the 5.2.2 release notes are also applicable to this release.

Component/s	AP
Issue	SCG-133489
Description	Client fingerprinting feature fails to correctly detect iPhone 12 mini (reported as iPhone 13,1).

Component/s	AP
Issue	SCG-133466
Description	iPhone 7 running iOS 15 may require multiple connection attempts to stay connected to WLAN.

Component/s	AP
Issue	SCG-133437, SCG-133087
Description	Application policy may fail to detect Zoom application traffic.

Component/s	AP
Issue	SCG-133114
Description	Application policy may fail to detect MS Teams traffic.

Component/s	AP
Issue	SCG-132870
Description	Client may fail to connect to WLAN that is using SoftGRE tunnel with AAA affinity feature enabled (automatic fallback disable is enabled in Authentication service) and primary SoftGRE gateway is down.

Component/s	UI/UX
Issue	ER-10411
Description	Switch tab in controller GUI may fail to load with error message <i>Timeout when requesting data from SZ</i> when admin user manages high number of switches and domains.
Workaround	Reduce the number of domains/zones in current GUI view.

Changed Behavior

The following are the changed behavior issues in this release.

Component/s	AP
Issue	SCG-130434
Description	Called Station ID RADIUS attribute includes now AP name as a new possible setting inside WLAN > Radius Options configuration.

Component/s	AP
Issue	AP-15736
Description	Behavior enhancement in Geo-Redundancy deployments where AP will keep Active and Standby controller list when none of the controller nodes are reachable.

Component/s	System
Issue	SCG-129718
Description	Maximum number of User Groups at controller (SmartZone) system level have been increased from 99 to 1000 entries.

Component/s	System
Issue	ER-10033
Description	Maximum number of Hotspot 2.0 WLAN profiles per cluster have been increased from 3000 to 10000 entries (per Zone maximum number remains at 16 entries).

Component/s	System
Issue	ER-9658
Description	Multiple softGRE profiles with duplicate IP addresses are now allowed.

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]
- Upgraded NGINX package in controller (SmartZone) to version 1.20.1. [ER-10618, ER-10400, ER-9893]
- FTP port 21 is now closed in controller when related service (lwapp2scg) is configured to deny this communication [ER-10225]
- Diffie-Hellman group key strength has been increased in controller when cluster is upgraded. [ER-9830]
- Upgraded *open-vm-tools* in controller to version 11. [ER-9797]
- Upgraded *Dnsmasq* library to version 2.84. [AP-15238]

Resolved Issues

The following are the resolved issues related to this release.

Component/s	AP
Issue	ER-9565
Description	Resolved an issue of 802.11x WLAN Ethernet profile display.

Component/s	AP
Issue	ER-9486
Description	Resolved an issue where UE may fail to connect to WLAN using External DPSK due to authentication timeout.

Component/s	AP
Issue	ER-10299
Description	Resolved an issue where an AP will not initiate a new RADIUS authentication on behalf of a client when there is another one in progress.

Component/s	AP
Issue	ER-10184
Description	Resolved an issue where R750 AP may reboot due to target assert.

Component/s	AP
Issue	ER-10115
Description	Resolved an issue where Band Balance setting in AP might have an invalid value.

Component/s	AP
Issue	ER-9545
Description	Resolved an issue of AP MAC address which at times caused UE traffic drop by Switch.

Component/s	AP
Issue	ER-10283
Description	Resolved an issue where UE failed to be redirected to portal page in WISPr WLAN when AP name has 64 characters.

Component/s	AP
Issue	ER-9831
Description	Resolved an issue where Apple clients may be disconnected due to inactivity because AP does not acknowledge client going into power save mode.

Component/s	AP
Issue	ER-10276

Resolved Issues

Component/s	AP
Description	Resolved an issue where Zone accounting server modification did not reflect on the AP configuration.

Component/s	AP
Issue	ER-9704
Description	Resolved an IPv6 format address issue for softGRE information which could lead to tunnel establishment issues from AP when using tunnel failover with AAA affinity.

Component/s	AP
Issue	ER-10493
Description	Resolved an airtime fairness performance related issue in 802.11ax APs.

Component/s	AP
Issue	ER-9581
Description	An issue where the UE may not be able to authenticate in WISPr WLAN is resolved by invoking DNS spoof update whenever WLAN scheduler changes WLAN state.

Component/s	AP
Issue	ER-10340
Description	Resolved an issue in 802.11ax AP models introduced by FragAttacks fix where UE will lose network connectivity when roaming between radios in same AP in encrypted WLAN.

Component/s	AP
Issue	ER-10284
Description	Resolved an issue where SSH traffic for wired client was dropped when the port was configured as trunk port with VLAN1 untagged.

Component/s	AP
Issue	ER-9483
Description	Resolved an issue where unnecessary Ekahau related log were removed from the AP support information.

Component/s	AP
Issue	ER-9930
Description	Resolved an issue where 5GHz channel 140 might be available in APs even when not selected in configuration.

Component/s	AP
Issue	ER-10425
Description	Resolved a temporary communication issue with a client that might happen when it has roamed to a new AP using 802.11r (Fast Transition).

Component/s	AP
Issue	ER-9813
Description	Resolved an issue where 5GHz channel 144 was not available in 802.11ax AP models for Japan country code.

Component/s	AP
Issue	ER-9858
Description	Resolved an issue where AP management SSH connection with controller might flap between controllers when using IPv6 addresses.

Component/s	AP
Issue	ER-9516
Description	Resolved an MU-MIMO (multi-user, multiple-input, multiple-output) performance related issue in 802.11ax APs.

Component/s	AP
Issue	ER-10181
Description	Resolved an AP packet forwarding issue in 802.11ac wave-2 APs related to background scanning being enabled.

Component/s	AP
Issue	ER-10454
Description	Resolved an issue where AP CLI command get lbs-server displayed an error if venue name exceeds 15 characters long.

Component/s	AP
Issue	ER-9838
Description	Resolved an issue which caused AP SGRE throughput drop.

Component/s	AP
Issue	ER-10451
Description	Resolved an issue where AP was providing incomplete information about client connection failures due to negotiation issues to upper systems like RUCKUS Analytics.

Component/s	AP
Issue	ER-10320, ER-10450
Description	Resolved an issue where client might get disconnected shortly after joining or roaming to an AP.

Component/s	AP
Issue	ER-9965
Description	Resolved an issue where redundant neighbor AP related log is removed from the AP support information.

Resolved Issues

Component/s	AP
Issue	ER-10057
Description	Resolved an issue where AP verbose log entry <i>user.warn kernel: Reached buffer limit</i> is removed from default log level.

Component/s	AP
Issue	ER-9274
Description	Resolved an issue of 11ax AP reboot caused by target assert.

Component/s	AP
Issue	ER-9874
Description	Resolved an issue where AP might send an invalid ARP response for gateway MAC address when proxy ARP feature is enabled.

Component/s	AP
Issue	ER-6970
Description	Resolved an issue where incorrect number of active clients was obtained from AP SNMP query.

Component/s	AP
Issue	ER-10142
Description	Resolved an issue where APs may be incorrectly reported as disconnected in controller GUI or through SNMP polling.

Component/s	AP
Issue	ER-9787
Description	Resolved an issue where UE authentication failed when AP handled <i>EAPOL-Start</i> from the UE.

Component/s	AP
Issue	ER-8562
Description	Resolved an issue related to DHCP troubleshooting tool.

Component/s	AP
Issue	ER-10090
Description	Resolved an issue where UE was unable to join Web authentication WLAN due to uploaded customer certificated exceeded 9216 bytes.

Component/s	AP
Issue	ER-10241
Description	Resolved an issue in 802.11ax APs where incorrect MAC addresses were being sent to Ekahau application.

Component/s	AP
Issue	ER-10047, ER-9682, ER-9988, ER-9910

Component/s	AP
Description	Resolved AP to controller SSH tunnel related issues when the controller is behind a NAT server.

Component/s	AP
Issue	ER-10422
Description	Resolved an issue where clients could not join the network in a WLAN with non-proxy authentication due to RADIUS server reply containing <i>Filter-ID</i> attribute with certain values.

Component/s	AP
Issue	ER-10350
Description	Resolved an issue where Communicator SmartZone process may run out of memory if very high number of APs are in discovery status while there are high number of DPSKs entries configured as well.

Component/s	AP
Issue	ER-9998
Description	Resolved an interoperability issue with certain Intel clients where they may fail to roam when using 802.11r (Fast Transition).

Component/s	AP
Issue	ER-10272
Description	Resolved an issue where controller services might stay down after a cluster restore due to configure process incorrectly restarting.

Component/s	AP
Issue	ER-9633
Description	Resolved an issue where WLAN templates extracted from Zones under Partner Domain could not be applied.

Component/s	AP
Issue	ER-9919
Description	Resolved an issue where controller RADIUS proxy process might restart when accounting message is received from IPv6-only AP.

Component/s	AP
Issue	ER-9810
Description	Resolved an issue where controller RADIUS proxy process might drop RADIUS messages because the queue is full when AAA affinity feature is enabled and some requests are not replied by AAA server.

Component/s	AP
Issue	ER-10070
Description	Resolved an issue of user name display related to client 802.11r roaming.

Resolved Issues

Component/s	AP
Issue	ER-10342
Description	Resolved an issue where unnecessary AP configuration updated where generated in SZ100 controller model when sync time.

Component/s	AP
Issue	ER-9522
Description	Resolved an issue where controller may fail to accept multi-byte characters when configuring AP parameters in CLI or public API.

Component/s	AP
Issue	ER-10183
Description	Resolved an issue where a new controller node may fail to join an existing cluster because it is using a certificate with password protected private key.

Component/s	AP
Issue	ER-10408
Description	Resolved an issue where thresholds for AP status in <i>Health</i> dashboard configuration could not be configured due to saving of some corrupted configuration.

Component/s	AP
Issue	ER-9864
Description	Performance enhancement in controller when applying Zone template configuration.

Component/s	AP
Issue	ER-9499
Description	Resolved an issue where Zone configuration using public API failed if all APs in the Zone are offline and DHCP/NAT feature is enabled.

Component/s	AP
Issue	ER-10477
Description	Resolved an issue where APs may move to different controller in the cluster due to controller process receiving messages from APs being restarted.

Component/s	AP
Issue	SCG-132592
Description	Resolved an issue where AP may not honor session timeout and Accounting Interim interval received from AAA server when client roams using 802.11r (Fast Transition).

Component/s	Control Plane
Issue	ER-9622
Description	Resolved an issue where AP controller auto discovery did not work in SZ144 model.

Component/s	Control Plane
Issue	ER-10440, ER-9989
Description	Resolved an issue where memory leak was observed in RADIUS Proxy controller process when CoA/Disconnect messages was received from AAA server.

Component/s	Control Plane
Issue	ER-9925
Description	Resolved an issue where authentication while controller is acting as AAA proxy could failover to secondary AAA server even when primary server responds within the response window configured.

Component/s	Data Plane
Issue	ER-9621
Description	Resolved an issue where exporting log files from data plane CLI using SFTP protocol did not work.

Component/s	Data Plane
Issue	ER-9882
Description	Resolved an issue where data plane may drop some random user traffic when connected to a northbound L2oGRE server due to unnecessary log lines.

Component/s	Data Plane
Issue	ER-10258
Description	Resolved an issue where data plane may crash when using encrypted RUCKUS GRE tunnels.

Component/s	Public API
Issue	ER-10018
Description	Resolved an issue where SmartZone Public API <i>domains</i> return some incorrect information related to AP and Zone count.

Component/s	Public API
Issue	ER-10246
Description	Resolved an issue where Public API query for block clients was returning incomplete information.

Component/s	Public API
Issue	ER-10119
Description	Resolved an issue where public API queries related to Switch do not provide correct information in <i>hasMore</i> parameter.

Component/s	Switch Management
Issue	ER-10257
Description	Resolved an issue where Switch cannot be rebooted from the controller GUI.

Resolved Issues

Component/s	System
Issue	ER-10193
Description	Resolved an issue where controller may fail to re-onboard into RUCKUS Analytics with error <i>Unable to verify the SSL certificate with Ruckus Cloud services.</i>

Component/s	System
Issue	ER-9373
Description	Resolved an issue where controller may fail to send data to RUCKUS Analytics.

Component/s	System
Issue	ER-9846
Description	Resolved an issue where Northbound Interface cannot complete user authentication when using complex interface password if log level is set to debug.

Component/s	System
Issue	ER-9556
Description	Resolved an issue where alarm report failed to be exported from the controller in CSV format when it contains more than 50000 entries.

Component/s	System
Issue	ER-9529
Description	Resolved an issue where controller is unable to remove WLANs from WLAN Groups with multi-thread API requests.

Component/s	System
Issue	ER-10060
Description	Resolved an issue where RUCKUS Analytics may fail to obtain AP list from controller cluster due to message size limit.

Component/s	System
Issue	ER-9597
Description	Resolved an issue where static routes in the controller may be incorrectly applied after software upgrade if the controller had access-core separation and UDI interface.

Component/s	System
Issue	ER-10374
Description	Resolved an issue to prevent null value from being retrieved on port status fields when switch data is requested using public API.

Component/s	System
Issue	ER-10347
Description	Resolved an issue where controller was still using TLS 1.0 for SMTP when <i>Start-TLS</i> option is enabled even when TLS 1.0 is disabled globally.

Component/s	System
Issue	ER-10437
Description	Resolved an issue where certain Elliptic Curve certificates did not work on the controller.

Component/s	System
Issue	ER-10390
Description	Resolved an issue where a new SmartZone node may fail to join an existing cluster because synching configuration and firmware was timing out.

Component/s	System
Issue	ER-9954
Description	Resolved an issue where Bonjour Gateway with Chromecast rules could not be configured in 3.6.x AP Zone.

Component/s	System
Issue	ER-9612
Description	Resolved an issue where controller second management interface was not configured correctly when controller has access-core separation and UDI interface.

Component/s	System
Issue	ER-10591
Description	Resolved an issue where incorrect LED status may be displayed in SZ300 power supply unit.

Component/s	System
Issue	ER-9558
Description	Improvement in controller CLI response time when cluster is connected to SCI.

Component/s	System
Issue	ER-9423
Description	Resolved an issue where SNMP traps were not being sent for Switch event/alarms.

Component/s	System
Issue	ER-9926
Description	Improvement in controller configuration load times when there are large number of Hotspot 2.0 profiles.

Component/s	System
Issue	SCG-130152
Description	Resolved an issue where Admin AAA profile could not be configured using the same LDAP or AD server IP address but different realm.

Component/s	System
Issue	ER-10352

Resolved Issues

Component/s	System
Description	Resolved an issue where memory leak is observed in RADIUS proxy controller process when sending Accounting On/Off messages.

Component/s	System
Issue	ER-9997
Description	Removed remote capture commands from data plane CLI since the feature was already removed.

Component/s	UI/UX
Issue	ER-10106
Description	Resolved an issue where different AP registration rules may have the same priority when they are re-ordered in controller GUI.

Component/s	UI/UX
Issue	ER-9744
Description	Resolved an issue where controller GUI was showing incorrect number of AP direct tunnel licenses consumed.

Component/s	UI/UX
Issue	ER-9484
Description	Resolved an issue where Guest pass page in controller GUI may contain blank pages/records.

Component/s	UI/UX
Issue	ER-10172
Description	Resolved an issue where switch port settings page is blank in controller GUI when configuring large stacks.

Component/s	UI/UX
Issue	ER-9607
Description	Resolved an issue where controller GUI was unable to filter in WLAN menu by keyword once results were sorted.

Component/s	UI/UX
Issue	ER-10426
Description	Resolved an issue where WLAN configuration could not be edited twice in the controller GUI during the same session without refreshing the browser.

Component/s	UI/UX
Issue	ER-10136
Description	Resolved a display issue in controller GUI where AP image status may show as <i>Unknown</i> .

Component/s	UI/UX
Issue	ER-10327

Component/s	UI/UX
Description	Resolved a display issue in Switch Remote CLI available in controller GUI where characters may be displayed repeated if typed at high speed.

Component/s	UI/UX
Issue	ER-10381
Description	Resolved an issue where triggering AP binary log from the controller GUI may fail but it was displaying a success message.

Component/s	UI/UX
Issue	ER-10526
Description	Resolved an issue where Switch configuration backup and firmware upgrade done via controller GUI fails if the Switch name contains the character #.

Component/s	UI/UX
Issue	ER-9476
Description	Resolved an issue where there is missing information in Realm Based Proxy configuration in controller GUI.

Component/s	UI/UX
Issue	ER-10265
Description	Resolved an issue where switch support log error banner was persistent in controller GUI.

Component/s	UI/UX
Issue	ER-10134
Description	Resolved a typing mistake in System > Cluster > Network Settings in inbound port 91 description.

Component/s	UI/UX
Issue	ER-9977
Description	Resolved an issue where logs will fail to correctly download from controller GUI when it exceeds 2GB.

Component/s	UI/UX
Issue	ER-10498
Description	Resolved an issue where WLAN algorithm configured is not displayed correctly in the controller GUI when opening WLAN settings.

Component/s	Virtual SmartZone (vSZ)
Issue	ER-10592
Description	Resolved an issue where public API returned incorrect AP status if DHCP/NAT feature was enabled in the Zone.

Interoperability Information

Component/s	Virtual SmartZone (vSZ)
Issue	ER-9291
Description	Resolved an issue where controller events 1601 and 1602 may be raised incorrectly.

Component/s	Virtual SmartZone (vSZ)
Issue	ER-10566
Description	Improvement in SmartZone CLI response time when going into Zone configuration.

Component/s	Virtual SmartZone (vSZ)
Issue	ER-10449
Description	Resolved an issue where the controller may not correctly detect hardware resources assigned to it when installed in AWS (Amazon Web Services) public cloud.

Component/s	Virtual SmartZone (vSZ)
Issue	ER-10574
Description	Resolved an issue where rebooting AP variable was not provided in system inventory public API.

Component/s	Virtual SmartZone (vSZ)
Issue	ER-10627
Description	Resolved an issue where Session Timeout is set to 60 seconds instead of the value configured in WLAN when value received from RADIUS server is 0.

Component/s	Virtual SmartZone Data Plane (vSZ-D)
Issue	ER-9422
Description	Resolved an issue where virtual data plane may crash when configured with Direct I/O interface.

Interoperability Information

Cluster Network Requirements

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

TABLE 3 Minimum Cluster Network Requirement

Model	SZ300	vSZ-H	SZ144	SZ100	vSZ-E
Latency	77ms	68ms	85ms	119ms	119ms
Jitter	10ms	10ms	10ms	10ms	10ms
Bandwidth	69Mbps	69Mbps	46Mbps	23Mbps	23Mbps

Client Interoperability

NOTE

Client Interoperability issues stated in the 5.2.2 release notes are also applicable to this patch release.

COMMScope®
RUCKUS®

© 2021 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
<https://www.commscope.com>