RELEASE NOTES

# RUCKUS SmartZone (LT-GA) Release Notes, 7.1.0

## Supporting SmartZone R7.1.0

*Part Number: 800-73624-001 Rev A*
*Publication Date: December 2024*

# 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* | December 19, 2024 |

# New Features in SmartZone 7.1.0

The following outlines the hardware and software features introduced in SmartZone release R7.1.0.

## New Software Features

This section describes the new and enhanced software features introduced in SmartZone release R7.1.0.

| Feature | Description |
|---|---|
| **Additional Hotspot 2.0 (Passpoint) Data Points** | Specific data points, including Access Network Query Protocol (ANQP) request and response counts, will now be collected from both APs and SmartZone systems. These data points will be integrated into RUCKUS AI, enabling enhanced analysis and insights. |
| **AFC Phase 2 Features** | An enhancement is implemented to ensure that Low Power Indoor (LPI) mode is disabled for outdoor 6 GHz APs, effectively restricting LPI mode from being used on outdoor APs. |
| **CALEA Support in SmartZone** | Communications Assistance for Law Enforcement Act (CALEA) support has been removed in SZ/vSZ release 7.1.1. Users who need CALEA support will need to utilize versions earlier than SZ/vSZ release 7.1.1 (for example, 7.1.0, 7.0, 6.1.2). |
| **Dynamic Pre-Shared Key (DPSK3) Enhancement** | The Dynamic Pre-Shared Key version 3 (DPSK3) enhancement optimizes the overall design to improve the end-user's connectivity experience, including while steering between WLANs. |
| **ICX Switch Features and Enhancements** | • **Pre-Provisioning the Controller** - SmartZone now supports importing a *CSV* file to manage switch association with the desired **Switch Group**.<br>• **Increase Port Profile VLAN Limit** - Added support for editing port settings directly from the **Front Panel** view by double-clicking on a port.<br>• **Double click for port configuration** - User information is now included in all SmartZone- initiated configuration change or update logs.<br>• **Create an ICX CLI template from an existing ICX backup** - SmartZone now supports selecting an existing switch configuration backup and converting it into a CLI template, enabling bulk deployment to other selected switches.<br>• **SmartZone ICX logging improvements** -The port template now supports defining a range of VLANs, eliminating the need to type each VLAN individually.<br>• **BGP EVPN VxLAN Management** - SmartZone now supports provisioning ICX switches with BGP EVPN including Dual Homing.<br>• **Geo Redundancy Active-Active Support** - SmartZone now supports **Active-Active Geo Redundancy** mode for switches. |
| **IPv6 Controller to RAI Communication** | The cross-platform high-performance remote procedure call (gRPC) network protocol used for communication between RUCKUS AI and SmartZone now includes support for IPv6, ensuring compatibility with modern IP addressing standards. |

| Feature | Description |
|---|---|
| **SmartZone IPv6 Deployment** | SmartZone now includes support for IPv6 addresses as part of the IPv6 initiative for Federal support. |
| **SmartZone Secure Communication Enhancements** | SmartZone generated certificates are now signed using a 3072-bit key length. |
| **Virtual SmartZone Support on Proxmox Hypervisor** | Virtual SmartZone now offers support for the Proxmox Hypervisor. |
| **Enhancements** | • The SmartZone cluster upgrade mechanism is enhanced to efficiently handle firmware upgrades, even when **Elasticsearch** is in a busy or RED state.<br>• The RabbitMQ version is upgraded, enhancing cluster stability and improving AP and switch management during node outages. |

# RUCKUS Standard AP LED Description for Wi-Fi 7 Capable APs

The specified LED states for Wi-Fi 7 capable APs are outlined as follows. The LED is designed to transition from *Red* to *Amber* to *Green*. Additionally, there are exception states listed, which will only be activated if the AP is engaged in specific functions as defined below.

**TABLE 1** LED Color, Description, and Patterns

| LED Color | Description | Light Pattern |
|---|---|---|
| Red | AP is in the process of determining its power mode. | Solid Red |
| | AP is currently operating in IEEE 802.3af power mode. | Slow Blinking Red |
| | AP is currently undergoing a factory reset. | Blinking (alternating Red and Green) |
| Amber | AP has an adequate power supply and is currently in the process of booting up. | Solid Amber |
| | AP is currently in setup mode. | Blinking Amber |
| | AP has lost connectivity to the system controller interface. | Slow Blinking Amber |
| | AP is currently undergoing a firmware or configuration update. | Fast Blinking Amber |
| Green | WLAN services and controller management on the AP are currently operational. | Solid Green |
| | The WLAN on the AP has at least one client connected. | |
| | The WLAN on the AP has at least one client connected, and mesh networking is enabled. | |

# Countries Supported on 6GHz

Wi-Fi 7 APs and the 320MHz channel are supported in controller version R7.1.0 for the following country codes.

1. Countries supported on 6Ghz U-NII frequency bands 5, 6, 7, and 8 supporting channels: 1, 5, ..., 233:
   - BR: Brazil
   - CA: Canada
   - CL: Chile
   - CO: Colombia
   - DO: Dominican Republic
   - HN: Honduras

- KR: South Korea
- PE: Peru
- PG: Papua New Guinea
- SA: Saudi Arabia
- SV: El Salvador
- US: United States

2. Countries supported on 6Ghz U-NII frequency band 5 supporting channels: 1, 5, ..., 93:
   - AE: United Arab Emirates
   - AL: Albania
   - AT: Austria
   - AU: Australia
   - AZ: Azerbaijan
   - BE: Belgium
   - BH: Bahrain
   - BG: Bulgaria
   - BN: Brunei
   - BZ: Belize
   - BY: Belarus
   - CH: Switzerland
   - CY: Cyprus
   - CZ: Czech Republic
   - DE: Germany
   - DK: Denmark
   - EE: Estonia
   - EH: Western Sahara
   - ES: Spain
   - FI: Finland
   - FR: France
   - GB: United Kingdom
   - GR: Greece
   - HK: Hong Kong
   - HR: Croatia
   - HU: Hungary
   - IE: Ireland
   - IL: Israel
   - IS: Iceland
   - IT: Italy
   - JO: Jordan
   - JP: Japan

- KE: Kenya
- KW: Kuwait
- LI: Liechtenstein
- LT: Lithuania
- LU: Luxembourg
- LV: Latvia
- MA: Morocco
- MC: Monaco
- MN: Mongolia
- MO: Macau
- MT: Malta
- MU: Mauritius
- MX: Mexico
- MY: Malaysia
- NL: Netherlands
- NO: Norway
- PL: Poland
- PT: Portugal
- QA: Qatar
- RO: Romania
- RU: Russia
- SE: Sweden
- SG: Singapore
- SI: Slovenia
- SK: Slovakia
- TH: Thailand
- TR: Turkey
- TW: Taiwan
- ZM: Zambia
- ZA: South Africa
- ZW: Zimbabwe

# Hardware and Software Support

## Overview

This section provides release information about SmartZone controllers and Access Point features.

- The SZ300 RUCKUS Networks flagship, large-scale WLAN controller is designed for Service Providers 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 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.
- The Virtual SmartZone (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 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 an NFV-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 SZ144-D is the second-generation Data Plane hardware appliance which is functionally equivalent to the vSZ-D virtual Data Plane. The appliance provides turnkey deployment capabilities for customers who need a hardware appliance. The SZ144-D is managed by a vSZ Controller only and cannot work in a standalone mode.

## Release Information

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

RUCKUS recommends the SmartZone R7.1.0 release for users of Wi-Fi 7 APs. For users with legacy APs that are not End-of-Support (EOS), RUCKUS suggests using the SmartZone R6.1.2 release along with its patch updates.

**ATTENTION**
It is recommended to upgrade the vSZ controller before updating the vSZ-D version. If the data plane version exceeds the vSZ controller version, the data plane cannot be managed by the vSZ platform.

**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 10.0.10b (or any 10.0.10 patches that may become available after 10.0.10b).

**CAUTION**
**SmartZone upgrade from R6.1.2.0 Patch 3 to R7.1.0 is not supported. Refer to the Technical Support Bulletin for details regarding the upgrade limitation - https://support.ruckuswireless.com/technical_support_bulletins/642.**

**NOTE**
RUCKUS IoT version R2.2.0 and 2.2.1.0 MR is not compatible with controller version R7.1.0.

### *SZ300*

- Controller Version: **7.1.0.0.586**
- Control Plane Software Version: **7.1.0.0.440**

- Data Plane Software Version: **7.1.0.0.586**
- AP Firmware Version: **7.1.0.0.915**

### *SZ144*

- Controller Version: **7.1.0.0.586**
- Control Plane Software Version: **7.1.0.0.440**
- Data Plane Software Version: **7.1.0.0.73**
- AP Firmware Version: **7.1.0.0.915**

### *vSZ-H and vSZ-E*

- Controller Version: **7.1.0.0.586**
- Control Plane Software Version: **7.1.0.0.440**
- AP Firmware Version: **7.1.0.0.915**

### *vSZ-D/144D*

- Data plane software version: **7.1.0.0.586**

## *Upgrade Information*

- Users on SmartZone R6.1.0, 6.1.1, 6.1.2, and 7.0.0 can upgrade to GA base release R7.1.0. However, versions prior to R6.1.0 are not eligible for this upgrade.
- Fresh installations are supported.
- The following SmartZone upgrade paths to R7.1.0 are supported:
  - Upgrade from R6.1.2 Patch 2 to R7.1.0.
  - Upgrade from R7.0.0 and its subsequent patches to R7.1.0.

## *Dynamic Signature Package Update*

Administrators or users can dynamically upgrade the Signature Package from the RUCKUS support site. Signature Package version 1.670.2 is applicable for SmartZone R7.0.0 and R7.1.0.

Follow the steps below to execute a manual upgrade:

1. Download the Signature Package from the RUCKUS support site:
   - SmartZone R7.1.0 Signature Package version 1.670.2: https://support.ruckuswireless.com/software/4220-smartzone-7-0-0-st-ga-patch-2-sigpack-v2-1-670-2-application-signature-package.
   - SmartZone R7.1.0 Signature Package version 1.670.2-regular: https://support.ruckuswireless.com/software/4221-smartzone-7-0-0-st-ga-patch-2-ruckussigpack-v2-1-670-2-regular-application-signature-package.
2. Manually upgrade the Signature package by navigating to **Security** > **Application Signature Package**.

   **NOTE**
   For more information, refer to the **Application Signature Packages** in *RUCKUS SmartZone (LT-GA) Controller Administration Guide, 7.1.0*

**NOTE**
Upgrading to R7.1.0 from versions earlier than R6.1.0 is not supported. It is important to note that RUCKUS does not impose any signature-package upgrade restrictions during the Zone upgrade process.

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

Refer to *RUCKUS SmartZone Getting Started on SZ GPB/MQTT Interface* and download the latest `SmartZone GPB.proto files` from the RUCKUS support site:

1. SmartZone **7.1.0** (GA) GPB.proto (Google ProtoBuf) image for GPB/MQTT [DNP] - https://support.ruckuswireless.com/software/4301-smartzone-7-1-0-ga-gpb-proto-google-protobuf-image-for-gpb-mqtt.
2. SmartZone **7.1.0** MockSCI-TLS (SZ to SCI MQTT subscriber software) for CentOS/Ubuntu - https://support.ruckuswireless.com/software/4302-smartzone-7-1-0-ga-mocksci-tls-sz-to-sci-mqtt-subscriber-software-for-centos-ubuntu.

### *Public API*

Click on the following links to view Public API documents:

- *SmartZone 7.1.0 Public API Reference Guide (ICX Management)*

  https://support.ruckuswireless.com/documents/4931
- *SmartZone 7.1.0 Public API Reference Guide (SZ144)*

  https://support.ruckuswireless.com/documents/4932
- *SmartZone 7.1.0 Public API Reference Guide (SZ300)*

  https://support.ruckuswireless.com/documents/4933
- *SmartZone 7.1.0 Public API Reference Guide (vSZ-E)*

  https://support.ruckuswireless.com/documents/4934
- *SmartZone 7.1.0 Public API Reference Guide (vSZ-H)*

  https://support.ruckuswireless.com/documents/4935

## Supported Matrix and Unsupported Models

Before upgrading to this release, check if the controller is currently managing APs, Switches, or IoT devices.

APs preconfigured with the SmartZone AP firmware may be used with SZ300 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 the controller if Solo APs running 104.x are being moved under controller 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 or later can connect to both Zone Director and SmartZone platforms. If an AP is running release 104.x or later and the LWAPP2SCG service is enabled on the controller, a race condition will occur.

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

## *Supported AP Models*

This release supports the following RUCKUS AP models. All RUCKUS APs support IEEE 802.11 standards.

**TABLE 2** Supported AP Models

| Wi-Fi 6 (802.11ax) | | Wi-Fi 6E (802.11ax) | Wi-Fi 7 (802.11be) | |
|---|---|---|---|---|
| **Indoor** | **Outdoor** | **Indoor** | **Indoor** | **Outdoor** |
| R850 | T750SE | R760 | R770 | T670 |
| R750 | T750 | R560 | R670 | |
| R650 | T350C | | | |
| R550 | T350SE | | | |
| R350 | T350D | | | |
| R350e | | | | |
| H550 | | | | |
| H350 | | | | |

The following lists the supported AP models in this SmartZone release when placed in an AP Zone that uses an older AP version.

**ATTENTION**
The R730 AP must be removed from the AP Zone before upgrading the AP Zone to the AP firmware version 6.1.1 or later.

**ATTENTION**
For APs that are not compatible with R7.1.0, it is essential to maintain them with AP firmware versions of R6.1, 6.1.1, 6.1.2, and 7.0.0 and its subsequent patches. The upgrade of the Zone for APs that are not supported in R6.1, 6.1.1, 6.1.2, and 7.0.0 and its subsequent patches is not feasible.

**TABLE 3** Supported AP Models for AP Zones Using Older AP Versions

| Wi-Fi 6 (802.11ax) (supported on R6.1.0, 6.1.1, and 6.1.2) | Wi-Fi 5 (802.11ac Wave 2) | |
|---|---|---|
| | **Indoor** | **Outdoor** |
| T750SE | R720 | T811CM |
| T750 | R710 | T710S |
| T350SE | R610 | T710 |
| T350D | R510 | T610S |
| T350C | R320 | T610 |
| R850 | M510 | T310S |
| R760 (not supported on R6.1.0) | H510 | T310N |
| R750 | H320 | T310D |
| R730 | C110 | T310C |
| R650 | | T305I |
| R560 (not supported on R6.1.0) | | T305E |
| R550 | | E510 |
| R350 | | |
| H550 | | |
| H350 | | |

**ATTENTION**
AP R310 is Wave 1 and supports WPA3 – this is the one exception, the rest of the APs that support WPA3 are IEEE 802.11ac Wave 2 or IEEE 802.11ax.

### *Unsupported AP Models*

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

**TABLE 4** Unsupported AP Models

| Unsupported AP Models | | | | |
|---|---|---|---|---|
| SC8800-S | SC8800-S-AC | ZF2741 | ZF2741-EXT | ZF2942 |
| ZF7025 | ZF7321 | ZF7321-U | ZF7341 | ZF7343 |
| ZF7343-U | ZF7351 | ZF7351-U | ZF7363 | ZF7363-U |
| ZF7441 | ZF7761-CM | ZF7762 | ZF7762-AC | ZF7762-S |
| ZF7762-S-AC | ZF7762-T | ZF7962 | ZF7781CM | ZF7982 |
| ZF7782-S | ZF7782-E | ZF7782 | ZF7372-E | ZF7372 |
| ZF7352 | ZF7055 | R300 | R310 | R700 |
| C500 | H500 | R600 | R500 | R310 |
| R500E | T504 | T300 | T300E | T301N |
| T301S | FZM300 | FZP300 | | |

## Supported ICX Models

The following ICX switch models can be managed from SmartZone:

**TABLE 5** ICX Firmware Versions Compatible with SmartZone

| ICX Model | First Supported FastIron Release | Last Supported FastIron Release |
|---|---|---|
| ICX 7150[1] | 08.0.80a | 09.0.10a and subsequent patches |
| ICX 7150-C08P, -C08PT, -24F, -10ZP | 08.0.92 | 09.0.10a and subsequent patches |
| ICX 7250 | 08.0.80a | 09.0.10a and subsequent patches |
| ICX 7450 | 08.0.80a | 09.0.10a and subsequent patches |
| ICX 7550 | 08.0.95a | - |
| ICX 7650 | 08.0.80a | - |
| ICX 7750 | 08.0.80a | 08.0.95 and subsequent patches |
| ICX 7850 | 08.0.90 | - |
| ICX 7850-48C | 09.0.10a | - |
| ICX 8200[2] | 10.0.00 | - |
| ICX 8200-24ZP, -48ZP2, -24FX, -24F, -48F, -C08ZP | 10.0.10 | - |

The following table defines ICX and SmartZone release compatibility.

[1] SmartZone does not support ICX 7150-ES models.
[2] SmartZone does not currently support the ICX 8200-24PV and ICX 8200-C08PFV models. Support for these models will be added in a future release.

**NOTE**
ICX switches must be running FastIron 08.0.80a at a minimum to connect to SmartZone. An ICX switch running unsupported firmware can still connect to the SmartZone controller. After the switch is connected, you must upgrade it to a firmware version that is compatible with the SmartZone controller version. This can be achieved using the switch firmware upgrade option in the Switch Group or by selecting one or more switches and performing the upgrade.

**NOTE**
FastIron 09.0.10a and later releases support management by SmartZone 6.1 and later.

**NOTE**
ICX switches with FIPS mode enabled do not support management by SmartZone.

**TABLE 6** ICX and SmartZone Release Compatibility Matrix

| | SmartZone 5.1.1 | SmartZone 5.1.2 | SmartZone 5.2 | SmartZone 5.2.1 / 5.2.2 | SmartZone 6.0 | SmartZone 6.1 | SmartZone 6.1.1 | SmartZone 6.1.2 | SmartZone 7.0.0 | SmartZone 7.1 |
|---|---|---|---|---|---|---|---|---|---|---|
| FastIron 08.0.90a | Yes | Yes | Yes | Yes | Yes | No | No | No | No | No |
| FastIron 08.0.91 | Yes | Yes | Yes | No | No | No | No | No | No | No |
| FastIron 08.0.92 | No | Yes | Yes | Yes | Yes | Yes | No | No | No | No |
| FastIron 08.0.95 and subsequent patches | No | No | No | No | Yes | Yes | Yes | Yes | No | No |
| FastIron 09.0.10a and subsequent patches | No | No | No | No | No | Yes | Yes | Yes | Yes | Yes |
| FastIron 10.0.00 and subsequent patches | No | No | No | No | No | No | Yes | Yes | Yes | Yes |
| FastIron 10.0.10 and subsequent patches | No | No | No | No | No | Yes | Yes | Yes | Yes | Yes |
| FastIron 10.0.20 and subsequent patches | No | No | No | No | No | Yes | Yes | Yes | Yes | Yes |

The following table provides details on switch management feature compatibility between ICX and SmartZone releases.

**TABLE 7** Switch Management Feature Compatibility Matrix

| Feature | SmartZone 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 |
| Remote CLI Change | 5.2.1 and later | 08.0.90 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-144 / vSZ-E | 5.1.2 and later | 08.0.90a and later |
| DNS-based SmartZone Discovery | 5.1.2 and later | 08.0.95c and later |
| Download Syslogs for a Selected Switch[3] | 5.2.1 and later | 08.0.92 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[4] |
| Change Default VLAN | 5.2.1 and later | 08.0.95 and later |
| Configure the PoE Budget per Port on ICX through the Controller GUI with 1W Granularity | 5.2.1 and later | 08.0.95 and later |
| Configuring Protected Ports | 5.2.1 and later | 08.0.95 and later |
| Configuring QoS | 5.2.1 and later | 08.0.95 and later |
| Configuring Syslog | 5.2.1 and later | 08.0.95 and later |
| Geo Redundancy Active-Standby Mode | 6.0 and later | 08.0.95b and later |
| Generic CLI Configuration | 6.0 and later | 08.0.95b and later |
| Port-Level Override | 6.0 and later | 08.0.95b and later |
| Port-Level Storm Control Configuration | 6.1 and later | 08.0.95 and later |
| IPv6 Support (connection through static configuration only) | 6.1 and later | 09.0.10a and later |
| Save Boot Preference | 6.1 and later | 09.0.10a and later |
| Virtual Cable Testing | 6.1 and later | 09.0.10a and later |
| Blink LEDs | 6.1 and later | 09.0.10a and later |
| Send Event Email Notifications at Tenant Level | 6.1 and later | 09.0.10a and later |

[3] To download system logs from SmartZone for a particular ICX switch, TFTP must be enabled.
[4] FastIron 10.0.00 and later releases do not support management VLANs.

**TABLE 7** Switch Management Feature Compatibility Matrix (continued)

| Feature | SmartZone Release | ICX FastIron Release |
|---|---|---|
| Update the status of a Switch | 6.1 and later | 09.0.10a and later |
| Convert Standalone Switch | 6.1 and later | 09.0.10a and later |
| Flexible Authentication Configuration | 6.1 and later | 09.0.10a and later |
| Network Segmentation | 6.1.1 and later | 09.0.10d and later[5] |
| Breakout Port Support | 7.0.0 and later | 09.0.10h and later |
| Enhancement in Firmware Upgrade Status | 7.0.0 and later | 09.0.10h and later |
| SmartZone Usernames in ICX Syslogs | 7.0.0 and later | 09.0.10h and later, 10.0.10c and later |
| Configuring Separate Authentication and Accounting in AAA server | 7.0.0 and later | 09.0.10h and later |
| Geo Redundancy Active-Active Mode | 7.1.0 and later | 10.0.20a and later |
| BGP EVPN VxLAN Management | 7.1.0 and later | 10.0.20a and later |

# Product Documentation

The product guides for R7.1.0 are updated. Refer to the *New in this Document* section in each publication for detailed changes.

**TABLE 8** Product Guides

| Category | Name of The Guide |
|---|---|
| **User and Administrator Guides** | • *RUCKUS SmartZone (ST-GA) SmartZone Upgrade Guide, 7.1.0*<br>• *RUCKUS SmartZone (LT-GA) Network Administration Guide, 7.1.0*<br>• *RUCKUS SmartZone (LT-GA) Access and Security Services Guide, 7.1.0*<br>• *RUCKUS SmartZone (LT-GA) Controller Administration Guide, 7.1.0*<br>• *RUCKUS SmartZone (LT-GA) Troubleshooting and Diagnostics, 7.1.0*<br>• *RUCKUS SmartZone (LT-GA) Tunnel and Data Plane, 7.1.0* |
| **Interface Guides** | • *RUCKUS SmartZone (ST-GA) Tunnelling Interface Reference Guide, 7.1.0*<br>• *RUCKUS SmartZone (ST-GA) Alarm and Event Reference Guide, 7.1.0*<br>• *RUCKUS SmartZone (ST-GA) AAA Interface Reference Guide, 7.1.0*<br>• *RUCKUS SmartZone (ST-GA) Hotspot WISPr Interface Reference Guide, 7.1.0*<br>• *RUCKUS SmartZone (ST-GA) Hotspot 2.0 Reference Guide, 7.1.0*<br>• *RUCKUS SmartZone (ST-GA) SNMP Reference Guide (SZ300/vSZ-H), 7.1.0*<br>• *RUCKUS SmartZone (ST-GA) SNMP Reference Guide (SZ144/vSZ-E), 7.1.0*<br>• *RUCKUS SmartZone (ST-GA) Command Reference Guide, 7.1.0*<br>• *RUCKUS SmartZone (ST-GA) Getting Started on SZ GPB/MQTT Interface, 7.1.0* |
| **Release Independent Guides** | • *RUCKUS SmartZone 100, SmartZone 144 Getting Started Guide*<br>• *RUCKUS Virtual SmartZone Quick Setup Guide (vSZ)*<br>• *RUCKUS Virtual SmartZone Data Plane Configuration Guide*<br>• *RUCKUS Virtual SmartZone Getting Started Guide* |

[5] As an exception, FastIron release 10.0.00 does not support this feature.

**TABLE 8** Product Guides (continued)

| Category | Name of The Guide |
|---|---|
| **API Reference Guide** | • *RUCKUS SmartZone 7.1.0 (LT-GA) Public API Reference Guide (SZ144)*<br>• *RUCKUS SmartZone 7.1.0 (LT-GA) Public API Reference Guide (SZ300)*<br>• *RUCKUS SmartZone 7.1.0 (LT-GA) Public API Reference Guide (vSZ-E)*<br>• *RUCKUS SmartZone 7.1.0 (LT-GA) Public API Reference Guide (vSZ-H)*<br>• *RUCKUS SmartZone 7.1.0 (LT-GA) Public API Reference Guide (ICX Management)* |

# Known Issues

This section outlines known behaviors and provides recommended workarounds, if available.

## AP Limitations

| **Component/s** | AP |
|---|---|
| **Issue** | AP-38228 |
| **Description** | The radio of Band Steering and Transition Management (BTM) events are reported as 5GHz for the upper 5GHz band. |

| **Component/s** | AP |
|---|---|
| **Issue** | AP-35011 |
| **Description** | Service validation consistently fails due to a Domain Name System (DNS) failure for APs that support only IPv6. |

| **Component/s** | AP |
|---|---|
| **Issue** | AP-28483 |
| **Description** | Clients are disconnected due to excessive retries during roaming. |

| **Component/s** | AP |
|---|---|
| **Issue** | AP-32774 |
| **Description** | Occasionally, in some dense deployments, client roaming events may fail to populate, which can result in missing events on the controller **Event Log** and on the RUCKUS AI **Troubleshooting** page. |

| **Component/s** | Control Plane |
|---|---|
| **Issue** | SCG-159040 |
| **Description** | **Self-sign Guest Pass** creation fails if the special character '#' is used in the **Guest Pass** username credential. |

| **Component/s** | Control Plane |
|---|---|
| **Issue** | SCG-161322 |
| **Description** | While executing the Administrator Authentication, Authorization, and Accounting (AAA) test using the Protected Extensible Authentication Protocol (PEAP), the Calling-Station-ID is incorrectly sent in the RADIUS **Access-Request** message. |

| Component/s | AP |
|---|---|
| **Issue** | AP-37777 |
| **Description** | The downlink performance may be slightly reduced when using SoftGRE on the AP R670. |

| Component/s | AP |
|---|---|
| **Issue** | AP-37234 |
| **Description** | AP channel recovery is not working as expected. APs remain limited in a 20MHz channel width after DFS radar signal disappears. |

| Component/s | AP |
|---|---|
| **Issue** | AP-37253 |
| **Description** | Location-Based Services (LBS) is not supported on the 6GHz radio. |

| Component/s | AP |
|---|---|
| **Issue** | AP-35718, AP-32531, AP-35075 |
| **Description** | An intermittent drop in Modulation and Coding Scheme (MCS) has been observed during longevity testing. |

| Component/s | AP |
|---|---|
| **Issue** | AP-35910 |
| **Description** | During longevity tests, clients may disconnect, and the AP may not accept new client connections under certain conditions. |
| **Workaround** | Reboot the AP to restore normal operation. |

| Component/s | AP |
|---|---|
| **Issue** | SCG-151928 |
| **Description** | It is recommended to use 802.3bt or direct current (DC) power for the R560, R760, and R770 APs when connecting a wired client to the AP. Using 802.3at power on the R560, R760, or R770 will disable the Ethernet 0 port. |

| Component/s | AP |
|---|---|
| **Issue** | AP-33568 |
| **Description** | T670 and R670 APs do not support the thermal throttling mechanism. |

| Component/s | AP |
|---|---|
| **Issue** | SCG-142998 |
| **Description** | For 802.11ax or later AP models: When the user selects the PoE Operating Mode as 802.3at, by design, the USB Port option is forcibly turned off (the toggle is grayed out and cannot be enabled). Subsequently, when the user changes the PoE Operating Mode to Auto, the USB Port toggle changes to edit mode; however, the controller web user interface does not automatically enable the USB Port option. If USB functionality is desired, you must manually enable the USB Port option. |
| **Workaround** | If USB functionality is desired, manually enable the USB Port option. |

| Component/s | AP |
|---|---|
| **Issue** | SCG-142102 |
| **Description** | There is a disparity in the Time To Live (TTL) definition between Link Layer Discovery Protocol (LLDP) version 0.7.1 and version 1.0.15 as outlined below:<br>• LLDP 1.0.15 defines TTL as hold time multiplied by the interval (TTL = hold time * interval). In contrast, LLDP 0.7.1 defines TTL as equal to the hold time (TTL = hold time).<br>• The default interval in LLDP 1.0.15 is set to 30 seconds.<br>Following are the TTL examples in LLDP 1.0.15.<br>• If hold time is set to 10 seconds, TTL is calculated as 30 * 10 = 300 seconds.<br>• If hold time is set to 200 seconds, TTL is calculated as 30 * 200 = 6,000 seconds.<br>• If hold time is set to 500 seconds, TTL is calculated as 30 * 500 = 15,000 seconds.<br>• If hold time is set to 1000 seconds, TTL is calculated as 30 * 1000 = 30,000 seconds. |

| Component/s | AP |
|---|---|
| **Issue** | AP-26728 |
| **Description** | The Deep Packet Inspection (DPI) system may be unable to detect or classify ongoing traffic during roaming because of the contextual information associated with the initial control flow. |

| Component/s | AP |
|---|---|
| **Issue** | AP-25573 |
| **Description** | The Fast Transition (FT) framework mechanism does not support Pairwise Master Key - R1 (PMKR1) key re-dispatch to the Access Point (AP) that has newly joined the mobility domain. |

| Component/s | AP |
|---|---|
| **Issue** | AP-24758 |
| **Description** | Uplink traffic associated with multicast, including protocols like Internet Group Management Protocol (IGMP) (224.0.0.22), may experience rate limiting. This restriction occurs because only certain IGMP control packets, such as *IGMP_MEMBERSHIP_REPORT* and *IGMP_HOST_LEAVE*, are recognized as known multicast traffic, leading to potential rate limitations. |

| Component/s | AP |
|---|---|
| **Issue** | AP-26297 |
| **Description** | AP R560 does not support IEEE 802.3az Energy Efficient Ethernet (EEE). |

| Component/s | AP |
|---|---|
| **Issue** | AP-33444 |
| **Description** | Under heavy load conditions, Wi-Fi 7 clients experience reduced throughput performance compared to Wi-Fi 6E clients on the same network. |

| Component/s | AP |
|---|---|
| **Issue** | SCG-143239 |
| **Description** | The throughput of the 6GHz radio on the AP R560 or R760 decreases under heavy load conditions, particularly when Wi-Fi 6E clients are connected. |

| Component/s | AP |
|---|---|
| **Issue** | AP-32531 |
| **Description** | Throughput performance may drop in certain conditions when a mix of scaled 802.11ac and 802.11ax clients connect to a Wi-Fi 7 AP. |

| Component/s | AP |
|---|---|
| **Issue** | SCG-146150 |
| **Description** | AP R760 6Ghz radio supports up to 30 Microsoft Teams calls, encompassing both voice and video, without any lag. |

| Component/s | AP |
|---|---|
| **Issue** | AP-33145 |
| **Description** | The AeroScout Wi-Fi 6E and Wi-Fi 7 APs are unable to send Tag reports. |

| Component/s | AP |
|---|---|
| **Issue** | AP-34774 |
| **Description** | Random client roaming failures due to *Invalid FTIE* (Fast Transition Information Element) are observed when the AP is configured with WPA2/WPA3 mixed mode and 802.11r enabled. This behavior is not observed with WPA2 or WPA3 configurations. |

| Component/s | AP |
|---|---|
| **Issue** | AP-32419 |
| **Description** | The downlink performance of R670 with 320MHz is slightly lower compared to the R770 performance. |

| Component/s | AP |
|---|---|
| **Issue** | AP-32827 |
| **Description** | Downlink performance with RUCKUS GRE might be slightly lower than uplink performance for APs R670 or T670. |

| Component/s | AP |
|---|---|
| **Description** | When using Automated Frequency Coordination (AFC), the APs transmit power is capped by both Power Spectral Density (PSD) and Maximum Effective Isotropic Radiated Power (EIRP), using the lower of the two values. In some cases, the AP may assign Low Power (LP) in the U-NII-5 and U-NII-7 bands due to the Maximum EIRP returned in the AFC response. The Web UI displays LP instead of Standard Power (SP), which is normal under these conditions. |

| Component/s | AP |
|---|---|
| **Description** | AP R670 operates in low power indoor mode on channel 53, while AP R770 operates at standard power on the same channel. Make sure to collect the support log before rebooting the AP. |

| Component/s | Switches |
|---|---|
| **Issue** | FI-280394 |
| **Description** | In the event that SmartZone users add, modify, or delete a static route for an ICX Switch, the ICX Switch will not display the SmartZone username in its syslog entries. |

| Component/s | Switches |
|---|---|
| **Issue** | FI-273372 |
| **Description** | If the ICX Switch platform 7750 has already been configured with port 1/2/1 set to breakout mode, the breakout port *1/2/1:1* might still retain its stack port configuration. |

| Component/s | Control Plane |
|---|---|
| **Issue** | SCG-161578 |
| **Description** | When a device (User Equipment) connected to a wi-fi network (SSID) with the Single Accounting Session ID feature enabled moves between Access Points (APs), it sends an INTERIM-UPDATE and a START message to update the session status. If it moves repeatedly, a START message is sent, starting a new accounting session and changing the Accounting-Session-ID. |

## *Multi-Link Operation (MLO)*

| Component/s | AP |
|---|---|
| **Issue** | AP-31300 |
| **Description** | The Multicast Listener Discovery (MLD) MAC address and the Partner Link MAC address are identical. |

| Component/s | AP |
|---|---|
| **Issue** | AP-30749 |
| **Description** | In Windows 11 devices with the BE200 chipset, during a successful MLO connection, the partner link Received Signal Strength Indicator (RSSI) is weak. This severely disrupts traffic flow on the secondary link, greatly diminishing the effectiveness of MLO. |

| Component/s | AP |
|---|---|
| **Issue** | AP-29341 |
| **Description** | When connected to both 2.4GHz and 5GHz bands through MLO, the client fails to switch to the 2.4GHz band when the 5GHz signal weakens with distance from the AP. This causes a disconnection, as the client does not seamlessly transition to the stronger 2.4GHz link. |

| Component/s | AP |
|---|---|
| **Issue** | AP-37778 |
| **Description** | The Multi-Link Operation (MLO) tag is included in the beacon on a Dynamic Pre-Shared Key 3 (DPSK3) Wireless Local Area Network (WLAN), even though MLO is disabled by default. |

| Component/s | AP |
|---|---|
| **Issue** | SCG-146645 |
| **Description** | The *MQ Statistics* API CLI provides insights into various metrics related to messaging queues. When querying *MQ Statistics* for an MLO Client, the counters may display as zero, indicating no impact on the MLO client's connectivity. |

| Component/s | AP |
|---|---|
| **Issue** | AP-36456 |
| **Description** | The Samsung S24 device disconnects from the MLO WLAN, showing an error that the *Previous authentication is no longer valid* when attempting to connect using 802.11ax APs. |

| Component/s | AP |
|---|---|
| **Issue** | SCG-146331 |
| **Description** | *Google Pixel 8* phone experiences connection failures when attempting to connect as an MLO client with a partner link on an MLO WLAN configured with Open+OWE security and utilizing both 2.4GHz and 5GHz frequencies for MLO. |

| Component/s | AP |
|---|---|
| **Issue** | AP-34776 |
| **Description** | The **Stats** command does not provide specific information regarding data transfer per link for MLO clients. Instead, it displays the overall data transfer for the client session, which is also reported in the controller user interface. |

| Component/s | AP |
|---|---|
| **Issue** | AP-31726 |
| **Description** | MLO is not supported on mesh-enabled APs in this release. |

| Component/s | AP |
|---|---|
| **Issue** | SCG-145743 |
| **Description** | • It is advised not to use iPerf 3 for Access Point (AP) QoS testing. Instead, it is recommended to utilize iPerf 2 for this purpose. The reason for avoiding iPerf 3 in AP QoS testing is that the initial packets transacted before the actual traffic starts are treated with best effort QoS. This leads to the fastpath being configured with an incorrect value, impacting subsequent QoS values. Using iPerf 2 is recommended to avoid this issue.<br>• When a non-default AP management VLAN (VLAN greater than 1) is assigned to a WLAN, it may result in all traffic on that WLAN egressing with video priority. |

| Component/s | Switch Management |
|---|---|
| **Issue** | FI-300729 |
| **Description** | The switch overlay gateway configuration cannot be deleted. |
| **Workaround** | Reboot the switch and manually delete the overlay gateway configuration through the CLI console. |

| Component/s | System |
|---|---|
| **Issue** | SCG-153432 |
| **Description** | The SZ300 controller system cannot manage more than 40 GB of Elasticsearch index data generated within a single day for the following reasons:<br>• SZ300 has limited disk I/O bandwidth.<br>• When the Elasticsearch index exceeds 40 GB in a day, disk I/O reaches 100% utilization for approximately three hours during the Elasticsearch merge time (from 23:30 to 2:30).<br>• This high I/O consumption can cause the system to slow down or hang, affecting overall functionality. |
| **Workaround** | Users must limit the number of persisted event codes by avoiding the persistence of all events. This will help prevent disk I/O exhaustion and ensure system stability. |

| Component/s | System |
|---|---|
| **Issue** | SCG-160739 |
| **Description** | A small number of APs fail to reconnect on the first re-home attempt and take 15 minutes to re-home successfully to the active cluster on the second attempt. |

| Component/s | System |
|---|---|
| **Issue** | SCG-161594 |
| **Description** | Configuring a 5GHz channel using the CLI mode with Dynamic Frequency Selection (DFS) enabled for United States country code results in an error. |
| **Workaround** | Configure the 5GHz channels in the controller web user interface. |

# Client Interoperability

**NOTE**

SmartZone controllers and RUCKUS 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** | AP-31799 |
| **Description** | In Samsung Galaxy Tab S8 devices, the client selects different Simultaneous Authentication of Equals (SAE) mechanisms (PWE or H2E) between the authentication and association packets, causing inconsistencies. This results in client connection failures. |

| Component/s | AP |
|---|---|
| **Issue** | AP-36295 |
| **Description** | In Samsung Galaxy S24 Ultra devices, WLAN connectivity issues occur due to the absence of an IEEE 802.11be in the information element association request packet. As a result, the client's Radio Type displays **a/n/ac/ax** instead of **a/n/ac/ax/be**. |

| Component/s | AP |
|---|---|
| **Issue** | AP-29046 |
| **Description** | Google Pixel 8 devices fail to establish MLO links when fast roaming is enabled. As a result, with fast roaming activated, Pixel 8 cannot leverage MLO features, restricting potential performance and reliability enhancements. |

| Component/s | AP |
|---|---|
| **Issue** | AP-34316 |
| **Description** | Apple devices running the latest OS versions (iOS 18.x or MACos 15.x) do not transmit hostname information in the DHCP request when the hostname is changed to a non-default value. |
| **Workaround** | Use the default hostname for devices running these OS versions. |

| Component/s | AP |
|---|---|
| **Issue** | AP-32542 |

| Component/s | AP |
|---|---|
| Description | Apple iPad and Samsung Galaxy S21 devices intermittently fail to execute Fast Transition (FT) roaming due to an *Invalid FTIE* error. This issue occurs when WPA2/WPA3 mixed mode is enabled with Pre-Shared Key (PSK) authentication and FT is enabled.<br><br>**NOTE**<br>If a client encounters this issue, the system falls back to executing a full authentication to roam to the target AP. |

| Component/s | AP |
|---|---|
| Issue | AP-37576 |
| Description | When 6GHz is enabled, the Samsung S23 devices fails to connect to the Dynamic Segmentation and Authentication Enabled (DSAE) WLAN, which is configured with WPA2-WPA3 mixed mode and DPSK. |
| Workaround | Disable 6GHz when DSAE WLAN is configured with WPA2-WPA3 mixed mode and DPSK. |

| Component/s | AP |
|---|---|
| Issue | AP-34359 |
| Description | A device equipped with the Qualcomm FastConnect 7800 Wi-Fi 7 chip and running driver version 3.1.0.1238 is unable to associate with the 6GHz radio on the R770 AP. This issue occurs specifically when the AP is configured for Austria. |

| Component/s | AP |
|---|---|
| Issue | AP-33390, SCG-146331 |
| Description | Enabling Multi-Link Operation (MLO) with 802.11x is not recommended until all client vendors officially support 802.11x with MLO, due to limitations and inconsistent behavior across various vendors. This limitation does not apply to WPA3-SAE WLAN. |

| Component/s | AP |
|---|---|
| Issue | AP-27747 |
| Description | When tested on 802.11ax APs, the device type for a OnePlus running Android 14 and an iPhone 13 is incorrectly identified as a tablet instead of a smartphone. |

# Changed Behavior

The following are the behavioral changes in this release.

| Component/s | AP |
|---|---|
| Issue | ER-12755 |
| Description | Added the option to disable image resizing when adding an indoor map for preventing image degradation. |

| Component/s | System |
|---|---|
| Issue | ER-14161 |
| Description | Enhanced performance and memory usage of zone update. |

| Component/s | Control Plane |
|---|---|
| Issue | ER-13671 |
| Description | Improved the Switch Management API to resolve the slowness experienced during switch operations executed through the Web user interface or CLI mode. |

| Component/s | Control Plane |
|---|---|
| Issue | ER-13972 |
| Description | Updated the API documentation to reflect the validity of the Service Ticket for Public API version 11.1. |

| Component/s | System |
|---|---|
| Issue | ER-13302 |
| Description | In the customer-uploaded Guest Pass HTML template, a new variable, **GP_LOGO_BASE64**, is added to include the base64 string of the customer-uploaded Guest Portal logo. |

# Security Considerations

The following security fixes are included in this release.

| Component/s | System |
|---|---|
| Issue | ER-13296 |
| Description | Addressed vulnerabilities linked to National Institute of Standards and Technology (NIST) Common Vulnerability and Exposure (CVE) issue CVE-2024-21733 (*Generation of Error Message Containing Sensitive Information vulnerability in Apache Tomcat*.). . |

# Resolved Issues

| Component/s | AP |
|---|---|
| Issue | ER-14180 |
| Description | APs sent malformed Link Layer Discovery Protocol (LLDP) packets, resulting in a Power over Ethernet (PoE) negotiation failure. |

| Component/s | AP |
|---|---|
| Issue | ER-14098 |
| Description | The AP failed to update its configuration after being set up using the controller CLI command. |

| Component/s | AP |
|---|---|
| Issue | ER-13134 |
| Description | All APs appeared offline because the RabbitMQ cluster failed to form due to a node being offline or on a prolonged network issue. |

| Component/s | AP |
|---|---|
| Issue | ER-14038 |

| Component/s | AP |
|---|---|
| Description | Disabled client fingerprinting would incorrectly appear as *enabled* after refreshing the page. |

| Component/s | AP |
|---|---|
| Issue | ER-14097 |
| Description | A client connection issue was reported on IEEE 802.11x WLAN due to RADIUS authentication failure when the end-user delayed entry of their username and password credentials. |

| Component/s | AP |
|---|---|
| Issue | ER-14041 |
| Description | An invalid 6GHz channel was displayed though 6GHz was disabled. |

| Component/s | AP |
|---|---|
| Issue | ER-13634 |
| Description | An unexpected 2.4GHz channel seen on the controller web user interface when the 2.4GHz radio was disabled. |

| Component/s | AP |
|---|---|
| Issue | ER-13602 |
| Description | Incorrect LED status on APs R560/R760 when Mesh is enabled. |

| Component/s | AP |
|---|---|
| Issue | ER-13801 |
| Description | Apple iOS devices could not authenticate when connected to a *WebAuth* WLAN. |

| Component/s | AP |
|---|---|
| Issue | ER-13772 |
| Description | Resolved a target assertion issue that occurred when only the monitoring WLAN was active. |

| Component/s | AP |
|---|---|
| Issue | ER-14218 |
| Description | Excessive ChannelFly Background Scan (Chanbkgndscan) and ChannelFly Background (Channelflybg) process logs, along with frequent Radio Management Plane (RPM) configuration saves, lead to flash memory corruption and a shortened lifespan.<br><br>It is recommended not to reference the RPM key when updating the Signal-to-Noise Ratio (SNR) threshold through automatic channel selection. |

| Component/s | AP |
|---|---|
| Issue | ER-14076 |
| Description | Chromebooks with OS version 126.0.6478.x were not identified during the DHCP procedure. |

| Component/s | AP |
|---|---|
| Issue | ER-14050 |

| Component/s | AP |
|---|---|
| Description | Ethernet statistics showed all values as zeros when connected to a 2.5G Ethernet switch port. |

| Component/s | AP |
|---|---|
| Issue | ER-13981 |
| Description | A kernel panic issue occurred during target recovery. |

| Component/s | AP |
|---|---|
| Issue | SCG-146726 |
| Description | The communication between APs does not adhere to Bundesamt für Sicherheit in der Informationstechnik (BSI) compliance standards. |

| Component/s | AP |
|---|---|
| Issue | ER-13882 |
| Description | The AP failed to report AeroScout T3/T2 tags accurately. |

| Component/s | AP |
|---|---|
| Issue | ER-13445 |
| Description | AP failed to set Wi-Fi calling Tx priority for certain service providers. |

| Component/s | AP |
|---|---|
| Issue | ER-13461 |
| Description | An unexpected authentication issue occurred before the session timeout was reached. |

| Component/s | AP |
|---|---|
| Issue | ER-13605 |
| Description | Rx data packets failed to process on 802.11ax driver. |

| Component/s | AP |
|---|---|
| Issue | ER-13680 |
| Description | AP was unable to migrate to a new controller node. |

| Component/s | AP |
|---|---|
| Issue | ER-13685, ER-12934 |
| Description | 5GHz channel could not be set due to radar detection. |

| Component/s | AP |
|---|---|
| Issue | ER-13728 |
| Description | Packet drops occurred when both Wi-Fi Calling and Link Aggregation Control Protocol (LACP) features were enabled. |

| Component/s | AP |
|---|---|
| Issue | ER-13759, ER-14052 |
| Description | The AP could disconnect from controller. |

| Component/s | AP |
|---|---|
| Issue | ER-13806 |
| Description | An invalid AP neighbor report caused a kernel panic reboot on Wi-Fi 7 (IEEE 802.11be) APs. |

| Component/s | AP |
|---|---|
| Issue | ER-14051 |
| Description | A client authentication issue involving multiple Pairwise Master Key Identifiers (PMKIDs) in a re-association message. |

**********

| Component/s | AP |
|---|---|
| Issue | ER-14193 |
| Description | The Electronic Shelf Label (ESL) module failed to enable on AP R670. |

| Component/s | AP |
|---|---|
| Issue | ER-14190 |
| Description | No client **Connection Events** are displayed on the **Troubleshooting** page due to an exception caused by the presence of an @ symbol in the Account, Venue, or AP name. |

| Component/s | AP |
|---|---|
| Issue | ER-13721 |
| Description | The U-NII-1 and U-NII-2A bands were unavailable on Wi-Fi 6 (IEEE 802.1ax) configured with the Indonesia country code. |

| Component/s | AP |
|---|---|
| Issue | AP-33056 |
| Description | This issue was specific to channel 52 where an AP operating on this channel failed to switch to a new channel when a radar was detected. This problem affected both Wi-Fi 6E and Wi-Fi 7 APs. |

| Component/s | AP |
|---|---|
| Issue | AP-31384 |
| Description | The BSS Priority feature did not function correctly with Wi-Fi 6E and Wi-Fi 7 APs. Due to this bug, all clients received the same airtime and performance, regardless of the configured BSS Priority. |

| Component/s | AP |
|---|---|
| Issue | AP-36960 |
| Description | Downlink performance was slightly slower when using SoftGRE on the R770 AP. |

## Resolved Issues

| Component/s | AP |
|---|---|
| **Issue** | AP-32006 |
| **Description** | Apple devices are experiencing random client authentication failures with reason code 3 and unspecified reason when connected to WPA2/WPA3 mixed mode.<br><br>This behavior is not observed with all Apple devices and does not occur with WPA2-only or WPA3-only configurations. |

| Component/s | AP |
|---|---|
| **Issue** | ER-14009 |
| **Description** | Resolved an issue where the IP address of the user equipment was inaccurately reported as 0.0.0.0 via SNMP. |

| Component/s | AP |
|---|---|
| **Issue** | AP-34218 |
| **Description** | Channels 100-140 were blocked for Nepal (NP), and channels 149-165 were blocked for Egypt (EG). This issue was specific to the R670 AP model. |

| Component/s | AP |
|---|---|
| **Issue** | SCG-146540 |
| **Description** | Clients connected to the non-mesh interface of R560 or R760 Mesh APs experienced performance degradation. |

| Component/s | AP |
|---|---|
| **Issue** | AP-33800 |
| **Description** | In high-density environments, an AP could store up to 20 neighbor entries in the Neighbor Discovery (NBRD) peer list. This limitation was consistent across all APs and was considered a legacy behavior. |

| Component/s | AP |
|---|---|
| **Issue** | AP-31501 |
| **Description** | When back-to-back channel or channel bandwidth configurations were applied from the controller web interface, some blacklisted channels, such as 149-161, were enabled on the AP. This issue was specific to APs configured for 80MHz channelization on the upper band of 5GHz. |

| Component/s | AP |
|---|---|
| **Issue** | ER-13703 |
| **Description** | The channelization of Wi-Fi 7 APs remained fixed at 20 MHz under certain conditions. |

| Component/s | AP |
|---|---|
| **Issue** | AP-33958 |
| **Description** | Random client roaming failures were observed after roaming to the target AP, as the source AP de-authenticated the clients with *reason code 8*. |

| Component/s | AP |
|---|---|
| Issue | AP-33930 |
| Description | Bidirectional performance with Low Bandwidth Operation (LBO) was slightly lower compared to uplink or downlink performance for AP R670. |

| Component/s | AP |
|---|---|
| Issue | AP-33344 |
| Description | Random clients disconnect with reason code 4 (Client inactivity) were observed and were specific to Wi-Fi 7 APs. |

| Component/s | AP |
|---|---|
| Issue | AP-32474, AP-32965 |
| Description | The available channel list on the Wi-Fi 6E AP operating in Norway did not include Channel 157. |

| Component/s | AP |
|---|---|
| Issue | SCG-157756 |
| Description | Channels 169 and 173 at 20MHz could not be enabled by the user in the controller web user interface for Germany. This issue was specific to the T670 AP. |

| Component/s | AP |
|---|---|
| Issue | AP-34197, AP-35311 |
| Description | Resolved an issue where downlink performance with SoftGRE was slightly lower than uplink for APs R670 or T670. |

| Component/s | AP |
|---|---|
| Issue | AP-33853, AP-33854 |
| Description | A random target assert was observed when an MLO client disconnected from an OWE WLAN and connected to a new SSID with WPA3-SAE. |

| Component/s | AP |
|---|---|
| Issue | AP-34836 |
| Description | Resolved an issue where the AP could go offline during the upgrade process. |

| Component/s | AP |
|---|---|
| Issue | AP-33920 |
| Description | During bootup, the AP R670 requested 25.5W of power from the switch, and after bootup, it requested 25W. This change in power consumption could cause a reset in power mode, potentially resulting in connectivity loss for connected clients. This issue occurred randomly and was not limited to any specific switch model. |

| Component/s | AP |
|---|---|
| Issue | AP-33873 |
| Description | The **crashdump upload** command failed to copy both *q6dumps* files from the */tmp* (temporary) folder. |

| Component/s | AP |
|---|---|
| Issue | AP-33486 |
| Description | Clients randomly failed to reconnect to the AP when using Multi-Link Operation (MLO) in 5GHz with 6GHz mode. |

| Component/s | AP |
|---|---|
| Issue | AP-32876, AP-33066, AP-33108, AP-30095, AP-32161, AP-32939 |
| Description | The issue where channels 149-161 could not be configured arose because the AP CLI indicated that these channels were blocked, while the AP configuration through the controller's Web UI showed support for them. This inconsistency between the CLI and Web UI resulted in the channels being unavailable for configuration despite appearing functional in the UI. |

| Component/s | AP |
|---|---|
| Issue | AP-32811 |
| Description | Channel 165 was accessible in the controller web interface when the AP Zone is configured with Israel as the country and Channel Width (CW) as 40/80MHz. |

| Component/s | AP |
|---|---|
| Issue | AP-32736 |
| Description | In the controller web interface, there were a minor cosmetic issue where Channels 52–64 was marked as DFS for Hong Kong, but the AP considered them to be non-DFS. |

| Component/s | AP |
|---|---|
| Issue | AP-32049 |
| Description | The AP randomly encountered a target assert error under heavy load conditions. |

| Component/s | AP |
|---|---|
| Issue | AP-31322 |
| Description | The AP at times encountered a target assert error when collecting Wi-Fi statistics frequently from AP CLI. |

| Component/s | AP |
|---|---|
| Issue | AP-19942 |
| Description | When SSID Radio Load (RL) was enabled on R560 or R760 or R770 APs with only one WLAN or Virtual Access Point (VAP) deployed, users at times experienced packet loss and reduced throughput in the uplink direction. |

| Component/s | AP |
|---|---|
| Issue | SCG-159402 |
| Description | After executing multiple test cases, no logs were generated through *log read*. |

| Component/s | AP |
|---|---|
| Issue | SCG-159180 |
| Description | Request to Send (RTS) frames will not comply with the BSS Minimum Rate Configuration in WLAN. |

| Component/s | AP |
|---|---|
| Issue | SCG-158601 |
| Description | Target assert was observed at WLAN (wlan_buf_internal.c:915), causing the test automation to terminate in 2-5-6/2-5 mode. |

| Component/s | AP |
|---|---|
| Issue | AP-34348 |
| Description | The issue of channels 149-161 being blocked for Iceland, specific to APs R670 and T670 configured in 2.4GHz-5GHz mode, is resolved. |

| Component/s | AP |
|---|---|
| Issue | AP-34259, AP-34258 |
| Description | Resolved random kernel panics observed in high-density environments with a large number of clients roaming across Wi-Fi 7 APs. |

| Component/s | AP |
|---|---|
| Issue | AP-34081, AP-34080, AP-34078 |
| Description | A cosmetic issue where U-NII-3 channels were incorrectly marked as non-DFS for the countries of Argentina (AR), New Zealand (NZ), and Australia (AU) is resolved. |

| Component/s | AP |
|---|---|
| Issue | AP-33764 |
| Description | Resolved target assertion issues encountered in a high-scale environment. |

| Component/s | AP |
|---|---|
| Issue | AP-33461 |
| Description | The issue involving Multi-Link Operation (MLO) formation inconsistencies with 2.4GHz and 6GHz bands on *Google Pixel 8* is resolved. |

| Component/s | AP |
|---|---|
| Issue | AP-32729 |
| Description | The kernel panic issue caused during a Dynamic Frequency Selection (DFS) channel change event is resolved. |

| Component/s | AP |
|---|---|
| Issue | AP-30718 |
| Description | The log level for the monitor interface has been updated, with the default setting changed from debug to error to improve log management and reduce unnecessary debug output. |

| Component/s | AP |
|---|---|
| Issue | AP-31597, AP-30539 |
| Description | The issue with Location Based Service (LBS) functionality on APs T670 and R670 is resolved. |

| Component/s | AP |
|---|---|
| Issue | SCG-157670 |
| Description | The issue with *Zero Touch Mesh* discovery in standalone builds of APs T670 and R670 is resolved. |

| Component/s | AP |
|---|---|
| Issue | AP-34022 |
| Description | A target assert was reported on R750 Density APs. |

| Component/s | AP |
|---|---|
| Issue | AP-33380 |
| Description | Resolved discrepancies related to Tx Power support for countries in the 2-5-6 GHz mode, specifically affecting AP R670. |

| Component/s | AP |
|---|---|
| Issue | SCG-159467 |
| Description | Rate limiting failed to occur when traffic was sent from a wired client connected to a Remote Access Point (RAP) to a wireless client on a Mesh AP. This issue was specific to Wi-Fi 7 AP models. |

| Component/s | AP |
|---|---|
| Issue | SCG-146685 |
| Description | When the R770 MLO-2 2.4GHz and 5GHz active link was utilized on both the 2.4GHz and 5GHz bands, the single client Over-The-Air (OTA) downlink throughput on 5GHz was observed to be lower compared to the non-MLO 5GHz configuration. |

| Component/s | Control Plane |
|---|---|
| Issue | ER-12836 |
| Description | CLI Guest passes counter did not match the count displayed in the controller web user interface. |

| Component/s | Control Plane |
|---|---|
| Issue | ER-13756 |
| Description | Alarm *SoftGRE unreachable (614)* failed to clear automatically. |

| Component/s | Control Plane |
|---|---|
| Issue | ER-14029 |
| Description | The cluster displayed an *Overloading* status in Switches, which caused the APs to be in a rejected state. |

| Component/s | Data Plane |
|---|---|
| Issue | ER-13434 |
| Description | The controller web user interface displayed an inconsistency in the RUCKUS GRE tunnel results. |

| Component/s | Public API |
|---|---|
| Issue | ER-13604 |

| Component/s | Public API |
|---|---|
| Description | The *firstIndex* field was incorrect in the query for Switch API. |

| Component/s | RUCKUS AI |
|---|---|
| Issue | ER-12927 |
| Description | Resolved an issue that caused the Radio Access (RA) / Virtual Radio Unit Emulation (VRUE) test to fail. |

| Component/s | RUCKUS AI |
|---|---|
| Issue | ER-13611 |
| Description | Incorrect RADIUS failure incidents were reported on the RUCKUS AI (RAI) cloud service. |

| Component/s | System |
|---|---|
| Issue | ER-14025 |
| Description | The controller failed to forward SMTP/email notifications for Switch events. |

| Component/s | Switches |
|---|---|
| Issue | ER-14101 |
| Description | Resolved the web user interface configuration error for ICX port configuration. |

| Component/s | System |
|---|---|
| Issue | ER-13924 |
| Description | Failed configuration backup was not being deleted. |

| Component/s | System |
|---|---|
| Issue | ER-12631 |
| Description | Resolved an issue of falsely triggered PSU related alarms. |

| Component/s | System |
|---|---|
| Issue | ER-13403 |
| Description | Saving the variable *ueMac* for Group DPSK resulted in an error. |

| Component/s | System |
|---|---|
| Issue | ER-13404 |
| Description | Controller upgrade failed if the Elasticsearch (ES) stalled in *RED* health status. |

| Component/s | System |
|---|---|
| Issue | ER-13465 |
| Description | Enhanced the controller ChatBot error message to provide clearer information when file uploads to customer support fail due to a Domain Name System (DNS) issue. |

## Resolved Issues

| Component/s | System |
|---|---|
| **Issue** | ER-13615 |
| **Description** | When changing an OWE-Transition WLAN to another WLAN type with the encryption method set to *None* the system failed to delete its paired OWE WLAN. |

| Component/s | System |
|---|---|
| **Issue** | ER-13752 |
| **Description** | The *DELETE ServiceTicket* option on the API returned an error stating *Service Ticket does not exist*. |

| Component/s | System |
|---|---|
| **Issue** | ER-13904 |
| **Description** | A follower node failed to join the cluster due to an excessive number of uploaded firmware files for APs, Data Planes, and Switches. |

| Component/s | System |
|---|---|
| **Issue** | ER-13930 |
| **Description** | Resolved an issue with SNMP returning incorrect values. |

| Component/s | System |
|---|---|
| **Issue** | ER-13967 |
| **Description** | Resolved the misleading error message *Service is in maintenance and upgrading*, that appeared while ElasticSearch processed internal recovery tasks. |

| Component/s | System |
|---|---|
| **Issue** | ER-14096 |
| **Description** | The **Captive Portal** feature displayed text in English instead of German when a guest connected to the Wi-Fi with the German language setting enabled. |

| Component/s | System |
|---|---|
| **Issue** | ER-14087 |
| **Description** | The controller snapshot log could not be generated or downloaded due to the large size of the collected data. |

| Component/s | UI/UX |
|---|---|
| **Issue** | ER-13985 |
| **Description** | The error message *Ambiguous method overloading for method...* was displayed when accessing the controller web user interface. |

| Component/s | UI/UX |
|---|---|
| **Issue** | SCG-159070 |
| **Description** | In the controller web interface, there was a cosmetic issue where the Tx Modulation and Coding Scheme (MCS) and Rx MCS for clients appeared the same for both 2.4GHz and 5GHz links. |

# Interoperability Information

## Cluster Network Requirements

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

### *Minimum Cluster Network Requirement*

| | Model | | | |
|---|---|---|---|---|
| | **SZ300** | **vSZ-H** | **SZ144** | **vSZ-E** |
| **Latency** | 60ms | 42ms | 93ms | 229ms |
| **Jitter** | 10ms | 10ms | 10ms | 10ms |
| **Bandwidth** | 115Mbps | 92Mbps | 40.25Mbps | 23Mbps |



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