

Ruckus SmartZone 3.6.2 (MR2) Release Notes

Supporting AP R730

Copyright, Trademark and Proprietary Rights Information

© 2018 ARRIS Enterprises LLC. All rights reserved.

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

Export Restrictions

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

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

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, 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, Edgelron, 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 Adding AP730 to the Controller.....	4
Access Point: R730.....	4
Adding AP R730 to the Controller.....	5
Hardware/Software Compatibility and Supported AP Models.....	6
Overview.....	6
Release Information.....	7
Supported and Unsupported Access Point Models.....	8
Caveats, Limitations, and Known Issues.....	9
Caveats, Limitations, and Known Issues.....	9
Upgrading to This Release.....	12
Overview.....	12
Virtual SmartZone Recommended Resources.....	13
Supported Upgrade Paths.....	14
Multiple AP Firmware Support in the SZ100/vSZ-E/SCG200-C/SZ300/vSZ-H.....	15
EoL APs and APs Running Unsupported Firmware Behavior.....	16
Interoperability Information.....	16
AP Interoperability.....	16
Redeploying ZoneFlex APs with SmartZone Controllers.....	17
Converting Standalone APs to SmartZone.....	17
ZoneDirector Controller and SmartZone Controller Compatibility.....	18
Client Interoperability.....	18

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
- DVLAN
- 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	Enabled	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

This SmartZone release supports the registration of new AP model R730.

Before starting this procedure, verify that the controller is running on release version 3.6.2 (Build 3.6.2.0.78)

ATTENTION

Before uploading the new AP patch, Ruckus strongly recommends saving a cluster backup. If you need to restore the controller to the previous AP patch, you can use this cluster backup. Before uploading the new AP patch, it is recommended that you save and export the configuration backup file. If you need to restore the configuration in case of anomaly, you can restore the configuration backup.

NOTE

This procedure will upgrade all APs that are registered with the Zone including R730.

- **In Enterprise controller version**, the default Zone must be changed to reflect the AP patch version before R730 is connected to the network.
- **In High Scale controller version**, 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.

Procedural Steps

Follow these steps to register the new AP model with the controller.

1. Log on to the [Ruckus support site](#).
2. Download the patch file, which enables the controller to support the new AP model. For example, `ap_r730_patch_pkg-3.6.2.0-509.noarch.patch`
3. Move the patch to a location where you can access the controller's web user interface.
4. Log on to the controller's web interface.
5. Navigate to **Administration > Upgrade**.
6. In **AP Patch** tab, browse to select the downloaded file in the option, **Upload the AP patch**.
7. Click on **Upload**.
8. Based on your web browser a browse or open dialog box appears.
9. Click on **Apply Patch**.
10. Manually change the AP firmware (using the option **Change AP firmware** in the controller web interface) to the latest AP image (3.6.2.0.509) in the default zone in case of Enterprise version or specific the zone in case of High Scale.
11. Navigate to **Monitor > Access Points** page, to verify that the new AP model added to the controller is listed on AP list page. Also, verify that all AP's in the default or specific zone are upgraded to build 3.6.2.0.509.
12. In the **Registration State** column, verify that the new AP model is approved.

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.

ATTENTION

The AP firmware version will change to 3.6.2.0.509 on upgrading to AP R730.

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**

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 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.



CAUTION

If you chose to apply AP R730 patch on SZ 3.6.2, you will not be able to migrate to SZ 5.0 and SZ 5.1 releases. You can only migrate to SZ 5.1.1 release, which is not yet released.

Supported AP Models

This release supports the following Ruckus AP models.

TABLE 1 Supported AP Models

11ac-Wave2		802.11ax	11ac-Wave1		11n	
Indoor	Outdoor	Indoor	Indoor	Outdoor	Indoor	Outdoor
R720	T710	R730	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

The following are the caveats, limitations and known issues.

Component/s	Wi-Fi Client Inter-Operability
Description	Windows laptops with Intel wireless card do not show SSID of APs advertising 11ax capability in their scan report. Hence user cannot connect to any 11ax capable AP
Solution	Latest Intel wireless driver has addressed this problem and we recommend a driver upgrade

Component/s	AP
Issue	SCG-91345
Description	During conductive VeriWave performance testing with multiple clients there is a high probability to run in to a Kernel panic and cause the AP to reboot

Component/s	AP
Issue	SCG-89295
Description	The target assert counter resets after every reboot or power cycle

Caveats, Limitations, and Known Issues

Component/s	AP Control Plane
Issue	SCG-93051
Description	<p>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.</p> <p>To configure 5G radio to 11ac mode, use the following command on AP:</p> <pre>set mode wifi1 11ac</pre> <p>To configure 2.4G radio to 11ng mode, use the following command on AP:</p> <pre>set mode wifi0 11ng</pre>

Component/s	AP Configuration
Issue	SCG-83730
Description	AP does not advertise 2.5 and 5 Gbps speed capabilities for POE (eth1) 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 Configuration
Issue	SCG-83734
Description	Users will not be able to set the speed using RKS CLI for POE (Ethernet1) interface. Users would need to change the speed on switch side and the AP will automatically come up with the specified speed.

Component/s	AP Configuration
Issue	SCG-84785
Description	802.1x supplicant functionality on Ethernet 0 or Ethernet 1 does not work

Component/s	AP Data Plane
Issue	SCG-84002
Description	Configuring SmartCast L2 and L3 IPv6 filters on WLAN interface drops all traffic from the UE

Component/s	AP Data Plane
Issue	SCG-93834
Description	<p>You may encounter traffic failure in the following scenarios:</p> <ul style="list-style-type: none"> 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	<p>It is recommended to disable the <i>offload</i> option on the AP using the below RKS CLI command. This command is persistent across AP reboots and available only through AP CLI</p> <pre>set rflow-offload disable</pre>

Component/s	AP Data Plane
Issue	SCG-89991
Description	AP might reset twice and reconnect to controller or data plane in following scenarios: <ul style="list-style-type: none"> • Randomly when AP is rebooted • When the controller is rebooted, power cycled or link is lost and recovered • When data plane appliance is rebooted, power cycled connection is lost and recovered

Component/s	AP Others
Issue	SCG-84849
Description	Some times false radar detection on DFS enabled channels cause AP to change channel. You can expect to see one false detect per day per AP in a typical enterprise environment

Component/s	AP Others
Issue	SCG-91950
Description	SZ web user interface will not have any latency data or populate any corresponding graph data

Component/s	AP Others
Issue	SCG-91912
Description	AP stays in new configuration state for almost 300 seconds after joining the controller. After 300 seconds, the configuration state changes to <i>up-to-date</i>

Component/s	AP Others
Issue	SCG-92102
Description	Ath statistics does not show probe or MCS histogram on R730 AP. This issue does not affect the general functionality of the AP

Component/s	AP Others
Issue	SCG-83626
Description	AP might take 120 to 180 seconds to join the controller when the controller is configured behind NAT

Component/s	R730 AP Platform
Issue	SCG-92886
Description	AP may occasionally perform a kernel panic reboot during single client downstream traffic to VeriWave client in 4x4 11ac mode

Component/s	R730 AP Platform
Issue	SCG-92330
Description	VeriWave conductive performance testing fails with AP in 2.4ghz 20 Mhz mode. Performance is OK when AP is in 40Mhz mode. Over the air performance of 2.4ghz radio is OK

Component/s	R730 AP Platform
Issue	SCG-92027, SCG-89768, SCG-90232, SCG-90646, SCG-90644, SCG-89668, SCG-84551 and SCG-89863
Description	In high density environment AP might occasionally target assert and recover. R730 target recovery mechanism does not cause the AP to reboot, but causes the clients to be booted out for approximately 20 seconds

Component/s	R730 AP Platform
Issue	SCG-94006
Description	Using EAP-SIM profile Sony Xperia Z5, Sony Xperia Z3, LG G3 Stylus do not connect to R730 successfully. This is due to a client limitation

Component/s	R730 AP Platform
Issue	SCG-92038
Description	Airtime utilization busy sometimes shows 0%. This does not always show zero as it is environment dependent

Component/s	R730 AP Platform
Issue	SCG-93052
Description	With MAC OS 10.9 (Maverick) it is noticed in multi client testing that few clients lose their IP address and can manually recover by reconnecting to the Wi-Fi. This issue is not observed with MAC OS 10.13 (HighSierra) or higher.

Component/s	System
Issue	SCG-91624
Description	Initial R730 release does not support dynamic VLAN feature. If the RADIUS returns with VLAN attribute, the AP will ignore this VLAN and use VLAN associated to the profile or WLAN.

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

If you chose to apply AP R730 patch on SZ 3.6.2, you will not be able to migrate to SZ 5.0 and SZ 5.1 releases. You can only migrate to SZ 5.1.1 release, which is not yet released.

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.

ATTENTION

The AP firmware version will change to 3.6.2.0.509 on upgrading to AP R730.



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.

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

The screenshot shows the 'Setup Wizard - Virtual SmartZone' interface. On the left is a navigation menu with options: Language, Profile, Management IP Address, Cluster Information (highlighted), Administrator, Confirmation, and Configuration. The main area is titled 'Cluster Information' and contains the following fields:

- vSZ Cluster Setting: New Cluster (dropdown)
- Cluster Name: cluster (text input)
- Controller Name: controller (text input)
- Controller Description: controller (text input)
- HTP Server: ntp.ruckuswireless.com (text input)
- AP Conversion: Convert ZoneDirector APs in factory settings to Virtual SmartZone APs automatically (checkbox with description)

At the bottom right, there are 'Back' and 'Next' buttons.

Interoperability Information

ZoneDirector Controller and SmartZone Controller Compatibility

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>



© 2018 ARRIS Enterprises LLC. All rights reserved.
Ruckus Wireless, Inc., a wholly owned subsidiary of ARRIS International plc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com