RELEASE NOTES

Ruckus SmartZone

Supporting SmartZone 3.5.1 Patch 1

Part Number: 800-71725-001
Publication Date: September 2017

Copyright Notice and Proprietary Information

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader's responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN ("MATERIAL") IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. BROCADE and RUCKUS WIRELESS, INC. AND THEIR LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. BROCADE and RUCKUS RESERVE THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL BROCADE or RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless, Ruckus, the bark logo, BeamFlex, ChannelFly, Dynamic PSK, FlexMaster, Simply Better Wireless, SmartCell, SmartMesh, SmartZone, Unleashed, ZoneDirector and ZoneFlex are trademarks of Ruckus Wireless, Inc. in the United States and in other countries. Brocade, the B-wing symbol, MyBrocade, and ICX are trademarks of Brocade Communications Systems, Inc. in the United States and in other countries. Other trademarks may belong to third parties.

Contents

Changed Features in This Release

The following are the changed features in this release.

- When generating the AP configuration, at time the L2ACL service gets applied to the wrong WLAN. To avoid this issue, fix the WLAN mapping logic address on the SmartZone controller to ensure that L2ACL is applied to the right WLAN. [ER-5537]
- Enhancement to enable DFS channels 52, 56, 60, and 64 on 11n AP models for Singapore country code (SG). These DFS channels can also be enabled or disabled through SCG or vSZ controller user interface. [AP- 6082 ER-5507]
- HTTP header data encoding needs to be in a URL encoded format since it cannot be sent as UTF-8 direct. [ER-5445]
- Using CLI mode configure the subnet as 10.254.0.0 in SZ100 and vSZ controller platforms. [ER-5552]
- Enhanced SCG to support NSAPI values from range 0 to15. [ER-5486]
- Fixed the code logic to export more than 500 historical client statistics when exported to a *.csv* file. [ER-5465]
- Guest Pass expiration validation will be invalid when the authentication fails after the expiration time. [ER-5399]

Hardware/Software Compatibility and Supported AP Models

Overview

This section provides release information about the SmartZone 300 (SZ300), the SmartCell Gateway 200 (SCG200), 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, 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, 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.

  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 Wireless 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 Wireless 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.

Release Information

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

SZ 300

- Controller Version: **3.5.1.0.862**
- Control Plane Software Version: **3.5.1.0.820**
- Data Plane Software Version: **3.5.1.0.862**
- AP Firmware Version: **3.5.1.0.1010**

SCG 200

- Controller Version: **3.5.1.0.862**
- Control Plane Software Version: **3.5.1.0.820**
- Data Plane Software Version: **3.5.1.0.801**
- AP Firmware Version: **3.5.1.0.1010**

SZ 100

- Controller Version: **3.5.1.0.862**
- Control Plane Software Version: **3.5.1.0.820**
- Data Plane Software Version: **3.5.1.0.807**
- AP Firmware Version: **3.5.1.0.1010**

vSZ-H and vSZ-E

- Controller Version: **3.5.1.0.862**
- Control Plane Software Version: **3.5.1.0.820**
- AP Firmware Version: **3.5.1.0.1010**

vSZ-D

- vSZ-D software version: **3.5.1.0.862**

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

On solo APs running release 104.x, the LWAPP2SCG service must be disabled. To disable the LWAPP2SCG service on an AP, log on to the CLI, and then go to enable **mode** > **config** > **lwapp2scg** > **policy deny-all**. Enter Yes to save your changes.

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

Supported AP Models

This release supports the following Ruckus Wireless AP models.

TABLE 1 Supported AP Models

11ac-Wave2		11ac-Wave1		11n	
Indoor	Outdoor	Indoor	Outdoor	Indoor	Outdoor
R720	T710	R700	T504	R300	ZF7782
R710	T710s	R600	T300	ZF7982	ZF7782-E
R610	T610	R500	T300E	ZF7372	ZF7782-N
R510		C500	T301N	ZF7372-E	E ZF7782-S
H510		H500	T301S	ZF7352	ZF7781CM
C110		R310	FZM300	ZF7055	
H-320			FZP300		

NOTE
Release H320 has native support.

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

NOTE
When the R720, R710, T610, or R610 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	Unsupported AP Models
SC8800-S	SC8800-S-AC
ZF7321	ZF7321-U
ZF7441	ZF7761-CM
ZF7762	ZF7762-AC
ZF7762-T	ZF7762-S
ZF7762-S-AC	ZF7363
ZF7343	ZF7341
ZF7363-U	ZF7343-U
ZF7025	ZF7351
ZF7351-U	ZF2942

TABLE 2 Unsupported AP Models (continued)

Unsupported AP Models	Unsupported AP Models
ZF2741	ZF2741-EXT
ZF7962	

Caveats, Limitations, and Known Issues

This section lists the caveats, limitations, and known issues in this release.

NOTE
The caveats stated in 3.5 release notes are also applicable to 3.5.1 patch 1

Control and Data Plane

The following are the known issues related to the control and data plane.

- 10.254.x.x is reserved for internal use as communication between control plane and data plane. If a client or a device in the network uses this address, the control plane will not be able to communicate to the data plane due to the ARP being resolved by the client or device. Ensure that this address is reserved and not used.

Customized Certificates

The following are the known issues related to the customized certificates.

- When customized certificates are applied for services such as Management Web, AP Portal, Hotspot (WISPr) and Communicator and when upgrading the controllers SCG or SZ from 3.2.x to 3.5.1 Patch-1, the status of the certificates changes to **default**.

  Workaround:

  Step-1: Select the corresponding certificates that you need to change from default using the drop down menu. Click OK. This action will restart the services.

  Step-2: If Web/WISPr/Portal redirection continues to direct to the default certificate on restarting the services the controllers SCG or SZ needs to rebooted.

System

The following are the known issues related to systems.

- In release R3.5.1 Patch 1 Smart Zone software (vSZ-E, vSZ-H, SZ-100, SZ-200 and SZ-300), some of the web pages in the web user interface are affected with XSS (Cross Site Scripting) vulnerabilities. These vulnerabilities are manifested due to lack of the input validation in some of the fields of the web pages. However, to carry out XSS attacks or exploit these vulnerabilities, attacker requires access to valid login username and password. Therefore, the degree and severity of impact because of these vulnerabilities is low.

  Workaround: All the XSS vulnerabilities reported can be exploited only if a user successfully logins to Web UI with valid login credentials in main login page. The main login page is not impacted by the XSS vulnerability and if attacker does not know the login credentials then it is not possible to exploit the XSS vulnerabilities in subsequent web pages. It is recommended that the login credentials should be shared only with valid and authorized users.

  Fix: Ruckus Wireless has fixed this XSS vulnerabilties in the forthcoming 3.6 GA release.

Resolved Issues

This section lists previously known issues and internally-found issues that have been resolved in this release.

AP Resolved Issues

- Resolved an AP kernel panic reboot issue caused when receiving malformed BTM (BSS Transition Management) frames response frames from certain clients. [AP-5480 ER-5386]
- Resolved a H510 Ethernet issue where the Ethernet data rate was configured as 10/100 Mbps and the AP was trying to send a higher data rate to a wired client connected to the Ethernet port. [ER-5329]
- APs learn about one another's internal states regularly, which helps in improving roaming and load balancing. There were several issues in memory management and over-processing of the same network data, which caused CPU to overload. These issues have been fixed. [ER-5524]
- Resolved an issue where the AP event reports showed a future time stamp. [ER-4739]
- Resolved an issue where Ruckus APs marked 3rd party APs as SSID spoofing rogue after removing the WLAN which had the same SSID on the Ruckus AP. [SCG-67332]

System Resolved Issues

- Resolved an issue where Cloudpath was not able to get the DPSK passphrase from the SmartZone (SZ) controller and timed out due to a design defect of SZ DPSK. [ER-5490]
- Resolved an issue where incorrect traffic counter values were included in Accounting Stop for a TTG client, which roamed across different data and control planes in quick succession. [ER-5372]
- Resolved an issue where the session manager process crashed regularly. [ER-5447]
- Resolved an issue where the controller allows a guestpass administrator to view their own guest pass. [ER-5510]
- Resolved an issue where the failed login files are sent to the remote syslog server. [ER-5443]
- Resolved an issue where the secondary DNS server with a large IP addresses was not showing correctly on the client. [ER-5494]
- Resolved an issue where rate limiting would not work for WLANs which are enabled with the option *drop multicast packets from associated clients*. [ER-5319 ER-5534 SCG-51924]
- Resolved an issue where 802.1x authentication using local database failed for users with leading P or R in their username. [ER-5574]
- Resolved an issue where wired user equipments were not able to get the IP address when tunnel encryption was enabled. [ER-5589 SCG-72041]
- Resolved an issue where wired clients on different APs were not able to ping each other if the tunnel encryption was enabled. [ER-5569]
- Resolved an issue where the tunnel WLAN was crypto enabled and involved file transfer, which caused an occasional blip in the packet being corrupted. [ER-5570]
- Resolved an issue where wireless client on the tunneled WLAN could not ping the controller. [ER-5511]
- Resolved an issue where the controller showed incorrect GRE tunnel numbers occasionally. [ER-5311]
- Resolved an issue where the channel background application sent the channel number without checking whether the current channel mode supports the channel number. [SCG-60820]

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 Wireless 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.

If you are upgrading from an earlier release, you will likely need to upgrade the system resources allocated to the virtual machine on which vSZ is installed. However, changing the system resources could result in an issue where the vSZ cluster goes out of service [SCG-47455]. To prevent this issue from occurring, you must do the following

1. Contact Ruckus Wireless Support and obtain

   ```
   SCG47455_WorkAround_RP_OS_433930.ksp.
   ```

2. Apply SCG47455_WorkAround_RP_OS_433930.ksp, which fixes SCG-47455.
3. Adjust the system resources allocated to the virtual machine on which vSZ is installed (see the recommended resource tables below).
4. Upgrade vSZ to this release

vSZ High Scale recommended resources

TABLE 3 vSZ High Scale recommended resources

Nodes per Cluster	AP Count per Node	AP Count per Cluster		Client Count per Cluster	Disk Size	vCPU	RAM	Max Preserved Events	Resource Level
	Max	Min	Max		GB	Core[1]	GB	Max	
3-4	10,000	10,001	30,000	300,000	600	24	48	3M	8
1-2	10,000	5,001	10,000	100,000	600	24	48	3M	7
1-2	5,000	2,501	5,000	50,000	300	12	28	2M	6.5
1-2	2,500	1,001	2,500	50,000	300	6	22	1.5M	6
1-2	1,000	501	1,000	20,000	100	4	18	600K	5
1-2	500	101	500	10,000	100	4	16	300K	4
1-2	100	1	100	2,000	100	2	13	60K	3

vSZ Essentials recommended resources

TABLE 4 vSZ Essentials recommended resources

Nodes per Cluster	AP Count per Node	AP Count per Cluster		Client Count per Cluster	Disk Size	vCPU	RAM	Max Preserved Events	Resource Level
	Max	Min	Max		GB	Core[2]	GB	Max	
3-4	1,024	1,025	3,000	60,000	250	8	18	10K	2
1-2	1,024	101	1,024	25,000	250	8	18	10K	2
1-2	100	1	100	2,000	100	2	13	1K	1

NOTE
Core[1] Azure with low CPU throughput unsupported
Core[2] Azure with low CPU throughput unsupported

Supported Upgrade Paths

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

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	3.2.0.0.790
SCG200	3.2.1.0.163
SZ100	3.2.1.0.193
vSZ (vSCG)	3.2.1.0.217
vSZ-D	3.2.1.0.245
	3.2.1.0.253
	3.4.0.0.976
	3.4.1.0.208
	3.4.2.0.152
	3.5.0.0.808
	3.5.0.0.832
	3.5.1.0.296
	3.4.2.0.169
	3.4.2.0.176

Upgrading With Unsupported APs

If the controller is currently managing APs that are unsupported in this release, here are a few issues that you may encounter when you upgrade to this release and their workarounds.

AP models that have already reached End-of-Life (EoL) status (for example, the 2942) are unsupported in this release. If you currently have AP models that are unsupported, you will be able to upgrade the controller to this release but not the AP zones to which the EoL APs belong.

- After you upload the upgrade (`.ximg`) file the **Administration** > **Upgrade** page of the web interface, the web interface will inform you that the upgrade cannot be started because the controller is managing at least one AP that is unsupported by this release.
- If you click Upgrade or Backup & Upgrade on the **Administration** > **Upgrade**page, the upgrade process will start, but it will eventually fail. [SCG-41229]

Issues and Workarounds for Upgrading Unsupported APs to This Release

The following tables summarize some of the upgrade issues that you may encounter if the SZ100 or SCG200 is managing APs that have reached EoL and the possible workarounds for each issue. [SCG-42511, SCG-43360]

TABLE 6 Issues and workarounds for upgrading the SZ100 with EoL APs

Release	Issue Workaround	Version
3.2	When you attempt to upgrade the controller, a warning message appears and informs you that the system cannot be upgraded because there are APs that are unsupported in the new release. The message identifies these unsupported APs. The **Upgrade** and **Backup & Upgrade** buttons are hidden to prevent you from attempting to upgrade the system before one of available workarounds to the issue is applied.	To be able to upgrade the system, do one of the following: • On the web interface, clear the Automatically approve all join requests from APs check box. • Delete any unsupported APs from the controller. • Before running the upgrade, apply the KSP file for this issue. Contact Ruckus Wireless Support for more information.

When you attempt to upgrade the SCG200 to this release, the upgrade script will check if the controller has any AP zones using AP firmware releases that are unsupported in this release. If the upgrade script finds at least one AP zone that is using an unsupported AP firmware release, the upgrade process will aborted.

TABLE 7 Issues and workarounds for upgrading the SCG200 with EoL APs

Release	Issue Workaround	Version
3.2	When you attempt to upgrade the controller, a warning message appears and informs you that the system cannot be upgraded because there are APs that are unsupported in the new release. The message identifies these unsupported APs. The **Upgrade** and **Backup & Upgrade** buttons are hidden to prevent you from attempting to upgrade the system before one of available workarounds to the issue is applied.	To be able to upgrade the system, do one of the following: • Move the EoL APs to the *Staging Zone*. • Upgrade the AP zones to the latest available AP firmware release. • Before running the upgrade, apply the KSP file for this issue. Contact Ruckus Wireless Support for more information.

Multiple AP Firmware Support in the SCG200/vSZ-H

In the SCG200/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
Some earlier AP models can only support AP firmware 3.1.x and earlier. If you have these AP models, note that they cannot be upgraded to this release.

NOTE
If you have AP zones that are using 3.1.x and the AP models that belong to these zones support AP firmware 3.2 (and later), change the AP firmware of these zones to 3.2 (or later) to force these APs to upgrade their firmware. After you verify that all of the APs have been upgraded to AP firmware 3.2 (or later), proceed with upgrading the controller software to release 3.5.
In the current release and earlier releases, when the SCG200/vSZ-H software is upgraded to a newer release, the upgrade mechanism does not require the administrator to upgrade the AP firmware releases that managed APs are using.

NOTE
In contrast, in 3.5 and earlier releases, the SZ100/vSZ-E automatically upgrade both the controller firmware and AP firmware when the system is upgraded. In release 3.5.1, however, the concept of "zones" is introduced, which slightly changes the upgrade workflow. The system and the AP zones in SZ100/vSZ-E are now upgraded independently. The administrator must now proactively upgrade the AP zones (and thus, the APs in them) after upgrading the system to the new firmware.

Up to Three Previous Major AP Releases Supported

Every SCG200/vSZ-H 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, 3.5 and 3.5.1 are considered part of the same major release version, which is 3.5.

The following releases can be upgraded to release 3.6:

- 3.5.x
- 3.5
- 3.4.x
- 3.4
- 3.2
- 3.2.x

The AP firmware releases that the SCG200/vSZ-H will retain depend on the SCG200/vSZ-H release version from which you are upgrading.

- If you are upgrading the SCG200/vSZ-H from release 3.5, then the AP firmware releases that it will retain after the upgrade will be 3.5 and 3.5.1
- If you are upgrading the SCG200/vSZ-H from release 3.4, then the AP firmware releases that it will retain after the upgrade will be 3.5 and 3.4.

All other AP firmware releases that were previously available on the SCG200/vSZ-H will be deleted automatically.

EoL APs and APs Running Unsupported Firmware Behavior

Understanding how the SCG200 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.

EoL APs

NOTE
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 Wireless Support website. The icons for EoL APs appear with the *END OF LIFE* watermark.

- An EoL AP that has not registered with the SCG200 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.
- If an EoL AP is already being managed by the SCG200 and you attempt to upgrade the controller, the firmware upgrade process will be unsuccessful. The web interface may or may not display a warning message (see Upgrading With Unsupported APs). You will need to move the EoL AP to the Staging Zone to upgrade the controller successfully.

An EoL AP that has not registered with the SCG200 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.

APs Running Unsupported Firmware Releases

- APs running AP firmware releases that are unsupported by the SCG200 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 Wireless controller products including ZoneDirector, SCG200, vSZ, SZ- 100, and SAMs.

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 AP 100.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, vSZ, or SAMs controller.

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

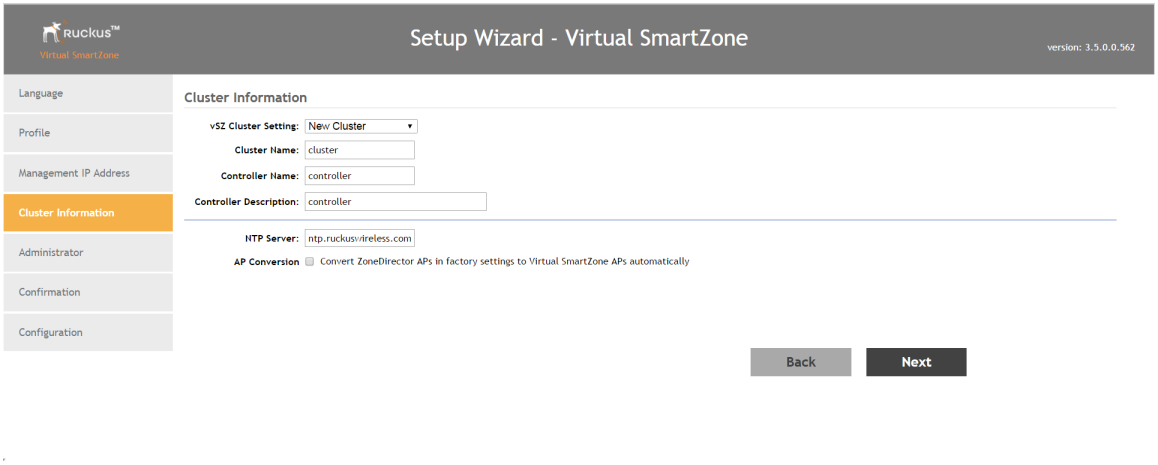
You can convert standalone ZoneFlex APs (those that are not managed by ZoneDirector)in factory default configuration to be managed by a SmartZone controller.

Follow these steps to convert standalone ZoneFlex APs to the SmartZone controller firmware so that they can be managed by the SZ300, SCG200, 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, SCG200, or SZ100 the check box description may be slightly different.

FIGURE 1 Select the AP Conversion check box to convert standalone ZoneFlex APs to SCG 200/SZ100/vSZ 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 (SCG, SZ, vSZ, SAMs controllers) 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 Wireless qualifies its functionality on the most common clients.