RELEASE NOTES

Ruckus SmartZone Release Notes

Supporting SmartZone 3.6.2

Part Number: 800-71974-001 Rev A
Publication Date: September 2018

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, ARRIS 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. ARRIS 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. ARRIS 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 ARRIS 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 ARRIS, ARRIS 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 ARRIS 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, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, ZoneFlex are trademarks of ARRIS International plc and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access (WPA), the Wi-Fi Protected Setup logo, and WMM are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

New Features and Changed Behavior

General Data Protection Regulation

The European Union GDPR (General Data Protection Regulation) has been approved and has replaced EU DPD (Data Protection Directive) regulation.

The new regulation is in effect from May 2018 and requires organizations to put much stricter focus on data protection. The GDPR provides broad guidance across all aspects of data protection, but is not prescriptive in terms of information security requirements needed to adequately protect PII (Personally Identifiable Information).

GDPR regulates processing and storage end-user (EU data subject) related data. End-user could be any EU citizen. Ruckus is providing necessary tools to customers to help with the regulation compliance. Penalty for non-compliance can go up to 20M Euro or 4% of annual revenue, whichever is bigger.

Regulation details is available at http://www.eugdpr.org/.

Changed Behavior

The following is the changed behavior.

- Added a new attribute in the URL (identified as '*msg*') if and only if the hotspot user login fails with ZD-Style Login API. The value of the new attribute is an error messages from Northbound Interface (NBI) or a customized reply message from the RADIUS attribute of Reply-Message. **[SCG-91621 RFC 2865]**

Hardware/Software Compatibility and Supported AP Models

Overview

This section provides release information about the SmartZone 300 (SZ300), the SmartCell Gateway 200 (SCG200-C), the SmartZone 100 (SZ100), Virtual SmartZone (vSZ), and Virtual SmartZone Data Plane (vSZ-D) features with notes on known issues, caveats, and workarounds.

- 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 SCG200-C, developed for the service provider market, combines a WLAN access controller with Wi-Fi traffic aggregation, along with a built-in carrier-grade element management system in a 2U rack-mountable, all-in-one hardware form factor.
- 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 leading SCG200-C, while also enabling the rollout of highly scalable and resilient wireless LAN cloud services.

- The vSZ-D offers organizations more flexibility in deploying the SZ data plane as needed in an NFV architecture-aligned fashion. Deploying vSZ-D offers secured tunneling of user data traffic that encrypts payload traffic, maintains flat network topology, enables mobility across L2 subnets, supports POS data traffic for PCI compliance, and offers differentiated per site policy control and QoS, etc.

Release Information

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

SZ300

- Controller Version: **3.6.2.0.78**
- Control Plane Software Version: **3.6.2.0.57**
- Data Plane Software Version: **3.6.2.0.78**
- AP Firmware Version: **3.6.2.0.254**

SCG200-C

- Controller Version: **3.6.2.0.78**
- Control Plane Software Version: **3.6.2.0.57**
- AP Firmware Version: **3.6.2.0.254**

SZ100

- Controller Version: **3.6.2.0.78**
- Control Plane Software Version: **3.6.2.0.57**
- Data Plane Software Version: **3.6.2.0.21**
- AP Firmware Version: **3.6.2.0.254**

vSZ-H and vSZ-E

- Controller Version: **3.6.2.0.78**
- Control Plane Software Version: **3.6.2.0.57**
- AP Firmware Version: **3.6.2.0.254**

vSZ-D

- Controller Version: **3.6.2.0.78**

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 at: https://support.ruckuswireless.com/documents/2432-smartzone-3-6-2-getting-started-guide-on-gpb-mqtt-interface-sz100-sz300-scg200-vsz

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.

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

Supported and Unsupported Access Point Models

Before upgrading to this release, check if the controller is currently managing AP models that are no longer supported in this release.

APs preconfigured with the SmartZone AP firmware may be used with the SZ300, SCG200-C, SZ100, or vSZ in their native default configuration. APs factory-configured with the ZoneFlex-AP firmware may be used with the SCG200-C/SZ100/vSZ when LWAPP discovery services are enabled.

On solo APs running release 104.x, the LWAPP2SCG service must be disabled. To disable the LWAPP2SCG service on an AP, 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 release 104.x are capable of connecting to both ZD and SZ controllers. If an AP is running release 104.x and the LWAPP2SCG service is enabled on the SZ controller, a race condition will occur.

Supported AP Models

This release supports the following Ruckus AP models.

TABLE 1 Supported AP Models

11ac-Wave2		11ac-Wave1		11n	
Indoor	**Outdoor**	**Indoor**	**Outdoor**	**Indoor**	**Outdoor**
R720	T710	R700	T504	R300	ZF7782
R710	T710S	R600	T300	ZF7982	ZF7782-E
R610	T610	R500	T300E	ZF7372	ZF7782-N
R510	T310C	C500	T301N	ZF7372-E	ZF7782-S
H510	T310S	H500	T301S	ZF7352	ZF7781CM
C110	T310N	R310	FZM300	ZF7055	
H320	T310D	R500E	FZP300		
	T811CM				
	T610S				
	E510				

Important Note About the PoE Power Modes of the R720, R710, T610, and R610 APs

NOTE
When the R720, R710, T610 series AP is connected to an 802.3af PoE power source, the USB interface and the second Ethernet port are disabled, and the AP radios do not operate in maximum capacity. For more information, refer to the latest Outdoor Access Point User Guide or Indoor Access Point User Guide.

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	
ZF7762-T	ZF7351-U	ZF7761-CM	ZF7343-U	

Caveats, Limitations, and Known Issues

Caveats, Limitations, and Known Issues

The following are the caveats, limitations and known issues.

NOTE
The caveats stated in 3.6.1 release notes are also applicable this release.

Issue	ER-6619
Description	Unable to map VLAN pools using the VLAN override option from WLAN Group
Component/s	UI/UX

Issue	SCG-85554
Description	In vSZ-D DHCP/NAT feature, when Tunnel NAT is enabled and Tunnel DHCP is disabled in a multi-VLAN deployment, user has to enable DHCP relay to forward the DHCP packets
Component/s	Virtual SmartZone Data Plane

Issue	SCG-88854
Description	When URL Filtering policy is created and applied to UTP, which is mapped to a WLAN, the blacklisted sites in the URL policy are not blocked. The URL filtering settings has to be enabled at WLAN level along with UTP. UTP policy will take precedence over WLAN level.
Component/s	UI/UX

Caveats, Limitations, and Known Issues

Issue	SCG-89015
Description	vSZ-D does not assign the IP address when DHCP packets are relayed by another vSZ-D with Option82 and sub options
Component/s	Virtual SmartZone Data Plane

Issue	SCG-89553
Description	When PMTU (Path Maximum Transmission Unit) for a SoftGRE profile is set to 1238, the *br8* interface of AP has the MTU (Maximum Transmission Unit) as 1200. On sending traffic with data size greater than 1200, the packets do not get fragmented.
Component/s	AP Data Plane

Issue	SCG-90059
Description	Zone templates get created with more than the allowed characters while importing
Component/s	UI/UX

Issue	SCG-90604
Description	Bonjour Gateway feature does not work for tunnel enabled WLANs on vSZ-D. Multicast DNS (mDNS) has been added in the SZ100 to support multicast forwarding of the vSZ-D service. Currently mDNS is not supported on a vSZ-D managed by vSZ.
Component/s	Bonjour Gateway

Issue	SCG-90693
Description	When cluster redundancy settings on the controller is configured and the outbound firewall is enabled, the packets are dropped at Active controller
Workaround	Configure the outbound firewall rule for TCP port 8443
Component/s	System

Issue	SCG-91670
Description	Unable to retrieve the saved map scale data when accessing the controller through the user interface
Component/s	UI/UX

Issue	SCG-91885
Description	Unable to display the AP information when the UE switches to another SSID, Radio or AP
Component/s	UI/UX

Issue	SCG-91940
Description	Syslog IPv6 address configuration is not seen for dual mode AP Zone and on system level when dual stack on vSZ is enabled
Component/s	Syslog

Issue	SCG-89292 SCG-89276
Description	vSZ-D assigns the earlier IP address based on UE VLAN to client DHCP request instead of matching the DHCP pool received in Option82

Issue	SCG-89292 SCG-89276
Component/s	Virtual SmartZone Date Plane

Issue	SCG-93096
Description	The exported CSV report for APs and Clients carry a null entry in the last row
Component/s	SZ Management Plane

Issue	SCG-93369
Description	Schedule backup in **Backup & Restore** > **Configuration** is not triggered on restoring a configuration backup
Workaround	Disable the feature and enable it for the configuration to be applied properly
Component/s	SZ Management Plane

Issue	SCG-93368
Description	On restoring the configuration backup with Syslog server disabled, messages are still sent to the old syslog server even though the web interface shows that the syslog server was disabled
Workaround	Reset the Syslog configuration by configuring new syslog server IP address and apply the settings or Reboot all the nodes in the cluster after configuration restore is successful
Component/s	Syslog

Issue	SCG-93691
Description	After vSZ-D upgrades to build 3.6.2.0.73 from 3.4.2.0.176, it takes 15 to 20 minutes to come back online.
Component/s	Virtual SmartZone Data Plane

Issue	ER-6675
Description	AP R710 reboot problem detected
Component/s	AP

Issue	ER-6586
Description	The AP tags incorrect VLAN on the client's first packet
Component/s	AP

Issue	ER-6555
Description	SNMP poll does not show the AP Group information after editing the AP Group
Component/s	System

Issue	ER-6702 SCG-93897
Description	For SZ100 one port group is configured with User Defined Interface (UDI). On rebooting the SZ100 the data plane gateway is overwritten by the UDI gateway IP address

Issue	ER-6702 SCG-93897
Workaround	Remove the UDI configuration and reboot the controller. Once all services are UP and the data plane gets the correct gateway, add the UDI interface configuration again
Component/s	SZ Control Plane

Issue	SCG-84002
Description	Corrupted UDP and TCP traffic are sent by the AP when Smartcast classification is configured for IPv6 addresses. IPv6 packets are dropped at the receiver as IP address version is set to 0 instead of 6. This limitation is applicable only to IPv6 and **NOT** for IPv4 address .
Component/s	AP Data Plane

Issue	SCG-94175
Description	GDPR (General Data Protection Regulation) PII (Personally Identifiable Information) search or delete command is missing some lines of information in command output when the MAC address format is in lower case, but complete report will be sent to FTP server
Workaround	Execute the command using MAC address format in upper case to get expected command output in CLI
Component/s	SZ Control Plane

Issue	SCG-77032 SCG-89454
Description	When the system boots it does not display the IPv6 address since DHCP IPv6 address in the management IP address is not auto updated
Workaround	Restart the system for it to display the DHCP IPv6 address in the management IP address
Component/s	System

Issue	SCG-89292
Description	If DHCP/NAT pool profile names are modified for Radius profile DHCP/NAT service in vSZ-D, new UEs connecting may receive IP address from incorrect pool.
Workaround	Reboot vSZ-Ds to clean old information
Component/s	Virtual SmartZone Data Plane

Resolved Issues

Resolved Issues

The following are the resolved issues.

Issue	SCG-90909 ER-6445
Description	Added Windows 10 to the fingerprint database
Component/s	AP Data Plane

Issue	SCG-82650
Description	SmartZone will not validate the static routes for DHCP/DHCPv6 interface before adding them
Component/s	Network

Issue	SCG-82367 ER-6160
Description	Resolved an issue where when VLAN tag is enabled with access/core separation, static route cannot be persisted after rebooting. This is a configuration limitation for vSZ-D and SZ300 internal data plane.
Component/s	Data Plane

Issue	SCG-81432
Description	Resolved an issue where the controller now checks the validity of the added IPv6 static routes
Component/s	Network

Issue	SCG-70831
Description	Resolved an issue where if 802.11R roaming was enabled and when a client roamed from AP1 to AP2, the Class and Chargeable-User-Identity attributes were missing in the Interim-Update packet sent by AP2
Component/s	AP Control Plane

Issue	ER-6522
Description	Resolved an issue caused by duplicate close of TLS socket
Component/s	Virtual Data Plane

Issue	ER-6450 ER-5656
Description	Resolved an issue where when viewing the list of active clients on the controller, it incorrectly listed clients that have been disconnected
Component/s	AP

Issue	ER-6430 ER-6317
Description	Resolved the memory leak caused by L2UF disconnect packets
Component/s	System

Issue	ER-6388
Description	Resolved an issue where after upgrade, most of the maps with APs coordination showed incorrect placement of APs
Component/s	Virtual SmartZone

Issue	ER-6382 ER-5602
Description	Resolved an issue where certificate was not seen correctly on the controller web interface
Component/s	Virtual SmartZone

Issue	ER-6338
Description	Resolved an issue where if the SSID contained the keyword AP, reports related to this SSID failed to be generated
Component/s	System

Issue	ER-6336
Description	Resolved an issue where detaching the second volume on AWS caused the controller to crash
Component/s	Virtual SmartZone

Issue	ER-6332 ER-6327 ER-6462 ER-6299 ER-6453
Description	Resolved an issue where the ElasticSearch went offline on all the nodes
Component/s	System

Issue	ER-6298
Description	Resolved an issue where the AP rebooted due to watchdog timeout
Component/s	AP

Issue	ER-6062 ER-6494 ER-6282
Description	Resolved an issue where the AP randomly got disconnected from the controller and was not accessible until a manual reboot for recovery was performed
Component/s	AP

Issue	ER-6262
Description	Resolved an issue where the Z2 county codes could be changed to any other country code using AP CLI command
Component/s	AP

Issue	ER-6251
Description	Resolved an issue where channels for few AP's were populated as BLANK in the CSV file even though they were assigned a channel
Component/s	AP

Issue	ER-6235
Description	Resolved an issue where the serial number of vSZ changed after reboot, especially seen in AWS based vSZ
Component/s	Virtual SmartZone

Issue	ER-6228
Description	Resolved an issue where by changing the BSS minimum rate on WLAN through Public API defaulted the client isolation whitelist settings on the WLAN
Component/s	Public API

Issue	ER-6218
Description	Resolved an issue where mesh view was not displaying all mesh APs in a zone
Component/s	AP

Issue	ER-6216
Description	Resolved an issue where API call for Access Point events returned the description as null
Component/s	AP

Issue	ER-6198
Description	Resolved an issue where the controller kept a track of old client connection data, which resulted in incorrect display of client connection failures
Component/s	System

Issue	ER-6173
Description	Resolved an issue where the system was unable to retrieve the DPID (Delivery Point Identifier) to show AP tunnel connectivity
Component/s	Public API

Issue	ER-6138
Description	Resolved an issue where special characters ` and $ (are allowed as RADIUS shared secret
Component/s	System

Issue	ER-6020
Description	Resolved an issue where captive portal referrer failed in handling unsupported encoding exception and Captive Portal Constants
Component/s	System

Issue	ER-6007
Description	Resolved an issue where incorrect key attributes was sent to the LDAP server for authentication
Component/s	System

Issue	ER-5977
Description	Resolved a target fail detected issue on 11ac wave2 APs
Component/s	AP

Issue	ER-5912
Description	Resolved an issue where a Wi-Fi client with extended ASCII characters in its hostname was unable to get an IP address if an OS Policy was applied to the WLAN
Component/s	System

Issue	ER-5906 ER-6399
Description	Resolved an issue where the serial port logging was enabled on the client. It is now disabled
Component/s	AP

Issue	ER-5739
Description	Resolved an issue where SNMP did not enhance OID 25053.1.4.2.1.1.1.2.1.12 SNMP walk script resulting in invalid value
Component/s	AP

Issue	ER-5660
Description	Resolved an issue where on blacklisting more than one user associated to AP ZF-7352 resulted in a disconnect of the AP from the network and was inaccessible
Component/s	AP

Issue	ER-5023
Description	Resolved an issue where the Ascom i62 VOIP (Voice over Internet Protocol) phones were unreachable after period of inactivity or doze state
Component/s	Virtual SmartZone Data Plane

Issue	ER-5935
Description	Resolved an issue where the AeroScout RFID tag detection did not function properly on 11ac Wave2 APs
Component/s	AP

Issue	ER-5971
Description	Resolved an issue where due to false MAC address on the AP caused vSPOT in detecting incorrect amount of visitors when the hash tag was enabled
Component/s	AP

Issue	ER-6037
Description	Resolved an issue where the DHCP server failover detection was incorrect
Component/s	System

Issue	ER-6136
Description	Resolved an issue where cache memory occupied considerable space on the system, which resulted in performance issues
Component/s	System

Issue	ER-6139
Description	Resolved an issue where the protocol and device types were incorrect in the Ekahau tag frame
Component/s	AP

Issue	ER-6185
Description	Resolved an issue where AP administrator could not edit guest pass portal
Component/s	AP

Issue	ER-6214 ER-6233
Description	Resolved an target fail detected issue on 11ac wave2 APs when MU-MIMO was enabled
Component/s	AP

Issue	ER-6240
Description	Internal data plane will shut down gracefully when shutdown or reboot is initiated from SZ300 control plane
Component/s	SZ300

Issue	ER-6256
Description	Resolved an issue where the hostname and operating system type data is now picked from the Client report since the session manager failed in updating these fields
Component/s	System

Issue	ER-6258
Description	Resolved an issue where **Troubleshooting** > **Spectrum Analysis** output was not displaying data when you leave it enabled. Navigate to some other page and then return to this menu
Component/s	System

Issue	ER-6261
Description	Resolved an issue where the AP DHCP configuration on a cloned zone failed due to a null error
Component/s	AP

Issue	ER-6281
Description	Resolved an issue where if there is only one zone in the global filter and the global filter is currently used, deleting this global filter caused errors
Component/s	AP

Issue	ER-6293
Description	Resolved an issue setting NTP configuration in vSZ controllers
Component/s	Virtual SmartZone

Issue	ER-6325
Description	Resolved an issue where the client fingerprint would not work properly when the Client runs Ubuntu version 17
Component/s	System

Issue	ER-6423
Description	Resolved an issue where the maximum length of guest pass terms and conditions column was set to 3999, which was insufficient. It is now increased to 16000
Component/s	Virtual SmartZone

Issue	ER-6451

Description	Added exponential back-off behavior to AP2AP communication process when the process initially starts and cannot establish the communication channel. The AP2AP communication can also be completely stopped by setting the new RPMKEY as follows:
	• To start the process:
	`set rpmkey nbrd/disable-wson 0`
	• To stop the process:
	`set rpmkey nbrd/disable-wson 1`

Component/s	System

Issue	ER-6463
Description	Resolved an issue where the default DHCP82 format was not working
Component/s	System

Issue	ER-6477
Description	Resolved an issue where changes to DNS configuration settings on the controller web interface and CLI failed
Component/s	System

Issue	ER-6483
Description	Resolved an issue where the heartbeat was sent every 30 seconds. The correct behavior is where the controller needs to send only one heartbeat lost event before the AP is marked as disconnected
Component/s	System

Issue	ER-6548
Description	Resolved an issue where setting the AP number allocation at domains level, blocked the user from moving APs within Zones or Groups under the same domain
Component/s	Virtual SmartZone Data Plane

Issue	ER-6555
Description	Resolved an issue where SNMP poll did not show the AP Group information after editing the AP Group
Component/s	AP

Issue	SCG-91414
Description	Resolved an issue where iPhone X users not able to renew DHCP IP address after the client roams from one AP to other. This happens when the source AP sends de-authentication frame to client and clients starts the authentication request again to complete associated process
Component/s	Log Manager

Issue	ER-6247
Description	Resolved an issue where iPhone X users not able to renew DHCP IP address after the client roams from one AP to other. This happens when the source AP sends de-authentication frame to client and clients starts the authentication request again to complete associated process
Component/s	AP

Issue	ER-6528
Description	Resolved an issue where traffic was not able to pass through vSZ-D host table
Component/s	Virtual SmartZone Data Plane

Issue	ER-6586
Description	Resolved an issue where the AP tagged the UE's first packet with the lowest VLAN ID in the VLAN pool
Component/s	AP

Issue	ER-6570
Description	Resolved an issue where the AP failed to get the guest logo communicating to the controller though the SSH tunnel was established to the Public IP address.
Component/s	AP

Issue	ER-6559
Description	Resolved an issue where the WISPr client was not able to access the domain in the walledgarden whitelist
Component/s	System

Issue	ER-6546
Description	Resolved an issue where UE context was incorrectly updated by the Session Manager after the client roamed across the controllers.
Component/s	System

Issue	SCG-85557
Description	Resolved an issue where clients roaming on a wispr based wlan caused memory leak at session manager
Component/s	Session Manager

Issue	SCG-91547
Description	Resolved any issue where log manager process consumed high CPU and restarted on receiving a bad packet
Component/s	Virtual SmartZone

Issue	ER-6470
Description	Resolved an issue where **show license** got into an infinite loop
Component/s	System

Issue	ER-6468
Description	Resolved an issue where there TACACS user name and password was recorded in the log files.
Component/s	System

Issue	ER-6367
Description	Resolved an issue where the Vlan pooling included commas in the 65 character limit
Component/s	System

Issue	ER-6124
Description	Resolved an issue where User Defined Interface could not forward the traffic correctly
Component/s	System

Issue	ER-6204
Description	Fixed TLS1.0 invalid configured issue by modifying sslProtocol and sslEnaledProtocols setting in tomcat.cnf
Component/s	System

Issue	SCG-88983
Description	Resolved an issue where the class attribute gets truncated in the accounting request authentication.
Component/s	AP Control Plane

Issue	SCG-92878
Description	Resolved an issue where the events for vSZ-D NAT pool usage were not displayed correctly on the controller web user interface
Component/s	UI/UX

Issue	ER-6004
Description	Resolved an issue where AP R710 reboot due to target failed to be detected
Component/s	AP

Upgrading to This Release

Overview

This section lists important information that you must be aware of when upgrading the controller to this release.

Step-by-step instructions for performing the upgrade are provided in the Upgrade Guide.

CAUTION
Before uploading a new AP patch, it is strongly recommends that you save a cluster backup, in case you want to restore the previous AP patch.
Before upgrading the controller, it strongly recommends that you back up the entire cluster. In case the upgrade fails, you can use the cluster backup to roll back the cluster to its previous state.

NOTE
When upgrading vSZ-E/vSZ-H, if the memory/CPU allocation of the current VM instance does not match the lowest resource level of the new VM instance to which the new vSZ-E/vSZ-H version will be installed, you will be unable to perform the upgrade. On the other hand, if the new VM instance has insufficient hard disk space, a warning message appears after you upload the upgrade image but you will still be able to perform the upgrade.

Virtual SmartZone Recommended Resources

Before upgrading vSZ to this release, verify that the virtual machine on which vSZ is installed has sufficient resources to handle the number of APs and wireless clients that you plan to manage. See the tables below for the virtual machine system resources that Ruckus recommends.

NOTE
These vSZ recommended resources may change from release to release. Before upgrading vSZ, always check the recommended resource tables for the release to which you are upgrading.

vSZ High Scale recommended resources

TABLE 3 vSZ High Scale recommended resources

AP Count Range		Max Clients	Nodes per Cluster	AP Count per Node	vCPU	RAM	Disk Size	Preserved Events	Concurrent CLI Connection	Resource Level
From	**To**			**Max**	**Logic Processor** [1][2]	**GB**	**GB**	**Max**	**Max**	
10,001	30,000	300,000	4	10,000	24	48	600	3 M	4	8
	20,000	200,000	3							
5,001	10,000	100,000	1-2	10,000	24	48	600	3 M	4	7
2,501	5,000	50,000	1-2	5,000	12	28	300	2 M	2	6.5
1,001	2,500	50,000	1-2	2,500	6	22	300	1.5 M	2	6
501	1,000	20,000	1-2	1,000	4	18	100	600 K	2	5
101	500	10,000	1-2	500	4	16	100	300 K	2	4
1	100	2,000	1-2	100	2	13	100	60 K	2	3

vSZ Essentials recommended resources

TABLE 4 vSZ Essentials recommended resources

AP Count Range		Max Clients	Nodes per Cluster	AP Count per Node	vCPU	RAM	Disk Size	Preserved Events	Concurrent CLI Connection	Resource Level
From	**To**			**Max**	**Logic Processor [1] [2]**	**GB**	**GB**	**Max**	**Max**	
1025	3,000	60,000	4	1,024	8	18	250	10 K	2	3
	2,000	40,000	3							
501	1,024	25,000	1-2	1,024	8	18	250	10 K	2	2
101	500	10,000	1-2	500	4	16	100	5 K	2	1.5
1	100	2,000	1-2	100	2	13	100	1 K	2	1

NOTE
Logic Processor [1] vCPU requirement is based on Intel Xeon CPU E5- 2630v2 @2.60 GHz.
Logic Processor [2] Azure with low CPU throughput unsupported. The vSZ with the lowest resource plan (2 core CPU, 13 GB memory) can NOT be supported due to the low CPU throughput on Azure.

Supported Upgrade Paths

Before you upgrade the controller, verify that it is running a release build that can be upgraded to this release.

WARNING
SZ300 release 3.6.2.0.49 fails to upgrade to release 5.0.0.0.675. **[SCG-92096]**

To help ensure that the cluster firmware upgrade process can be completed successfully, the cluster interfaces of all nodes must be connected and up. **[SCG-34801]**

The table below lists previous releases that can be upgraded to this release.

NOTE
SZ300 supports upgrade from 3.5 builds. 3.4 builds are not supported.

TABLE 5 Previous release builds that can be upgraded to this release

Platform	Release Build
SZ300	3.4.0.0.976
SCG200-C	3.4.1.0.208
SZ100	3.4.2.0.152
vSZ (vSCG)	3.4.2.0.169
vSZ-D	3.4.2.0.176
	3.4.2.0.217
	3.5.0.0.808
	3.5.0.0.832
	3.5.1.0.296
	3.5.1.0.862
	3.6.0.0.510
	3.6.1.0.227

Multiple AP Firmware Support in the SZ100/vSZ-E/SCG200-C/SZ300/vSZ-H

The AP firmware releases that APs use are configured at the zone level. This means that APs that belong to one zone could use a different AP firmware release from APs that belong to another zone.

NOTE
SZ100/vSZ-E/SCG200-C/SZ300/vSZ-H is referred as **controller** in this section.

NOTE
Some older AP models only support AP firmware 3.1.x and earlier. If you have these AP models, note that the controller cannot be upgraded to this release.

NOTE
If you have AP zones that are using 3.2.x and the AP models that belong to these zones support AP firmware 3.4 (and later), change the AP firmware of these zones to 3.4 (or later) to force these APs to upgrade their firmware. After you verify that all of the APs have been upgraded to AP firmware 3.4 (or later), proceed with upgrading the controller software to release 3.6.

NOTE
In earlier releases, Essentials controllers (vSZ-E or SZ100) automatically upgraded both the controller firmware and AP firmware when the system is upgraded. In release 3.5, however, the concept of *Multi-Zone* was introduced, which slightly changed the upgrade workflow where the system and the AP zones upgraded independently. When upgrading the controller to 3.6.1, the AP Zone firmware remains the same.

Up to Three Previous Major AP Releases Supported

Every platform release can support up to three major AP firmware releases, including (1) the latest AP firmware release and (2) two of the most recent major AP firmware releases. This is known as the N-2 (n minus two) firmware policy.

NOTE
A major release version refers to the first two digits of the release number. For example, 3.6.1 and 3.6.2 are considered part of the same major release version, which is 3.6.

The following releases can be upgraded to release 3.6.2:

- 3.5.x
- 3.5
- 3.4.x
- 3.4

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

- If you are upgrading the controller from release 3.5, then the AP firmware releases that it will retain after the upgrade will be 3.6.2 and 3.5 (and 3.4 if this controller was previously in release 3.4)
- If you are upgrading the SCG200-C/vSZ-H from release 3.4, then the AP firmware releases that it will retain after the upgrade will be 3.6.2 and 3.4.

All other AP firmware releases that were previously available on the controller will be deleted automatically.

EoL APs and APs Running Unsupported Firmware Behavior

Understanding how the SCG200-C/SZ300/vSZ-H handles APs that have reached EoL status and AP running unsupported firmware can help you design an upgrade plan that will minimize impact on wireless users in your organization.

> **NOTE**
> SCG200-C/SZ300/vSZ-H is referred as **controller** in this section.

EoL APs

To check if an AP that you are managing has reached EoL status, visit the ZoneFlex Indoor AP and ZoneFlex Outdoor AP product pages on the Ruckus Support website. The icons for EoL APs appear with the *END OF LIFE* watermark.

1. An EoL AP that has not registered with the controller will be moved to the Staging Zone and its state set to Pending. This AP will be unable to provide WLAN service to wireless clients.
2. The EOL AP affects the upgrade only in the following conditions. Otherwise, the upgrade be successful.
   a. Upgrade should be prior to 3.5 release
   b. This is applicable in SZ100 or vSZ-E controllers

APs Running Unsupported Firmware Releases

- APs running AP firmware releases that are unsupported by the controller release can still connect to the controller.
- Once connected to the controller and assigned to a zone, the AP will be upgraded to the AP firmware assigned to the zone to which it belongs.

Interoperability Information

AP Interoperability

APs with ordering number prefix 901- (example 901-T300-WW81) may now be supplied with an AP base image release 100.0 or later (including 104.0).

The AP base image is optimized for controller-discovery compatibility to support all Ruckus controller products including ZoneDirector, vSZ and SZ100.

Once the AP discovers and joins a controller (for example, the SZ100), the AP is updated to the compatible controller-specific AP firmware version. The updated AP firmware version becomes the factory-default image. The updated AP firmware version (for example, vSZ AP100.x) will remain persistent on the AP after reset to factory defaults.

An AP configured with base image release 100.0 may be managed by the FlexMaster management tool or may be used in standalone controller-less operation if controller discovery is disabled on the AP web interface.

Enabling ZoneFlex AP Discovery to a SmartZone Controller Using DHCP Option 43

To ensure reliable discovery of ZoneFlex APs to SmartZone controllers, the DHCP server must be configured to support DHCP Option 43 settings as outlined in the Getting Started Guide for your controller. DHCP option 43 sub codes 03 and 06 IP address assignments must both point to the SmartZone controller's control plane IP address to ensure reliable discovery services.

Enabling ZoneFlex AP Discovery to a SmartZone Controller Using DNS

To ensure reliable discovery of ZoneFlex APs to SmartZone controllers using DNS resolution, the DNS server must be configured to have two DNS entries. The first DNS entry must use the “RuckusController” prefix and the second entry the “zonedirector” prefix.

Refer to the *Getting Started Guide* for your SmartZone controller for instructions on how to connect the AP to the controller using DNS.

Redeploying ZoneFlex APs with SmartZone Controllers

NOTE
A supported ZoneFlex AP configured to operate with ZoneDirector will require an upgrade to a compatible SmartZone controller approved software release prior to interoperating with an SCG, SZ, or vSZ.

Once the AP firmware is updated, the AP will no longer be able to communicate with its old ZoneDirector controller. The AP must be reset to factory default setting before attempting to configure the AP from the SmartZone controller.

NOTE
There are established ZoneDirector to SmartZone controller migration tools and procedures. Contact support.ruckuswireless.com for the latest available procedures and utilities.

Converting Standalone APs to SmartZone

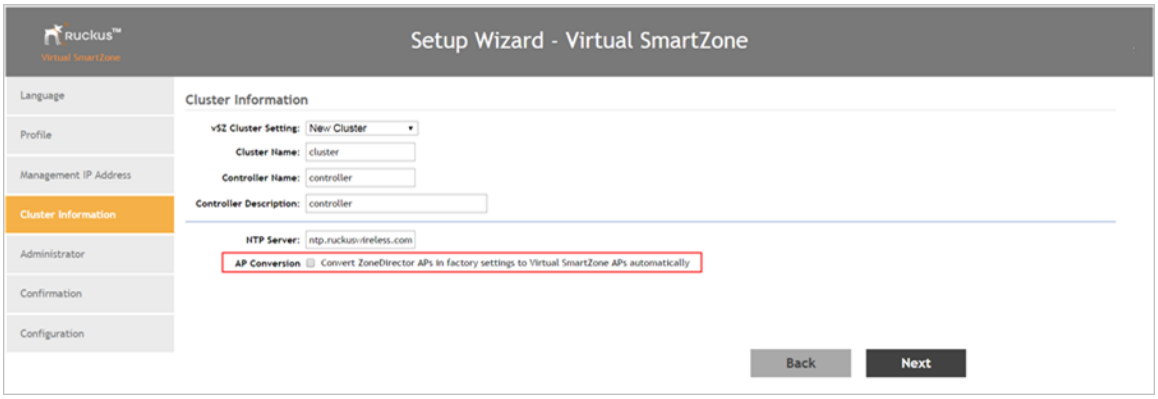
You can convert standalone ZoneFlex APs (those that are not managed by ZoneDirector) in factory default configuration to be managed by a SmartZone controller.

Follow these steps to convert standalone ZoneFlex APs to the SmartZone controller firmware so that they can be managed by the SZ300, SZ100, or vSZ

1. When you run the SmartZone Setup Wizard, select the **AP Conversion** check box on the **Cluster Information** page.

NOTE
The figure below shows the AP Conversion check box for the vSZ Setup Wizard. If you are setting up SZ300, or SZ100 the check box description may be slightly different.

FIGURE 1 Select the AP Conversion check box to convert standalone ZoneFlex APs to controller APs



2. After you complete the Setup Wizard, connect the APs to the same subnet as the SmartZone controller.

   When the APs are connected to the same subnet, they will detect the SmartZone controller on the network, and then they will download and install the AP firmware from SmartZone controller. After the SmartZone firmware is installed on the APs, the APs will automatically become managed by the SmartZone controller on the network.

ZoneDirector Controller and SmartZone Controller Compatibility

If you have a ZoneDirector controller on the same network, take note of this important information.

To ensure reliable network operations, it is recommended that ZoneDirector controllers and SmartZone controllers (SZ or vSZ) not be deployed on the same IP subnet or in such a way as the controllers share the same DHCP address scopes and domain name servers (DNS) as there may be limitations or restrictions in AP controller discovery capabilities. An effective network segmentation strategy should be developed when ZoneDirector and SmartZone controllers coexist on the same network.

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.

Users will not be redirected to WISPr Internal Logon URL with Chrome browser 65. This is the behavior of Chrome browser version starting from 63. **[SCG-85552]**

Workaround: Add the following URLs in Walled Garden list for WISPr redirection to work.

- connectivitycheck.gstatic.com
- clients3.google.com
- connectivitycheck.android.com
- play.googleapis.com
- gstatic.com

For details refer to https://www.chromium.org/chromium-os/chromiumos-design-docs/network-portal-detection

Ruckus Wireless, Inc., a wholly owned subsidiary of ARRIS International plc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com