

Ruckus SmartZone Release Notes

Supporting SmartZone Release 3.6.1

© 2018 ARRIS Enterprises LLC. All rights reserved.

ARRIS, the ARRIS logo, Ruckus, Ruckus Wireless, the Ruckus logo, and the Big Dog design are trademarks of ARRIS International plc and/or its affiliates. All other trademarks are the property of their respective owners.

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

ARRIS provides this content without warranty of any kind, implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. ARRIS may make improvements or changes in the products or services described in this content at any time. The capabilities, system requirements and/or compatibility with third-party products described herein are subject to change without notice.

Contents

New and Changed Features.....	4
New and Changed Features.....	4
Changed Features.....	5
Hardware/Software Compatibility and Supported AP Models.....	6
Overview.....	6
Release Information.....	7
Supported and Unsupported Access Point Models.....	8
Caveats, Limitations, and Known Issues.....	9
AP Known Issues.....	9
Control Domain Known Issues.....	10
System Known Issues.....	10
Virtual SmartZone Data Plane.....	10
Resolved Issues.....	10
AAA Resolved Issues.....	10
AP Resolved Issues.....	10
AVC Resolved Issues.....	11
Bonjour Gateway Resolved Issues.....	11
Control Domain Resolved Issues.....	12
SCI Resolved Issues.....	12
System Resolved Issues.....	12
Virtual SmartZone.....	12
WISPr Resolved Issues.....	12
Upgrading to This Release.....	13
Overview.....	13
Virtual SmartZone Recommended Resources.....	13
SmartZone Upgrade Paths.....	14
Multiple AP Firmware Support.....	15
EoL APs and APs Running Unsupported Firmware Behavior.....	16
Interoperability Information.....	17
AP Interoperability.....	17
Redeploying ZoneFlex APs with SmartZone Controllers.....	17
Converting Standalone APs to SmartZone.....	18
ZoneDirector Controller and SmartZone Controller Compatibility.....	18
Client Interoperability.....	18
BSD Clause.....	19
BSD 3-Clause for New and Revised Licenses for URL Filtering.....	19
BSD License Compliance for SimpleCaptcha.....	19

New and Changed Features

New and Changed Features

This section provides a high-level overview of several key features that are introduced in the SmartZone (SZ) software release 3.6.1. For detailed descriptions of these features and configuration help, refer to the respective 3.6.1 documentation guides.

The SZ release 3.6.1 is applicable to the Ruckus SmartZone 300, SmartCell Gateway 200, SmartZone 100, vSZ-H, and vSZ-E controller platforms. For additional details, do refer to the SmartZone Controller Documentation Suite for Release 3.6.1.

Admin Account Security Controls

In this release, the administrative accounts have been enhanced with additional (optional) security controls. Specifically, there are four new enhancements to security, which can be applied to an administrative group as a profile:

1. **Account Lockout:** When an administrator fails authentication multiple consecutive times, the account will become locked for a defined period of time. Both the number of consecutive failures and the duration of the lockout are configurable. If necessary, a super admin can also manually unlock a locked account.
2. **Password Expiration:** Administrative passwords can be configured for expiration after a predefined duration. The system will force the admin to change his/her account password after the password has expired.
3. **Password Reuse:** Administrative passwords can now be controlled to avoid reuse of the same password. Administrators can control the number of unique passwords required before reuse.
4. **CAPTCHA:** To avoid login attacks on the SmartZone system by bots or other malicious programs, a CAPTCHA service is also added. CAPTCHA provides a way to validate that the user is in fact a person. CAPTCHA is a global service, which means it is either enabled or disabled globally for all users of the system.

Airtime Detail Display

In the AP health page, a new display component has been added to view airtime utilization details.

NOTE

This is in beta phase.

The airtime detail display allows the administrator to view components of airtime utilization, such as the amount of unicast vs broadcast traffic for transmit or receive functions, or the amount of management or data traffic being transmitted. These additional details can be helpful for deeper troubleshooting and awareness of airtime consumption.

vSZ vCenter Management Enhancement

Some of Ruckus customers have VMware ESX6.5 managed by vCenter. The existing vSZ *.ova* files can not be installed on the ESX6.5 hosts via vCenter, nor can they be installed when using direct interface with the ESX host. The error generated in both cases is the same, *Invalid manifest entry*.

It appears that the free version ESXi6.5 may not enforce the same *.ova* file requirements that fully licenses ESX6.5 does because some customers can install 3.2.1, 3.4 and 3.5 on the free version of ESXi6.5, but when using the exact same *.ova* files from the Ruckus support site on the fully licensed ESX6.5 host via vCenter the install fails on the 3rd step with *Invalid manifest entry*.

So, this delivery is to address that issue and make *.ova* files available for installations on fully licensed ESX6.5 managed by vCenter.

Ability to Disable AP Ethernet Ports

The SmartZone now allows the administrator to disable all AP ports, as desired.

In the past, some ports (notably, the uplink port - the PoE-In port, which is commonly used for network connectivity) could not be disabled by an administrator. This change now allows all the ports to be disabled, which may be helpful in mesh environments where the network administrator wants to prevent users from plugging devices into AP ports, which could impact mesh connectivity.

AAA Affinity and Gateway Failover

Some of Ruckus customer deployments have AAA and Gateway at one site and a second AAA and Gateway at another site. When connection to one site fails, AP needs to failover (both AAA and Gateway connections) simultaneously to the second site.

Therefore, in this release, an option is added to allow each AP to disconnect its authenticated or attached users and failover to second gateway and AAA server in the case the first gateway or AAA server is unreachable. So, instead of a cluster-wide AP failover to the second site, each AP decides if it needs to failover.

When an AP's data plane fails, that AP will disconnect its control plane and fail AAA to the backup AAA and connects data plane to the backup gateway. When an AP's control plane fails, the AP will disconnect all its clients and re-establish control and data plane connects to backup AAA and gateway. In this case, all UEs will need to attach or authenticate again and new sessions will be created on the second gateway.

Client Count Drop Monitoring

The feature is to compare the current maximum client count (for example, 2000 clients at 10:00) with previous data (for example, 1500 clients at 09:00) in *client count summary*. The following arguments are supported:

1. **Comparing Period:** You can configure the initial minimum client count. You need to have at least that number of clients for this feature to kick in.
2. **Declination Rate:** The threshold at which an alarm will be generated if the declination rate is too high.
3. **GUI Notification:** GUI to inform user the event in #2 is checked.

AP Support

The following AP models have been added for support on the 3.6.1 release:

1. T811 native support
2. E510 native support - When a Ruckus antenna (Product Number: 902-2101-0000) with Beamflex is connected, users should *disable* the "external" antenna setting in the AP/AP group configuration. When a third-party antenna (Non Ruckus) is used, users should *enable* the external antenna check boxes and configure gain values according to calculated cable loss, etc.
3. T310 native support

Changed Features

AP Behavior Change

- The AP E510 will be automatically rebooted when external antenna gain setting is modified. [SCG-78247]
- The AP E510 requires a manual **reboot** when switching between internal/external antenna. [SCG-81588]

System Behavior Change

- Ruckus recommends that customers should not leave Debug log levels on for longer period of time. A similar message is now displayed in Web UI. [SCG-77525]
- From this release 3.6.1, support for a new country code setting for Russia is added (Russia_Low_Power), using a low-power RF output mode for low-range applications. [FR-2869]
- Added support for C-band (5725-5850 MHz) in several European country codes:
 - **UK country code:** Supported by default in indoor and outdoor APs (with limited power output). Added an option to enable full power in outdoor APs if licensed.
 - **Germany and Spain country codes:** Option to enable it for outdoor APs. [SCG-70675]
- **New ARC Signature Package:** [SCG-78016 SCG-82138] This release includes the same ARC signature package as release 3.6 (version 1.074). Along with 3.6.1, an updated ARC signature package (version 1.092) is published in support website to improve the scope of applications detected by the application inspection engine. This new package includes the following differences compared with the one available in previous release:
 - **Added applications:** Naver Cloud, CinemaNow/FilmOn, FilmOn, SMB2, Microsoft Office, Skype for Business, Microsoft Office 365
 - **Removed applications** (this needs to be deleted from Application Policy before uploading the new package): Naver Ndrive, Adobe Flash, CinemaNow, Friendfeed

Signature package from earlier release will be kept to maintain backward compatibility in the application rules defined. If the new package is required, it can be downloaded from Support website and uploaded into the controller in **Services & Profiles > Application Control > Signature Package** (more details can be found in Administrator Guide, in section **Importing an Application Signature Package**).

NOTE

The ARC feature was introduced in 3.5, therefore the 3.6.1 package will be used when upgrading the controller from 3.4.x.

Hardware/Software Compatibility and Supported AP Models

Overview

This section provides release information about the SmartZone 300 (SZ300), the SmartCell Gateway 200 (SCG200-C), the SmartZone 100 (SZ100), Virtual SmartZone (vSZ), and Virtual SmartZone Data Plane (vSZ-D) features with notes on known issues, caveats, and workarounds.

- The SZ300 Flagship Large Scale WLAN Controller is designed for Service Provider and Large Enterprises, which prefer to use appliances. The Carrier Grade platform supports N+1 Active/Active clustering, comprehensive integrated management functionality, high performance operations and flexibility to address many different implementation scenarios.
- The SCG200-C, developed for the service provider market, combines a WLAN access controller with Wi-Fi traffic aggregation, along with a built-in carrier-grade element management system in a 2U rack-mountable, all-in-one hardware form factor.
- The SZ100, developed for the enterprise market, is the next generation midrange, rack-mountable WLAN controller platform for the enterprise and service provider markets. There are two SZ100 models: the SZ104 and the SZ124.

- The vSZ, which is available in *High Scale* and *Essentials* versions, is a Network Functions Virtualization (NFV) based WLAN controller for service providers and enterprises that desire a carrier-class solution that runs in the cloud. It supports all of the WLAN controller features of the industry leading SCG200-C, while also enabling the rollout of highly scalable and resilient wireless LAN cloud services.
- The vSZ-D offers organizations more flexibility in deploying the SZ data plane as needed in an NFV architecture-aligned fashion. Deploying vSZ-D offers secured tunneling of user data traffic that encrypts payload traffic, maintains flat network topology, enables mobility across L2 subnets, supports POS data traffic for PCI compliance, and offers differentiated per site policy control and QoS, etc.

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.

SZ300

- Controller Version: **3.6.1.0.227**
- Control Plane Software Version: **3.6.1.0.164**
- Data Plane Software Version: **3.6.1.0.227**
- AP Firmware Version: **3.6.1.0.354**

SCG200-C

- Controller Version: **3.6.1.0.227**
- Control Plane Software Version: **3.6.1.0.164**
- AP Firmware Version: **3.6.1.0.354**

SZ100

- Controller Version: **3.6.1.0.227**
- Control Plane Software Version: **3.6.1.0.164**
- Data Plane Software Version: **3.6.1.0.40**
- AP Firmware Version: **3.6.1.0.354**

SZ100-D

- Data Plane Software Version: **3.6.1.0.227**

vSZ-H and vSZ-E

- Controller Version: **3.6.1.0.227**
- Control Plane Software Version: **3.6.1.0.164**
- AP Firmware Version: **3.6.1.0.354**

vSZ-D

- vSZ-D software version: **3.6.1.0.227**

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 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 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	T310C	C500	T301N	ZF7372-E	ZF7782-S
H510	T310S	H500	T301S	ZF7352	ZF7781CM
C110	T310N	R310	FZM300	ZF7055	
H320	T310D	R500E	FZP300		
	T811CM				
	T610S				
	E510				

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

NOTE

When the R720, R710, T610 series AP is connected to an 802.3af PoE power source, the USB interface and the second Ethernet port are disabled, and the AP radios do not operate in maximum capacity. For more information, refer to the latest Outdoor Access Point User Guide or Indoor Access Point User Guide.

Unsupported AP Models

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

TABLE 2 Unsupported AP Models

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

Caveats, Limitations, and Known Issues

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

NOTE

The caveats stated in 3.6 release notes are also applicable to this release.

AP Known Issues

The following are the known issues related to APs.

- If a zone that has been added to a report is deleted, the corresponding report will fail to be completed because the zone is missing. **[SCG-76181]**
- AP model ZF-7372 (128 MB RAM) should not be used in high density environment. **[AP-7201]**
- NAT IP and port configuration is only used by AP, therefore when it is configured by the controller, this configuration does not move it to the data plane. Data plane always reports the NAT information, which is configured through virtual data plane CLI. **[SCG-76345]**
- SNMPv1 gets enabled on the AP when enabling SNMPv2. **[SCG-77981]**
- AVC does not work properly when user defined AVC is created but it is not associated with any UTP profile. **[SCG-80218]**
- AP page configuration incorrectly allows administrators to change mesh mode when DHCP-NAT is enabled. **[SCG-79713]**
- After moving an AP from IPv6 to IPv4 zone, the external IP address in controller web interface still shows the IP address as IPv6 address. **[SCG-81469]**
- Session termination cause in Accounting Stop packet is incorrect when the client is disconnected using Block operation. **[SCG-76876]**
- After creating an Ethernet profile for an Ethernet port and adding VLAN tag, the Ethernet profile is not available for AP T811 Lan3 and Lan4 Ethernet ports. The created profile is available for other APs. **[SCG-77639]**

Workaround: Logon to vSZ CLI and run the below command. To verify, navigate to vSZ web interface to view the created profile.

```
ruckus> enable
ruckus# config
ruckus(config)# eth-port-validate-one-trunk disable
```

- AP TxPower does not revert to default values after applying external antenna gain and switching back to internal Ruckus antenna. **[SCG-81705]**

Workaround:

Resolved Issues

Control Domain Known Issues

Option 1: For 2.4 GHz set the dbi as 3 and for 5 GHz set the dbi as 5, apply the configuration and disable the external antenna.

Option 2: Use the set factory option for the AP.

Control Domain Known Issues

The following are the known issues related to control domain.

- Modified preference session time out setting does not get updated on the vSZ-H controller. [SCG-81141]
- Unable to move the AP to same the Zone AP Group when DHCP/NAT is enabled. [SCG-81356]

System Known Issues

The following are the known issues related to the system.

- The search text allows users to search text from the beginning of the string. For example, if the string is *RuckusWireless*, you should search for *Ruckus* instead of *Wireless*. [SCG-76950]
- Special characters are used as tokenizers for indexed texts in the system, and, when performing a search, special characters are used to separate search terms into smaller segments before performing a search. Therefore search terms with special characters are not supported and is ignored. [SCG-76953]
- The controller does not check if IPv6 static routes added are valid. [SCG-81432]
- Schedule backup does not work on restoring configuration. [SCG-82275]

Workaround: Reload the scheduler or all services.

Virtual SmartZone Data Plane

The following are the known issues related to Virtual SmartZone Data Plane.

- If a client connects to a WLAN that uses Radius profile based DHCP/NAT service, Web UI UE entry will report VLAN where NAT IP address belongs instead of the private one assigned by Radius server. [SCG-72776]
- When VLAN tag is enabled with access/core separation, static route cannot be persisted after rebooting. This is a configuration limitation for vSZ-D and SZ300 internal data plane. [SCG-82367 ER-6160]

Resolved Issues

AAA Resolved Issues

The following are the resolved issues related to AAA resolved issues.

- Resolved an issue where Radius Accounting packets had in some roaming scenarios the MAC address in the user name attribute. [ER-5623]

AP Resolved Issues

The following are the resolved issues related to AP.

- Resolved an issue where Calea mirroring failed when the packet size was more than 1440 and the option *dont fragment* was set. [AP-4034]

- Resolved an issue where if the network connectivity between primary and secondary APs running DHCP service was not correct, upon recovery of primary AP, DHCP service failed for several minutes. [SCG-76056]
- Resolved an issue where different APs generated the same Acct-session-id value in Radius Accounting traffic for two clients. [SCG-76210 ER-5806]
- Resolved an interoperability issue where Aeroscout tag feature didn't work properly on H510/R510/R710 APs. [ER-5191]
- Resolved an issue where 802.11r AP keys were not shared with all second hop APs. [ER-5405]
- Modified log severity for some events starting with *user.warn kernel: FWLOG* from Error to Warning . [ER-5277]
- Resolved an issue where AP T300 was sending flow control packets with its reversed MAC address during bootup. [ER-5598]
- Resolved an issue where when setting up AP 7352 in mesh the AP was configured but the mesh was not formed. [ER-5706]
- Resolved an issue where the SNMP ID of WLAN interface changed after AP reboot or failover. [ER-5718]
- Resolved an issue where when configuring the SNMP settings in the AP Zone using CLI, the auto-complete function shows incorrect values by listing commands that are not related to AP SNMP settings. [ER-5771]
- Resolved an issue where the AP failed to update the configuration when a new WLAN profile with WEP encryption was configured and moved to the WLAN Group. [ER-5795]
- Resolved an issue where the AP was unable to move between two mesh enabled zones which had the identical configurations. [ER-5816]
- Resolved an issue where AP name did not change via Public API when the AP was offline. [ER-5837]
- Resolved an issue where the signal levels of the mesh AP's was not seen. [ER-5862]
- Resolved an issue where AP sent packets back in RGRE tunnel from non-authorized client. [ER-5949]
- Resolved an issue where clients could not connect properly when AP was assigned to AP Group with 32 character length. [ER-5980]
- Resolved an issue where large TCP packets were not handled correctly in R710/R610 due to incorrect MSS negotiation. [ER-6003]
- Resolved an issue where controller public API was not accepting Cyrillic characters for AP description and location fields. [ER-5747]
- Resolved an issue where APs using SoftGRE over IPv6 went into a GRE inactive state and closed their SSIDs. [ER-6008]
- Improved user traffic performance when AP DHCP/NAT feature is used in all APs that support this feature. [SCG-71968]
- Resolved an issue where the Ethernet profile was not available for T811 Lan3 and Lan4 Ethernet ports. [SCG-76639]
- Resolved an issue where R710 did not report the correct number of active clients via SNMP. [ER-5893]

AVC Resolved Issues

The following are the resolved issues related to AVC

- Resolved an issue where AVC identified YouTube as googlevideo.com. [SCG-61150]

Bonjour Gateway Resolved Issues

The following are the resolved issues related to Bonjour Gateway.

- Resolved an issue where Bonjour Gateway was not working when the Apple TV and MacBook Air are in two different VLAN's on the same WLAN on the same AP. [SCG-73788]

Resolved Issues

Control Domain Resolved Issues

Control Domain Resolved Issues

The following are the resolved issues related to Control Domain.

- Resolved an issue where the AP local-subnet discovery did not work properly in the default-enabled state due to the data plane design limitation. This only affected SZ100 controller in port group 1. [SCG-75012 ER-5565]
- Resolved an issue where disabling of *ap-control-mgmt-tos* option did not work. [SCG-74695]
- Resolved an issue where cluster backup was not visible on the web interface or in CLI even after it is was successfully copied from the FTP server only if both backups shared the same timestamp and version. [SCG-74488]
- Resolved an issue where the DPSK failed to work after upgrade under certain conditions where the controller was upgraded to 3.6 (but not the zone), zone configuration using DPSK was modified, and finally the zone was upgraded to 3.6. [SCG-73628]
- Resolved an issue in SZ300 where DHCP relay functionality on the data plane did not generate the corresponding events for no response of failover. [ER-5750]
- Resolved an issue where the overwrite of VLAN option *Untag id* was not being saved on the AP configuration page. [SCG-81439]

SCI Resolved Issues

The following are the resolved issues related to SCI.

- Resolved an issue where APs were reporting incorrect negative SNR values to SCI. [ER-4795]

System Resolved Issues

- Resolved an issue where if you were restoring a backup configuration which includes more than 100 indoor maps you were not redirected automatically to the login page. [SCG-74911]
- Resolved an issue where the controller SZ100 was not able to display the IPv6 gateway on the control interface. [SCG-72261]
- Resolved an issue where Report results page was showing the same reports in all pages. [ER-5914]
- Resolved an issue in SZ300 where power supply alarms were not raised. [ER-5916]
- Resolved an issue where clients were unable to view generated guest passes when logged in as Guest pass administrator. [ER-5960]
- Resolved an issue where AP registration rules for IP range was not working properly. [ER-5578]

Virtual SmartZone

The following are the resolved issues related to Virtual SmartZone.

- Resolved an issue that could prevent WISPr clients to be successfully authorized in multi-node clusters. [ER-5767]
- Resolved an issue where a Wi-Fi client with extended ASCII characters in its hostname was unable to get an IP address if an OS Policy was applied to the WLAN. [ER-5912]
- Resolved an issue where vSZ-D suddenly restarted due to some malformed packets. [ER-5983]

WISPr Resolved Issues

- Resolved an issue where the zone template created with HS2.0 settings, WISPr WLAN and Radius accounting applied to create a new zone failed to work properly. [SCG-71137]

Upgrading to This Release

Overview

This section lists important information that you must be aware of when upgrading the controller to this release.

Step-by-step instructions for performing the upgrade are provided in the corresponding Administrator Guide for your controller platform.

NOTE

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

NOTE

Before upgrading the controller, Ruckus Networks strongly recommends that you back up the entire cluster. In case the upgrade fails, you can use the cluster backup to roll back the cluster to its previous state.

NOTE

When upgrading vSZ-E/vSZ-H, if the memory/CPU allocation of the current VM instance does not match the lowest resource level of the new VM instance to which the new vSZ-E/vSZ-H version will be installed, you will be unable to perform the upgrade. On the other hand, if the new VM instance has insufficient hard disk space, a warning message appears after you upload the upgrade image but you will still be able to perform the upgrade.

Virtual SmartZone Recommended Resources

Before upgrading vSZ to this release, verify that the virtual machine on which vSZ is installed has sufficient resources to handle the number of APs and wireless clients that you plan to manage. See the tables below for the virtual machine system resources that Ruckus recommends.

NOTE

These vSZ recommended resources may change from release to release. Before upgrading vSZ, always check the recommended resource tables for the release to which you are upgrading.

NOTE

It is recommended that there should be only one concurrent CLI connection per cluster when configuring vSZ.

TABLE 3 vSZ High Scale recommended resources

AP Count Range		Maximum 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 (per node not per cluster)	
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

TABLE 4 vSZ Essentials recommended resources

AP Count Range		Maximum 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 (per node not per cluster)	
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.

SmartZone Upgrade Paths

To help ensure that the cluster firmware upgrade process can be completed successfully, the cluster interfaces of all nodes must be connected and up.

Previous release builds that can be upgraded to SmartZone Controller version 3.6.1.

NOTE

SZ300 supports upgrade from 3.5 builds. 3.4 builds are not supported.

NOTE

Any reference in this document to the SCG200 actually refers to the SCG200-C. In the following table, we have referenced the SCG200-C.

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
	3.5.0.0.808
	3.5.0.0.832
	3.5.1.0.296
	3.5.1.0.862
	3.6.0.0.510

If you are running an earlier version, you must first upgrade to appropriate version for your model, as shown in the above list, before upgrading to this release.

Multiple AP Firmware Support

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 devices are referred to as controllers 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.x.

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.x, the AP Zone firmware remains the same.

Up to Three Previous Major AP Releases Supported

Every controller 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.

Upgrading to This Release

EoL APs and APs Running Unsupported Firmware Behavior

NOTE

A major release version refers to the first two digits of the release number. For example, 3.6 and 3.6.1 are considered part of the same major release version, which is 3.6.

The following releases can be upgraded to release 3.6.1:

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

The AP firmware releases that the controller will retain depend 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 3.6.1 and 3.5 (and 3.4 if this controller was previously in release 3.4)
- If you are upgrading the controller from release 3.4, then the AP firmware releases that it will retain after the upgrade will be 3.6.1 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 controllers handle APs that have reached End-of-Life (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 devices are referred to as controllers in this section.

NOTE

There are no EoL APs between SZ releases 3.2 to 3.6.1.

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 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.
- The EoL AP affects the upgrade only in the following conditions. Otherwise, the upgrade is successful.
 1. Upgrade must be prior to the SZ 3.5 release.
 2. This is applicable only 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, SZ100, 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 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, 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.

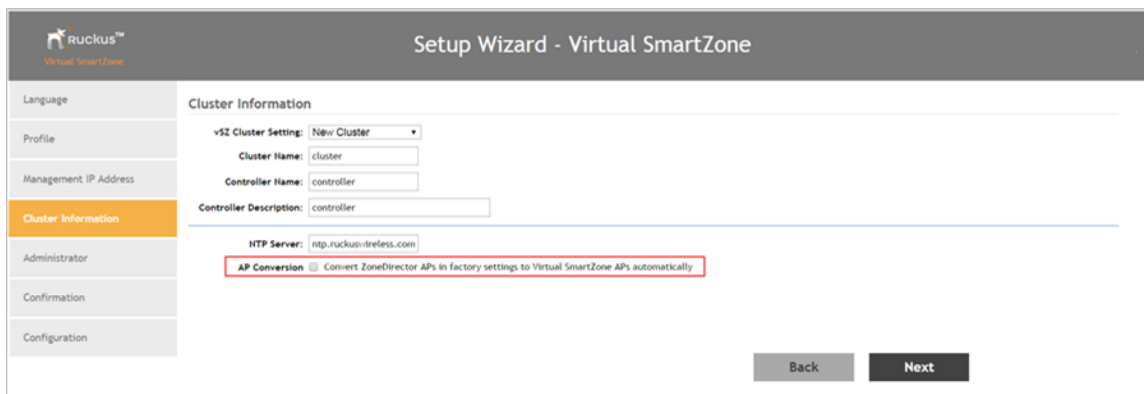
Follow these steps to convert standalone ZoneFlex APs to the SmartZone controller firmware so that they can be managed by the SZ300, SZ100, or vSZ

1. When you run the SmartZone Setup Wizard, select the **AP Conversion** check box on the **Cluster Information** page.

NOTE

The figure below shows the AP Conversion check box for the vSZ Setup Wizard. If you are setting up SZ300, or SZ100 the check box description may be slightly different.

FIGURE 1 Select the AP Conversion check box to convert standalone ZoneFlex APs to controller APs



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

- vSZ Cluster Setting: New Cluster (dropdown)
- Cluster Name: cluster
- Controller Name: controller
- Controller Description: controller
- NTP Server: ntp.ruckus-ireless.com
- AP Conversion: Convert ZoneDirector APs in factory settings to Virtual SmartZone APs automatically

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

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 qualifies its functionality on the most common clients.

BSD Clause

BSD 3-Clause for New and Revised Licenses for URL Filtering

A permissive license similar to the BSD 2-Clause License, but with a 3rd clause that prohibits others from using the name of the project or its contributors to promote derived products without written consent.

Copyright (c) 2005, Google Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

ATTENTION

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

BSD License Compliance for SimpleCaptcha

Copyright (c) 2008, James Childers

All rights reserved.

BSD License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of SimpleCaptcha nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

BSD Clause

BSD License Compliance for SimpleCaptcha

ATTENTION

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.



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