RELEASE NOTES

# RUCKUS SmartZone 5.2.2 LT GD Release Notes

## Supporting SmartZone 5.2.2 LT GD MR 2

*Part Number: 800-73200-001 Rev A*
*Publication Date: June 2022*

# Copyright, Trademark and Proprietary Rights Information

## Export Restrictions

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

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

## Disclaimer

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

## Limitation of Liability

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

## Trademarks

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

# Contents

# Document History

| Revision Number | Summary of changes | Publication date |
|---|---|---|
| A | Initial release notes | 15, June 2022 |

# 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 General Deployment (LT GD) release. This section lists the version of each component in this release.

### *SZ300*

- Controller Version: **5.2.2.0.1562**
- Control Plane Software Version: **5.2.2.0.1539**
- Data Plane Software Version: **5.2.2.0.1562**

- AP Firmware Version: **5.2.2.0.2064**

## *SZ100/SZ144*

- Controller Version: **5.2.2.0.1562**
- Control Plane Software Version: **5.2.2.0.1539**
- Data Plane Software Version: **5.2.2.0.1519**
- AP Firmware Version: **5.2.2.0.2064**

## *SZ100D/SZ144D*

- Data plane software version: **5.2.2.0.1562**

## *vSZ-H / vSZ-E*

- Controller Version: **5.2.2.0.1562**
- Control Plane Software Version: **5.2.2.0.1539**
- AP Firmware Version: **5.2.2.0.2064**

## *vSZ-D*

- Data plane software version: **5.2.2.0.1562**

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

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

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

## *SZ Google Protobuf (GPB) Binding Class*

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

1. SmartZone 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)*

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-v2-1.540.1.tar.gz.** ) is installed.

Do follow this mandatory process before upgrading AP zone firmware:

1. Download Signature package by visiting the RUCKUS support site.
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 1.470.1, 1.510.1 and 1.540.1 are supported on our current 5.2.2.0.1562 controller version.

## *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 Alarms Events Guide (SZ300/vSZ-H)
2. SmartZone 5.2.2 Alarms Events Guide (SZ-100/vSZ-E)

The below set of documents, released with SmartZone 5.2.2 can be referred as well.

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.

**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 | | |

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

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

| 11n | 11ac-Wave1 |
|---|---|
| R300 | C500 |
| ZF7055 | H500 |
| ZF7352 | R700 |
| ZF7372 | |
| ZF7372-E | |
| ZF7781CM | |
| ZF7782 | |
| ZF7782-E | |
| ZF7782-S | |
| ZF7982 | |
| ZF7782-N | |

**ATTENTION**

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

**IMPORTANT**

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

## Unsupported AP Models

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

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

## Switch Management Feature Support Matrix

**NOTE**

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

## IoT Suite

**NOTE**

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

# Known Issues

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

**NOTE**
Known issues stated in the 5.2.2 LT GD and 5.2.2 LT GD MR 1 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) for iOS earlier to 15.4. |

| Component/s | AP |
|---|---|
| **Issue** | SCG-136726 |
| **Description** | IoT controller is not supported in APs connected to IPv6 only mode Zone. |

| Component/s | AP |
|---|---|
| **Issue** | SCG-136165 |
| **Description** | In vSZ-H with single interface deployment, use NAS IP RADIUS attribute set to *SZ Control IP* if AAA server needs to receive controller IP address in this attribute.<br>**NOTE**<br>Do not use option *SZ Management IP*, which does not apply for single interface deployment. |

| Component/s | System |
|---|---|
| **Issue** | SCG-133227 |
| **Description** | Controller reports may fail to be viewed or downloaded when result file size is too big if PDF format is selected. |
| **Workaround** | Create the report only using CSV format. |

| Component/s | AP |
|---|---|
| **Issue** | ER-10924 |
| **Description** | Client throughput may drastically reduced when connected to low priority WLAN, if high priority WLANs are also deployed in the same 802.11ax APs. |
| **Workaround** | Configure all WLANs with priority set to high when 802.11ax AP are in use. |

| Component/s | AP |
|---|---|
| **Issue** | ER-10763 |
| **Description** | SNMP Walks to query controller for RUCKUS-SCGAP group MIB may fail for some APs. |

# Changed Behavior

The following are the changed behavior issues in this release.

| Component/s | AP |
|---|---|
| **Issue** | ER-11019 |
| **Description** | In case of data plane upgrade failure, an enhancement has been made where a new event code will be generated (554) and the device will reboot by itself to recover from this state. |

| Component/s | AP |
|---|---|
| **Issue** | ER-10927 |
| **Description** | Enhancement in Northbound Interface 401 response code to differentiate errors between RADIUS server and the controller. |

| Component/s | AP |
|---|---|
| **Issue** | ER-10768 |
| **Description** | Enhanced port description in controller web user interface **System** > **Cluster** > **Network Setting** view. |

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

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

# Security Considerations

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

- Resolved security vulnerability CVE-2021-4034. [**ER-11084**]
- Disabled some weak KEX, MAC and Host key algorithms on the controller. [**ER-11049**]
- Resolved security vulnerability CVE-2021-44228 (Apache Log4j vulnerability). [**ER-10935**]
- Upgraded NGINX package in controller (SmartZone) to version 1.20.2. [**SCG-135566**]

# Resolved Issues

The following are the resolved issues related to this release.

| Component/s | AP |
|---|---|
| Issue | ER-11361 |
| Description | Resolved an issue where R720 may reboot due to kernel panic. |

| Component/s | AP |
|---|---|
| Issue | ER-11327, ER-10799, ER-11346 |
| Description | Resolved an issue where R720 may reboot due to kernel panic. |

| Component/s | AP |
|---|---|
| Issue | ER-11189, ER-11164, ER-11277 |
| Description | Resolved an issue where R850 may reboot due to system fault. |

| Component/s | AP |
|---|---|
| Issue | ER-11188 |
| Description | Resolved an issue in 802.11ac wave 1 AP models where clients were unable to pass traffic in a WLAN using DHCP/NAT feature and the network was using VRRP gateway. |

| Component/s | AP |
|---|---|
| Issue | ER-11149 |
| Description | Resolved an issue about packet handling in AP when exceeded maximum MTU (maximum transmission unit) and DF (Do-Not-Fragment) flag is set and used tunneled WLAN. |

| Component/s | AP |
|---|---|
| Issue | ER-11140 |
| Description | Resolved an issue where client HTTP traffic was dropped when accessing an URL with *all* in its domain name if Application Policy rule value *all* was selected for an application category. |

| Component/s | AP |
|---|---|
| Issue | ER-11118 |
| Description | Resolved an issue where manual TX power in AP may fail to set correctly when changing from auto (ACS enabled) mode. |

| Component/s | AP |
|---|---|
| Issue | ER-11113 |
| Description | Resolved an issue where 802.11ac wave 1 AP models may reboot due to watchdog timeout. |

| Component/s | AP |
|---|---|
| Issue | ER-11061 |

| Component/s | AP |
|---|---|
| Description | Resolved an issue in 802.11ax AP models where in a WLAN with VLAN pool enabled, the first packet from the UE is tagged with an incorrect VLAN ID. |

| Component/s | AP |
|---|---|
| Issue | ER-11053 |
| Description | Resolved an issue where in a WLAN with DHCP/NAT feature enabled, some random few packets from client may not be translated to the uplink. |

| Component/s | AP |
|---|---|
| Issue | ER-11048 |
| Description | Resolved an issue where R650 may reboot due to kernel panic. |

| Component/s | AP |
|---|---|
| Issue | ER-11021 |
| Description | Resolved an issue where traffic statistics would get reported as zero in open WLAN when *Ignore statistics from unauthorized clients* option is selected. |

| Component/s | AP |
|---|---|
| Issue | ER-11001 |
| Description | Resolved an issue where AP did not accept " character as part of the password. |

| Component/s | AP |
|---|---|
| Issue | ER-10985 |
| Description | Resolved a memory leakage issue related to SNMP process inside AP. |

| Component/s | AP |
|---|---|
| Issue | ER-10972 |
| Description | Resolved an issue where clients were unable to connect to WLAN until the affected AP is rebooted. |

| Component/s | AP |
|---|---|
| Issue | ER-10971, ER-10981 |
| Description | Client fingerprinting is now able to detect iOS 15.0, MAC OS 12.0, Windows 11 and Eye-Fi wireless memory card. |

| Component/s | AP |
|---|---|
| Issue | ER-10944 |
| Description | Resolved an issue where R850 may reboot due to kernel panic. |

| Component/s | AP |
|---|---|
| Issue | ER-10918 |
| Description | Resolved an issue where R710 may reboot due to kernel panic. |

| Component/s | AP |
|---|---|
| Issue | ER-10917, ER-11153 |
| Description | Resolved an issue where client may be unable to onboard in WISPr WLAN or get final redirection. |

| Component/s | AP |
|---|---|
| Issue | ER-10907 |
| Description | Resolved an issue where clients may be unable to connect to WLAN due to encrypted WLAN being broadcasted as open. |

| Component/s | AP |
|---|---|
| Issue | ER-10904 |
| Description | Resolved an issue where AP may end up offline and fails to update the configuration when using batch provisioning. |

| Component/s | AP |
|---|---|
| Issue | ER-10844 |
| Description | Resolved an issue where AP was not correctly clearing client stale entries. |

| Component/s | AP |
|---|---|
| Issue | ER-10837 |
| Description | Resolved an issue where random throughput/connectivity issues may be observed in R510. |

| Component/s | AP |
|---|---|
| Issue | ER-10824 |
| Description | Resolved an issue where client latency may be incorrectly reported as zero. |

| Component/s | AP |
|---|---|
| Issue | ER-10823 |
| Description | Resolved an issue where client may get redirected to landing page after being authorized in 802.1x+WISPr WLAN. |

| Component/s | AP |
|---|---|
| Issue | ER-10797 |
| Description | Resolved an issue where AP may lose connection with controller and clients may disconnect due to very high number of entries in AP DNS cache table. |

| Component/s | AP |
|---|---|
| Issue | ER-10795 |
| Description | Resolved an issue where R750 may reboot due to kernel panic. |

| Component/s | AP |
|---|---|
| Issue | ER-10775 |

| Component/s | AP |
|---|---|
| Description | Resolved an issue where AP would fail to update its configuration after upgrade if its device name has 64 characters. |

| Component/s | AP |
|---|---|
| Issue | ER-10746 |
| Description | Resolved an issue where clients may fail to connect to WLAN due to AP DNS spoof table getting disabled after an internal target assert. |

| Component/s | AP |
|---|---|
| Issue | ER-10656, ER-10607, ER-10725, ER-10890, ER-11137 |
| Description | Resolved an issue where 802.11ac wave 2 AP models may reboot due to kernel panic. |

| Component/s | AP |
|---|---|
| Issue | ER-10648 |
| Description | Resolved an issue where RADIUS accounting attribute *Acct-Session-Time* had incorrect value. |

| Component/s | AP |
|---|---|
| Issue | ER-10633 |
| Description | Resolved an AP packet forwarding issue in 802.11ac wave-1 APs related to background scanning being enabled. |

| Component/s | AP |
|---|---|
| Issue | ER-10593 |
| Description | Resolved an issue where some specific client devices could not complete DHCP DORA process when proxy ARP feature is enabled. |

| Component/s | AP |
|---|---|
| Issue | ER-10562 |
| Description | Resolved an issue where client redirection to Web authentication internal portal page may fail if LDAP authentication service was unreachable. |

| Component/s | AP |
|---|---|
| Issue | ER-10227 |
| Description | Resolved an issue where R750 may reboot due to target assert. |

| Component/s | AP |
|---|---|
| Issue | ER-10125 |
| Description | Resolved an issue where 802.11ax AP models may reboot due to kernel panic. |

| Component/s | AP |
|---|---|
| Issue | ER-8577 |

| **Component/s** | AP |
|---|---|
| **Description** | Resolved an issue where statistical information provided to RUCKUS SmartCell Insight (SCI) may result in discrepancies between total traffic sessions summary and binned sessions reports available in SCI. |

| **Component/s** | Control Plane |
|---|---|
| **Issue** | ER-10900 |
| **Description** | Resolved an issue where balanced AP connection to data planes was not working as expected. |

| **Component/s** | Control Plane |
|---|---|
| **Issue** | ER-11276 |
| **Description** | Resolved an issue where the controller RADIUS proxy process may restart on receiving certain unsupported specific 3rd party vendor attribute in *Access Accept* message. |

| **Component/s** | Data Plane |
|---|---|
| **Issue** | ER-11197 |
| **Description** | Resolved an issue where data plane upgrade using CLI from a release prior to 5.2 may fail and leave the device unrecoverable. |

| **Component/s** | Data Plane |
|---|---|
| **Issue** | ER-10058, ER-10631, ER-10635, ER-10694, ER-10912, ER-10819, ER-10866, ER-10954, ER-11247, ER-11269, ER-10538, ER-10550, ER-10871, ER-11097 |
| **Description** | Resolved an issue controller platforms SZ100/SZ144 in *One Port Group* mode or where data plane devices may become unreachable due to some malformed packet. |

| **Component/s** | Data Plane |
|---|---|
| **Issue** | ER-10611 |
| **Description** | Resolved an issue where data plane statistics were not displayed in the controller web user interface in case of large deployments. |

| **Component/s** | IoT |
|---|---|
| **Issue** | ER-10780, ER-10983 |
| **Description** | Resolved an issue where IoT devices may get disconnected from the network after AP software upgrade. |

| **Component/s** | Public API |
|---|---|
| **Issue** | ER-11316 |
| **Description** | Resolved an issue where SmartZone API */aps/totalCount* returned the error message *Permission denied (Access is denied)*. |

| **Component/s** | Switch Management |
|---|---|
| **Issue** | ER-11243 |
| **Description** | Resolved an issue where exported CSV file from Switches web user interface was empty. |

| **Component/s** | Switch Management |
|---|---|
| **Issue** | ER-11214 |
| **Description** | Resolved an issue where Switch could not be managed from the controller web user interface due to randomly disappearing Switch menu. |

| **Component/s** | Switch Management |
|---|---|
| **Issue** | ER-10765 |
| **Description** | Resolved an issue where Switch software upgrade may fail to start if managed by a node in a cluster with issues in internal scheduler. |

| **Component/s** | Switch Management |
|---|---|
| **Issue** | ER-10473 |
| **Description** | Resolved an issue where Switch alarm code 20008 was not displayed in controller web user interface. |

| **Component/s** | Switch Management |
|---|---|
| **Issue** | ER-10637 |
| **Description** | Resolved an issue where Switch may fail to be approved by the controller. |

| **Component/s** | Switch Management |
|---|---|
| **Issue** | ER-10719 |
| **Description** | Resolved an issue where Switch configuration backup was failing from the controller web user interface if switch had a banner. |

| **Component/s** | Switch Management |
|---|---|
| **Issue** | ER-10722 |
| **Description** | Resolved an issue where Switch software upgrade may timeout. |

| **Component/s** | Switch Management |
|---|---|
| **Issue** | ER-10836 |
| **Description** | Resolved an issue where switch may fail to reconnect to the controller cluster after restarting the leader node. |

| **Component/s** | System |
|---|---|
| **Issue** | ER-10948 |
| **Description** | Resolved an issue where a 3-node controller cluster may stay out-of-service when multiple node addition/removal operations are performed. |

| **Component/s** | System |
|---|---|
| **Issue** | ER-11121 |
| **Description** | Resolved an issue where SFTP connection could not be established due to incompatible security settings with server, resulting in failure to upload configuration backup. |

| **Component/s** | System |
|---|---|
| **Issue** | ER-11098 |
| **Description** | Resolved an issue where RADIUS NAS IP attribute is set incorrectly when configured as *Management/Control IP* for SZ144 controller model. |

| **Component/s** | System |
|---|---|
| **Issue** | ER-11072 |
| **Description** | Resolved an issue where *default* Account Security profile could change its domain and be deleted by deleting the domain and cause non-admin users unable to login to the controller. |

| **Component/s** | System |
|---|---|
| **Issue** | ER-11015 |
| **Description** | Resolved an issue where DNS spoofing profile rule did not accept hyphen character in domain name field. |

| **Component/s** | System |
|---|---|
| **Issue** | ER-10973 |
| **Description** | Resolved an issue where zones containing special characters in their names could not be configured in SmartZone CLI. |

| **Component/s** | System |
|---|---|
| **Issue** | ER-10959 |
| **Description** | Resolved an issue where controller patches (KSPs) may fail to get applied in SZ300 controller model. |

| **Component/s** | System |
|---|---|
| **Issue** | ER-10842 |
| **Description** | Resolved an issue where inconsistent Guest Pass counter is detected and automatically corrected. |

| **Component/s** | System |
|---|---|
| **Issue** | ER-10747 |
| **Description** | Resolved an issue where RADIUS NAS IP address attribute in WLAN configuration was disabled when authentication server was modified. |

| **Component/s** | System |
|---|---|
| **Issue** | ER-10729 |
| **Description** | Resolved an issue where SmartZone Essential controllers were unable to create a report in CLI filtering by AP. |

| **Component/s** | System |
|---|---|
| **Issue** | ER-10649 |
| **Description** | Resolved an issue where clients may fail to connect to portal WLANs due to receiving unexpected certificate. |

| Component/s | System |
|---|---|
| Issue | ER-10613 |
| Description | Resolved an issue where UPnP (Universal Plug and Play) service was still enabled in SZ100 even after successful setup. |

| Component/s | System |
|---|---|
| Issue | ER-10776 |
| Description | Resolved an issue where a new certificate may fail to get imported into controller. |

| Component/s | System |
|---|---|
| Issue | ER-10703 |
| Description | Resolved an issue where system may be unable to generate Guest passes due to incorrect internal counter. |

| Component/s | System |
|---|---|
| Issue | ER-10998 |
| Description | Resolved an issue where controller web services may fail to start. |

| Component/s | UI/UX |
|---|---|
| Issue | ER-11125 |
| Description | Resolved an issue where APs could be flagged in the controller web user interface even with threshold flag options was set to OFF. |

| Component/s | UI/UX |
|---|---|
| Issue | ER-10874 |
| Description | Improved controller web user interface performance in clusters with large database. |

| Component/s | UI/UX |
|---|---|
| Issue | ER-10943 |
| Description | Resolved an issue where SZ300 controller model had incorrect LED status behavior. |

| Component/s | UI/UX |
|---|---|
| Issue | ER-10923 |
| Description | Resolved an issue where incorrect switch stack information is provided in controller web user interface when some units are removed/added. |

| Component/s | UI/UX |
|---|---|
| Issue | ER-10831 |
| Description | Resolved a display issue in controller web user interface where it is shows duplicate entries for Switch VLAN and ACL. |

| Component/s | UI/UX |
|---|---|
| Issue | ER-10914 |

| **Component/s** | UI/UX |
|---|---|
| **Description** | Resolved an issue where internal controller web may be out of memory due to frequent API queries. |

| **Component/s** | UI/UX |
|---|---|
| **Issue** | ER-10651, ER-10495 |
| **Description** | Resolved an issue where incorrect RSSI and SNR values for clients connected are reported in the controller web user interface. |

| **Component/s** | UI/UX |
|---|---|
| **Issue** | ER-10660 |
| **Description** | Resolved an issue where a pop-up error may appear in *URL Filtering License* on the controller web user interface page. |

| **Component/s** | UI/UX |
|---|---|
| **Issue** | ER-10411 |
| **Description** | Resolved an issue where Switch tab in controller web user interface may fail to load with error message *Timeout when requesting data from SZ when admin user manages high number of switches and domains*. |

# 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 maintenance release.

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