RELEASE NOTES

Ruckus SmartZone Release Notes

Supporting SmartZone 3.6.2 Patch 1

Part Number: 800-72136-001 Rev B
Publication Date: February 2019

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

Document History

Revision Number	Summary of changes	Publication date
B	1. Added resolved issue ER-6640, SCG-91518	February 21, 2019

New Features and Adding AP730 to the Controller

Access Point: R730

This release adds native support for the R730 dual-band 802.11ax indoor access point. The R730 is the first Ruckus access point based on the 802.11ax standard, the next generation Wi-Fi standard supporting peak PHY rates up to 10 Gbps. The R730 features one 5 Gbps PoE+ (802.3at/at+) Ethernet port, one 1 Gbps non-PoE port, and a USB port for IoT applications

R730 Feature Limitations

The following R730 AP features are unsupported in this release:

- TXBF
- MU-MIMO
- ATF/BSSP
- OFDMA
- 160Mhz and 80+80Mhz
- MESH
- Auto Cell Size
- Transient Client Management
- Airtime Decongestion
- LACP
- Onboard BLE/Zigbee is not supported
- Spectrum Analysis

R730 Power Modes

The R730 can be powered by 48V DC power, or 802.3at or 802.3at+ PoE (Power over Ethernet) switch or PoE injector. 802.3af PoE is *NOT* supported. Refer to the following table for power modes supported, and AP limitations when powered with sub-maximum power supply.

NOTE
The 5 Gbps PoE In port supports auto-negotiation with support for the following speeds: 100/1000/2500/5000 Mbps.

NOTE
The PoE switch port must run link layer discovery protocol (LLDP) power over Ethernet/MDI (PoE+) in order for the R730 to operate in full-power mode. This may require enabling both LLDP and Power via MDI (dot3) on the switch, if available.

Power Mode	2.4 GHz Radio		5 GHz Radio		5 Gbps Eth Port	1 Gbps Eth Port	USB Port	Comments
	Tx/Rx chains	Tx/Rx streams	Tx/Rx chains	Tx/Rx streams				
DC	4/4	4/4	8/8	8/8	Enabled	Enabled	Enabled (3W limit)	Requires 35W power
802.3af PoE **(not supported)**	N/A	N/A	N/A	N/A	N/A	N/A	N/A	**Not Supported**
802.3at PoE switch	4/4	4/4	4/8	4/4	Enabled	Disabled	Enabled (0.5W limit)	
802.3at+ PoE switch	4/4	4/4	8/8	8/8	Enabled	Enabled	Enabled (3W limit)	Requires 35W power
PoE injector Model GRT-480125A (In GUI select POE operation mode = AT+)	4/4	4/4	8/8	8/8	Enabled (1 Gbps speed)	Enabled	Enabled (3W limit)	Injector model GRT-480125A is rated only for 1Gbps speed. If POE operating mode = Auto, POE injector will power AP in AT mode only.

Adding AP R730 to the Controller

It is recommended that you read the following content carefully before upgrading to this release.

IMPORTANT
Refer to **Option 1** if you have already applied AP R730 patch on top of 3.6.2 GD (Build 3.6.2.0.78) , you can now upgrade to 3.6.2 Patch 1 (Build 3.6.2.0.222) with AP R730 as a native support with additional fixes. Refer to **Option 2**, if you are upgrading from 3.6.2 GD (Build 3.6.2.0.78) to 3.6.2 Patch 1 (Build 3.6.2.0.222) .

Option 1

If you are applying R730 AP patch on top of 3.6.2.0.78 (GD) (Build 3.6.2.0.78) the R730 firmware version will be 3.6.2.0.509. After the upgrade, the new available AP firmware version is 3.6.2.0.695. The AP R730 will continue to operate on 3.6.2.0.509 firmware till the AP zone is upgraded.

Option 2

If you are adding AP R730 after upgrading to 3.6.2 Patch 1 controller and no AP patch was applied previously then the available AP firmware version is 3.6.2.0.695. The AP R730 will not register unless and until the AP zone is upgraded to the latest 3.6.2 Patch 1 AP firmware.

When the customer adds an R730 after upgrading to 3.6.2 P1 controller and no AP patch was applied previously, the available AP firmware version is 3.6.2.0.695.

NOTE
When AP R730 is added to a zone, the non supported AP firmware version will not be available for downgrade in that zone. In a scenario where the customer did not have any R730 APs and adds few of them to the network, the APs will be in default zone. Subsequently, R730 APs can be moved to a new zone, if desired. The R730 having a latest firmware can only be moved to an existing AP zone provided it is upgraded to the latest 3.6.2 Patch1 AP firmware.

- **In Enterprise controller version,** the default Zone must be changed to reflect the AP patch version before AP R730 is connected to the network.
- **In High Scale controller version,** AP R730 registers to the staging Zone and it needs to be moved to a specified Zone with the AP patch version.

CAUTION
During the upgrade process, service outage will occur as the APs will restart automatically to complete the upgrade.

Upgrade Path

The upgrade path from 3.6.2 Patch 1 (Build 3.6.2.0.222) is SmartZone 5.1.1 where AP R730 is also natively supported.

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.

  ATTENTION
  Data plane functionality is not supported in this release.

- 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: **3.6.2.0.222**
- Control Plane Software Version: **3.6.2.0.63**
- Data Plane Software Version: **3.6.2.0.222**
- AP Firmware Version: **3.6.2.0.695**

SCG200-C

- Controller Version: **3.6.2.0.222**
- Control Plane Software Version: **3.6.2.0.63**
- AP Firmware Version: **3.6.2.0.695**

SZ100

- Controller Version: **3.6.2.0.222**
- Control Plane Software Version: **3.6.2.0.63**
- Data Plane Software Version: **3.6.2.0.27**
- AP Firmware Version: **3.6.2.0.695**

vSZ-H and vSZ-E

- Controller Version: **3.6.2.0.222**
- Control Plane Software Version: **3.6.2.0.63**
- AP Firmware Version: **3.6.2.0.695**

vSZ-D

- Controller Version: **3.6.2.0.222**

  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.

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 releases 104.x and higher, 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 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.

Supported AP Models

This release supports the following Ruckus AP models.

TABLE 1 Supported AP Models

11ac-Wave2		11ac-Wave1		11n		802.11ax
Indoor	**Outdoor**	**Indoor**	**Outdoor**	**Indoor**	**Outdoor**	**Indoor**
R720	T710	R700	T504	R300	ZF7782	R730
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.

NOTE
Refer to Access Point: R730 on page 4 PoE power modes for R730

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

NOTE

The caveats stated in 3.6.2 release notes are also applicable this release.

Component/s	AP
Issue	SCG-99923, SCG-101365
Description	If the untagged VLAN ID on any of the AP Ethernet ports is configured with a value other than VLAN ID 1 then none of the AP's WLAN can be mapped to VLAN ID of 1
Workaround	Map the WLAN to a VLAN ID other than 1

Component/s	AP
Issue	SCG-100054
Description	Radius interim updates are sent based on Radius start time and is not reset and sent if there is an update in-between (UE receives an IPv6 address)

Component/s	AP R730
Issue	SCG-83730
Description	AP does not advertise 2.5 and 5 Gbps speed capabilities for POE (Ethernet1) interface in LLDP (Link Layer Discovery Protocol) frames. The speed reflected in the LLDP frames does not match actual negotiated link speed

Component/s	AP R730
Issue	SCG-91950, SCG-97553
Description	Controller web user interface will not have any latency data or corresponding graph data populated

Component/s	AP R730
Issue	SCG-83734
Description	User will not be able to set speed using RKSCLI for POE (Ethernet1) interface
Workaround	User would need to change the speed on switch side and the AP will automatically come up with that speed

Component/s	System
Issue	SCG-92012
Description	SNMP option of *Write or Read* button greys out at times when a user select either of them

Component/s	System
Issue	ER-7003
Description	AP status in SZ WebUI Access Point tab may be Online although the AP is actually disconnected from the controller

Component/s	System
Issue	ER-7017
Description	When AP allocation feature is enabled, you may be unable to move new APs from the staging zone to a production zone

Component/s	System
Issue	ER-6980
Description	When *Access&Core Separation* feature is enabled, and a static route is defined on Control Plane for Location Based Service, this traffic does not use the specified gateway

Component/s	System
Issue	SCG-97253
Description	When user carries out an SNMP walk of a node the administrative activity shows as, *Administrator [admin] logged on from [0:0:0:0:0:0:0:1]*

Resolved Issues

The following are the resolved issues for this release.

Component/s	AP R730
Issue	SCG-93834
Description	Resolved an issue where traffic may fail in the following scenarios: • Ethernet WAN port VLAN - This is a non-default untag VLAN • Traffic from the second Ethernet port and WAN port VLAN. This is a non-default untag VLAN
Workaround	It is recommended to disable the offload option on the AP using the below RKS CLI command. This command is persistent across AP reboots and available only through AP CLI **set rflow-offload disable**

Component/s	AP R730
Issue	ER-6640, SCG-91518
Description	Resolved an issue where channel-fly did not change the channel

Component/s	AP R730
Issue	SCG-92038
Description	Resolved an issue where airtime utilization was showing sometimes 0%

Component/s	AP R730
Issue	SCG-92102
Description	Resolved an issue where Athstats were not showing MCS histogram.

Component/s	AP R730
Issue	SCG-91345
Description	Resolved an issue where AP may reboot during conductive VeriWave performance testing with multiple clients

Component/s	AP
Issue	SCG-92886
Description	Resolved an issue where AP R730 had instances of kernel panic and reboot while running single client downstream traffic using VeriWave in 11ac 4x4 mode

Component/s	AP
Issue	SCG-91624
Description	Resolved an issue where the initial AP R730 release did not support dynamic VLAN feature. If Radius returns with an VLAN attribute, the AP ignored this VLAN and used the VLAN associated to the profile or WLAN

Component/s	AP
Issue	ER-6593
Description	Resolved target failure issue for 11ac wave2 APs

Component/s	AP
Issue	ER-6606
Description	This enhancement allows configurable *Multicast Airtime* in percentage on Wave 1 APs. The default value is 25%

Component/s	AP
Issue	ER-6664
Description	Resolved an issue where the APs selected the channels 149-161 though they were not visible in the Zone/AP Group

Component/s	AP
Issue	ER-6658
Description	Resolved Kernel Panic issue for 11ac wave1 APs

Component/s	AP
Issue	ER-6732
Description	Resolved an issue where AD authentication could not accept the variable *and* in the user group

Component/s	AP
Issue	ER-6567, ER-6576, ER-6830
Description	Resolved an issue on R720 APs where wireless clients could experience low uplink throughput if they had previously associated to a WLAN with rate limiting enabled on the same R720 AP

Component/s	AP
Issue	ER-6607
Description	Resolved an issue where the AP now reports the statistics to SZ resulting in the display of the current information

Component/s	AP
Issue	ER-6627
Description	Resolved an issue that client may not be able to obtain IP address.

Component/s	AP
Issue	ER-6008
Description	Resolved an issue where APs using SoftGRE over IPv6 went into a GRE inactive state and closed their SSIDs.

Component/s	AP
Issue	ER-6801
Description	Resolved AP R720 reboot issue due to target failure

Component/s	AP
Issue	ER-6821
Description	Resolved an issue where the AP at time stopped passing client traffic when force DHCP was enabled and with client roaming

Component/s	AP
Issue	ER-4644, ER-4988
Description	Resolved an issue on Wave 2 devices where when more than three SSIDs existed on the same radio, the fourth and other succeeding SSIDs sent beacon frames at every other beacon interval

Component/s	AP
Issue	ER-6586
Description	Resolved an issue where in a WLAN with VLAN pool enabled, the first packet from the UE is tagged with an incorrect VLAN ID

Component/s	CLI
Issue	ER-6517

Description	Introduced a new AP CLI command to modify multicast queue limit, that can help to improve unicast throughput performance in environments with high multicast traffic
	
	`<set mcast-q-limit> and`
	`<get mcast-q-limit>`

Component/s	CLI
Issue	ER-6067
Description	Resolved an issue where output generation failed (WLANs not listed under WLAN Group) for the command **show running-config wlan-group 0104-wifi (2.4GHz)**

Component/s	System
Issue	ER-6649
Description	Resolved an DPSK issue where the UE was not able to associate to the unbound key after its first connection

Component/s	System
Issue	ER-6682
Description	Resolved an issue where the node was out of service since Mosquitto service was offline because of invalid venue name configuration while configuring LBS (Location-Based Services) server

Component/s	System
Issue	ER-6702
Description	Resolved an issue where the data plane got the incorrect gateway after a reboot.

Component/s	System
Issue	ER-6807
Description	Resolved an issue where SNMP OID *ruckusSZAPRXBytes/TXBytes* were not providing correct information

Component/s	System
Issue	ER-6630
Description	Resolved an intermittent connectivity issue in a WLAN with DPSK (Dynamic Pre-Shared Key) enabled due to an internal race condition in the controller

Component/s	UI/UX
Issue	ER-6449
Description	Resolved an issue where AP name was displayed incorrectly in several menus in Web user interface

Component/s	UI/UX
Issue	ER-6743
Description	Enhanced the login message from Identifiant to Se Connecter on the French Hotspot login page

Component/s	UI/UX
Issue	ER-6751
Description	Resolved an issue where there were duplicated entries in mesh tree view, which could not be updated by refreshing the web user interface

Component/s	Virtual SmartZone
Issue	ER-6552
Description	The fix allows Novell LDAP authentication to pass in absence of dictionary group information response. This makes the SZ version in par with ZD version

Component/s	Virtual SmartZone
Issue	ER-6584
Description	Resolved an issue where Radius proxy process would go offline intermittently.

Component/s	Virtual SmartZone
Issue	ER-6710
Description	Resolved an issue where the auto cell sizing failed to be deleted properly when the value is null

Component/s	Virtual SmartZone
Issue	ER-6919
Description	Resolved an issue where query for SNMP OID-1.3.6.1.4.1.25053 failed

Component/s	Virtual SmartZone
Issue	ER-6787
Description	Resolved an issue where the exported GuestPass CSV file was empty from page 2 onwards

Component/s	Virtual SmartZone
Issue	ER-6619
Description	Resolved an issue where mapping VLAN pools using the VLAN override option from WLAN Group failed

Component/s	Virtual SmartZone
Issue	ER-6290
Description	Resolved an issue for managing vSZ using Chrome OS devices by adding event mapping for Chrome OS

Component/s	Virtual Data Plane
Issue	ER-6720
Description	Resolved an issue where vSZ-D may fail to reconnect to the controller if it has been disconnected for a long time

Component/s	Virtual Data Plane
Issue	ER-6393
Description	Resolved an issue where the AP was unable to connect to the vSZ-D after rebooting vSZ-D

Security Considerations

Security Considerations

Following are the security fixes for this release.

- Refer to the Security Advisory for the linux kernel vulnerability (CVE-2018-5390): https://www.ruckuswireless.com/security/285/view/pdf.
- Security: CVE-2018-5391 [FragmentSmack] - refer to `CVE-2018-5390/CVE-2018-5391`.
- Updated OpenSSH to 7.4 version on the controller. **[ER-6834]**

Upgrading to This Release

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.

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.

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
	3.6.2.0.78

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

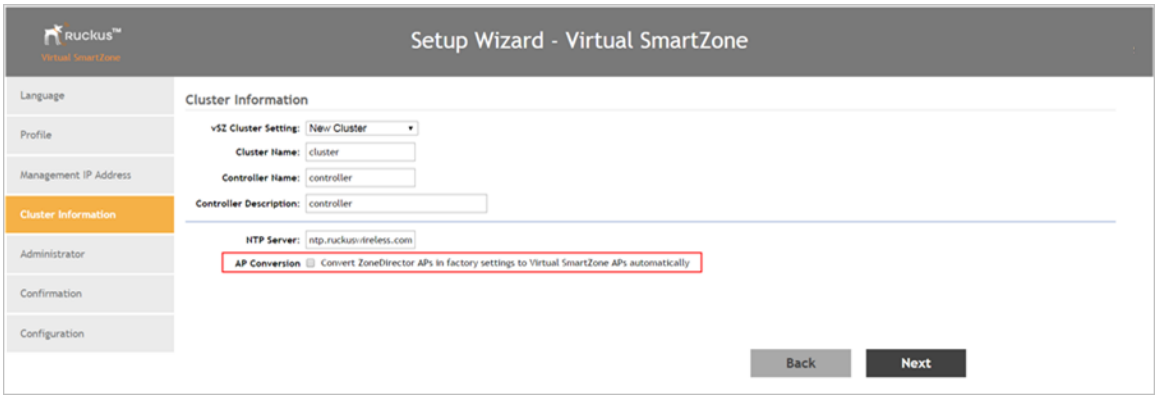
You can convert standalone ZoneFlex APs (those that are not managed by ZoneDirector) in factory default configuration to be managed by a SmartZone controller.

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

Using EAP-SIM profile Sony Xperia Z5, Sony Xperia Z3, LG G3 Stylus do not connect to AP R730 successfully. This is due to client limitation. **[SCG-94006]**

If clients encounter any interoperability issue with the AP operating in 11ax (default mode) the AP can be re-configured through RKS CLI to operate in 11ac mode including 5g and 2.4g commands. This mode can stay persistent across reboots. **[SCG-93051]**

- To configure 5G radio to 11ac mode, use the following command on AP:

  ```
  set mode wifi1 11ac
  ```

- To configure 2.4G radio to 11ng mode, use the following command on AP:

  ```
  set mode wifi0 11ng
  ```

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