RELEASE NOTES

RUCKUS SmartZone 6.1.0 LT GA Release Notes

Supporting SmartZone 6.1.0

Part Number: 800-72911-001 Rev H
Publication Date: January 2023

Copyright, Trademark and Proprietary Rights Information

Export Restrictions

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

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

Disclaimer

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

Limitation of Liability

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

Trademarks

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

Contents

Document History

Revision Number	Summary of changes	Publication date
H	Added ER-11377 in Resolved Issues on page 38	25, January 2023
G	Modified the section Supported Matrix and Unsupported Models on page 15 .	13, October 2022
F	Modified the section Increased Limit for Unbound/Group DPSK on page 6 to change from per WLAN to per Zone.	13, October 2022
E	Added the build number 5.2.2.0.1563 to ER-11538	01, August 2022
D	Added: 1. Warning on upgrade path from 5.2.2 to 6.1.0 release in Release Information on page 13. 2. A note to refer to the RUCKUS SmartZone Upgrade Guide in the AP Firmware Releases on page 16. 3. Known issue - ER-11538.	11, July 2022
C	• Changed the SZ104D/124D data plane software version to 6.1.0.0.961 • Added resolved issue ER-11154	28, March 2022
B	Updates to behavioral changes	2, March 2022
A	Initial release notes	28, December 2021

New in This Release

This section provides a high-level overview of several key features that are introduced in the SmartZone (SZ) software release 6.1. The release 6.1 is applicable to the RUCKUS SmartZone 300 (SZ300), SmartZone 144 (SZ144), SmartZone Data Plane virtual (vSZ-D) and physical (SZ100-D), Virtual SmartZone – High Scale (vSZ-H), Virtual SmartZone – Essentials (vSZ-E) and controller platforms.

AP to Cluster Failover Enhancement

In an active/standby controller deployment, when the AP's WAN connection fails, the AP cannot reach either active or standby controller. In this situation, the AP replaces its preferred controller from active to standby. When the connection is restored, AP will connect to standby controller instead of the original controller. Release 6.1 changes this behavior and once WAN connectivity is restored, AP will connect to active (primary) controller.

AP Name Addition to Called Station ID

For deployment scenarios where the customer's AAA infrastructure requires knowledge of AP name in Called Station ID, the administrator can now choose AP name to sent. Support for using WLAN BSSID, AP MAC, None, or AP Group remains unchanged.

Backup Configuration Custom File Name for NCM Compatibility

SmartZone can be configured to schedule the process of creating backup network configurations and automatically transfer them to an FTP server. This automated backup method cannot be used with SolarWinds Network Configuration Manager (NCM) because the backup file is automatically named based on the date the configuration was generated. This is a problem because NCM requires the ability to specify the filename of the exported configuration.

This feature allows users to define a backup file name prefix. The controller combines the prefix and date/time stamp to generate the filename for automatic backups. If the prefix is not defined, the prior behavior is retained.

Configurable SSH Tunnel Port between APs and Controller

In some deployments scenarios, controller is located in private data center and APs are installed in branch offices. For security reasons, IT policy may not allow the standard SHH port 22 for communication. In such situation, customers can configure a custom port for communication between AP and the controller.

> **NOTE**
> This setting is not stored in configuration backup from the controller and a restore operation on another node will require the user to configure the port manually.

Controller Server Certificate Renewal

Controller server certificate renewal without changing the private key.

When a user renews the server certificate on the controller, it automatically generates a new key pair. This may not be desirable in many situations as the other network devices (for example, APs, DPs) may lose communication with the controller.

In release 6.1, the default behavior on certificate renewal is to preserve the key pair. Users still have the option to generate a new key pair, if required.

Creating a Switch Group Automatically when Creating an AP Zone

For customers who have both APs and Switches under management, user needs to first create AP Zones and then Switch groups manually. Having to create Zones and Switch Groups separately is cumbersome and error prone.

Now users can enable *Link Switch Group* at the Zone level and this automatically creates the Switch Group. If the user modifies the name of the Zone, the change is also propagated to the Switch Group.

This is also supported via API.

Enable Partner Domain Login using AAA Server

Managed service providers (MSPs) using RADIUS to authenticate controller administrators need to maintain separation of information between tenants on the SmartZone system.

AAA server admin authentication is now supported at *Partner Domain* level.

Enhanced Threat Management via Web Reputation

This capability now provides an added layer of security to clients by utilizing Webroot reputation score for web sites. All traffic with a web reputation score below the threshold configured by the administrator will be blocked automatically.

> **NOTE**
> URL filtering and web reputation filtering work independently of each other. URL whitelist/blacklists take precedence over URL and web reputation based filtering.

Guest Pass Self Registration

Customer looking to provide guest WLAN access typically have to go through a cumbersome manual process. With the self registration feature, controller simplifies the guest access by allowing end users to request access to WLAN directly. This improves the overall user experience and also alleviates IT overhead.

Improved AP to Data Plane Failover

If a connectivity to Data Plane (DP) is lost in deployment scenarios where AP is tunneling data to the DP, the failure to another DP may take long time. In order to reduce the failover period, release 6.1 now allows administrator to enable dual tunnel that establishes tunnels with two DPs simultaneously. If connectivity to one DP is lost, the AP can switch over to the second DP quickly. The administrator can configure the keepalive timer and retry count to fine tune the failover.

NOTE
This capability is not available when IPSec encryption is enabled.

Increased Limit for Unbound/Group DPSK

in many scenarios, customers want to provision a large number of Dynamic Pre-Shared Key (DPSK) for situations such as a public event. To address such situations, release 6.1 increases the unbound/group DPSK scale from 500 to 5000 per Zone.

NOTE
If a large number of DPSKs are configured on the AP, the clients may experience delayed authentication.

LDAP Enhancements

LDAP Search Filter, Duplicate IP Allow and Support Domain Name (DN) as a Certificate Common Name (CN).

Customers are looking at preventing users from different DN from authenticating on non-designated SSID. This requires different AD / LDAP profile with different DN for same IP address and port number. The user is now able to configure multiple LDAP profiles with same IP address and port with a different base DN.

Release 6.1 allows users to configure search filter for LDAP server allowing a more flexible matching criteria compared to using only key attribute.

Prior to release 6.1, the certificate for LDAP server only accepted IP address for Common Name (CN). Now fully qualified domain name (*FQDN*) is supported as well.

Mode Setting for Standby Cluster

In 1:1 active/standby cluster deployments, users can now choose the behavior of the standby cluster on when to serve the end devices:

1. Only when the active cluster is down, or
2. Always, even when the active cluster is available.

NOTE
This option allows customers to mimic behavior prior to release 5.2.

Moving Several APs from an AP Zone in a single API call

Moving several APs from an AP Zone to an other AP Zone in a specific AP Group with a single API command.

Today, we can move APs from one AP Zone to another via API. However, APs need to be moved one by one where the API is invoked for each AP that needs to be moved. This causes an issue when the user has thousands of APs as the process becomes error prone.

The new API allows users to move multiple APs (up to 50) in a single API call.

Mutual Validation between AP/Data Plane and Controller Using Certificates

For **Zero Trust** deployments, customers now have the option of enabling mutual validation between the controller and the data plane and APs. Using X.509 certificates, customers can ensure that only valid devices are on the network.

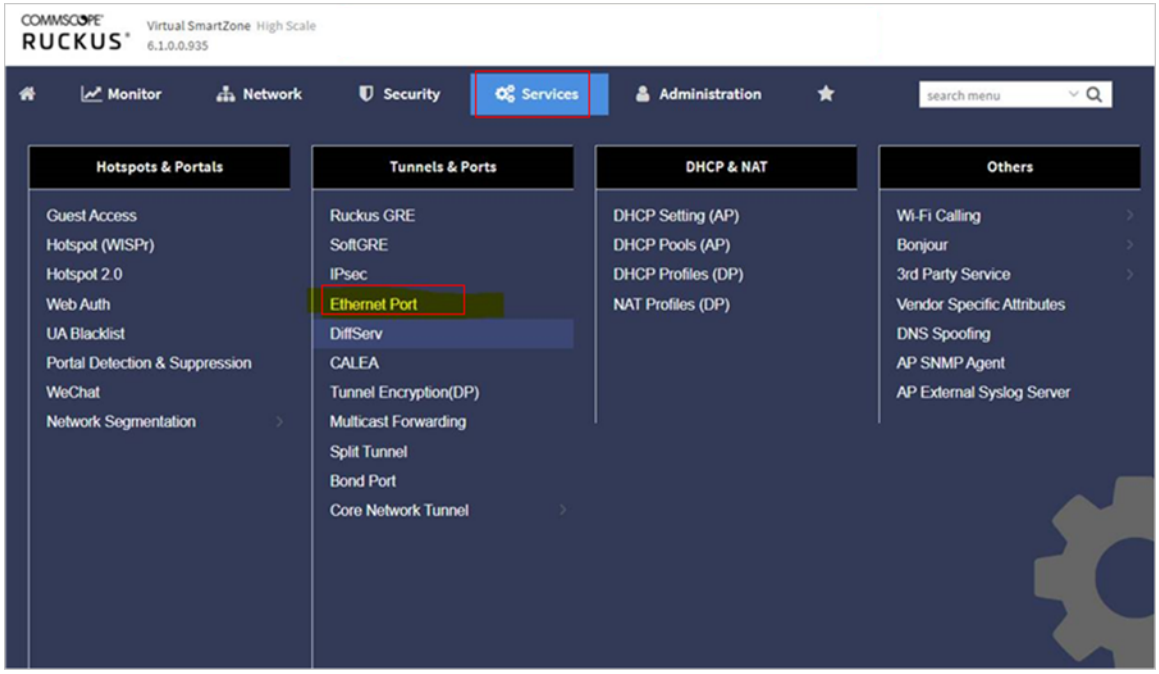
Network Segmentation

Network Segmentation allows a network administrator to easily on-board thousands of wireless and wired devices. Using *Dynamic Preshared Keys*, a network administrator can use Network Segmentation to provide highly scaled network segments. A user is provided their own network segment that is unique to them and their devices, and stays with them as they move through the property - MDU (multiple dwelling units) or a campus environment, for example.

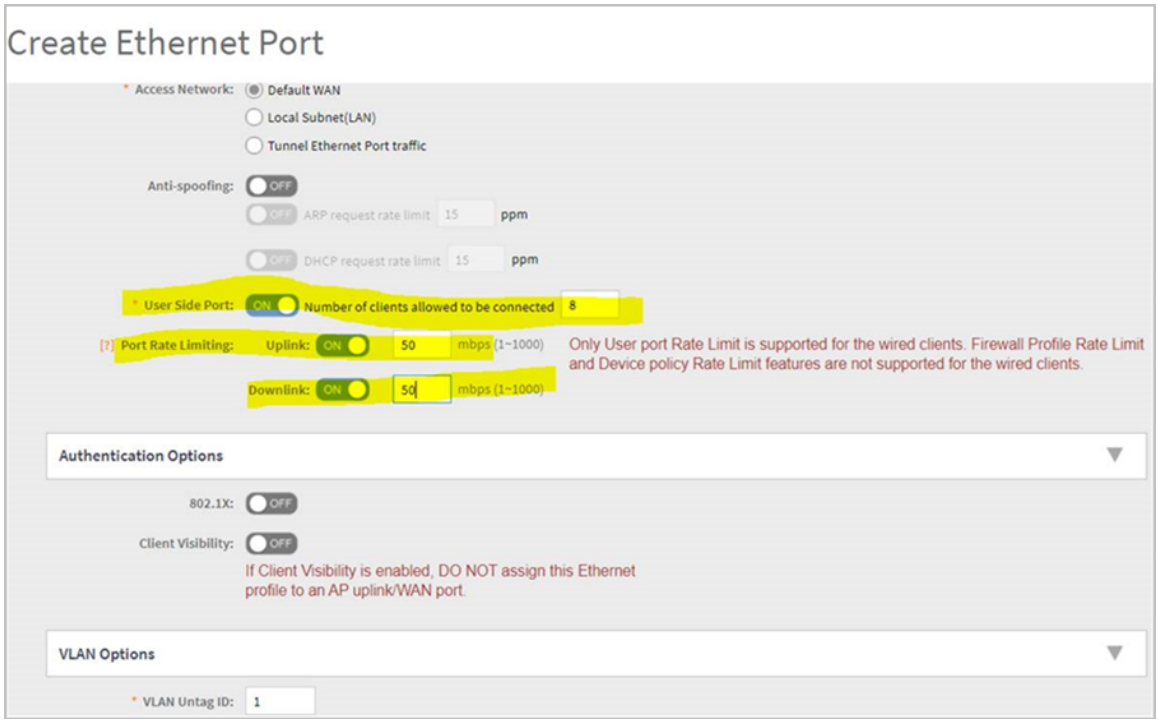
Rate Limit Enhancements

Rate limit enhancements are:

1. Rate limit for wired port is newly introduced in 6.1 and has configurable range of 1Mbps to 1000Mbps.
2. Maximum configurable Firewall profile rate limit values is increased to 500Mbps through controller web user interface and Public API.
3. Maximum configurable SSID rate limit values is increased to 500Mbps through controller web user interface and Public API.
4. Configurable device policy profile rate limit value is 0.1 to 200Mbps through controller web user interface and Public API.
    a. To set the rate limit on the controller web user interface navigate to **Services** > **Ethernet Port** .



b. Create an Ethernet Port Profile



NOTE

For details refer to the **Creating an Ethernet Port Profile** on the RUCKUS SmartZone Administrator Guide, 6.1.0 (SZ300/vSZ-H) or (SZ100/SZ144/vSZ-E).

Limitations and Exceptions

1. Wireless Clients will not be able to browse when wired clients send 500Mbps UDP (User Datagram Protocol) traffic in uplink or downlink with user port rate limit is set to 400Mbps on Ethernet 1 port. This is an HTB limitation, the total bandwidth consumed is very close to the maximum capacity of the HTB algorithm. This cannot be fixed with existing framework.
2. Throughput of Wireless client connected to non rate limit SSID and rate limit SSID gets affected when user port rate limit is enabled on Ethernet port. This is an HTB limitation and cannot be fixed with existing framework.

Rogue Filtering for Geo-Redundancy

Release 6.1 fixes an issue with rogue detection and mitigation when Geo-redundancy is enabled. When active/active Geo-redundancy is enabled, the controller marks the APs from the other geo-location as rouge and if protection is enabled, it starts mitigating actions against those APs.

SZ100 Resets to 1k Trial Licenses

SZ100 resets to 1k trial licenses every time it is factory defaulted.

When a customer sets the SZ100 to factory default, 1k AP trial licenses are renewed. Many Channel Partners complain about the fact end users are not buying AP Capacity licenses and just abuse the system by factory resetting the SZ100 on a periodic basis to expose the full capacity 1k AP trial licenses!

This release fixes the issue and also limits the default trial licenses to five for SZ100.

Scheduled Firmware Updates for AP Zones

Allows users to schedule firmware updates, either upgrades or downgrades for AP Zones. The schedule can be set for a single Zone or multiple Zones. Once the updates are completed, the user can also see the Zone firmware change history.

SNMP Monitoring Per Partner Domain

For MSP (Managed Services Providers) deployments, customers use partner domains to manage their own networks. Release 6.1 allows configuration of a per partner domain server for sending SNMP traps. Users can create profiles for SNMP server at a partner domain level and apply it to a Zone, AP Group or AP. Up to 16 profiles are supported.

Support Bundle for Troubleshooting

This feature helps administrators with improved troubleshooting capabilities and collects relevant logs into a single support bundle. Administrator can choose the types of logs to collect (including AP packet capture) as well as duration of log collection. Administrator can choose up to three APs in a WLAN for simultaneous troubleshooting.

Support for 80 Data Planes Per Four Node SmartZone Cluster

This feature improves the scalability of supported controller data planes. Support for 80 data planes (dp) per cluster (20 data planes per node) is available when CALEA / Flexi-VPN / L3Roaming are NOT being used.

Support 25 built-in AP Management Licenses for SZ144

Customers can now enjoy 25 built-in AP management licenses for SZ144 appliance. These licenses are for SZ144 only and not transferable to any other platform.

Support for Multi-VLAN Per MAC Address

SmartZone data plane now recognizes same MAC address with different VLAN ID as different end clients. This prevents situations where an end device uses different VLANs with the same MAC address and causes the data plane to constantly refresh MAC address table.

Switch Management

Below are the Switch Management features for this release.

Ability to save boot preference

Provides an option at the **switch level** to save the boot preference:

- Default
- Primary Flash
- Secondary Flash

Virtual cable testing on Switches

Provides an option to run a cable test on a selected Switch port and report the results. This feature is available for copper ports (1Gbps, 2.5Gbps and 10Gbps) with port speed set to auto.

Ability to send event email notifications at tenant level

Allows users to override domain level email notification settings for events. Users can now change settings at the Partner Domain, **Domain** (*under System Domain*), and **Switch Group**.

Update the status of a Switch

Allows users to view the latest information about switches on-demand. User can now click on the refresh icon to get an instant update on configuration status.

Ability to convert standalone Switch

Ability to convert standalone switch into a stack by adding member switches. User can select multiple switches and stack them together. They can also extend a stack by adding a new switch.

Port level storm control

User can now enable storm control including broadcast, unknown-unicast and multicast rate limiting at port level.

Blink LEDs on Switch remotely from Controller GUI

Users can now select a switch from SmartZone and blink its LEDs for a specified interval to easily identify the switch or stack.

NOTE
Requires FI 09.0.10 ICX 7250 and ICX 7450 series switches do not support this feature.

Supports ICX7850-48C

SmartZone controller can now manage ICX7850-48C switch.

IPv6 SSH tunnel connection support between Switches and Controller

Release 6.1 now supports connecting to switches through IPv6 control interface for IPv6 deployments.

Flexible authentication profile support

SmartZone now supports creation of flexible authentication profiles for switches that define how the administrator wants to handle the authentication of wired clients. Once defined, administrator can apply these profiles on any port. The following types are supported:

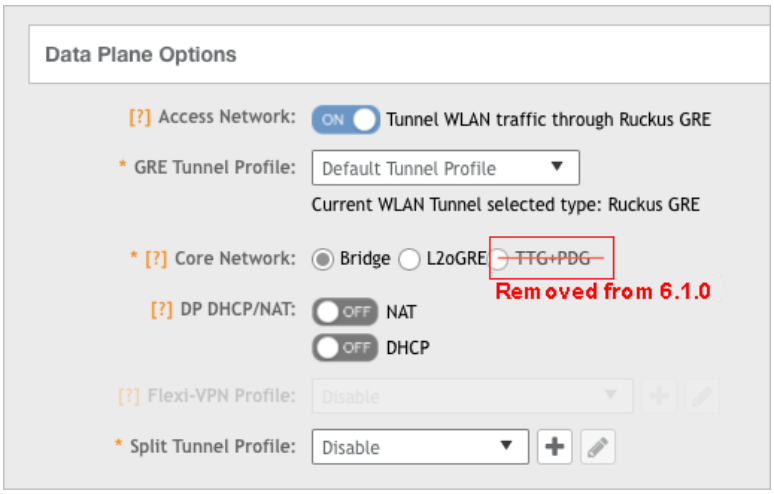
1. 802.1x
2. MAC address authentication
3. 802.1x and MAC address authentication

Syslog Setup Per Partner Domain

For MSP (Managed Services Providers) deployments, customers use partner domains to manage their own networks. Release 6.1 allows configuration of a per partner domain server for sending syslog entries. Users can create profiles for syslog server at a partner domain level and apply it to a Zone, AP Group or AP. Up to 16 profiles are supported.

TTG Feature

Starting from 6.1.0, the option TTG+PFDG in Core Network setting is removed.



User Interface Enhancements

User Interface enhancements include usability improvements, unified wired/wireless dashboard, clickable links in the dashboard and help tip improvements.

- **Unified wired/wireless dashboard**: Now it is easier to manage your wireless and wired network with controller. The dashboard has been enhanced to show both wireless and wired information so users do not have to go to two different pages for status information.
- **Usability improvements**: The tab order now defaults to showing more dynamic information.
- **Clickable links in the dashboard**: Support for deeper linking for dashboard is now available. Clicking on the **Host** in the dashboard navigates to page pointing the host selected and clicking on the **Clients** > > **Application Control (Summary Tab)** highlights the selected client.
- **Help tip improvements**: Miscellaneous improvements to help text in tool tips.

WPA R3 Features

Release 6.1 now supports WPA R3 (Wi-Fi Protected Access® 3) features:

1. **SAE Hash-2-Element** that mitigates side channel attacks. This is enabled by default on APs.
2. **Transition Disable Indication** that provides protection against transition mode downgrade attacks on clients. This feature is configurable through the controller web user interface.
3. For **Hotspot 2.0 access**, users can now choose WPA3 and WPA2/WPA3 mixed mode in the encryption option.

Hardware and Software Support

Overview

This section provides release information about SmartZone 300 (SZ300), SmartZone 100 (SZ100), Virtual SmartZone (vSZ), Virtual SmartZone Data Plane (vSZ-D), SmartZone Data Plane appliance (SZ100-D), SmartZone 144 (SZ-144), SmartZone 144 Data Plane appliance (SZ144-D) and Access Point features.

- The SZ300 Flagship Large Scale WLAN Controller is designed for Service Provider and Large Enterprises, which prefer to use appliances. The Carrier Grade platform supports N+1 Active/Active clustering, comprehensive integrated management functionality, high performance operations and flexibility to address many different implementation scenarios.
- The SZ100, developed for the enterprise market, is the next generation midrange, rack-mountable WLAN controller platform for the enterprise and service provider markets. There are two SZ100 models: the SZ104 and the SZ124.
- The vSZ, which is available in *High Scale* and *Essentials* versions, is a Network Functions Virtualization (NFV) based WLAN controller for service providers and enterprises that desire a carrier-class solution that runs in the cloud. It supports all of the WLAN controller features of the industry, while also enabling the rollout of highly scalable and resilient wireless LAN cloud services.
- The vSZ-D is a Virtual Data Plane aggregation appliance that is managed by the vSZ that offers organizations more flexibility in deploying a NFV architecture-aligned architecture. Deploying vSZ-D offers secured tunneling of wireless client data traffic that encrypts payload traffic; POS data traffic for PCI compliance, voice applications while enabling flat network topology, mobility across L2 subnets and add-on services like L3 Roaming, Flexi-VPN, DHCP Server/NAT as well as CALEA/Lawful Intercept.
- The SZ100-D, is the Data Plane hardware appliance, which is functionally equal to the vSZ-D virtual data plane product. The appliance provides turnkey deployment capabilities for customers that need a hardware appliance. The SZ100-D is managed by a vSZ Controller only and cannot work in a standalone mode.

- The SZ144 is the second generation mid-range rack-mountable WLAN controller platform developed for the Enterprise and Service provider markets. The SZ144 is functionally equivalent to the vSZ-E virtual controller product. SZ144 is first introduced in the software release 5.2.1. It cannot run any software prior to this release. It does not support any AP zones which run the AP firmware prior to 5.2.1.
- The SZ144-D is the second generation Data Plane hardware appliance which is functionally equivalent to the vSZ-D virtual Data Plan product. The appliance provides turnkey deployment capabilities for customers that need a hardware appliance. The SZ144-D is managed by a vSZ Controller only and cannot work in a standalone mode.
- Access Point (AP): Controllers support 1000 APs per zone.

Release Information

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

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

WARNING

- Upgrade from SmartZone (SZ) R5.2.0.0.699, R5.2.1.0.515, R5.2.2.0.317, R5.2.2.0.1161, R6.0.0.0.1331 to R6.1.0.0.935 is supported
- Upgrade from release 5.2.2.0.1562 to 6.1.0.0.935 is **not** supported. [ER-11538]

SZ300

- Controller Version: **6.1.0.0.935**
- Control Plane Software Version: **6.1.0.0.683**
- Data Plane Software Version: **6.1.0.0.935**
- AP Firmware Version: **6.1.0.0.1595**

SZ100/SZ124/SZ104/SZ144

- Controller Version: **6.1.0.0.935**
- Control Plane Software Version: **6.1.0.0.683**
- Data Plane Software Version: **6.1.0.0.601**
- AP Firmware Version:**6.1.0.0.1595**

vSZ-H and vSZ-E

- Controller Version: **6.1.0.0.935**
- Control Plane Software Version: **6.1.0.0.683**
- AP Firmware Version:**6.1.0.0.1595**

Cloudpath

- Cloudpath Version: **5.9 R3 (Build 5179) or later**

SZ104D and SZ124D

- Data plane software version: **6.1.0.0.961**

vSZ-D and SZ144D

- Data plane software version: **6.1.0.0.935**

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

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

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

SZ Google Protobuf (GPB) Binding Class

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

1. SmartZone **6.1.0.0.935** (GA) GPB.proto (Google ProtoBuf) image for GPB/MQTT [DNP] –

   https://support.ruckuswireless.com/software/3261

   File: ruckus_sz_6.1.0_protos.tar.gz

   Checksum: 168c1c8f0ad3702345de30e8cfec357f

2. SmartZone **6.1.0.0.935** MockSCI-TLS (SZ to SCI MQTT subscriber software) for CentOS / Ubuntu

   https://support.ruckuswireless.com/software/3262

   File: scg-mock-sci-6.1.0-20211129.082645-79.tar.gz

   Checksum: d6e3990d6d4c14148445efdf9e926f2d

IoT Suite

This section lists the version of each component in this release.

- vSCG (vSZ-H and vSZ-E), and SZ-124: **6.1.0.0.935**
- Control plane software version in the WLAN Controller : **6.1.0.0.683**
- AP firmware version in the WLAN Controller:**6.1.0.0.1595**

RUCKUS IoT Controller

- RUCKUS IoT Controller version: 1.8.2.0
- VMWare ESXi version: 6.5 and later
- KVM Linux Virtualizer version: 1:2.5+dfsg-5ubuntu 10.42 and later
- Google Chrome version: 78 and later
- Mozilla Firefox version: 71 and later

Public API

Click on the following links to view:

- SmartZone 6.1.0 Public API Reference Guide (ICX Management), visit

  SmartZone 6.1.0 Public API Reference Guide (ICX Management)
- SmartZone 6.1.0 Public API Reference Guide (SZ100), visit

  SmartZone 6.1.0 Public API Reference Guide (SZ100)

  NOTE
  SZ100 Public API link is for SZ144 as well.
- SmartZone 6.1.0 Public API Reference Guide (SZ300), visit

  SmartZone 6.1.0 Public API Reference Guide (SZ300)
- SmartZone 6.1.0 Public API Reference Guide (vSZ-E), visit

  SmartZone 6.1.0 Public API Reference Guide (vSZ-E)
- SmartZone 6.1.0 Public API Reference Guide (vSZ-H), visit

  SmartZone 6.1.0 Public API Reference Guide (vSZ-H)

Dynamic Signature Package (Sigpack) Update

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

For manual upgrade, follow below steps:

1. Download Signature package by visiting the RUCKUS support site:
   - Regular Sigpack only for controller release 6.1.0: https://support.ruckuswireless.com/software/3156-smartzone-6-1-0-0-675-sigpack-1-540-1-regular-application-signature-package
   - Non-Regular Sigpack for controller release 6.1.0 and older releases: https://support.ruckuswireless.com/software/3157-smartzone-6-1-0-0-675-sigpack-1-540-1-application-signature-package
2. Manually upgrade the signature package by navigating to **Security** > **Application Control** > **Application Signature Package**.

   NOTE
   More details can be found in Administrator Guide, in section *Working with Application Signature Package*

If 802.11ac Wave 1 APs are on legacy firmware (AP firmware prior to R6.1.0 release), you cannot download the current Sigpack version 1-540-1 regular Sigpack but can download the current non-regular Sigpack. If 802.11ac Wave 1 APs are on on R6.1 firmware, clients can download both 1-540-1 regular and non regular signature packs. **[SCG-123375]**

NOTE
As R5.1.x to R6.1.0 release upgrade is not supported, RUCKUS does not have any signature-package upgrade restrictions during zone upgrade.

Supported Matrix and Unsupported Models

Before upgrading to this release, check if the controller is currently managing AP models, IoT and Switch feature matrix.

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

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

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

AP Firmware Releases

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

Upgrade path	AP firmware releases in controller
5.2.x > 6.0.x > 6.1.x	5.2.x or 6.0.x > 6.1.x
5.1.x > 5.2.x > 6.1.x	5.2.x > 6.1.x
5.0 > 5.1.x > 5.2.x > 6.1.x	5.2.x > 6.1.x

NOTE
Refer to the *SmartZone Upgrade Paths* section in the *RUCKUS SmartZone Upgrade Guide, 6.1.0* for supported and not supported upgrade build paths.

Supported AP Models

This release supports the following RUCKUS AP models.

TABLE 1 Supported AP Models

11ax		11ac-Wave2		11ac-Wave1
Indoor	**Outdoor**	**Indoor**	**Outdoor**	**Indoor**
R730	T750	R720	T710	R310
R750	T750SE	R710	T710S	
R650	T350C	R610	T610	
R550	T350D	R510	T310C	
R850	T350SE	H510	T310S	
R350		C110	T310N	
H550		H320	T310D	
H350		M510	T811CM	
		R320	T610S	
			E510	
			T305E	
			T305I	

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

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

Unsupported AP Models

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

TABLE 2 Unsupported AP Models

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

Switch Management Feature Support Matrix

Following are the supported ICX models:

The following ICX switch models can be managed from SmartZone:

- ICX 7150
- ICX 7250
- ICX 7450
- ICX 7550
- ICX 7650
- ICX 7850

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

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

Following is the matrix for ICX and controller release compatibility:

TABLE 3 ICX and SmartZone Release Compatibility Matrix

	SmartZone 5.0	SmartZone 5.1	SmartZone 5.1.1	SmartZone 5.1.2	SmartZone 5.2.0	SmartZone5.2.1	SmartZone 6.0.0	SmartZone 6.1.0
FastIron 08.0.80	Yes	Yes	Yes	No	No	No	No	No
FastIron 08.0.90a	No	No	Yes	Yes	Yes	Yes	Yes	No
FastIron 08.0.91	No	No	Yes	Yes	Yes	No	No	No
FastIron 08.0.92	No	No	No	Yes	Yes	Yes	Yes	Yes
FastIron 08.0.95	No	No	No	No	No	Yes	Yes	Yes
FastIron 08.0.95a	No	No	No	No	No	Yes	Yes	Yes
FastIron 08.0.95b	No	No	No	No	No	Yes	Yes	Yes
FastIron 08.0.95c	No	No	No	No	Yes	Yes	Yes	Yes
FastIron 09.0.10a	No	No	No	No	No	No	No	Yes

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

TABLE 4 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-100/vSZ-E	5.1.2 and later	08.0.90a and later
Download Syslogs for a Selected Switch. **NOTE** To download system logs from SmartZone for a particular ICX switch, TFTP must be enabled.	5.2.1 and later	08.0.91 and later
Switch Topology	5.2 and later	08.0.92 and later
Designate a VLAN as Management VLAN	5.2.1 and later	08.0.95 and later
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
DNS-based SmartZone Discovery	5.1.2 and later	08.0.95c and later
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
Flexible Authentication Configuration	6.1 and later	09.0.10a and later

IoT Suite

This release supports IoT Controller release 1.8.2.0 and is compatible with the following controller and access point hardware and software.

Compatible Hardware

- C110 Access Point (C110)
- E510 Access Point (E510)
- H510 Access Point (H510)
- M510 Access Point (M510)
- R510 Access Point (R510)
- R550 Access Point (R550)
- R610 Access Point (R610)
- R650 Access Point (R650)
- R710 Access Point (R710)
- R720 Access Point (R720)
- R730 Access Point (R730)
- R750 Access Point (R750)
- T310 Access Point (T310)
- T610 Access Point (T610)
- T750 Access Point (T750)
- T750SE Access Point (T750SE)
- I100 IoT Module (I100)
- H550 Access Point (H550)
- H350 Access Point (H350)
- T350SE Access Point (T350SE)

Compatible Software

- Virtual SmartZone – High Scale (vSZ-H)
- Virtual SmartZone – Essentials (vSZ-E)
- SmartZone 100 (SZ100)
- RUCKUS IoT Controller (RIoT)

The below table lists the supported IoT end devices.

NOTE
Multiple other devices may work with this release but they have not been validated.

TABLE 5 Bulbs

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Lightify (RGB) Model 73674	Bulb	Zigbee	Osram	OSRAM	LIGHTFY A19 RGBW
Lightify Model 73693	Bulb	Zigbee	Osram	OSRAM	LIGHTIFY A19 Tunable White45856
Lightify Model 73824	Bulb	Zigbee	Osram	OSRAM	
Element Color Plus	Bulb	Zigbee	Sengled	sengled	E11-N1EA
Bulb - LED	Bulb	Zigbee	Sengled	sengled	Z01-A19NAE26
E11-G13	Bulb	Zigbee	Sengled	sengled	E11-G13
Lux	Bulb	Zigbee	Philips	Philips	LWB004
SLV E27 Lamp Valeto (Zigbee 3.0)	Bulb	Zigbee 3.0	SLV		
Bulb	Bulb	Zigbee	Aduro SMART ERIA		
Bulb	Bulb	Zigbee	Cree		BA19-08027OMF-12CE26-1C100
Hue	Bulb	Zigbee	Philips	Hue White	840 Lumens

TABLE 6 Locks

Device	Type	Model	Manufacturer	Basic Name	Basic Model
Vingcard Signature	Lock	Zigbee	Assa-Abloy	AA_LOCK	
Vingcard Essence	Lock	Zigbee	Assa-Abloy	AA_LOCK	
RT+	Lock	Zigbee	Dormakaba	Dormakaba	79PS01011ER-626
Yale YRD220/240 TSDB Display	Lock	Zigbee	Assa-Abloy	Yale	Yale YRD220/240 TSDB
Yale YRD210 Push Button	Lock	Zigbee	Assa-Abloy	Yale	YRD210 Push
Smartcode 916	Lock	Zigbee	Kwikset	Kwikset	SMARTCODE_DEADBOLT_10T
Smartcode 910 (450201)	Lock	Zigbee	Kwikset	Kwikset	

TABLE 7 SWITCHES/PLUGS/THERMOSTAT/ALARM/BLINDS

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
GE Smart Dimmer	Switch	Zigbee	GE	Jasco Products	45857
GE Smart Dimmer	Switch	Zigbee	GE	Jasco Products	45856
Smart Plug	Plug	Zigbee	CentraLite	CentraLite	
Smart Plug	Plug	Zigbee	Smart things	Samjin	
Smart Plug	Plug	Zigbee	INNR		
Zen Thermostat	Thermostat	Zigbee	Zen Within	Zen Within	Zen-01
EcoInsight Plus	Thermostat	Zigbee	Telkonet	Telkonet	
ZBALRM	Alarm	Zigbee	Smartenit		Model #1021 A
Smart Blinds	Blinds	Zigbee	Axis Gear		

TABLE 8 Sensors

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Garage Door Tilt Sensor	Sensor	Zigbee	NYCE	NYCE	NCZ-3014-HA
Curtain Motion Sensor	Sensor	Zigbee	NYCE	NYCE	NCZ-3045-HA
Door / Window Sensor	Sensor	Zigbee	NYCE	NYCE	NCZ-3011-HA
Temperature and Humidity Sensor	Sensor	Zigbee	Aqara	LUMI	WSDCGQ11LM
Motion Sensor	Sensor	Zigbee	Aqara	LUMI	RTCGQ11LM
ERIA Smart Door/ Window Sensor	Sensor	Zigbee	AduroSMART ERIA	ADUROLIGHT	81822
ERIA Smart Motion Sensor	Sensor	Zigbee	AduroSMART ERIA	ADUROLIGHT	81823
Multipurpose Sensor	Sensor	Zigbee	Smart things	Samjin	IM6001-MPP01
Button	Sensor	Zigbee	Smart things	Samjin	IM6001-WLP01
Motion Sensor	Sensor	Zigbee	Smart things	Samjin	IM6001-MTP01
Water Leak Sensor	Sensor	Zigbee	Smart things	Samjin	IM6001-BTP01
EcoSense Plus	Sensor	Zigbee	Telkonet	Telkonet	SS6205-W
EcoContact Plus	Sensor	Zigbee	Telkonet		SS6255-W
Temp, Humidity Sensor	Sensor	Zigbee	Heiman	HEIMAN	HS1HT-N
Gas detector	Sensor	Zigbee	Heiman	HEIMAN	HS3CG
Contact Sensor/Door Sensor	Sensor	Zigbee	CentraLite	CentraLite	3300-G
3-Series Motion Sensor	Sensor	Zigbee	CentraLite	CentraLite	3305-G
Temperature Sensor	Sensor	Zigbee	CentraLite	CentraLite	3310-G
3-Series Micro Door Sensor	Sensor	Zigbee	CentraLite	CentraLite	3323-G
Door Sensor	Sensor	Zigbee	Ecolink	Ecolink	4655BC0-R
Temp & Humidity Sensor	Sensor	Zigbee	Sonoff	Sonoff	SNZB-02
Celling Motion Sensor	Sensor	Zigbee	NYCE	NYCE	NCZ-3043-HA

TABLE 9 LoRa

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Picocell	Gateway	LoRa	Semtech		
Mini Hub/ Basic station	Gateway	LoRa	TABS		
Door Sensor	Sensor	LoRa	TABS		
Occupancy Sensor	Sensor	LoRa	TABS		

TABLE 10 BLE

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Panic Button	Beacon	BLE	TraknProtect		
Tray Beacon	Beacon	BLE	TraknProtect		
Asset Beacon	Beacon	BLE	TraknProtect		
Card Beacon	Beacon	BLE	TraknProtect		
Card Tag	Beacon	BLE	Kontakt.io		CT18-3
Beacon Pro	Beacon	BLE	Kontakt.io		BP16-3
Asset Tag	Beacon	BLE	Kontakt.io		S18-3

TABLE 11 Wired

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Vape/Sound Sensor	Sensor	Wired	Soter	-	FlySense

TABLE 12 Supported Devices tested with SmartThings

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Yale YRD220/240 TSDB Display	Lock	Zigbee	Assa-Abloy	Yale	YRD220/240 TSDB
Lightify (RGB) Model 73674	Bulb	Zigbee	Osram	OSRAM	LIGHTFY A19 RGBW
Multipurpose Sensor	Sensor	Zigbee	SmarThings	Samjin	
Button	Sensor	Zigbee	SmartThings	Samjin	
Motion Sensor	Sensor	Zigbee	SmartThings	Samjin	
Water Leak Sensor	Sensor	Zigbee	SmartThings	Samjin	
Smart Plug	Sensor	Zigbee	SmartThings	Samjin	
Bulb	Bulb	Zigbee	Aduro SMART ERIA		
AEOTEC Multi Sensor	Sensor	Zwave	AEOTEC	AEOTEC	ZW 100-A
Hue Hub	Hub	Wired	Philips	Philips	3241312018A

TABLE 13 Device not QA tested but supported

Device	Type	Mode	Manufacturer	Basic Name	Basic Model
Vingcard	Sigma	Lock	Zigbee	Assa-Abloy	AA_LOCK
Vingcard	Alpha	Lock	Zigbee	Assa-Abloy	AA_LOCK
Vingcard	Classic		Zigbee	Assa-Abloy	AA_LOCK
Vingcard	Allure		Zigbee	Assa-Abloy	AA_LOCK

Known Issues

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

NOTE
Known issues stated in the 6.0.0 release notes are also applicable to this release.

Component/s	System
Issue	ER-11538
Description	Upgrade from release 5.2.2.0.1562 or 5.2.2.0.1563 is **not** supported.

Component/s	AP
Issue	SCG-132557
Description	11ac AP disconnects idle clients before inactivity timeout.

Component/s	AP
Issue	SCG-134545
Description	iOS clients running on 15.x.x version does not send DHCP option 12. This results in the hostname field having client MAC address in *client-info*.

Component/s	AP
Issue	SCG-132339
Description	When GEO redundancy is enabled, the APs in controller will not be included in the rogue list.

Component/s	AP
Issue	SCG-130680
Description	Configuration backup/restore fails to contain the alias SSH port setting.
Workaround	The Alias SSH port setting is not included in the configuration backup file. The alias SSH port setting might be lost if the user changes the Alias SSH port setting while configuring backup and restore for the below two cases: • Standby cluster (geo-redundancy enabled) • SmartZone without Alias SSH port setting (for example, fresh installation of SmartZone). Users must manually setup the Alias SSH port settings. SmartZone retains the current Alias SSH port setting after configuration restore.

Component/s	AP
Issue	SCG-133952
Description	If a customer configures and maps AVC IPv6 profiles to wireless/wired interface in alpha or beta build and later upgrades the build without AVC IPv6 support, the controller shows the previously configured profiles and the AP shows the mapped IPv6 details. Configurations will be visible but feature (in IPv6 mode) is not supported.

Component/s	AP
Issue	SCG-134597

Component/s	AP
Description	Windows OS clients does not support 11r+WPA2-PSK FT roaming. Visit https://docs.microsoft.com/en-us/windows-hardware/drivers/network/fast-roaming-with-802-11k--802-11v--and-802-11r for details.

Component/s	AP
Issue	SCG-134597
Description	Microsoft Surface Pro with the below system combination is not able to connect to WLAN having WPA2/ WPA2-WPA3-Mixed and 11r + 11w both enabled. System specifications: • OS : Windows10-21H2 • WIFI NIC : Marvell AVASTAR wireless-AC network controller • Driver Version : 15.68.9127.58 OS : Windows10-21H2 WIFI NIC

Component/s	AP
Issue	SCG-132557
Description	11ac AP disconnects idle clients before inactivity timeout.

Component/s	AP
Issue	SCG-134021
Description	AP cannot honor session timeout value if it is less than 120 seconds. Minimum session time that AP can accept is 120 seconds.

Component/s	AP
Issue	AP-16966
Description	Firewall ID fails to update to the client, when client roams from one AP to another with FT enabled. This can occur only when there is high latency between AP to controller communication.

Component/s	AP
Issue	SCG-133417; AP-15840
Description	When streaming YouTube videos, traffic goes on*googlevideos.com* domain, and if safe-search is enabled, then even safe content cannot be loaded and is an application/website behavior.

Component/s	AP
Issue	AP-14102
Description	R850/R750 APs WAN Ethernet port fails when Ethernet speed on the Switch, connected to the AP is configured as 100 full. This limitation is observed with ICX7150-C12 10.1.11T225 (mnz10111) and not observed with ICX7150-48Z (SPS08092b.bin).

Component/s	AP
Issue	AP-14280 ; ER-7951
Description	Jumbo packets larger than 1620 bytes are dropped on 11ac wave-2, 11ax APs.

Component/s	AP
Issue	AP-16151
Description	If client sends a non-FT (Fast Transition) AKM (Authenticated Key Management) suite in FT association request, AP rejects it with association response status code set to invalid AKMP.

Component/s	AP
Issue	SCG-132916
Description	Windows 10/11 clients fails to connect to WPA3 configured WLAN. 1. Surface-Pro-1 • C4:9D:ED:91:63:AE • 10 Pro-20H2(19042.1165) • Marvell Semiconductors, Inc. • 15.68.17021.121 2. Desktop-76 • 34:F3:9A:8A:A1:DD • 10 Pro 21H1(19043.1165) • Intel Dual Band wireless AC-8260 • 20.70.21.2 3. surfacePro • 4C:0B:BE:0C:3D:C6 • 10 Pro 21H1(19043.1165) • Marvell Semiconductors, Inc. • 15.68.9127.58 4. Desktop-196 • C4:9D:ED:91:63:AE • 11 Pro 21H2(22000.16) • Intel WiFi6E AX210 160MGHZ • 22.70.3.2

Component/s	AP
Issue	SCG-131205
Description	Background scan channel selection algorithm fails to change to a better channel despite the current channel not providing adequate and expected service/performance.
Workaround	It is recommended to use Channelfly as channel selection algorithm instead.

Component/s	AP
Issue	SCG-133323
Description	After successful UEs Windows version 10 and 11 connection, if the device moves away from the AP RF coverage and if the client comes within the AP RF coverage and within inactivity timeout then the device goes for a full authentication instead of skipping authentication.

Component/s	AP
Issue	SCG-133325
Description	Mobile device with Android version 9 version goes for a full authentication after reconnecting within inactivity timeout.

Component/s	AP
Issue	SCG-123495
Description	AP runs out of memory and *Page allocation failure* is seen when moving UDP traffic from client in unidirectional. This limitation is not applicable to bidirectional traffic.

Component/s	AP
Issue	SCG-127767
Description	DHCP/NAT performance drop is observed, when running back to back performance tests with Ixia or any performance benchmark tool. This drop is observed due to rflow age out timer not updating or entry not being refreshed while running back to back test iterations.
Description	Give a five minute gap between each iteration of performance test, for rflow entries are cleared.

Component/s	AP
Issue	SCG-127791
Description	Inconsistent offload traffic is observed between two wireless client connecting to two different tunneled WLANs belonging to the same VLAN. This limitation is in case of non-default VLAN only, where first time a flow is created while moving traffic between two clients is seen offloaded and subsequent flows go through the host path.

Component/s	AP
Issue	SCG-123943
Description	When AP radios are disabled, the *get client-info* from AP CLI fails to show the updated client entries. This does not impact client connectivity.

Component/s	AP
Issue	SCG-130770
Description	To block torrents from downloading ubuntu file below apps need to blocked under ARC policy. • App Name: All Category : Peer to Peer • App Name: MoPub Category : Web • App Name: Liftoff Category : Web • App Name: Ubuntu Category : Web

Component/s	AP
Issue	SCG-131270
Description	Hotstar application fails to get detected when AP or the controller is running on Sigpack version 540.1 or below.

Component/s	AP
Issue	SCG-133049
Description	**arc-debug-start** is a command to enable ARC debug logs. This is a script which stores logs and*pcaps (packet capture)* in temporary folder of AP. If this script is run for a long duration it causes an OOM (Out of Memory) on AP. Its better to enable debug-log via CLI and capture "logread -f" traces if we need to capture logs for long duration..

Component/s	AP
Workaround	It is recommended to enable debug logs through CLI mode and to capture **logread -f** traces to capture logs of a long duration.

Component/s	AP
Issue	SCG-133408
Description	Most of the IPv4 flows are detected as stun or falls back to IP address based detection during audio and video calls.

Component/s	AP
Issue	SCG-133019
Description	For Network Segmentation by design, if *Bonjour Fencing hop0* is enabled for Chromecast service, SSDP (Simple Service Discovery Protocol) packets are dropped. Currently when a Zone is enabled with bonjour fencing, all WLAN (including the WLANs selected for the network segmentation) of that Zone is functioned with bonjour fencing. If a Zone has bonjour features turned on, the WLANs from that zone cannot be part of the network segmentation. If a Zone has WLANs in the network segmentation, the bonjour features cannot be turned on.

Component/s	AP
Issue	SCG-133641
Description	UDP packet size 1512bytes drops and traffic passes with 1000 bytes frame size.

Component/s	AP
Issue	SCG-127469
Description	When sending video, best effort and background traffic from wired to wireless client is observed all traffic goes with video priority even for best effort traffic even if the client disconnect and re-associates to AP. This limitation is only if WLAN VLAN and management VLAN of the AP uses the same VLAN. If AP management VLAN and WLAN VLAN are different then best effort traffic goes properly.

Component/s	AP
Issue	SCG-133739
Description	For Dakota based APs the RGRE tunnel with encryption may have slightly lower performance in SmartZone 6.1 release.

Component/s	AP
Issue	SCG-127253
Description	When DHCP-NAT hierarchy network is used, the Non-Gateway AP remains disconnected (goes offline) from the controller once firmware upgrade is completed. The non-gateway AP becomes operational after it is rebooted.

Component/s	AP
Issue	SCG-133418
Description	YouTube flows are detected as *forcesafesearch.google.com* when both Google and YouTube FQDN (Fully Qualified Domain Name) safe search is enabled.

Component/s	AP
Issue	SCG-133991
Description	Wi-Fi calling start and end time status gets updated, when client connects to DHCP-NAT enabled WLAN. Ideally the status should gets updated based on Wi-Fi calls made by the client. This issue is specific to DHCP-NAT case only.

Component/s	AP
Issue	SCG-128898
Description	In mixed 11ac and 11ax AP mesh deployment when MAP is 11ac AP and RAP (Remote AP) is 11ax AP, MAP fails to get IPv6 address in dual zone This limitation is not observed with IPv4 or 11ac MAP - 11ac RAP case.

Component/s	AP
Issue	SCG-134451
Description	For some wireless clients, namely STA connected to a MAP is not passing traffic. The transmit modulation coding scheme indicates zero. **NOTE** S21 works but S10 experiences the issue.

Component/s	AP
Issue	SCG-123157
Description	Android 10 and 11 version which has MAC address randomization features as default, it can affect the Wi-Fi experience.
Description	For MAC related authentication, disable Wi-Fi MAC randomization and select *Use Device MAC* while connecting to SSID.

Component/s	AP
Issue	SCG-131305
Description	MAC/IP address encrypt on WISPr profile only supports cloud profile.

Component/s	AP
Issue	SCG-133932
Description	Currently the controller only can see Network Segmentation wireless clients information and not wired clients.

Component/s	AP
Issue	SCG-127995
Description	Second wired client connected to the AP does not receive DHCP address and cannot browse, when Ethernet profile is configured for 802.1x port based MAC bypass and when non-default VLAN is used. This limitation is applicable only for RUCKUS 11ax AP's. **NOTE** This issue is not observed with VLAN 1 in Ethernet profile.
Workaround	Connect the second wired client and reboot the AP.

Component/s	AP
Issue	SCG-128235
Description	2.4G Airtime utilization shows high percentage though no clients are connected. This issue is random.

Component/s	AP
Issue	SCG-133894
Description	Sleeping clients may cause latency to be flagged on the controller web user interface even though radio frequency (RF) environment is clean.

Component/s	AP
Issue	SCG-132708
Description	Controller administrator can get all the AP information on *DRS-broker* by using API with any controller cloud access token.

Component/s	AP
Issue	SCG-134434
Description	In Japan country code, channels 132, 136, 140, 144 are applicable and these channels will be enabled only if *Allow Channel 144* is enabled in Zone. If both 11ac and 11ax APs are present in the configured Zone with one of these channels (132, 136, 140 or 144) it results in 11ac APs configuration update failure whereas 11ax configuration is successful.

Component/s	AP
Issue	SCG-134775
Description	Below MAC OS does not support WPA3 enterprise and PSK. • OS X EL CAPTAIN--10.11.6 • MACOS Mojave 10.14.5 • MACOS Sierra 10.12.6 • OS X 10.9.5
Workaround	Do not configure WPA3 personal or Enterprise WLAN. Configure WPA2/WPA3 mixed mode since clients supports mixed mode operation.

Component/s	AP
Issue	SCG-134376
Description	Microsoft Surface Pro with below system combination is not able to connect to WLAN having WPA2/ WPA2-WPA3- mixed mode and 11r with 11w both enabled. System specification is: • OS : Windows10-21H2WIFI NIC • Marvell AVASTAR wireless-AC network controller • Driver Version : 15.68.9127.58
Workaround	• Upgrade the Wi-Fi driver to latest version 15.68.17021.121.2. • Do not enable 11r and 11w together. Enable 11r or 11w

Component/s	AP
Issue	SCG-134087

Component/s	AP
Description	Windows10 Pro version 2004 laptop with 6E NIC fails to scan SSIDs when only 6G radio is enabled.
Workaround	Upgrade the laptop with Windows11 Pro version 21H2 to scan 6G radio.

Component/s	AP
Issue	SCG-134777
Description	Sometimes Netflix traffic can get detected as *Fast_com* due to recent integration of *Fast_com* speedtesting option on Netflix application.

Component/s	AP
Issue	SCG-134780
Description	Only 200Mbps SSID rate limit value gets applied to all 11ac AP models when SSID rate limit values are between 200 to 500 Mbps when configured on WLAN. Values between 200 - 500Mbps is applicable only to 11ax AP models.

Component/s	AP
Issue	AP-17000
Description	When SSID rate limit is set to 500Mbps in the controller GUI and if 11ac AP is configured in the Zone then the maximum rate limit value set on 11ac AP models is only 200Mbps. All 11ax APs is set with a maximum rate limit value of 500Mbps per design. Values between 200 - 500Mbps is applicable only to 11ax AP models.

Component/s	AP
Issue	AP-17160
Description	The maximum number of clients supported with all rate limit (SSID rate limit + Firewall profile rate limit + Device Policy profile rate limit) enabled is only 100. Since the administrator cannot control the number of devices connected with firewall or device policy rate limit RL / DP RL on WLAN using AAA server as the assigned firewall profiles. Any stability / performance / memory related problem can arise when more than 100 clients are connected.

Component/s	AP
Issue	AP-17087
Description	Inconsistent behavior observed with the throughput values obtained when rate limit enabled.

Component/s	AP
Issue	AP-16996
Description	Hostapd and Ethernet 1x process crash and restart after two hours of starting the longevity test. All 100 clients disconnect.

Component/s	AP
Issue	AP-15764
Description	When lower rate limit values are configured on the SSID device, the rate limit values is not accurate with the configured values.

Component/s	Control Plane
Issue	SCG-132335
Description	When GEO redundancy is enabled, the APs in SZ will not be included in the rogue list.

Component/s	Control Plane
Issue	SCG-134678
Description	Default zone AP firmware retains the previous version after the system upgrades to this release. When adding new APs that are listed below which are not supported in previous AP firmware version, they will not be seen in the controller default zone. **Impacted platform/AP models** : Enterprise platforms like SZ100/SZ144/vSZ-E when upgrading from 5.x/6.0.0 and adding 6.1.0 newly supported AP models such as R350/H550/T350C/T350D/T350SE.
Workaround	1. Upgrade default Zone version to 6.1.0 for new AP models to be recognized and shown in the default Zone. 2. Add 6.1.0 Zone and use AP registration rule to assign newly added AP (models listed above) to 6.1 AP Zone.

Component/s	Control Plane
Issue	SCG-134269; SCG-134678
Description	iPhone/iPad running iOS 14.8.1 does a full authentication on roaming and fails on FT roaming.

Component/s	Data Plane
Issue	SCG-116650
Description	Data plane fails reassemble fragmented packets.
Workaround	Make sure L2oGRE gateway forwarded traffic is not fragmented.

Component/s	Data Plane
Issue	SCG-126864
Description	When tunnel WLAN is turned on after AP establishes RGRE tunnel to data plane, user equipment connecting to the tunnel WLAN encounters TCP traffic failure of data plane inter-tunnel functions (Flexi-VPN / L3 Roaming).
Workaround	Reboot the AP for AP RGRE tunnel to re-establish.

Component/s	Switches
Issue	FI-250290
Description	Switch device does not switchover back to the new active controller, because the switchover configuration received from controller fails.
Workaround	1. Manually unconfigure the controller active-list and controller backup-list in the Switch. The unconfigured will erase the active-list and backup-list. 2. Set up the correct controller active-list IP address and re-establish SSH tunnel connection between the switch and the controller. 3. Reconfigure the active-list and backup-list and then re-establish the Switch tunnel between Switch and controller.

Component/s	Switch Management
Issue	SCG-122903
Description	Wired dashboard may have slow responsiveness in scaled environments.

Component/s	System
Issue	SCG-130614
Description	For returning VSA(RADIUS), User Group(AD/LDAP), and user-name(TACACS+), only the system domain's administrator AAA server profiles login to other domains is supported. Format *user@domain*, is invalid to partner domain's profiles.

Component/s	System
Issue	SCG-129876
Description	When the login realm pattern matches more than one realm, the system takes the most precise one.

Component/s	System
Issue	SCG-128233
Description	*ServiceTicket* may expire before the session ends in Tomcat server or Switch Management service due to the limitation of session expiration being one day.
Workaround	Refresh the browser and login again.

Component/s	System
Issue	SCG-127185
Description	AAA server fails to validate the common name in the server certificate and shows it as passed.

Component/s	System
Issue	SCG-133749
Description	User needs to delete *interface ve 1* (by default in Switch with FI09010 firmware) manually through console port if they use *Management Port* (interface management 1 with DHCP) to join the controller.

Component/s	System
Issue	SCG-133098
Description	If an AAA profile with the same realm is deleted and created within 30 seconds, the AAA profile will not take effect.

Component/s	System
Issue	SCG-132679
Description	Backup and restore operation causes CloudPath data to be out of sync.
Workaround	Administrator needs to reset the data on CloudPath.

Component/s	System
Issue	SCG-132623
Description	The network segmentation feature requires proper DHCP/NAT licenses to be functional.

Component/s	System
Issue	SCG-131411
Description	MAC/IP address encrypt on WISPr profile supports cloud profile.

Component/s	System
Issue	SCG-130354
Description	If the controller administrator retains the default time the automatic check occurs at the same time.
Description	It is recommended that the controller administrator configures the automatic check to some other time, or a manual trigger check.

Component/s	System
Issue	SCG-130466
Description	Existing public keys are overwritten if it is configured through Public APIs.

Component/s	System
Issue	SCG-132560
Description	Controller web user interface only support 1000 records on Guest Pass page. **NOTE** This is a design limitation and it will not be enhanced.

Component/s	UI/UX
Issue	SCG-134364
Description	User might encounter an error of *Unable to update the WLAN configuration. BssMinRate6G only supports 6mbps*when upgrading from 6.1 beta build to the latest build. [Workaround] 1.Delete WLAN with issue and create new WLAN 2.Use Public API to modify 6G BSS minrate and 6G mgmt tx rate value to 6mbps
Workaround	1. Delete the WLAN with this issue and create a new WLAN. 2. Use Public API to modify BssMinRate6G and 6G mgmt Tx rate value to 6mbps.

Component/s	UI/UX
Issue	SCG-129890
Description	Firmware schedule task only executes at 0/30 minutes every hour.

Component/s	UI/UX
Issue	SCG-126970
Description	Users cannot downgrade AP firmware versions since the previous versions of the AP firmware are not seen on the controller web user interface when upgrading the controller.
Workaround	Downgrade button is not visible when Zone is applied to a Data Plane Group. Assign the Zone to the default Data Plane Group for downgrading AP Zone firmware.

Component/s	UI/UX
Issue	SCG-129274

Component/s	UI/UX
Description	Guest Pass is deleted after applying the Zone template.

Component/s	UI/UX
Issue	SCG-133622
Description	Only Super Admin on the controller (SmartZone GUI) can configure network segmentation for now. All other created users cannot see network segmentation feature on the controller GUI.

Component/s	UI/UX
Issue	SCG-133464
Description	The traffic and health panel are hidden for switches in staging group.

Component/s	UI/UX
Issue	SCG-134603
Description	Unable to update the configuration of the AP Zone since *ChannelSelectMode[BgScan]* is not allowed for radios 5gLower/5gUpper/6g.
Workaround	Change BgScan to *ChannelFly* manually.

Component/s	UI/UX
Issue	SCG-133439
Description	IoT radio is seen as disabled for APs R850/R550 in the controller vSZ GUI.

Component/s	UI/UX
Issue	SCG-128233
Description	*ServiceTicket* may expire before the session ends in Tomcat server or Switch Management service due to the limitation of session expiration being one day.
Workaround	Refresh the browser and login again.

Component/s	UI/UX
Issue	SCG-134614
Description	This issue occurs when AP packet capture and support bundle cross execute at the same time. **NOTE** This issue will be fixed in future release.

Component/s	UI/UX
Issue	SCG-133460
Description	The search capability for Network Segmentation is completed in 6.1.0.0.685+ which is after the beta release.
Workaround	• Do a fresh installation of the system if your controller version is 6.1 with build number lower than 6.1.0.0.685. • If you upgrade from controller version 6.0 to version 6.1.0.0.685+, you do not need a fresh installation.

Component/s	UI/UX
Issue	SCG-133274
Description	Controller web user interface fails to show the channel changes in **Traffic** > **Client Chart** page.

Changed Behavior

The following are the changed behavior issues in this release.

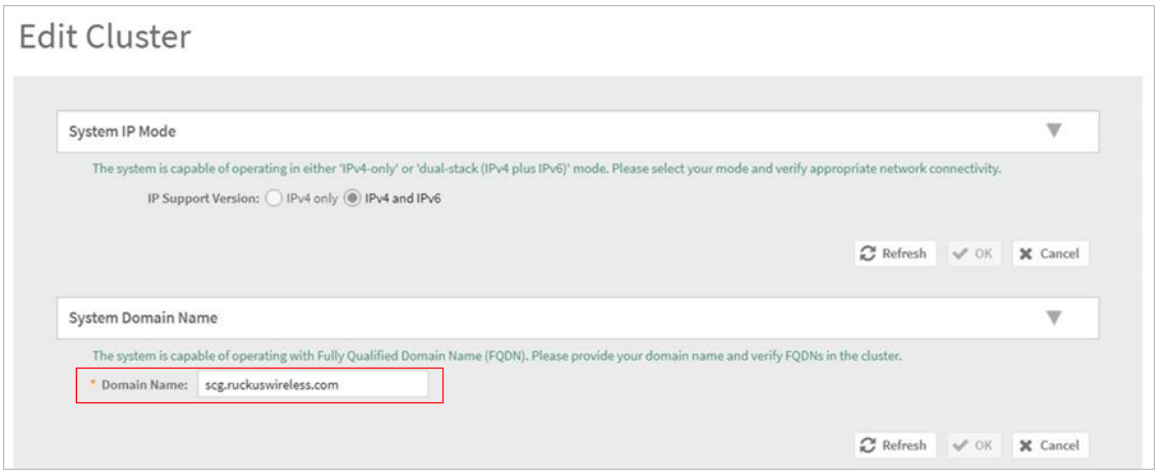
Component/s	vSZ
Issue	SCG-127759
Description	Starting SmartZone (SZ) R6.1, vSZ does not support network configuration with Control, Cluster, and Management interfaces to be in the same subnet or VLAN. As a workaround, separate the vSZ's Control, Cluster, and Management interfaces to different subnets or VLANs before upgrading.

Component/s	AP
Issue	SCG-131012
Description	Modified the algorithm to generate BSSID from AP base MAC address. As a result an AP upgraded to this release will use a different MAC identifier for the WLANs compared to previous releases.

For release 6.1 fresh installation of domain name is mandatory to support AP/DP validate the controller feature. FQDN (Fully Qualified Domain Name) consists of the domain name and the host name. The below table is an example of cluster deployment based on the domain name in a cluster deployment.

Cluster Domain Name	Node#	Host name	FQDN
ruckus.com	Master	master	master.ruckus.com
	Slave1	slave1	slave1.ruckus.com
	Slave2	slave2	slave2.ruckus.com
	Slave3	slave3	slave3.ruckus.com

Domain name can be modified after installation by navigating to **Network** > **Data and Control Plane** > **Cluster** > **Select the Cluster** > **Configuration** > **Configure** page on the controller GUI.


Edit Cluster
System IP Mode
The system is capable of operating in either 'IPv4-only' or 'dual-stack (IPv4 plus IPv6)' mode. Please select your mode and verify appropriate network connectivity.
IP Support Version: IPv4 only IPv4 and IPv6
Refresh
OK
Cancel
System Domain Name
The system is capable of operating with Fully Qualified Domain Name (FQDN). Please provide your domain name and verify FQDNs in the cluster.
* Domain Name: scg.ruckuswireless.com
Refresh
OK
Cancel

Resolved Issues

The following issue is resolved in this release.

Component/s	AP
Issue	ER-11377
Description	Resolved an issue of AP reboot due to target assert.

Component/s	Virtual SmartZone Data Plane
Issue	ER-11154
Description	Resolved an issue where SZ104-D/SZ124-D would fail to join the SmartZone post upgrade to 6.1.0 due to TPM certificate error.

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	SZ100	vSZ-E
Latency	34ms	34ms	68ms	76.5ms	76.5ms
Jitter	10ms	10ms	10ms	10ms	10ms
Bandwidth	115Mbps	92Mbps	40.25Mbps	23Mbps	23Mbps

Client Interoperability

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.

Component/s	AP
Issue	SCG-133133
Description	*Client-info* does not show the IPv6 address of connected Google Pixel client when it connects to WLAN with WLAN non-default VLAN.

Component/s	AP
Issue	SCG-130095
Description	Device type, OS vendor, model number is shown as unknown for Syska Smart Bulb and device type as smartphone for Amazon Alexa.

Component/s	AP
Issue	SCG-133325

Component/s	AP
Description	Mobile devices with Android version 9 go for a full authentication after it reconnects within an inactivity timeout.

Component/s	AP
Issue	SCG-132585
Description	Windows 11 device is not connected back to the saved WLAN profile after the AP reboots. This happens only when the device is connected by both wired and wireless connections. This issue is not seen when the Ethernet link of the device is removed.
Workaround	Remove Ethernet link of device and connect the client to a wireless connection for it connect back to a saved profile.

Component/s	AP
Issue	SCG-132583
Description	Client Mac Mini (M1 2020) does not support BSS Transition Management (802.1v).

Component/s	AP
Issue	SCG-133156
Description	After successful UEs iOS, MAC devices connection, if the device moves away from the AP RF coverage and if the client comes within the AP RF coverage and within the inactivity timeout then the device goes for a full authentication instead of skipping the authentication process.

Component/s	AP
Issue	SCG-126338
Description	With certain clients observing EAPOL failure due to *received EAPOL-Key 2/4 Pairwise with unexpected replay counter* and due to some conditions the AP fails to deauthenticate the client for invalid MIC in Key(2/4).

Component/s	AP
Issue	SCG-134433
Description	MAC OS does support 11v BSS Transition Management.

Component/s	AP
Issue	SCG-123018
Description	iPhone release iOS 14 version which has MAC address randomization features, can affect the Wi-Fi experience.
Workaround	For MAC related authentication, disable randomization features in iPhone, iPad , iWATCH iOS14 Wi-Fi configuration.

Resolved Issues

The following issue is resolved in this release.

Component/s	AP
Issue	ER-11377
Description	Resolved an issue of AP reboot due to target assert.

Component/s	Virtual SmartZone Data Plane
Issue	ER-11154
Description	Resolved an issue where SZ104-D/SZ124-D would fail to join the SmartZone post upgrade to 6.1.0 due to TPM certificate error.

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