RELEASE NOTES

Ruckus SmartZone 3.6.2 Patch 2 Release Notes

Supporting SmartZone 3.6.2 Patch 2

Part Number: 800-72447-001 Rev C
Publication Date: February 2020

Copyright, Trademark and Proprietary Rights Information

Export Restrictions

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

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

Disclaimer

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

Limitation of Liability

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

Trademarks

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

Contents

Document History

Revision Number	Summary of changes	Publication date
A	Initial release	October 07, 2019
B	Removed the note and link to R730 power modes	October 15, 2019
C	Added ER-7642 and ER-8026 to Known Issues	February 24, 2020

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

Overview

Refer to previously released official Release Notes *SmartZone-3-6-2-Patch1-Supporting802.11ax-ReleaseNotes-RevA-20190411* for the existing content of 3.6.2 Patch-1. This document is available by visiting the Ruckus website available at support.ruckuswireless.com

Release Information

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

SZ300

- Controller Version: **3.6.2.0.250**
- Control Plane Software Version: **3.6.2.0.78**
- Data Plane Software Version: **3.6.2.0.250**
- AP Firmware Version: **3.6.2.0.759**

SCG200-C

- Controller Version: **3.6.2.0.250**
- Control Plane Software Version: **3.6.2.0.78**
- AP Firmware Version: **3.6.2.0.759**

SZ100

- Controller Version: **3.6.2.0.250**
- Control Plane Software Version: **3.6.2.0.78**
- Data Plane Software Version: **3.6.2.0.30**
- AP Firmware Version: **3.6.2.0.759**

vSZ-H and vSZ-E

- Controller Version: **3.6.2.0.250**
- Control Plane Software Version: **3.6.2.0.78**
- AP Firmware Version: **3.6.2.0.759**

vSZ-D

- Data Plane Version: **3.6.2.0.250**

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	

TABLE 1 Supported AP Models (continued)

11ac-Wave2		11ac-Wave1		11n		802.11ax
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	

Known Issues

The following are the caveats, limitations and known issues.

NOTE
The caveats stated in the 3.6.2 Patch 1 Release Notes are also applicable to this release.

Component/s	AP
Issue	ER-7642, ER-8026
Description	Controller and AP time synchronization with NTP server only happens during controller bootup and when it is done manually in the controller web user interface (**System** > **General Settings** > **Time menu**). This may cause synchronization issues with SPoT server if it is used in the same network

Component/s	AP
Workaround	Contact Ruckus Technical Support if you need periodic synchronization in this release.

Component/s	AP
Issue	ER-6857
Description	R730 AP sends tunnel keepalive traffic with Ethernet interface as source MAC address instead of bridge interface when offload is enabled

Component/s	AP
Issue	SCG-111081
Description	R730 AP sends username attribute in Radius accounting messages as client MAC address instead of the username for WebAuth WLAN

Component/s	CLI
Issue	ER-7659
Description	Controller CLI command **show ap-stats** fails to be executed and only provides an error message

Component/s	System
Issue	SCG-108693
Description	A report may fail to generate in controller web user interface with an error message if it contains too many SSIDs
Workaround	Reduce the number of SSIDs selected under **Resource Filter Criteria** > **Report Configuration**. Maximum number of SSIDs in a report is 32, but it may be further reduced based on the length of the SSIDs

Resolved Issues

Issues Resolved in this Release

Component/s	AP
Issue	ER-6461
Description	Resolved an issue where in some cases an AP could broadcast a WLAN when it was configured with Scheduler option set to*Always Off*

Component/s	AP
Issue	ER-6780
Description	Resolved an issue where the group key was not set at fast roam

Component/s	AP
Issue	ER-6689
Description	Resolved a kernel panic issue on APs located in high density environments when associated wireless clients frequently roamed in and out of range

Component/s	AP
Issue	ER-6857
Description	Resolved an issue where AP sends tunnel keepalive traffic with Ethernet interface as source MAC address instead of bridge interface when offload is enabled. This is fixed in all AP models where applicable except R730

Component/s	AP
Issue	ER-6970
Description	Resolved an issue where incorrect number of active clients was obtained from AP SNMP query

Component/s	AP
Issue	ER-7018
Description	Resolved an issue on 11ac Wave 1 APs where unsupported data rates were used to send the first data packet to a wireless client over the 5 GHz radio

Component/s	AP
Issue	ER-7073
Description	Resolved an issue where the R700 APs rebooted on detection of target failure

Component/s	AP
Issue	ER-7079
Description	Resolved an issue that generates log messages in the APs containing ***wsgclient/timezone value too big***

Component/s	AP
Issue	ER-7259
Description	Added compliance with DHCP back off algorithm in APs as per RFC 2131, section 4.1

Component/s	AP
Issue	ER-7260
Description	Resolved an issue where a NULL pointer in mesh wave1 APs resulted in AP reboot

Component/s	AP
Issue	ER-7429
Description	Resolved an issue where T710 using SFP (Small Form-factor Pluggable) uplink port was failing to establish Ruckus GRE tunnel

Component/s	AP
Issue	ER-7331
Description	Resolved an issue where SSID spoofing rule in Rogue Classification Policy feature was not matching the expected SSIDs

Component/s	AP
Issue	ER-6748
Description	Resolved an issue where some ARPs packets to be transmitted as broadcast were being dropped at the AP

Component/s	AP
Issue	ER-7304
Description	Resolved an issue where updated AP device-name was not retrieved from SNMP query to the AP until it was rebooted

Component/s	AP
Issue	ER-7286
Description	Resolved an issue where AP sends tunnel user traffic with Ethernet interface as source MAC address instead of bridge interface when offload is enabled.

Component/s	AP
Issue	ER-6248
Description	Resolved an issue where Rogue Device reporting does not work properly when SSID name is configured as none English name

Component/s	Control Plane
Issue	ER-7202
Description	Resolved an issue where APs may fail to connect to the controller due to incorrect handling in controller database of DHCP/NAT configuration

Component/s	Control Plane
Issue	ER-7009
Description	Resolved an issue where controller CLI command **show ap <AP_MAC>** may take too long or time out for high number of APs in a zone

Component/s	Control Plane
Issue	ER-7199
Description	Resolved an issue where incorrect information in SZ database were causing reporting issues in SCI

Component/s	Control Plane
Issue	ER-7285
Description	Resolved an issue where AP zones created using the zone template could not be deleted later due to incorrect value in database

Component/s	Control Plane
Issue	ER-7288
Description	Resolved an issue where cluster went out of service as subscriber management failed frequently due to large number of configured WLANs

Resolved Issues

Issues Resolved in this Release

Component/s	Data Plane
Issue	ER-6885
Description	Resolved an issue where an AP deleted from a cluster could still establish Ruckus GRE tunnel with data plane

Component/s	Data Plane
Issue	ER-7254
Description	Resolved an issue where BPDUs with destination MAC address different than 01:80:C2:00:00:00 were dropped

Component/s	Data Plane
Issue	ER-7558
Description	Resolved an issue where data plane may slow down or fail to work properly due to excessive amount of logs when receiving small MTU packets

Component/s	Data Plane
Issue	ER-6997
Description	Resolved an issue in SZ100 data plane where user traffic is delayed in tunneled WLANs due to excessive MDNS (multicast DNS) traffic in core side

Component/s	Data Plane
Issue	ER-7399
Description	Enhanced watchdog to recover stuck processes

Component/s	SCI
Issue	ER-7497
Description	Resolved an issue where SCI could not distinguish correctly between authorized and unauthorized client types

Component/s	System
Issue	ER-7147
Description	Resolved an issue where controller CLI was unable to create a domain

Component/s	System
Issue	ER-6921
Description	Resolved an issue where validation was missing for maximum devices allowing when creating *Guest Passes* using Public API

Component/s	System
Issue	ER-6900
Description	Resolved an issue where updating a zone concurrently caused the zone configuration to be missing.

Component/s	System
Issue	ER-6980
Description	Enhanced control plane static route network configuration, which allows traffic to be routed through the control interface under the conditions: 1. Default gateway is set to management interface 2. Control plane access/core separation is enabled

Component/s	System
Issue	ER-6991
Description	Resolved an issue where SNMPD process in controller crashed frequently due to repeated queries to *ruckusCtrlApTable*

Component/s	System
Issue	ER-7003
Description	Resolved an issue where the AP status in the controller user interface AP tab is seen as online although the AP is disconnected from the controller

Component/s	System
Issue	ER-7017
Description	Resolved an issue where AP was not able to move from staging zone to production zone when AP number allocation was enabled

Component/s	System
Issue	ER-7065
Description	Resolved an issue where SFTP connection was not released after file transfer

Component/s	System
Issue	ER-7216
Description	Resolved an issue where controller Radius configuration may be not correct due to a race condition during system bootup

Component/s	System
Issue	ER-7261
Description	Resolved an issue where AP failed to move from the staging zone due to Public API enabling *wlanService50Enabled*

Component/s	System
Issue	ER-7283
Description	Enhanced an issue where the get zone list API was very slow in the current design

Component/s	System
Issue	ER-7350
Description	Resolved an issue where Radius proxy process stopped while printing the logs in an error scenario

Component/s	System
Issue	ER-7357
Description	Resolved an issue where CNR process would restart intermittently

Component/s	System
Issue	ER-7181
Description	Resolved an issue where corrupted values of *Acct-Input-Gigawords* and *Acct-Output-Gigawords* was present in Accounting messages

Component/s	System
Issue	ER-7481
Description	Resolved an issue where zone upgrade containing multiple different AP models could fail

Component/s	System
Issue	ER-7550
Description	Resolved an issue where the controller historical client TX and RX data was inaccurate

Security Considerations

Following are the security fixes and third party software upgrade for this release.

- Upgraded Dropbear SSH package in APs to version 2018.76. **[ER-7521]**
- Refer to the Security Advisory for the privilege escalation vulnerability (CVE-2019-11630) https://www.ruckuswireless.com/security/294/view/pdf **[ER-7011]**

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
	3.4.2.0.245
	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
	3.6.2.0.222

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

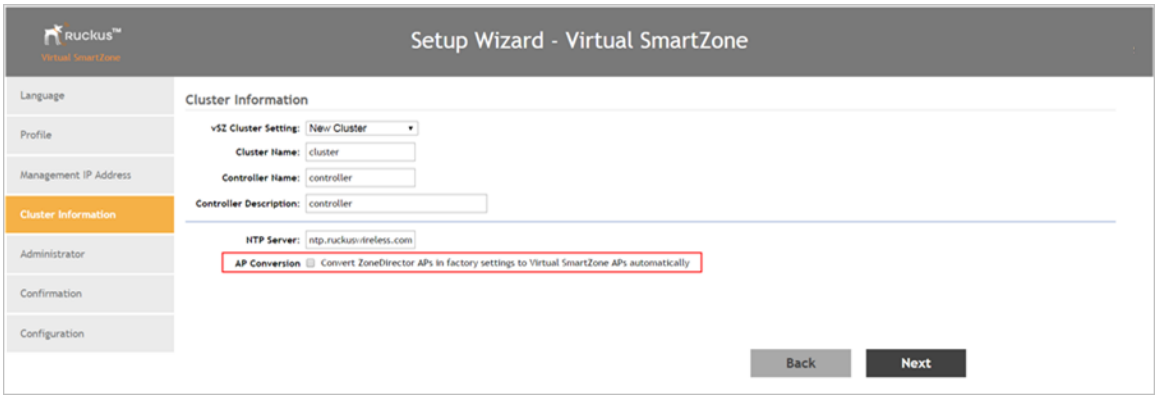
You can convert standalone ZoneFlex APs (those that are not managed by ZoneDirector) in factory default configuration to be managed by a SmartZone controller.

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
```

COMMSCOPE®
RUCKUS®

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