

RUCKUS SmartZone (ST-GA) Patch 1 Release Notes, 7.0.0

Supporting SmartZone Patch 1 7.0.0

© 2024 CommScope, Inc. All rights reserved.

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

Export Restrictions

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

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

Disclaimer

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

Limitation of Liability

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

Trademarks

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 | 4 |
| Hardware and Software Support | 4 |
| Overview..... | 4 |
| Release Information..... | 4 |
| Supported Matrix and Unsupported Models..... | 6 |
| Supported ICX Models..... | 9 |
| Product Documentation..... | 12 |
| Known Issues | 12 |
| Known Issues in R7.0.0 Patch1..... | 12 |
| Limitations..... | 16 |
| R770 Known Issues and Limitations..... | 16 |
| Resolved Issues | 18 |
| Resolved Issues in R7.0.0 Patch1..... | 18 |
| R770 Resolved Issues..... | 21 |
| Changed Behavior | 22 |
| Interoperability Information | 23 |
| Cluster Network Requirements..... | 23 |
| Client Interoperability..... | 23 |
| Adding AP Patch to the Controller | 28 |

Document History

| Revision Number | Summary of Changes | Publication Date |
|-----------------|------------------------------|------------------|
| A | Initial <i>Release Notes</i> | 02, April 2024 |

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 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 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 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 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 Short Term (ST) release. This section lists the version of each component in this release.

RUCKUS recommends SmartZone R7.0.0 Patch1 release for users utilizing Wi-Fi7 APs. For those with legacy APs, RUCKUS suggests using SmartZone R6.1.2 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

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).

NOTE

RUCKUS IoT R2.2.0 is not supported on SmartZone R7.0.0 and R7.0.0 Patch1. Refer to the *RUCKUS IoT 2.2.0.0 GA Release Notes* for the hardware and software support details.

SZ300

- Controller Version: **7.0.0.0.726**
- Control Plane Software Version: **7.0.0.0.465**
- Data Plane Software Version: **7.0.0.0.726**
- AP Firmware Version: **7.0.0.0.1404**

SZ144

- Controller Version: **7.0.0.0.726**
- Control Plane Software Version: **7.0.0.0.465**
- Data Plane Software Version: **7.0.0.0.77**
- AP Firmware Version: **7.0.0.0.1404**

vSZ-H and vSZ-E

- Controller Version: **7.0.0.0.726**
- Control Plane Software Version: **7.0.0.0.465**
- AP Firmware Version: **7.0.0.0.1404**

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

- Data plane software version: **7.0.0.0.726**

Cloudpath

- Cloudpath Version: **5.12 R6 (5.12.5584)**.

Upgrade Information

Upgrade to R7.0.0 is available for users currently on versions R6.1, 6.1.1, and 6.1.2. Versions preceding R6.1.0 are not supported for an upgrade to R7.0.0.

Dynamic Signature Package Update

Administrators or users can dynamically upgrade the Signature Package from the RUCKUS support site.

Complete the following steps to perform a manual upgrade:

1. Download the Signature package from the RUCKUS support site:
 - SmartZone R7.0.0 Signature Package version 1.670.2: <https://support.ruckuswireless.com/admin/software/3961-smartzone-7-0-ga-sigpack-1-670-2-application-signature-package>.
 - SmartZone R7.0.0 Signature Package version 1.670.2-regular: <https://support.ruckuswireless.com/admin/software/3960-smartzone-7-0-ga-sigpack-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 **Working with Application Signature Package** in *RUCKUS SmartZone Security Guide (ST-GA)*, 7.0.0

Hardware and Software Support

Supported Matrix and Unsupported Models

NOTE

Upgrade to R7.0.0 from versions prior to R6.1.0 is not supported. It's 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 (SZ) GPB .proto files from the RUCKUS support site:

1. SmartZone **7.0.0.0.726** (GA) GPB.proto (Google ProtoBuf) image for GPB/MQTT [DNP] - <https://support.ruckuswireless.com/software/3962-smartzone-7-0-0-ga-gpb-proto-google-protobuf-image-for-gpb-mqtt>.
2. SmartZone **7.0.0.0.726** MockSCI-TLS (SZ to SCI MQTT subscriber software) for CentOS/Ubuntu - <https://support.ruckuswireless.com/software/3963-smartzone-7-0-0-ga-mocksci-tls-sz-to-sci-mqtt-subscriber-software-for-centos-ubuntu-dnp>.

Public API

Click on the following links to view Public API documents:

- *SmartZone 7.0.0 Public API Reference Guide (ICX Management)*
<https://support.ruckuswireless.com/documents/4733>
- *SmartZone 7.0.0 Public API Reference Guide (SZ100)*
<https://support.ruckuswireless.com/documents/4734>

NOTE

SZ100 Public API link is for SZ144 as well.

- *SmartZone 7.0.0 Public API Reference Guide (SZ300)*
<https://support.ruckuswireless.com/documents/4735>
- *SmartZone 7.0.0 Public API Reference Guide (vSZ-E)*
<https://support.ruckuswireless.com/documents/4736>
- *SmartZone 7.0.0 Public API Reference Guide (vSZ-H)*
<https://support.ruckuswireless.com/documents/4737>

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 higher are capable of connecting 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.

TABLE 1 Supported AP Models

| 11ax | |
|--------|---------|
| Indoor | Outdoor |
| R850 | T750SE |
| R770 | T750 |
| R760 | T350SE |
| R750 | T350D |
| R650 | T350C |
| R560 | |
| R550 | |
| R350 | |
| 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.

Hardware and Software Support

Supported Matrix and Unsupported Models

ATTENTION

For APs that are not compatible with R7.0.0, it is essential to maintain them with AP firmware versions of R6.1, 6.1.1, and 6.1.2. The upgrade of the Zone for APs that are not supported in R6.1, 6.1.1, and 6.1.2 is not feasible.

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

| 11ax | 11ac-Wave2 | |
|--|------------|---------|
| NOTE Supported on R6.1.0, 6.1.1, and 6.1.2. | 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 802.11ac Wave2 or 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 3 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 4 ICX Firmware Versions Compatible with SmartZone

| ICX Model | First Supported FastIron Release | Last Supported FastIron Release |
|--|----------------------------------|---------------------------------|
| ICX 7150 | 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 | 10.0.00 | - |
| ICX 8200-24ZP, -48ZP2, -24FX, -24F, -48F, -C08ZP | 10.0.10 | - |

The following table defines ICX and SmartZone release compatibility.

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.

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 5 ICX and SmartZone Release Compatibility Matrix

| | SmartZone 5.1 ¹ | 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 |
|-------------------|----------------------------|------------------|-----------------|---------------|-------------------------|---------------|---------------|-----------------|-----------------|-----------------|
| FastIron 08.0.80 | Yes | Yes ¹ | No | No | No | No | No | No | No | No |
| FastIron 08.0.90a | No | Yes | Yes | Yes | Yes | Yes | No | No | No | No |

¹ Does not support ICX configuration.

TABLE 5 ICX and SmartZone Release Compatibility Matrix (continued)

| | SmartZone 5.1 ¹ | 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 |
|--|----------------------------|-----------------|-----------------|---------------|-------------------------|---------------|---------------|-----------------|-----------------|-----------------|
| FastIron 08.0.91 | No | Yes | Yes | Yes | No | No | No | No | No | No |
| FastIron 08.0.92 | No | No | Yes | Yes | Yes | Yes | Yes | No | No | No |
| FastIron 08.0.95 and subsequent patches | No | No | No | No | No | Yes | Yes | Yes | Yes | No |
| FastIron 09.0.10a and subsequent patches | No | No | No | No | No | No | Yes | Yes | Yes | Yes |
| FastIron 10.0.00 and subsequent patches | No | No | No | No | No | No | No | Yes | Yes | Yes |
| FastIron 10.0.10 and subsequent patches | No | No | No | No | No | No | Yes | Yes | Yes | Yes |

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

TABLE 6 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 |

¹ Does not support ICX configuration.

TABLE 6 Switch Management Feature Compatibility Matrix (continued)

| Feature | SmartZone Release | ICX FastIron Release |
|---|-------------------|--|
| Manage Switches from Default Group in SZ-100 / 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 ² | 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 ³ |
| 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 |
| 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 ⁴ |
| 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 |

² To download system logs from SmartZone for a particular ICX switch, TFTP must be enabled.

³ FastIron 10.0.00 and later releases do not support management VLANs.

⁴ As an exception, FastIron release 10.0.00 does not support this feature.

Product Documentation

The following product guides for R7.0.0 Patch1 have been updated. Refer to the *New in this Document* section in each publication for detailed changes.

TABLE 7 Product Guides

| Category | Name of The Guide |
|-------------------------------|---|
| User and Administrator Guides | <ul style="list-style-type: none">RUCKUS SmartZone (ST-GA) SmartZone Upgrade Guide, 7.0.0 |

Online Help Rendition

A number enhancements are introduced for Online Help (OLH) rendering for R7.0.0. Previous renditions navigated to the *RUCKUS SmartZone Administrator Guide* (consisting of 700+ pages). From R6.1.1, we have split the existing *RUCKUS SmartZone Administrator Guide* into 11 separate guides (Rev B of R6.1.1). This split is based on Taxonomy, and one of the main purposes for this change was for easy reading and keyword search. This enhancement caused a change in the way OLH renders.

The OLH now renders with all of the product guides listed under the relevant firmware release number. A short description appears for each guide. Select the relevant guide for reference.

Known Issues

This section describes known behaviors and recommended workarounds where they exist.

Known Issues in R7.0.0 Patch1

Following are the known issues in this release.

| Component/s | AP |
|-------------|--|
| Issue | SCG-145121 |
| Description | The results of SpeedFlex tests on a multihop mesh setup are not accessible through the <i>Public API</i> . This limitation only when PMTU (Path MTU (Maximum Transmission Unit)) is set to 1500. |

| Component/s | AP |
|-------------|---|
| Issue | SCG-142998 |
| Description | When the user selects the PoE operation mode to AT mode, 11AX or later AP models it is forcibly turned off, and the USB toggle is grayed. Subsequently, when the user changes the PoE operation mode to Auto, the USB toggle changes to edit mode. However, the controller web user interface does not automatically enable the USB toggle. |

| Component/s | AP |
|-------------|------------|
| Issue | SCG-142102 |

| Component/s | AP |
|-------------|---|
| Description | <p>There is a disparity in the TTL (Time To Live) definition between LLDP (Link Layer Discovery Protocol) version 0.7.1 and version 1.0.15 as outlined below:</p> <ul style="list-style-type: none"> • 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). • The default interval in LLDP 1.0.15 is set to 30 seconds. <p>Following are the TTL examples in LLDP 1.0.15. I.</p> <ul style="list-style-type: none"> • If hold time is set to 10 seconds, TTL is calculated as $30 * 10 = 300$ seconds. • If hold time is set to 200 seconds, TTL is calculated as $30 * 200 = 6,000$ seconds. • If hold time is set to 500 seconds, TTL is calculated as $30 * 500 = 15,000$ seconds. • If hold time is set to 1000 seconds, TTL is calculated as $30 * 1000 = 30,000$ seconds. |

| Component/s | AP |
|-------------|--|
| Issue | AP-26728 |
| Description | <p>In scenarios where a wireless client transitions from one access point (AP-1) to another (AP-2), the Deep Packet Inspection (DPI) engine on AP-2 may face challenges in accurately identifying and classifying certain applications.</p> <p>This issue is particularly evident for applications characterized by distinct control flows and data flows, such as FTP and YouTube. The difficulty arises because control flows may be initiated on AP-1, and by the time data flows commence, the client has already roamed to AP-2.</p> <p>Consequently, the DPI engine on AP-2 lacks the contextual information of the initial control flows, potentially resulting in a failure to detect or classify the ongoing traffic.</p> |

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

| Component/s | AP |
|-------------|--|
| Issue | AP-25953 |
| Description | Logs and events may not be visible in the external syslog server because syslog is sent to the server once the Access Point (AP) obtains an IP address. In the case of RNCSS (RUCKUS NOR Certificate Safe Storage) logs during bootup, occur before the AP acquires an IP address, resulting in the absence of events in the external syslog server. |

| Component/s | AP |
|-------------|---|
| Issue | SCG-141990 |
| Description | The CLI command get mode wlanx does not accurately reflect the current operating mode of the WLAN. |

| Component/s | AP |
|-------------|--|
| Issue | SCG-141611 |
| Description | The NSP (Network Services Platform) failed to configure the tunnel profile in the NSP Ethernet profile. |
| Workaround | Users are required to choose an AP group with a tunnel WLAN. If the selected AP group does not have a tunnel WLAN configured, the MDU (Multi-Dwelling Unit) wired client functionality will not operate as intended. |

Known Issues

Known Issues in R7.0.0 Patch1

| Component/s | AP |
|-------------|---|
| Issue | AP-27714 |
| Description | The WLAN AP directs the client to transmit to the Service WLAN on the same radio after the client passes through the intermediate WLAN. This behavior is regarded as a design limitation. |
| Workaround | For a client to connect to the 6GHz Service WLAN, the client needs to disconnect and reconnect after passing through the Service WLAN of 2.4 or 5GHz. |

| Component/s | AP |
|-------------|--|
| Issue | AP-25371 |
| Description | The RUDB (RUCKUS User Database) updates information for wired clients by analyzing the initial packet of the spoofed DHCP request or response, where the source and destination MAC addresses have been altered. |

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

| Component/s | AP |
|-------------|---|
| Issue | SCG-146391 |
| Description | Flow creation does not take into account fragmented packets, hence SmartCast rules are not applied. |

| Component/s | AP |
|-------------|--|
| Issue | AP-27922 |
| Description | Beacon protection is not enabled in MLO WLAN. This is specific to Wi-Fi7 configuration and does not affect the association of MLO clients. |

| Component/s | AP |
|-------------|--|
| Issue | AP-28024 |
| Description | <p>The <code>docker-24.0.7.tgz</code> for Wi-Fi7 APs is downloaded and installed in the <code>/ruckuswireless</code> directory which resides in a permanent storage (flash memory). In contrast, for non Wi-Fi7 APs, docker binaries are downloaded and installed in the <code>/tmp</code> directory which is a <code>tmpfs</code> (RAM). As a result, the download and installation process takes longer for Wi-Fi7 APs compared to non Wi-Fi7 APs.</p> <p>When downloading a tar file in the <code>/ruckuswireless</code> directory, the extraction process also takes longer compared to downloading and extracting in the <code>/tmp</code> directory. This is because accessing and processing data from permanent storage involves higher latency when compared to data stored in RAM.</p> |

| Component/s | AP |
|-------------|--|
| Issue | SCG-151853 |
| Description | The client inactivity timeout feature is not functioning as expected on the R550 AP model. Despite the expiration of the inactivity timer values, clients are disconnected, and continue to connect to the R550 AP. This issue is specific to R550 AP. |

| | |
|--------------------|---|
| Component/s | AP |
| Issue | SCG-151717 |
| Description | The rate limit specified through the user-role from AAA (Authentication, Authorization, and Accounting) server is not enforced on clients connected through 802.1x authentication with WISPr Express Wi-Fi proxy. |

| | |
|--------------------|---|
| Component/s | AP |
| Issue | AP-19942 |
| Description | When SSID Radio Load (RL) is enabled on R560 or R760 or R770 APs with only one WLAN or VAP (Virtual Access Points) deployed, users might experience packet loss and reduced throughput in the uplink direction. |
| Workaround | It is recommended to deploy multiple WLANs or VAPs. |

| | |
|--------------------|---|
| Component/s | AP |
| Issue | SCG-143239 |
| Description | The performance of the 6E radio on the AP R560 or R760 decreases when 60 or more WiFi 6E clients are connected. |

| | |
|--------------------|---|
| Component/s | AP |
| Issue | SCG-146177 |
| Description | The uplink performance of the AP R560 decreases when more than 40 WiFi 6/6E clients are connected and actively transmitting data. |

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

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

| | |
|--------------------|---|
| Component/s | AP |
| Issue | SCG-146726 |
| Description | <p>BSI Compliance Mode Limitations - The ECDSA (Elliptic Curve Digital Signature Algorithm) certificate issued by SmartZone has the following limitation:</p> <ul style="list-style-type: none"> The communication between Access Points (APs) does not adhere to BSI compliance standards. |

| | |
|--------------------|--|
| Component/s | AP |
| Issue | AP-26794 |
| Description | The AP directs the client to transmit to the Service WLAN on the same radio when the client successfully passes through the intermediate WLAN, This behavior is a design limitation. |
| Workaround | To connect to the 6Ghz Service WLAN, the client needs to disconnect and reconnect after passing through the Service WLAN of the 2.4 or 5Ghz frequency bands. |

Known Issues

Limitations

| 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. |

Limitations

There are currently no immediate plans to address these issues in the short term.

| Component/s | SmartCast |
|-------------|---|
| Issue | SCG-145743 |
| Description | <ul style="list-style-type: none">It is advised not to use iPerf 3 for AP (Access Point) 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.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. |

R770 Known Issues and Limitations

The following tables provides information on the known issues and limitation in the current release.

Multi-Link Operation (MLO)

| Component/s | AP |
|-------------|--|
| Issue | SCG-146645 |
| Description | The <i>MQ Statistics</i> API CLI provides insights into various metrics related to messaging queues. When querying <i>MQ Statistics</i> for an MLO Client, the counters may display as 0, indicating no impact on the MLO client's connectivity. |

| Component/s | AP |
|-------------|--|
| Issue | SCG-146331 |
| Description | <i>Google Pixel 8</i> 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 | SCG-146685 |

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

| | |
|--------------------|--|
| Component/s | AP |
| Issue | SCG-146638 |
| Description | Google Pixel 8 devices revert to connecting as non-MLO clients after a channel change on an MLO enabled WLAN which is configured to operate on both 2.4GHz and 5GHz frequencies. |

| | |
|--------------------|--|
| Component/s | AP |
| Issue | SCG-146672 |
| 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. |

Other Generic Issues

| | |
|--------------------|--|
| Component/s | AP |
| Issue | SCG-146513 |
| Description | When there are over 50 MS Teams calls, users may encounter poor voice quality or Video lag with AP R770. |

| | |
|--------------------|--|
| Component/s | AP |
| Issue | AP-25334, SCG-146151, AP-26815 |
| Description | Latency on R770 APs can spike when handling multiple clients, especially with <i>Best Effort</i> traffic. Latency may be randomly high on connecting Draeger M300 devices. |

| | |
|--------------------|--|
| Component/s | AP |
| Issue | SCG-145095 |
| Description | vRUE: Service validation is not supported. |

| | |
|--------------------|---|
| Component/s | AP |
| Issue | AP-26421 |
| Description | An association request is not triggered randomly by client. |

| | |
|--------------------|--|
| Component/s | UI/UX |
| Issue | SCG-151651 |
| Description | The controller web user interface intermittently fails to display an accurate client count and may also omit entries for connected clients. This is specific to R770 AP. |

| | |
|--------------------|-----------|
| Component/s | AP |
| Issue | ACX-48543 |

Resolved Issues

| Component/s | AP |
|-------------|--|
| Description | When a client is connected to an R770 Mesh AP, it may experience an inability to receive multicast traffic. This occurs when the R770 MAP (Mesh Access Point) is linked to an R770 RAP (Remote Access Point). However, this limitation is exclusive where the RAP is an R770 model. It does not occur when the RAP is a non Wi-Fi7 AP. |

Resolved Issues

This section details the issues that have been resolved for this release.

Resolved Issues in R7.0.0 Patch1

The tables below lists the resolved issues in the present release.

| Component/s | AP |
|-------------|---|
| Issue | SCG-151918 |
| Description | The WLAN scheduler failed to function as expected; WLANs remained active at all times regardless of the scheduled time. |

| Component/s | AP |
|-------------|---|
| Issue | SCG-151847 |
| Description | When the user unplugged the AP PoE interface cable, reconnected it to the ICX switch port, and manually adjusted the power setting to 802.3at through the controller web user interface or AP CLI, the power consumption status on the AP indicated it as <i>802.3bt5 Switch/Injector</i> . This problem specifically affected the R560, R760, and R770 models. |

| Component/s | AP |
|-------------|--|
| Issue | AP-28815 |
| Description | R560 and R550 APs encountered kernel panics when processing tunnelled multicast traffic. |

| Component/s | AP |
|-------------|--|
| Issue | AP-28589 |
| Description | The R770 AP with <i>JP</i> country code cannot detect radar waveforms. |

| Component/s | AP |
|-------------|--|
| Issue | AP-28485 |
| Description | Fixed an issue where the Traffic Identifier (TID) flows going into the wrong queues as per <i>athstats</i> output. Now, the <i>athstats</i> output is correctly showing the right queues being used. |

| Component/s | AP |
|-------------|--|
| Issue | AP-28481 |
| Description | DFS (Dynamic Frequency Selection) channels 52-65 were not available on R760 or R560 APs for NZ (New Zealand) country code. |

| | |
|--------------------|--|
| Component/s | AP |
| Issue | AP-28398 |
| Description | APs retain docker-related RPM keys after downgrading firmware from R7.0 GA to 6.1.2.0.x. So even if 6.1.2.0.x does not support IoT Containerization, the docker-related configuration is retained, which is addressed in this patch. |

| | |
|--------------------|--|
| Component/s | AP |
| Issue | AP-28388 |
| Description | 802.11ax APs experienced kernel panics when transmitting multicast traffic, especially when the multicast threshold was set to zero, directed multicast was disabled, and RGRE (Remote GRE) was enabled. |

| | |
|--------------------|--|
| Component/s | AP |
| Issue | SCG-146540, AP-28381 |
| Description | Clients connected to the non-mesh interface of R560 or R760 Mesh APs experienced performance degradation. This issue was particularly noticeable when the client was connected to the 2nd radio of R760 while a mesh link was established on the 5GHz 3rd radio of the R760. |

| | |
|--------------------|---|
| Component/s | AP |
| Issue | AP-27944 |
| Description | In RUCKUS AI, AP rogue data for the 2.4GHz band could include channels belonging to the 5GHz band |

| | |
|--------------------|--|
| Component/s | AP |
| Issue | AP-27817 |
| Description | Kernel panics occurred randomly on MAPs, especially when there was a channel change on the RAP due to radar detection. |

| | |
|--------------------|--|
| Component/s | AP |
| Issue | ACX-54246 |
| Description | After upgrading the version from 7.0.0.104.1274 to 7.0.0.104.1283, the status of 802.11ax APs was consistently reported as <i>disconnected from cloud</i> on RUCKUS One. |

| | |
|--------------------|---|
| Component/s | AP |
| Issue | ACX-51274 |
| Description | When R770 AP is configured with Germany, Austria, or UK country code, certain channels 149, 153, 157, 161 are not available. This is addressed in this patch. |

Resolved Issues

Resolved Issues in R7.0.0 Patch1

| Component/s | SZ UI/UX | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------------|---|----------|---------|--------|-------|--------|-------|-------|--|--|--|--|--|------|----------|----------|---------|--------|--|----------|----------|--|--|--|--|-------|---|---|---|--|--|
| Issue | SCG-151884 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Description | <p>Overall percentage of Airtime utilization pie-chart displays utilization more than 100% in some instances.</p> <p>KSP file name: SCG-151884_airtimePieChart-7_0_0_0_726-v1_a1d87d6.ksp</p> <p>NOTE Take cluster backup before applying the KSP.</p> <p>Complete the following steps to apply the KSP file to a single or multiple node cluster: Procedure:</p> <ol style="list-style-type: none"> 1. Log into the cluster UI, select Monitor > Troubleshooting & Diagnostics > Scripts, and upload the KSP file (SCG-151884_airtimePieChart-7_0_0_0_726-v1_a1d87d6.ksp). 2. After the KSP is uploaded to the cluster, log into the first cluster node and apply KSP using the following configuration. When services of the first node become operational, the KSP must be applied on the subsequent nodes individually. Log into a single node cluster CLI and apply the KSP using the following configuration: <pre> vszh7-p# patches vszh7-p(patches)# show applied-patches % Data not found vszh7-p(patches)# vszh7-p(patches)# apply SCG-151884_airtimePieChart-7_0_0_0_726-v1_a1d87d6.ksp INFO : Using a default root directory : /tmp/tmp.R9nZIREKVp Before Patch: 505352cb7511535eff8e582dd9592568 /opt/ruckuswireless/wsg/ apps/lib/scg-push-7.0.0-SNAPSHOT.jar Patch is done! After Patch: e45c963e6c4faad9b56e1b28a970ee25 /opt/ruckuswireless/wsg/ apps/lib/scg-push-7.0.0-SNAPSHOT.jar Before Patch: 09d1ecdleadb51e2d549b24d99062267 /opt/ruckuswireless/wsg/ apps/lib/scg-public-api-7.0.0-SNAPSHOT.jar Patch is done! After Patch: b1f2b900f60680f4ca40e0798bb0e546 /opt/ruckuswireless/wsg/ apps/lib/scg-public-api-7.0.0-SNAPSHOT.jar Restarting tomcat... Wait for tomcat down...(0/120) Wait for tomcat down...(2/120) Stop service tomcat done! Start service tomcat done! </pre> <table border="1"> <thead> <tr> <th></th> <th>total</th> <th>used</th> <th>free</th> <th>shared</th> <th>buff/</th> </tr> </thead> <tbody> <tr> <td>cache</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Mem:</td> <td>32946572</td> <td>11932248</td> <td>2430920</td> <td>234112</td> <td></td> </tr> <tr> <td>18583404</td> <td>20000416</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Swap:</td> <td>0</td> <td>0</td> <td>0</td> <td></td> <td></td> </tr> </tbody> </table> | | total | used | free | shared | buff/ | cache | | | | | | Mem: | 32946572 | 11932248 | 2430920 | 234112 | | 18583404 | 20000416 | | | | | Swap: | 0 | 0 | 0 | | |
| | total | used | free | shared | buff/ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| cache | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mem: | 32946572 | 11932248 | 2430920 | 234112 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 18583404 | 20000416 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Swap: | 0 | 0 | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| Component/s | SZ UI/UX |
|-------------|--|
| | <pre> Restarting core/statshandler... Wait for core down...(0/120) Wait for core down...(2/120) Stop service core done! Start service core done! total used free shared buff/ cache available Mem: 32946572 10473428 3903068 231612 18570076 21461532 Swap: 0 0 0 KSP is done. vszh7-p(patches)# show applied-patches No. Name Description Applied On Log ----- ----- ----- 1 SCG-151884_airtimePieChart-7_0_0_0_726- v1_a1d87d6.ksp fix_total percentage in SZ airtime pie 2024-04-01 07:00:06 /data/ng/rootfs2/hotfix/ 20240401070006-log-v1_0chart display vszh7-p(patches) # </pre> |

R770 Resolved Issues

The tables below lists the resolved issues in the present release.

Multi-Link Operation (MLO)

| Component/s | AP |
|-------------|---|
| Issue | SCG-146759 |
| Description | Occasionally, there was an issue where an AP would utilize a non-configured static channel after modifying the MLO Radio configuration on a WLAN from one radio combination to another. |

| Component/s | AP |
|-------------|---|
| Issue | AP-27786, ACX-49444, SCG-146572 |
| Description | Ping between wireless MLO to wired or wireless client including MLO might have failed depending on the primary link to which the MLO client was associated. |

Other Generic Issues

| Component/s | AP |
|-------------|------------|
| Issue | SCG-146070 |

Changed Behavior

| Component/s | AP |
|-------------|--|
| Description | Uplink Multi-User MIMO (MU-MIMO) is enabled by default on R770 APs. However, for an improved user experience with voice and video applications, it is recommended to disable UL MU-MIMO. Disable this feature through AP CLI by executing the command set ul_mu_mimo wlanx 0 (where x in wlanx represents the WLAN ID). |

| Component/s | AP |
|-------------|---|
| Issue | ACX-49222 |
| Description | The AP randomly encountered target assert or rebooted when a large number of clients roamed between two R770 APs. |

Changed Behavior

The following are the changed behavior issues in this release.


The changes for this release include:

- Controller web user interface legacy menu is not supported.
- Wave-2 APs are not supported.
- Cellular configuration at the Zone Level is unavailable.
- WPA3 (Wi-Fi Protected Access 3) is the default encryption method for Wi-Fi7 APs.
- Channelfly is the default for all radios in R7.0.0, with channelization changing from 80MHz to 40MHz for auto mode.
- Wi-Fi7 APs do not support NSS (Network Subsystem) Offload.

| Component/s | AP |
|-------------|---|
| Issue | SCG-146502 |
| Description | In the SmartZone R7.0.0, L3ACL (Layer 3 Access Control List) takes precedence over Split Tunnel as part of the configuration. |

| Component/s | AP |
|-------------|---|
| Issue | SCG-151928 |
| Description | For optimal performance when connecting a wired client to R560 or R760 or R770 APs, it is advisable to utilize either 802.3bt 5 or DC power. The usage of 802.3at power on these AP models results in the Eth0 port to disable. |

| Component/s | UI/UX |
|-------------|------------|
| Issue | SCG-151881 |

| Component/s | UI/UX |
|--------------------|--|
| Description | <p>In the controller web user interface, the following European Union (EU) countries indicate unsupported channels 149-161 (Ull-3 band) for 802.11ax APs, including models R560 and R760. Only the AP model R770 supports these channels.</p> <p> WARNING Attempting to configure these channels on the controller UI will result in AP configuration failures for all 11ax APs except R770.</p> <ul style="list-style-type: none"> • Austria • Belgium, Bulgaria • Croatia, Cyprus, Czech Republic • Denmark • Estonia • Finland, France • Germany, Greece • Hungary • Iceland, Italy • Latvia, Luxembourg • Malta • Netherlands • Poland • Romania • Slovakia, Slovenia, Spain, Sweden, Switzerland |
| Workaround | It is recommended to deploy R770 in a separate AP Zone if there are legacy 802.11ax APs coexisting in the same network. |

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 | 68ms | 42ms | 93ms | 229ms |
| Jitter | 10ms | 10ms | 10ms | 10ms |
| Bandwidth | 115Mbps | 92Mbps | 40.25Mbps | 23Mbps |

Client Interoperability

NOTE

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

Access Points (APs)

The following are the Client Interoperability issues for APs.

| Component/s | AP |
|-------------|---|
| Issue | AP-25118 |
| Description | The client, aiming to execute Simultaneous Authentication of Equals (SAE) with Pairwise Master Key (PMK) caching, initiates the process by transmitting an authentication frame with the authentication algorithm set to open. The APs responds with an authentication response. Following this, the client submits a re-association request with the Authentication and Key Management (AKM) set to SAE, and it includes the previously derived PMKID. |

| Component/s | AP |
|-------------|--|
| Issue | SCG-145513 |
| Description | Apple iPhone 15 using 17.0 through 17.3 iOS is not discovering 6Ghz networks as advertised in the co-located RnR (Reduced Neighbor Report) on the R560, R760 and R770 Access Points. |

| Component/s | AP |
|-------------|--|
| Issue | AP-26722 |
| Description | Samsung Galaxy S23 <i>Ultra</i> is experiencing disconnection from the Access Point (AP) after roaming to AP2, and this issue is attributed to an EAPOL (Extensible Authentication Protocol over LAN) timeout. |

| Component/s | AP |
|-------------|--|
| Issue | AP-24759 |
| Description | Windows 11 clients encounter difficulties in completing their 802.1x association with FreeRADIUS versions, specifically 3.0.15 and 3.0.16. However, this issue is resolved, and successful associations are observed when using FreeRADIUS versions 3.0.19 and 3.0.23. |

| Component/s | AP |
|-------------|--|
| Issue | AP-24727 |
| Description | A known issue with Windows 11 involves PMK roaming using the 802.1x+WPA3 WLAN. The problem lies in the incorrect calculation of the PMKID provided during re-association, resulting in OKC (Opportunistic Key Caching) failure and necessitating a complete re-authentication. |

| Component/s | AP |
|-------------|---|
| Issue | AP-26796 |
| Description | Clients that do not support WPA3 and send an Open authentication with SAE (Simultaneous Authentication of Equals) in the association request fail to connect to a WLAN in WPA2/WPA3 mixed mode. |

| Component/s | AP |
|-------------|--|
| Issue | SCG-146308 |
| Description | Some Wi-Fi7 clients do not support 320Mhz and still connect with the AP as 160Mhz. Check the client capability before trying 320Mhz channel width. |

| | |
|--------------------|--|
| Component/s | AP |
| Issue | AP-26727 |
| Description | When WPA2-PSK (Wi-Fi Protected Access 2 - Pre-Shared Key) and 802.11r are enabled, the iPhone 11 device processes a full authentication during roaming. However, there are known issues where the iPhone 11 fails to send a reassociate request with FTIE (Fast Transition Information Element). |

| | |
|--------------------|---|
| Component/s | AP |
| Issue | AP-26725 |
| Description | Samsung S23 device might not seamlessly transition (roam) to an R770 AP, even if the AP has a strong Received Signal Strength Indicator (RSSI) and sticky client feature enabled. |
| Workaround | It is recommended to enable sticky client steering to proactively force the roaming. |

| | |
|--------------------|--|
| Component/s | AP |
| Issue | AP-26145 |
| Description | Samsung S24 devices experience connectivity issues when connecting to the networks using WPA3-AES encryption and often displays a password error prompt. |
| Workaround | Update the client driver. |

| | |
|--------------------|---|
| Component/s | AP |
| Issue | AP-24355 |
| Description | Samsung Galaxy S21, does not support Fast Transition (FT) roaming with WPA3-SAE. It utilizes the Pairwise Master Key Security Association (PMKSA) when roaming back to a previously configured AP with WPA3-Personal. |

| | |
|--------------------|---|
| Component/s | AP |
| Issue | SCG-140280 |
| Description | The following devices fail to connect to WPA3-Enterprise networks with GCMP-256 bit encryption. <ul style="list-style-type: none"> • Samsung Galaxy S21 • Samsung Galaxy Z Fold4 • Google Pixel 5 • ASUS ROG • Mi 11 Ultra |

| | |
|--------------------|---|
| Component/s | AP |
| Issue | AP-24923 |
| Description | Apple iPad 1 lacks support for mixed mode profiles, such as WPA2/WPA3 mixed and WPA/WPA2 mixed, resulting in connection failures when connecting to networks with these profiles. |
| Workaround | Avoid configuring mixed mode profile on Apple iPad 1. |

| | |
|--------------------|---|
| Component/s | AP |
| Issue | AP-25255 |
| Description | Chromebook devices experience random disconnections with reason code 4. This is a behavior observed most frequently during roaming. |

Interoperability Information
Client Interoperability

| | |
|--------------------|---|
| Component/s | AP |
| Issue | SCG-141709 |
| Description | Microsoft <i>Surface Pro 4</i> fails to roam to the target AP and instead performs a full authentication process. |

| | |
|--------------------|--|
| Component/s | AP |
| Issue | AP-26791 |
| Description | This issue occurs when the client fails to maintain DHCP, resulting in DSAE (Dynamic Simultaneous Authentication of Equals) being unable to set the binding entry at the DSAE module. This is a limitation from the client device. |

| | |
|--------------------|---|
| Component/s | AP |
| Issue | SCG-140231 |
| Description | <p>The following clients fail to connect to the profile with WPA2/WPA3 mixed mode and 802.11r is enabled.</p> <p>By default, PMF (Protected Management Frames) is enabled. When PMF is set to <i>capable</i>, the mentioned clients fail to connect. However, when PMF is set to <i>required</i>, the clients establish connections.</p> <ul style="list-style-type: none"> • macOS <i>Ventura</i> (22D7750270d) • MacBook Air • macOS <i>Catalina</i> (19H2026) |

| | |
|--------------------|--|
| Component/s | AP |
| Issue | AP-24513 |
| Description | Microsoft <i>Surface Pro 8</i> devices experience frequent disconnections from the AP, often with reason codes 1 (unspecified failure) or 7 (Class 3 frame received from nonassociated STA). |

| | |
|--------------------|---|
| 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. |

| | |
|--------------------|---|
| Component/s | AP |
| Issue | ACX-40890 |
| Description | MacBooks running Big Sur 11.7.7 and macOS Monterey 12.6 see packet or ping loss when the 6GHz radio of the AP is active, and MacBooks are connected to the 5GHz radio of the AP. However, this issue is not observed with MacBooks running Monterey version 12.6.8 or Yosemite version 10.10.5. |

Dynamic Pre-Shared Key (DPSK3)

The following are the Client Interoperability issues for DPSK3.

| | |
|--------------------|--|
| Component/s | AP |
| Issue | AP-25946 |
| Description | Due to the deployment limitations for 6GHz, it is necessary for the client to complete the binding process at the DPSK (Dynamic Pre-Shared Key) service first. |

| Component/s | AP |
|-------------|--|
| Issue | AP-25940, AP-25537 |
| Description | In DPSK3 (DSAE), it is necessary for the client to establish connections with peer WLANs sequentially, starting from intermediate and then progressing to Service WLAN (designated workflow). If the client attempts to connect to the Service WLAN without following the designated workflow, they may encounter connection issues and may need to manually retry the connection. |

| Component/s | AP |
|-------------|---|
| Issue | AP-25897 |
| Description | Despite the caching of each PMK (Pairwise Master Keys) query result in the AP for 60 seconds, clients are still unable to connect even after changing to the correct password within that time frame. |

| Component/s | AP |
|-------------|---|
| Issue | AP-25372 |
| Description | This is a limitation in the deployment of DPSK3. It is essential for the client to follow the appropriate steps to revert to the intermediate WLAN to initiate a reconnection. |

| Component/s | AP |
|-------------|---|
| Issue | AP-25292 |
| Description | This is a design limitation inherent to DPSK3 (DSAE), particularly in relation to the behavior of Windows clients using Intel AX210 wireless cards. In the DPSK3 (DSAE) feature, the AP attempts to transition the client to the target WLAN, but there is no corresponding action from the client to initiate the connection flow. |

| Component/s | AP |
|-------------|--|
| Issue | AP-25194 |
| Description | In the DPSK3 (DSAE) feature, the AP attempt to guide the client to transmit to the Service WLAN. However, the client's behavior does not correspond as expected. |

| Component/s | AP |
|-------------|---|
| Issue | AP-25075 |
| Description | When a station (STA) utilizes the new password after the original binding is complete, the STA connects using WPA2-PSK (Wi-Fi Protected Access Pre-Shared Key) (Service WLAN) due to key rematching on the DPSK server. |

| Component/s | AP |
|-------------|---|
| Issue | AP-25007 |
| Description | Due to deployment restrictions in the 6GHz spectrum, it is necessary for clients to initially complete the binding process at the DPSK Service on 2.4GHz or 5GHz. |

| Component/s | AP |
|-------------|--|
| Issue | AP-24958, AP-24637, AP-24329 |
| Description | In the DPSK3 (DSAE) feature, the AP attempts to guide the client to transmit to the Service WLAN. However, the client's behavior does not correspond as expected, requiring a manual retry to connect to the SSID again. |

Adding AP Patch to the Controller

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

IMPORTANT

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

Follow these steps to apply an AP patch:

1. Download the patch file `ap-scg_7.0_p1_patch_pkg-7.0.0-1404.noarch.patch` and move the patch file to a location that you can access from the computer that you are using to access the controller's web interface.
2. Apply this patch to release 7.0.0 (build number 7.0.0.0.1404).
3. Log on to the SmartZone web interface.
4. Go to the page for uploading AP patches.
 - On the 7.0.0 web interface, go to **Administration > Upload AP Patch > and then click the AP Patch tab.**
5. In **Patch File Upload**, click **Browse** go to the location where you saved the AP patch file (`ap-scg_7.0_p1_patch_pkg-7.0.0-1404.noarch.patch`).
6. Click **Open**.
7. On the **AP Patch** tab, click **Upload**. After the patch file is uploaded, the section is populated with the Start time, AP firmware version number and AP model number.
8. Click **Apply Patch**.
9. After the firmware file is applied, the AP firmware information is populated with the following information:
 - Name of the patch file
 - Size of the patch file
 - AP firmware version number
 - AP model number
10. Go to **Configuration > AP Zone > Select a Zone**.
11. Click **Change AP Firmware**.
12. In the **Change AP Firmware** manually change the AP firmware to the latest AP image (7.0.0.0.1404) in the selected Zone.
13. Click **Yes**
14. When the controller completes updating the AP firmware of the zone, a message appears and notifies you that the zone's AP firmware was updated successfully.
15. Verify that all APs in selected zone are upgraded to 7.0.0.0.1404.
16. Repeat the steps from 10 to 15 for other Zones that need to be updated.

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



© 2024 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
<https://www.commscope.com>