RELEASE NOTES

Ruckus SmartZone 3.4.2 Patch 4 Release Notes

Supporting SmartZone 3.4.2

Part Number: 800-72311-001 Rev A
Publication Date: May 2019

Contents

New and Changed Features

Changed Features

The following are the changed features.

- Added a new attribute in the URL (identified as 'msg') if and only if the hotspot user login fails with ZD-Style Login API. The value of the new attribute is an error messages from Northbound Interface (NBI) or a customized reply message from the RADIUS attribute of Reply-Message. **[SCG-91621]**, **[ER-6613]**
- Native support for the GDPR feature. **[SCG-101964]**

Hardware/Software Compatibility and Supported AP Models

Overview

This section provides release information about 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 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 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.

Release Information

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

SCG 200

- Controller Version: **3.4.2.0.245**
- Control Plane Software Version: **3.4.2.0.118**
- Data Plane Software Version: **3.4.2.0.162**
- AP Firmware Version: **3.4.2.0.910**

SZ 100

- Controller Version: **3.4.2.0.245**
- Control Plane Software Version: **3.4.2.0.118**
- Data Plane Software Version: **3.4.2.0.53**
- AP Firmware Version: **3.4.2.0.910**

vSZ-H and vSZ-E

- Controller Version: **3.4.2.0.245**
- Control Plane Software Version: **3.4.2.0.118**
- AP Firmware Version: **3.4.2.0.910**

vSZ-D

- vSZ-D software version: **3.4.2.0.245**

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.

> **NOTE**
> APs preconfigured with the SCG200/SZ100/vSZ AP firmware may be used with the SCG200/SZ100/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.

Supported AP Models

This release supports the following AP models.

TABLE 1 Supported AP Models

C110	C500	R300	R310	R500	R500E
R510	R600	R610	R700	R710	T300
T300E	T301N	T301S	T504	T610	T610s
T710	T710S	H500	H510	ZF7055	ZF7352
ZF7372	ZF7372-E	ZF7781CM	ZF7782	ZF7782-E	ZF7782-N
ZF7782-S	ZF7982				

Unsupported AP Models

The following AP models have reached end-of-life (EoL) status and, therefore, are no longer supported in this release.

SC8800-S	ZF7762	ZF7343	ZF7351-U
SC8800-S-AC	ZF7762-AC	ZF7341	ZF2942
ZF7321	ZF7762-T	ZF7363-U	ZF2741
ZF7321-U	ZF7762-S	ZF7343-U	ZF2741-EXT
ZF7441	ZF7762-S-AC	ZF7025	ZF7962
ZF7761-CM	ZF7363	ZF7351	

Caveats, Limitations, and Known Issues

NOTE
The caveats stated in 3.4.2 Patch 3 Release Notes are also applicable to this release.

Component/s	CLI
Issue	SCG-102447
Description	The CLI does not validate and deny entering special characters such as ` when entering the radius shared secret
Workaround	Use the GUI which provides the correct validation for the characters which are NOT permitted

Component/s	CLI
Issue	SCG-103477
Description	The output of the controller CLI command **show ip name-server** appends junk characters to the DNS server name

Resolved Issues

The following are the resolved issues for this release.

Component/s	AP
Issue	ER-5457
Description	Resolved an issue with PDA connectivity on hidden SSIDs

Component/s	AP
Issue	ER-6138
Description	Resolved an issue in the GUI where special characters ` and $ are used to be allowed as part of the RADIUS shared secret.

Component/s	AP
Issue	ER-6948
Description	Resolved an issue where the AP power LED indicator of the ZF7055 was always displayed as red

Component/s	AP
Issue	ER-6954
Description	Resolved an issue where AP NTP setting was removed when AP was deleted from AP Zone

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

Component/s	AP
Issue	ER-6675
Description	Resolved an issue where AP R710 reboot problem was detected

Component/s	AP
Issue	SCG-102435
Description	Resolved an issue where the percentage sign in WLAN or SSID caused the AP to restart to restart which affected the UE connectivity

Component/s	AP
Issue	ER-5977
Description	Resolved a target fail detected issue on 11ac Wave2 APs

Component/s	AP
Issue	ER-5767
Description	Resolved an issue that could prevent WISPr clients to be successfully authorized in multi-node clusters

Component/s	AP
Issue	ER-6310
Description	Resolved an issue where the NBI connections failed to release on a session timeout

Component/s	AP
Issue	ER-6489
Description	Resolved an issue where *onDemandData* SZ Public API for 7781CM AP model was failing

Component/s	AP
Issue	ER-5971
Description	Resolved an issue where incorrect amount of visitors were reported in vSPoT due to false MAC address detection on the AP

Component/s	AP
Issue	ER-5980
Description	Resolved an issue where clients could not connect properly when an AP was assigned to AP Group with 32 character length

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

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

Component/s	Control Plane
Issue	ER-6077
Description	Resolved an issue where Radius accounting messages did not include one Class attribute on UE roaming when *Fast Roaming* was enabled

Component/s	Control Plane
Issue	ER-6448
Description	Resolved an issue where the control plane static IPv6 route was not validated

Component/s	Control Plane
Issue	SCG-102446
Description	Resolved an issue where the character $ was accepted as part of the Radius shared secret even though the error message mentioned it is as not allowed

Component/s	Data Plane
Issue	ER-6328
Description	Resolved an issue when configuring IPv6 static route by adding a prefix validation in web user interface and CLI

Component/s	Data Plane
Issue	ER-6678
Description	Resolved an issue where the under run packet caused the data plane to crash

Component/s	SNMP
Issue	SCG-102510
Description	Resolved an issue where WLAN count seen in *ruckusWLANSSID* and *ruckusSCGCONFIGWLANSSID* MIBs count do not match

Component/s	System
Issue	ER-6002
Description	Resolved an issue where the controller may be unresponsive or very slow under very high load of new WISPr users

Component/s	System
Issue	ER-6136, ER-6996
Description	Resolved an issue where cache memory occupied considerable space on the system, which resulted in performance issues

Component/s	System
Issue	ER-6994
Description	Resolved an issue where due to Captive Portal memory leak the login window failed to pop-up automatically for WISPr-based WLANs

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

Component/s	System
Issue	ER-6712
Description	Resolved an issue where client session expiration happened constantly before configured session timeout

Component/s	System
Issue	ER-6101
Description	Resolved an issue where nodes showed high memory utilization

Component/s	System, Control Plane
Issue	ER-6148, ER-6208
Description	Resolved an issue where client authentication failed

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

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

Component/s	System
Issue	ER-6451
Description	Added exponential back-off behavior to AP2AP communication process when the process initially starts and cannot establish the communication channel

Component/s	System
Issue	ER-6414
Description	Resolved an issue where the client fingerprint did not work properly on a client running with Window 10 version 1803 client

Component/s	System
Issue	ER-6989
Description	Resolved an issue where the subnet registration rule failed

Component/s	Virtual SmartZone
Issue	SCG-102162
Description	Resolved an issue where an error on the user interface **Monitor > System** page, prevented the events and alarms from being populated

Component/s	Virtual SmartZone
Issue	ER-5677
Description	Resolved an issue where Radius messages were not forwarded to AAA server

Component/s	Virtual SmartZone
Issue	ER-6839
Description	Resolved an issue where the default setting search was based on empty AP MAC criteria in Events page on the controller user interface

Component/s	Virtual SmartZone
Issue	ER-6516
Description	Resolved an issue where WISPr WLAN using ZD-style redirection for user authentication was failing

Component/s	Virtual SmartZone
Issue	ER-5302
Description	Resolved an issue where a user was unable to log on to a hotspot if the user's password contained the ampersand sign

Component/s	Virtual SmartZone
Issue	ER-5924
Description	Resolved an issue where Radius process core dumps when the client tries to authenticate against AD server because of the length of the user group associated with the user

Component/s	Virtual SmartZone 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

Security Considerations

Following are the security fixes for this release.

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

Upgrading to This Release

Upgrading to This Release

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 corresponding Administrator Guide for your controller platform.

NOTE
Before uploading a new AP patch, Ruckus strongly recommends that you save a cluster backup, in case you want to restore the previous AP patch.

NOTE
Before upgrading the controller, Ruckus 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.

NOTE

In pre-3.2 releases, AP firmware download from the controller is performed over an HTTP connection on port 91 in the clear.

In release 3.2, the controller uses an HTTPS connection and an encrypted path for the firmware downloads. The port used for AP firmware downloads was also changed from port 91 to 11443 to distinguish between the two methods.

In release 3.4, the controller uses port 443 for AP firmware downloads. To ensure that all APs can be upgraded successfully to release 3.4, open ports 443, 11443 (for cluster restore to release 3.2), and 91 in the network firewall.

Using the "Extend Upload Precheck Timeout" Script

Whenever you upload an upgrade image to the controller, the controller starts a timer to monitor the status of the upload process at set intervals. If the upload process is not completed within 10 minutes, the controller terminates the upload process and aborts the upgrade attempt.

In release 3.2.1, Ruckus introduced a data migration precheck process that must be completed before the upgrade process can start. When you upload an upgrade image, the controller will first check the database for issues before it starts the upgrade process. This new pre-check increases the duration of the image upload process and could potentially cause the upload timer to time out and the upgrade attempt to fail.

To ensure that the upload timer does not time out, apply the extend upload precheck timeout KSP (script file).

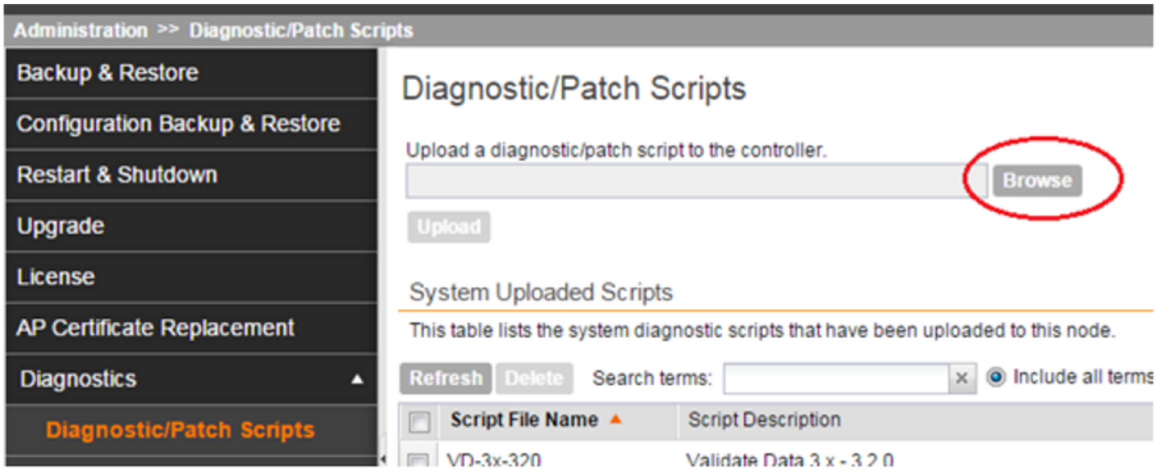
NOTE

Apply the KSP before you upload the upgrade image file.

NOTE

The precheck process requires at least 2GB of available system memory to proceed with the upgrade. If the system has less than 2GB of available system memory, the precheck process will abort the upgrade attempt.

1. Download the KSP file from the Support website to your computer. The file name is *extendPrecheckTimeout_0.ksp*.
2. Log on to the controller, and then go to **Administration** > **Diagnostics** > **Diagnostic/Patch Scripts**.
3. Click **Browse**, and select the KSP file that you downloaded.

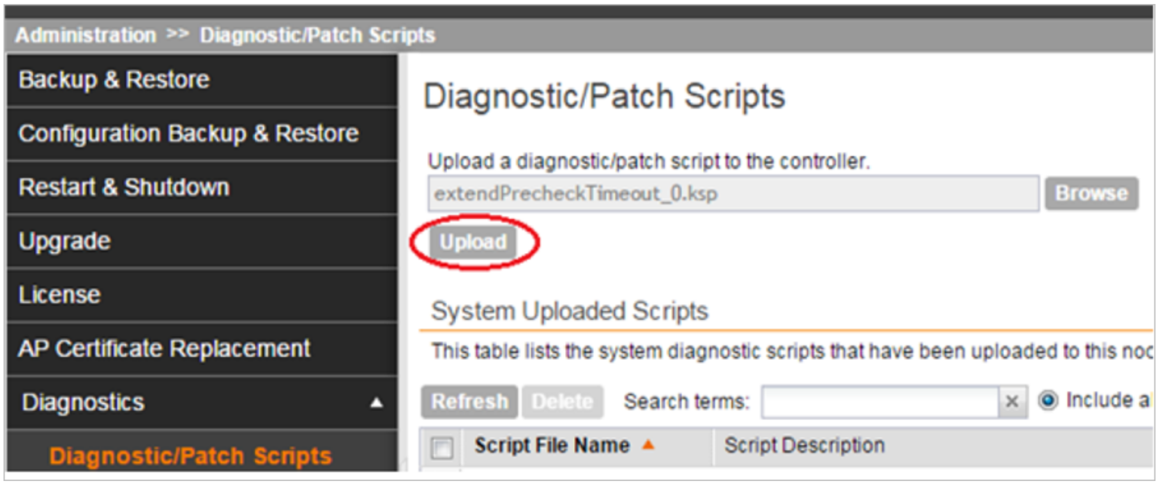


Upload a diagnostic/patch script to the controller.

This table lists the system diagnostic scripts that have been uploaded to this node.

	Script File Name	Script Description
□	VD-3x-320	Validate Data 3 x - 3 2 0

4. Click *Upload*.



Diagnostic/Patch Scripts

Upload a diagnostic/patch script to the controller.

extendPrecheckTimeout_0.ksp

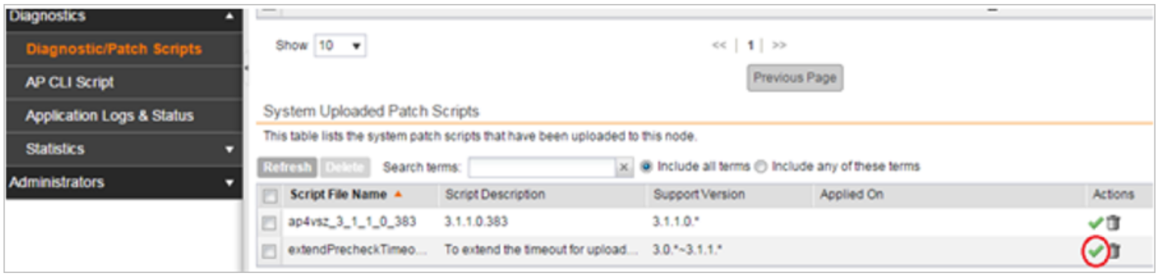
System Uploaded Scripts

This table lists the system diagnostic scripts that have been uploaded to this noc

Search terms:

□	Script File Name	Script Description

5. When the KSP file appears on the list of available scripts, click the green check mark under the Actions column.



System Uploaded Patch Scripts

This table lists the system patch scripts that have been uploaded to this node.

Search terms:

□	Script File Name	Script Description	Support Version	Applied On	Actions
□	ap4vsz_3_1_1_0_383	3.1.1.0.383	3.1.1.0.*		✓
□	extendPrecheckTimeo...	To extend the timeout for upload...	3.0.*~3.1.1.*		✓

After the KSP script is applied, upload the upgrade image file, and then upgrade the controller to this release.

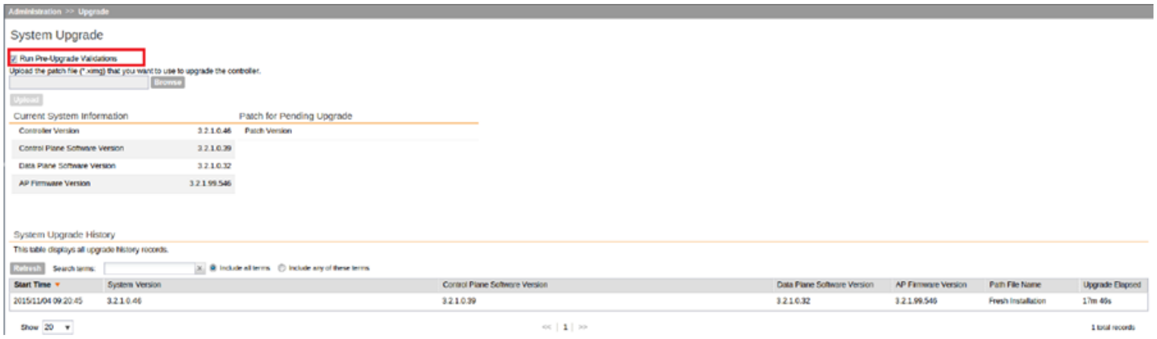
Performing Preupgrade Validation

Another enhancement to the upgrade process that added in this release is preupgrade validation.

Preupgrade validation automatically runs if you are upgrading from release 3.2 or earlier. However, if you are upgrading from an earlier 3.2.1 release, you need to manually enable preupgrade validation by going to **Administration** > **Upgrade**, and then selecting the **Run Pre-Upgrade Validations** check box.

Preupgrade validation checks for data migration errors before performing the upgrade. If data migration was unsuccessful, this error message is displayed: *Exception occurred during the validation of data migration. Please apply the system configuration backup and contact system administrator.* If this occurs, take a backup of the system configuration and contact Ruckus support to resolve the issue.

To access the logs of the validation process, log on to the web interface, and then navigate to **Administration** > **Diagnostics** > **Application Logs** > **Datamanager** > **datamanager.log**.



Administration >> Upgrade

System Upgrade

☑ Run Pre-Upgrade Validations

Upload the patch file (*.ximg) that you want to use to upgrade the controller.

Current System Information

Controller Version	3.2.1.0.46
Control Plane Software Version	3.2.1.0.39
Data Plane Software Version	3.2.1.0.32
AP Firmware Version	3.2.1.99.546

Patch for Pending Upgrade

Patch Version

System Upgrade History

This table displays all upgrade history records.

Start Time ▾	System Version	Control Plane Software Version	Data Plane Software Version	AP Firmware Version	Path File Name	Upgrade Elapsed
2015/11/04 09:20:45	3.2.1.0.46	3.2.1.0.39	3.2.1.0.32	3.2.1.99.546	Fresh Installation	17m 46s

1 total records

NOTE

If data migration validation fails due to insufficient memory, the following error message appears: *Insufficient memory. The system requires at least 2 GB of available memory to complete data validation*. Therefore, it recommends the following:

- If you are upgrading a physical controller, restart the controller to free up memory.
- If you are upgrading a virtual controller, allocate additional memory to the virtual machine, and then restart the virtual machine instance.
- Alternatively, clear the check box above to upgrade the controller to the new release without completing data validation.

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 2 Previous release builds that can be upgraded to this release

Platform	Release Build	Release Build
SCG200 SZ100 vSZ (vSCG) vSZ-D	3.1.0.0.236	3.2.1.0.134
	3.1.0.0.249	3.2.1.0.139
	3.1.1.0.442	3.2.1.0.163
	3.1.1.0.450	3.2.1.0.193
	3.1.1.0.474	3.2.1.0.217
	3.1.1.0.476	3.2.1.0.245
	3.1.2.0.95	3.2.1.0.247
	3.1.2.0.513	3.2.1.0.253
	3.1.2.0.520	3.4.0.0.659
	3.1.2.0.536	3.4.0.0.745
	3.1.2.0.1015	3.4.1.0.208
	3.4.0.0.976	3.4.2.0.169
	3.4.2.0.152	3.4.2.0.176
	3.2.0.0.790	3.4.2.0.217

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 3 Issues and workarounds for upgrading the SZ100 with EoL APs

Release	Issue Workaround	Version
3.1, 3.1.1	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 following is an example of the warning message: Your current system cannot be upgraded. Reason: The system cannot be upgraded, because the following AP model(s) will be unsupported: ZF7343 * 1" Despite this limitation, the Upgrade and Backup & Upgrade buttons remain visible and clickable, which seem to indicate that the controller can still be upgraded. However, when you click Upgrade or Backup & Upgrade, the upgrade attempt fails because of the unsupported APs.	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 support for more information.
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 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 4 Issues and workarounds for upgrading the SCG200 with EoL APs

Release	Issue Workaround	Version
3.1, 3.1.1	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 following is an example of the warning message: Your current system cannot be upgraded. Reason: The system cannot be upgraded, because the following AP model(s) will be unsupported: ZF7343 * 1" The following is an example of the warning message: Your current system cannot be upgraded. Reason: The system cannot be upgraded, because the following zone(s) will be unsupported: v1.1.2.0.93 * Despite this limitation, the Upgrade and Backup & Upgrade buttons remain visible and clickable, which seem to indicate that the controller can still be upgraded. However, when you click Upgrade or Backup & Upgrade, the upgrade attempt fails because of the unsupported APs.	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 support for more information.
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 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.

In the current release and earlier releases, when the SCG200 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. In contrast, the SZ100 and vSZ-E automatically upgrade both the controller firmware and AP firmware when the system is upgraded.

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 3.1.

The following releases can be upgraded to release 3.4.x:

- 3.2
- 3.2.x
- 3.1.x
- 3.1

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 3.2, then the AP firmware releases that it will retain after the upgrade will be 3.4 and 3.2
- If you are upgrading the SCG200 from release 3.1, then the AP firmware releases that it will retain after the upgrade will be 3.4 and 3.2 and 3.1.

All other AP firmware releases that were previously available on the SCG200 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 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.

Compatibility with 64MB APs

Ruckus APs with 64MB memory have reached end-of-life (EoL) status and are no longer supported in this and later releases. If you have 64MB APs that are being managed by the controller and you want to keep using these APs to provide Wi-Fi services to users, ensure that these APs belong to zones running release 3.1.x or earlier.

TABLE 5 To continue managing 64MB APs, they must belong to zones running release 3.1.x or earlier

Release	Compatible Release as a 64MB AP Support Zone	64MB AP Support
3.4	• 3.1 • 3.1.x • 3.2 • 3.2.x	64MB APs must belong to a zone running release 3.1.x or earlier.

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, 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

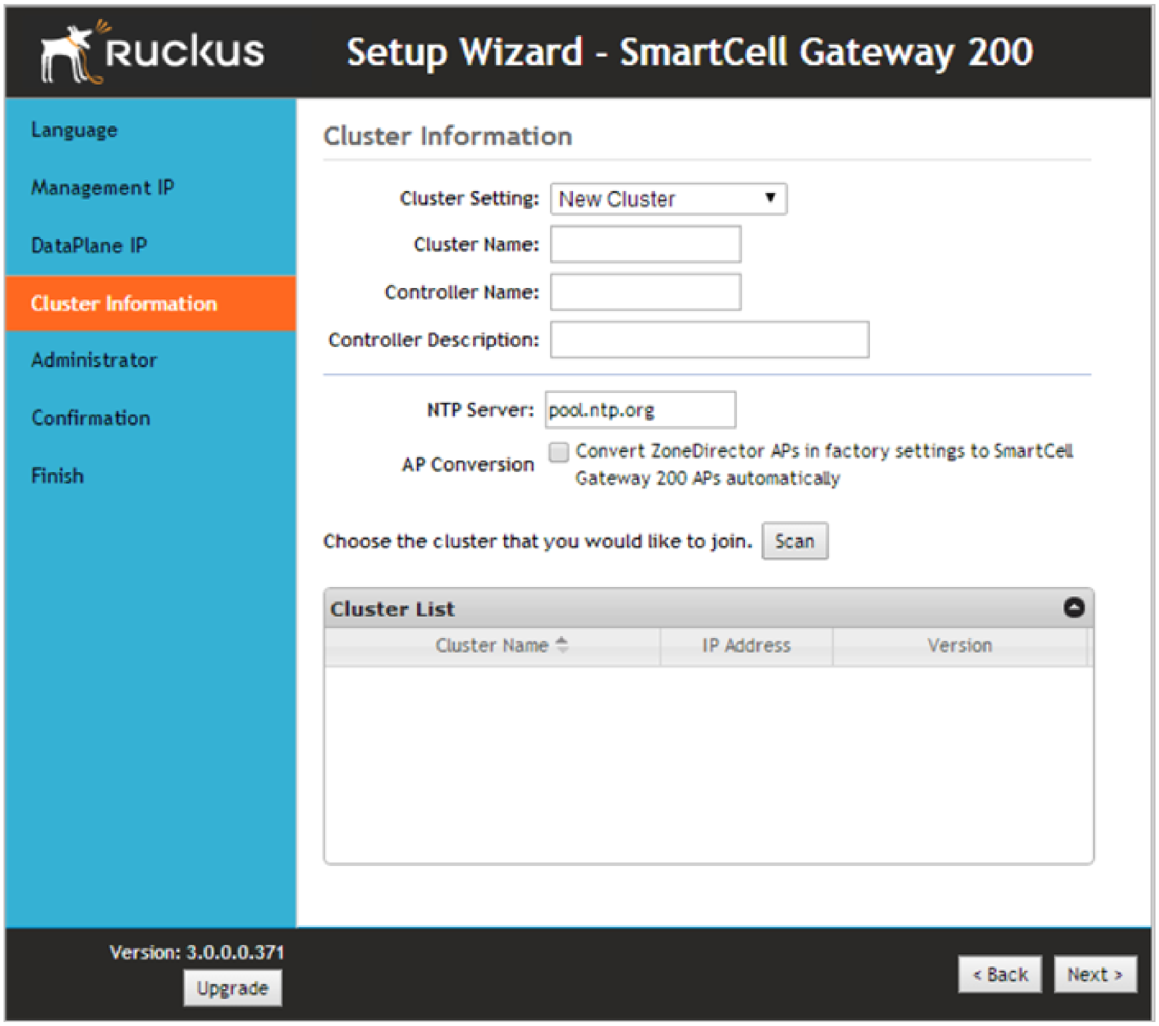
The information in this section applies to standalone ZoneFlex APs (those that are not managed by ZoneDirector), in factory default configuration, to the SCG- 200/SZ-100/vSZ.

Follow these steps to convert standalone ZoneFlex APs to the SCG-200/SZ-100/ vSZ firmware so that they can be managed by the SCG-200, SZ-100, or vSZ.

1. When you run the SCG-200, SZ-100, or vSZ 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



Setup Wizard - SmartCell Gateway 200

Cluster Information

Cluster Setting: New Cluster
Cluster Name:
Controller Name:
Controller Description:

NTP Server: pool.ntp.org
AP Conversion □ Convert ZoneDirector APs in factory settings to SmartCell Gateway 200 APs automatically

Choose the cluster that you would like to join.

Cluster List

Cluster Name	IP Address	Version

Version: 3.0.0.0.371

2. After you complete the Setup Wizard, connect the APs to the same subnet as the SCG-200/SZ-100/vSZ.

   When the APs are connected to the same subnet, they will detect the SCG-200/ SZ-100/vSZ on the network, and then they will download and install the AP firmware from SCG-200/SZ-100/vSZ. After the SCG-200/SZ-100 firmware is installed on the APs, the APs will automatically become managed by the SCG-200/SZ-100/vSZ 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 qualifies its functionality on the most common clients.

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