RELEASE NOTES

RUCKUS SmartZone (LT-GD) Patch Release Notes, 6.1.2

Supporting ECDSA P256/P384 on build number 6.1.2.0.404

Part Number: 800-73549-001 Rev A
Publication Date: December 2023

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

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see https://www.commscope.com/trademarks. All product names, trademarks, and registered trademarks are the property of their respective owners.

Patent Marking Notice

For applicable patents, see www.cs-pat.com.

Contents

Document History

Revision Number	Summary of Changes	Publication Date
A	Initial *Release Notes*	22, December 2023

Overview of BSI C5 Compliance Mode

BSI C5 Cloud Mode supports certain information security requirements for cloud computing, referred to as Cloud Computing Compliance Controls Catalog (C5). The requirements were developed by the German Federal Office for Information Security (BSI).

BSI Compliance mode is enabled when a RUCKUS device is managed by a SmartZone controller that is configured for BSI C5 compliance and is using Elliptic Curve Digital Signature Algorithm (ECDSA) for public key certificate validation.

BSI Compliance mode can also be enabled through the CLI to make the device compliant with BSI C5 requirements for SSH, HTTPs-based image copy, and Web Management.

BSI Compliance Mode Supported Features

The following are the secure features in AP and SmartZone controller:

- Uses a stronger certificate and key in both client and server authentication.
- Removes weak ciphers and algorithms (TLS and SSH).
- RadSec (AAA) server certificate supports ECDSA-P256 and RSA-3072 certificates for Authentication and Accounting Services in proxy mode.

BSI Compliance Mode Limitations

The ECDSA certificate issued by SmartZone has the following limitations:

- The communication between Access Points (APs) does not adhere to BSI compliance standards.
- The communication between the controller (SmartZone) and the external SFTP server, which utilizes Java-based SSH, is not compliant with BSI (Bundesamt für Sicherheit in der Informationstechnik) standards.
- Virtual SmartZone Data Plane (vSZ-D) is not BSI compliant.
- The communication between Access Points (AP) and Data Plane (DP) in *Tunnel Mode*' does not adhere to BSI compliance standards.
- The current cluster communication exclusively employs unsecured channels, with neither SSH nor TLS in use. However, TLS communication is implemented specifically in *Cluster Backup Download* to ensure BSI compliance.
- APs do not have the capability to support RSA-3072 certificates.
- Zero-touch MESH is not compliant with BSI standards.

Release Information

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

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

ATTENTION
Upgrade from release 5.2.2.0.1562 to 6.1.2.0.354 requires a patch to be installed first. Please refer to https://support.ruckuswireless.com/documents/4223 for details.

ATTENTION
For Network Segmentation:

- Ensure that all ICX switches are upgraded to firmware version 09.0.10d (or any 09.0.10 patches that may become available after 09.0.10d) or version 10.0.10a (or any 10.0.10 patches that may become available after 10.0.10a).

SZ300

- Controller Version: **6.1.2.0.404**
- Control Plane Software Version: **6.1.2.0.208**
- Data Plane Software Version: **6.1.2.0.404**
- AP Firmware Version: **6.1.2.0.981**

SZ100/SZ124/SZ104

- Controller Version: **6.1.2.0.404**
- Control Plane Software Version: **6.1.2.0.208**
- Data Plane Software Version: **6.1.2.0.20**
- AP Firmware Version:**6.1.2.0.981**

SZ144

- Controller Version: **6.1.2.0.404**
- Control Plane Software Version: **6.1.2.0.208**
- Data Plane Software Version: **6.1.2.0.20**
- AP Firmware Version:**6.1.2.0.981**

vSZ-H and vSZ-E

- Controller Version: **6.1.2.0.404**
- Control Plane Software Version: **6.1.2.0.208**
- AP Firmware Version:**6.1.2.0.981**

ICX Models

- Supported ICX Firmware: **10.0.10c and 09.0.10j and subsequent patches**

Known Issues

IMPORTANT

A software fix has been delivered in Releases 6.1.1 and later in which the RSSI/SNR is more accurate for the prevailing RF conditions of the wireless network. The reported RSSI/SNR values have a +/- 3db variation from the mean value because the noise floor, while usually constant, could vary within that range.

Releases prior to 6.1.1 do not contain this fix. As a result, users upgrading from Release 6.0.0 to 6.1.1 and later releases will see a difference in RSSI/SNR values and should not assume any AP performance degradation in Releases 6.1.1 and later due to seeing lower RSSI/SNR values as compared to the previous releases. **[SCG-138506]**

Component/s	AP
Issue	AP-27160
Description	On enabling the 5.8GHz channel license, the configuration does not take effect.

Component/s	AP
Issue	SCG-146761
Description	Following the restoration of the SmartZone to version 3.6.2 with APs currently running on 6.1.2, there is an issue where the APs cannot establish a connection to the SmartZone due to a cipher mismatch.
Workaround	Move the APs to a version below 6.1.2.0.895 and then restore the SmartZone or SmartZone cluster to R3.6.2.

Resolved Issues with Code Changes in Release 6.1.2.0.404

The following are the resolved issues in this release.

Component/s	AP
Issue	ER-12386
Description	The access point (AP) fails to transmit the Service Set Identifier (SSID) following the upgrade.

Component/s	AP
Issue	ER-12480
Description	A memory leakage problem related to SNMP (Simple Network Management Protocol).

Component/s	AP
Issue	ER-12492
Description	The problem involves a flip-flop between LTE and Ethernet interfaces, likely caused by the external site being intermittently reachable.

Component/s	AP
Issue	ER-12565
Description	An issue with the forwarding of VLAN packets.

Component/s	AP
Issue	ER-12634
Description	APs were rebooting with kernel panic.

Component/s	AP
Issue	ER-12671
Description	The overridden 5G DFS channels in AP Groups persist even after disallowing 5G DFS channels in the zone.

Component/s	AP
Issue	ER-12687
Description	Unable to delete DPSK (Dynamic Pre-Shared Key) and its absence from the *get DPSKs* API call due to DPSK data corruption.

Component/s	AP
Issue	ER-12719
Description	In the controller the issue has been fixed wherein changing the country code in the zone configuration did not result in a modification of the default AP Group configuration. On the APs the 5G channels for certain country codes have been updated to address outdated information.

Resolved Issues with Code Changes in Release 6.1.2.0.404

Component/s	AP
Issue	ER-12762
Description	Disconnection of all access points (APs) due to a proxy connection leak.

Component/s	AP
Issue	ER-12767
Description	Multiple R510s rebooted due to a kernel panic issue.

Component/s	AP
Issue	ER-12842
Description	APs rebooted due to target assert and kernel panic.

Component/s	AP
Issue	ER-12899
Description	User Equipment (UE) authentication failure with tunneled WLAN and AP configuration management VLAN.

Component/s	AP
Issue	ER-12962
Description	Incorrect Ethernet port mapping for the T750/SE APs was the cause for AP offline issues.

Component/s	AP
Issue	ER-12970
Description	Resolved a kernel panic seen in the 802.11ax driver.

Component/s	AP
Issue	ER-13016
Description	The second Ethernet port was disabled on the T750 AP.

Component/s	AP
Issue	ER-13048
Description	Access Points were unable to receive Aeroscout and Ekahau RTLS tag frames.

Component/s	AP
Issue	ER-13066
Description	Resolved an issue with Dynamic VLAN (DVLAN) during Fast Transition (FT) roaming.

Component/s	AP
Issue	ER-13075
Description	The values displayed by the **get airtime** AP CLI command was incorrect.

Component/s	AP
Issue	ER-13163
Description	Incorrect Ekahau content was transmitted to the server due to Frame Check Sequence (FCS) errors.

Component/s	Control Plane
Issue	ER-12876
Description	Enhanced the output text for the **service restart** CLI command.

Component/s	Control Plane
Issue	ER-12551
Description	Enhanced the CLI command **service restart** to include the restart of Control Plane, addressing and resolving issues related to the automatic recovery failure of Control Plane applications.

Component/s	System
Issue	ER-12527
Description	The Operator Profile was not being populated while modifying the HS20 WLAN Profile.

Component/s	UI/UX
Issue	ER-12921
Description	Ports 13 to 16 are not visible on the user interface (UI) for the ICX8200-24FX.

Component/s	Virtual SmartZone
Issue	ER-12874
Description	Delay in the delivery of mail notifications when the controller interface experienced a brief period of downtime and was subsequently restored.

Component/s	Virtual SmartZone
Issue	ER-12992
Description	The recently introduced CLI configuration command, **ssh-security-level**, allows users to disable *diffie-hellman-group-exchange-sha1* and *hmac-sha1* by setting it to medium or high levels.

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