

Ruckus SmartZone 5.1.1 Release Notes

Supporting SmartZone 5.1.1

© 2019 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

Document History	4
New Features and Changed Behavior	4
New Features	4
Changed Behavior.....	7
Hardware/Software Compatibility, Supported AP Models and Switches	8
Overview.....	8
Release Information.....	8
Supported, Unsupported Access Point Models and Switch Management Support Matrix	9
Caveats, Limitations, and Known Issues in this Release	12
Resolved Issues	23
Upgrading to This Release	27
Before Upgrading to This Release	27
Virtual SmartZone Required Resources.....	29
Maximum Supported AP and Switch Management.....	31
SmartZone Upgrade Paths.....	32
Supported SmartZone and Data Plane Platform.....	32
Multiple AP Firmware Support in the SZ100/vSZ-E/SZ300/vSZ-H.....	33
EoL APs and APs Running Unsupported Firmware Behavior.....	34
Interoperability Information	35
AP Interoperability.....	35
Redeploying ZoneFlex APs with SmartZone Controllers.....	36
Converting Standalone APs to SmartZone.....	36
ZoneDirector Controller and SmartZone Controller Compatibility.....	36
Client Interoperability.....	37

Document History

Revision Number	Summary of changes	Publication date
A	Initial release notes	April 30, 2019
B	Refresh of 5.1.1 with: <ul style="list-style-type: none">• Release build numbers of SZ 598 and AP 624• Resolved issues:<ul style="list-style-type: none">- SCG-104659- SCG-104740	May 09, 2019

New Features and Changed Behavior

New Features

This section provides a high-level overview of several key features that are introduced in the SmartZone (SZ) software release 5.1.1

The SZ release 5.1.1 is applicable to the Ruckus SmartZone 300, SmartZone 100, vSZ-H, and vSZ-E controller platforms. For additional details, do refer to the SmartZone Controller Documentation Suite for Release 5.1.1.

NOTE

For detailed descriptions of these features and configuration help, refer to the respective 5.1.1 documentation guides available at <https://www.ruckuswireless.com>

Switch Management

SmartZone 5.1.1 adds support for Switch Configuration management (Switch Monitoring, Config Backup/restore, Firmware upgrade have been available since SmartZone 5.0)

- **Zero Touch Provisioning:** Greatly simplifies initial deployment of switches. Users can define switch configuration at a switch group level. Any brand new switch joining the group automatically gets provisioned.
- **Ongoing Configuration Changes:** Users can further modify the switch configuration as a part of network maintenance. This includes modifying switch group level settings, port settings as well as routing interfaces.
- **Stack formation:** Users can configure individual switches to be formed into a stack directly from SmartZone.
- **Configuration copy:** Users can copy configuration from a working switch to one or multiple new switches seamlessly.

Customized Radius VSA

This feature is designed to add agility in system to include new Radius VSA dynamically based on customer needs in the authentication and/or accounting messages. With this feature, the system supports specific VSAs the user wants on the fly instead of having the limitation to use only Ruckus defined VSAs.

Some highlights of this feature:

- Option to upload the new attributes specified by customer using input mechanism in csv format.
- UI provides a new profile, which will contain the attribute the user can configure. These fields are derived from the input provided by customer/user.

- AP will include these new attributes (VSAs) in Authentication and/or Accounting messages. Attributes to be included in Authentication or Accounting messages will be configurable in UI/CSV file

Data Plane (DP) Priority of Zone Affinity

In prior releases, Ruckus APs are assigned to DPs randomly and administrators connect to a specific DP. In this release, we introduced this DP zone affinity feature to allow administrators to create DP zone affinity profile when creating an AP zone. The administrator can prioritize the DPs in the DP zone affinity profile, so that when the APs are being added to the AP zone, they will look for the DP to connect to based on the priority listed in the DP zone affinity profile defined for that AP zone.

Configure Group

Name: Description:

Type: Domain Zone AP Group

Parent Group:

Configuration

[?] Historical Connection Failures: OFF

[?] DP Zone Affinity Profile:

OFF **Enforce the priority of Affinity Profile**
This action will disconnect the already established tunnels to vDPs and re-establish to new vDPs as per the priority defined.

SSH Tunnel Encryption: AES 128 AES 256

Mesh Options

OFF Enable mesh networking in this zone

Edit DP Zone Affinity Profile: [ZA1]

* Name:

Description:

Priority ▲	DP Name	Up
1	SZ100-D@00:1D:2E:45:10:01	
2	SZ124-D@00:1D:2E:55:66:01	
3	dhcp-10-206-80-18@00:0C:29:A0:46:CC	

Full URL Reporting on Customer Visits with GPB Streaming

URL Filtering feature lets the administrator manage internet usage by preventing access to inappropriate web sites. The websites to be blocked can be configured based on available categories with the feature.

Full URL reporting on customer visits with GPB streaming feature reports statistics to any listener of the GPB streaming (i.e. SCI) of all URL sessions of all clients connected to the AP every five minutes in GPB format with a limit of maximum 1024 URL statistics per five minutes interval and provides the session duration as well. Based on design, a web session is declared to have ended where there is inactivity for more than five minutes. The web session is declared to have started when AP first creates a flow entry.

Ruckus IoT Suite

The 5.1.1 release of Smart Zone integrates the Ruckus IoT Suite v1.2-MR1. A dedicated IoT branch will be available (SZ 5.1.1.2) with Ruckus IoT Suite v1.3-GA and is the recommended version for IoT deployments

The Ruckus IoT Suite offers a secure, scalable networking solution for enterprise IoT devices in combination with Ruckus Wi-Fi and Switch products. The IoT Suite is a collection of hardware and software infrastructure components used to create an IoT access network for a wide variety of IoT devices. A key benefit of the IoT Suite is that it leverages Ruckus Wi-Fi infrastructure and avoids expensive gateways, cabling and installation that may be needed for dedicated IoT networks.

Ruckus IoT Suite v1.2-MR1 key features and components supported in this release are listed below.

1. **IoT device/protocol support:** Bluetooth 5.0 (BLE) and ZigBee 3.0 enabled devices are supported in this release. Standard ZigBee HA Clusters, iBeacon and Eddystone BLE beacons are supported. Support for additional IoT protocols will be added in future releases of the IoT Suite.

2. **Ruckus IoT module:** I100, an IoT module (USB dongle form factor) that attaches securely to Ruckus IoT-ready Access Points, and internal IoT in the R730.
3. **Ruckus IoT-ready Access Points:** H510, R510, R610, R710, R720, R730, E510, T310, and T610
4. **Ruckus IoT Controller:** A virtual controller (SW only) deployed in tandem with Ruckus SmartZone Controller, that performs network layer device on-boarding, connectivity and security functions for IoT devices. The IoT Controller aggregates sensor data from various 3rd party sensors and provides APIs for northbound integration with IoT cloud services.

Additional details can be found at <https://www.ruckuswireless.com/products/iot> and at <https://support.ruckuswireless.com/>

Limitation: When using IoT with AP R730 and a I100 IoT module is connected to it, only one IoT radio, the one in the I100 IoT module, will be active. Re-enable the AP R730 internal IoT radio by disconnecting the I100 module. **[SCG-100868]**

Changed Behavior

Changed Behavior

The following are the changed behavior issues.

Adaptive Client Load Balancing for AP R730

Adaptive Client Load Balancing (ACLB) is not supported on AP R730 in this release. AP R730 supports only legacy Client Load Balancing (CLB). ACLB is disabled by default if *capacity mode* is configured on the controller and if *station mode* is configured, the ACLB acts as legacy CLB on the AP. **[SCG-97975]**

Control Public API

- From this release, attribute *dhcp82Format* is no longer supported. This is replaced with a new attribute *dhcp82SubOpt1Format SUBOPT1_AP_INFO*, which is a new function with a sub-option format. **[SCG-97486]**

Command Line Reference (CLI)

- The *curl* command is removed from enable, admin mode and moved to debug tools as a hidden command. **[ER-7011]**

Switch Management License

Switch management licences are now enforced from SmartZone release 5.1. If the customers upgrade to release 5.1, they will lose visibility of their switches if they do not add the required licenses to their controller.

NOTICE

Switches will continue to function normally, but will appear as *Offline* on the controller and will no longer be manageable through the controller.

Virtual SmartZone Data Plane

- Added an enhancement to send ICMP *packet too big* for PDU's (Protocol Data Unit) from core larger than tunnel MTU (Maximum Transmission Unit). **[ER-6641]**

Hardware/Software Compatibility, Supported AP Models and Switches

Overview

This section provides release information about the SmartZone 300 (SZ300), the SmartZone 100 (SZ100), Virtual SmartZone (vSZ), Virtual SmartZone Data Plane (vSZ-D) and SmartZone 100 - Data Plane (SZ 100-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 instances/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 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 the WLAN controller features of the industry, while also enabling the rollout of highly scalable and resilient wireless LAN cloud services.
- The vSZ-D is a Virtual Data Plane aggregation is a virtual instance that is managed by the vSZ that offers organizations more flexibility in deploying a NFV architecture-aligned architecture. Deploying vSZ-D offers secured tunneling of wireless client data traffic that encrypts payload traffic; POS data traffic for PCI compliance, voice applications while enabling flat network topology, mobility across L2 subnets and add-on services like L3 Roaming, Flexi-VPN, DHCP Server/NAT as well as CALEA/Lawful Intercept.
- The SZ100-D, is the Data Plane hardware appliance, which is functionally equal to the vSZ-D virtual data plane product. The appliance provides turnkey deployment capabilities for customers that need a hardware appliance. The SZ100-D is managed by a vSZ Controller only and cannot work in a standalone mode.

Release Information

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.

ATTENTION

It is strongly recommended to reboot the controller after restoring the configuration backup.

ATTENTION

VMware VMotion is not supported.

This SmartZone release is a Long Term (LT) release. This section lists the version of each component in this release.

SZ300

- Controller Version: **5.1.1.0.598**
- Control Plane Software Version: **5.1.1.0.405**
- Data Plane Software Version: **5.1.1.0.112**
- AP Firmware Version: **5.1.1.0.624**

SZ100

- Controller Version: **5.1.1.0.598**
- Control Plane Software Version: **5.1.1.0.405**
- Data Plane Software Version: **5.1.1.0.598**
- AP Firmware Version: **5.1.1.0.624**

vSZ-H and vSZ-E

- Controller Version: **5.1.1.0.598**
- Control Plane Software Version: **5.1.1.0.405**
- AP Firmware Version: **5.1.1.0.624**

vSZ-D

- vSZ-D software version: **5.1.1.0.598**

SZ Google Protobuf (GPB) Binding Class

Refer to the GPB MQTT Getting Started Guide and download the latest SmartZone (SZ) GPB .proto files from the Ruckus support site at: <https://support.ruckuswireless.com/documents/2501-smartzone-5-1-ga-getting-started-guide-on-gpb-mqtt-interface-sz100-sz300-vsZ>

Reference Documents

SZ100-D hardware appliance ships with a quick setup guide, which is tied to the SmartZone Release 5.1. In 5.1.1, SZ100-D is supported. Refer to the existing SZ100-D Quick Setup Guide by visiting the Ruckus website available at support.ruckuswireless.com.

Supported, Unsupported Access Point Models and Switch Management Support Matrix

Before upgrading to this release, check if the controller is currently managing AP models and Switch features that are no longer supported in this release.

APs preconfigured with the SmartZone AP firmware may be used with SZ300, SZ100, or vSZ in their native default configuration. APs factory-configured with the ZoneFlex-AP firmware may be used with the controller when LWAPP discovery services are enabled.

LWAPP2SCG must be disabled on controller if Solo AP's running 104.x being moved under SZ Management. To disable the LWAPP2SCG service on the controller, log on to the CLI, and then go to **enable > mode > config > lwapp2scg > policy deny-all**. Enter **Yes** to save your changes.

NOTE

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

Supported AP Models

This release supports the following Ruckus AP models.

TABLE 1 Supported AP Models

11ax	11ac-Wave2		11ac-Wave1	
Indoor	Indoor	Outdoor	Indoor	Outdoor
R730	R720	T710	R700	T504
R750	R710	T710S	R600	T300
	R610	T610	R500	T300E
	R510	T310C	R310	T301N
	H510	T310S	R500E	T301S
	C110	T310N		FZM300
	H320	T310D		FZP300
	M510	T811CM		
	R320	T610S		
		E510		

Important Note About the PoE Power Modes of the R730, 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.

Switch Management Feature Support Matrix

Following are the supported ICX models:

TABLE 2 Supported ICX Models

Supported ICX Models		
ICX 7150	ICX 7450	ICX 7750
ICX 7250	ICX 7650	ICX 7850

Following is the matrix for ICX and SZ release compatibility:

TABLE 3 ICX and SZ Release Compatibility Matrix

	SZ 5.0	SZ 5.1	SZ 5.1.1
FastIron 08.0.80	Y	Y	Y
FastIron 08.0.90a	N	N	Y

Following is the matrix for switch management feature compatibility:

TABLE 4 Switch Management Feature Compatibility Matrix

	SZ Release	ICX FastIron Release
Switch Registration	5.0 and above	08.0.80 and above
Switch Inventory	5.0 and above	08.0.80 and above
Switch Health and Performance Monitoring	5.0 and above	08.0.80 and above
Switch Firmware Upgrade	5.0 and above	08.0.80 and above
Switch Configuration File Backup and Restore	5.0 and above	08.0.80 and above
Client Troubleshooting - search by Client MAC	5.1 and above	08.0.80 and above
Remote PING and TRACEROUTE	5.1 and above	08.0.80 and above
Switch Custom Events	5.1 and above	08.0.80 and above
Switch Configuration - Zero Touch Provisioning	5.1.1 and above	08.0.90a and above
Switch-specific settings - Hostname, Jumbo Mode, IGMP Snooping, and DHCP Server	5.1.1 and above	08.0.90a and above
Switch Port Configuration	5.1.1 and above	08.0.90a and above
Switch AAA Configuration	5.1.1 and above	08.0.90a and above

Unsupported AP Models

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

TABLE 5 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	ZF7352
ZF7762-T	ZF7351-U	ZF7761-CM	ZF7343-U	ZF7781CM
R300	ZF7782	ZF7982	ZF7782-E	ZF7055
ZF7372	ZF7782-N	ZF7372-E	ZF7782-S	C500
H500				

Caveats, Limitations, and Known Issues in this Release

The following are the Caveats, Limitations, and Known issues in this release.

NOTE

The caveats, limitations, and known issues stated in the 5.1 release notes are also applicable to this release.

Component	AP
Issue	SCG-100467
Description	Configuration scenario where the same GW used for WLAN1 with IPSec and for WLAN2 without IPSec is not supported. SoftGRE GW mapped to WLAN either has to be configured for SoftGRE+IPSec or only SoftGRE.

Component	AP
Issue	AP-10461
Description	Incompatibility between MacBook Air OS 10.10.5 and Apple TV OS 11.0 when both are on the same VLAN. Since the protocol is proprietary to the Apple products this is a system limitation. Ruckus has extensively tested on the following services, limited to these client devices: Bonjour Airplay - Apple TV 11.0

Component	AP
Issue	SCG-101150
Description	If hop 0 and hop 1 service record comes in same packet from a Bonjour server, AP will always give priority to hop 1 service record. Since tagging happens for hop1 service, hop 0 service can also be discovered by Bonjour clients

Component	AP
Issue	SCG-103846
Description	When a MAP is configured with a static channel it does not follow a channel change initiated by the RAP and therefore MAP will be disconnected from the Mesh tree
Workaround	Do not configure a static channel on a MAP

Component	AP
Issue	SCG-99923, SCG-101365
Description	If the untagged VLAN ID on any of the AP Ethernet ports is configured with a value other than VLAN ID 1 then none of the AP's WLAN can be mapped to VLAN ID of 1
Workaround	Map the WLAN to a VLAN ID other than 1

Component	AP
Issue	SCG-99984
Description	<p>Macbook devices (Macbook air OS-10.14, Macbook Pro OS-10.11.4, Macbook 10.10.5) with only IPv6 enabled fails to connect to Apple TV (version 11.0, 11.2.6 and 12.1), if the MacBook device and Apple TV are on different VLANs.</p> <p>Since link-local IPv6 addresses cannot be routed across VLAN's, it is expected that Bonjour Services will not work if the Bonjour Server advertises the MDNS service using link-local IPv6 as advertised address after enabling Bonjour Gateway. Hence, for different VLAN case when Bonjour Gateway is enabled and if the MDNS discovery is successfully completed between Bonjour Clients and Bonjour Server (example Apple TV) using Global IPv6, the Bonjour Services should work if the clients initiate data traffic using global IPv6 address.</p> <p>However, if Bonjour clients initiates data traffic using link-local IPv6 address, then again the services fails for the reason mentioned above</p> <p>Macbook devices mentioned above (Macbook air OS-10.14, Macbook Pro OS-10.11.4, Macbook 10.10.5) initiating data traffic using link-local IPv6 address cause the services to fail. Also, since Bonjour Fencing depends on Bonjour Gateway in different VLAN case, Bonjour Fencing will also not work for the same reasons mentioned.</p> <p>This results in failing of Bonjour Gateway for IPv6 when clients initiate traffic on link-to a local IPv6 address. Due to this Bonjour Fencing also fails for different VLAN cases. This is a system limitation.</p> <p>Ruckus has tested below listed services, with combination of following Apple Devices (clients/servers) and found them NOT working when Bonjour Gateway is enabled due to the limitation mentioned above.</p> <p>Bonjour Airplay - Apple TV version 11.0, 11.2.6 and 12.1 as a Bonjour server with the combination of MacBook Air 10.14, 10.10.5 and MacBook Pro 10.12.4 as a Bonjour Clients</p> <p>File Sharing and Screen Sharing - MacBook Pro 10.12.4 and MacBook Air 10.14</p> <p>NOTE If there is change in behavior of the iOS clients / Applications (data traffic is initiated with global IPv6 instead of link-local IPv6), then this limitation becomes irrelevant</p>

Component	AP
Issue	SCG-100064
Description	LACP (Link Aggregation Control Protocol) or Bonding feature is configurable using AP RKS CLI mode though the web user interface configuration option is limited to APs R720, R710 and R610

Component	AP
Issue	SCG-101252, SCG-101290
Description	LACP (Link Aggregation Control Protocol) or Bonding feature option <i>enable</i> or <i>disable</i> is service affecting feature configuration. This feature can be used during setup or maintenance mode only when <i>No Active Traffic DL/UL</i> is in progress

Caveats, Limitations, and Known Issues in this Release

Component	AP
Issue	SCG-95651
Description	L2 hashing algorithm on bonding interface fails to load balance the traffic if the last byte of all clients MAC address has the same value

Component	AP
Issue	AP-10145
Description	<p>Bonjour fencing does not work if services like SSH, Apple TV and Airdrop are discovered through any other interface other than WLAN interface of the client.</p> <p>It is observed bluetooth is able to discover the services for Apple TV and MAC devices.</p> <p>To effectively make Bonjour Fencing work, had to disable Mac UE bluetooth interface down with below commands:</p>
Workaround	<p>For Bonjour fencing to work on the Airplay devices, below mentioned configurations on Apple TV and MAC OS needs to done.</p> <ol style="list-style-type: none"> 1. Bluetooth option needs to be disabled on Apple TV device. 2. Disable Apple Wireless Direct Link feature on Mac book devices using: <pre>sudo ifconfig awdl0 down</pre> 3. In Apple TV navigate to Airplay configuration select the option Anyone on the same network 4. Disable bluetooth from system setting of Apple Wireless clients <p>NOTE If there is no provision to disable bluetooth, Bonjour fencing will not work effectively.</p>

Component	AP
Issue	AP-10346
Description	TCM with auth/assoc threshold/wait-time set can impact seamless roaming

Component	AP
Issue	AP-9572
Description	The default LACP rate is now 30 seconds

Component	AP
Issue	AP-9311
Description	RA Throttle on DVLAN/VLAN pool enabled WLAN considers RA from all the VLAN's irrespective of client association on those VLAN's. This can impact valid associated clients from receiving RA packets once RA throttle limit is reached
Workaround	<ul style="list-style-type: none"> • Preferred lifetime for the wireless network VLANs should be at least double the RA throttle duration configured and the periodic RA interval for these VLANs should be less than other VLANs in the network

Component	AP R720
Issue	AP-10409
Description	<p>For file sharing to work, Bonjour Client need standard string in MDNS response message from Bonjour server. Earlier versions of Bonjour servers were sending standard string as <i>_afpovertcp.local</i> for both IPv4 and IPv6. This standard string is learned by Bonjour Gateway running at AP and sent to clients for the MDNS discovery. However, after the MAC OS updates, the Bonjour servers are sending new standard string <i>_smb_tcp.local</i> which is not added on the Bonjour Gateway. This is also the reason why the this issue was not seen earlier releases.</p> <p>The fix for the issue is available as part of custom string feature of Bonjour Gateway at Ruckus AP. Customers need to check which latest string is coming in the MDNS response from the Bonjour servers (in this case <i>_smb_tcp.local</i>) and add the same in the Bonjour Gateway (BG) profile. Also, note that the standard services for the service file sharing of the Bonjour Gateway and Bonjour Fencing are not same and hence for file sharing if the Bonjour server is sending <i>_smb_tcp.local</i> then this service needs to be added as custom string in the BG profile. The Bonjour Fencing profile already takes care of the <i>_smb_tcp.local</i> and user need not to add it.</p> <p>However, in future if Bonjour sever sends any new string for file sharing (or any other application) then that string should be added in both the custom profiles in Bonjour Gateway as well as Bonjour Fencing</p>

Component	AP R730
Issue	SCG-98063
Description	When configuring CLB method to the option <i>capacity</i> on the controller web user interface, AP R730 disables the CLB on all WLANs.
Workaround	<p>Use AP CLI to manually enable CLB on some WLANs, in which case AP R730 runs the CLB with a STA count method on these WLANs. This creates a network , in which the non-11ax APs are based on capacity CLB while AP R730 are based on STA count CLB. Having two different CLBs could cause confusion.</p> <p>It is recommended to avoid AP CLI usage when the controller is set to CLB capacity method.</p>

Component	AP R730
Issue	SCG-91950, SCG-97553
Description	Controller web user interface will not have any latency data or corresponding graph data populated

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

Component	AP
Issue	SCG-97669
Description	Samsung A8 plus cannot connect to AP R730 in 5GHz radio

Caveats, Limitations, and Known Issues in this Release

Component	AP
Issue	SCG-97465
Description	The GPS history in the web user interface does not always work when <i>lte-gps-probeinterval</i> is 1

Component	AP
Issue	SCG-82191
Description	Cellular backhaul connection in M510 has roaming feature enabled by default and this option cannot be changed

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

Component	AP
Issue	SCG-89373
Description	AP packet capture shows PHY type as 11n under <i>802.11 Radio information</i> though the capture is for 11ac mode

Component	AP R730
Issue	SCG-96374
Description	Occasional target assert with 400+ clients

Component	AP
Issue	SCG-103174
Description	Channel 144 feature does not work on other countries except USA

Component	AP
Issue	SCG-104323
Description	Client data rate in client health tab does not show the correct downlink rate

Component	AP
Issue	SCG-100594
Description	<p>AP supports:</p> <ol style="list-style-type: none"> 1. SoftGRE+IPsec WLANs in a Zone or 2. Multiple SoftGREs (without IPsec) in a Zone per AP <p>NOTE A mix of both is not supported</p>

Component	AP
Issue	SCG-104268, AP-9208
Description	AP R510, R710 and R730 RKSCLI access is seen as shell prompt instead of login prompt after a RKSCLI session time out

Component	AP
Issue	SCG-101173
Description	Roaming performance for Samsung S5 or iPhone in tunnel downlink mode shows a drop beyond acceptable values

Component	AP
Issue	SCG-101173
Description	Roaming performance for Samsung S5 or iPhone in tunnel downlink mode shows a drop beyond acceptable values

Component	AP
Issue	SCG-94143
Description	To support LACP (Link Aggregation Control Protocol) or Link Aggregation Group (LAG) feature on Ruckus APs, the administrator needs to ensure the correct PoE power modes to Bring-Up LAN1 and 2 ports. For example, PoE-at+ for R720, PoE-at for R710, and so on. Refer to the respective AP product guides for details. NOTE LACP/LAG uplink throughput is limited to 1Gbps.

Component	ARC
Issue	SCG-104145
Description	YouTube deny setting does not work Apple IPAD IOS 12.2, iPhone 12.1.4 and MAC book Air-10.14.4

Component	ARC
Issue	SCG-103307
Description	Amazon music and Pokemon game do not get denied as per the ARC configured policy

Component	CLI
Issue	SCG-103274
Description	Not able to modify vSZ-E network setting on the CLI console
Workaround	Modify the network setting

Component	Control Plane
Issue	SCG-97577
Description	UDI interface cannot be reached since the default network driver of the controller is VMXNET3 which has a limitation for VLAN interface of VM.
Workaround	Change the network driver to E1000

Caveats, Limitations, and Known Issues in this Release

Component	Control Plane
Issue	SCG-97340
Description	The domain name used in Common Criteria (CC) deployment and the user need to use their X.509 certificate and corresponding infra preparation. For regular deployment, there is no need for default self-signed certificate.

Component	Data Plane
Issue	SCG-94395
Description	IPv6 packets processing goes through a slow path and has performance limitation

Component	Data Plane
Issue	SCG-100950
Description	Communication between AP and data plane always use self signed certificates from the controller

Component	Data Plane (AP-D, SZ-D/vSZ-D)
Issue	SCG-98143
Description	Throughput drops to 20% with IPSec on Tunnel WLAN. NOTE There are no issues with GRE tunnel without IPSec

Component	Hotspot WISPr
Issue	SCG-101617
Description	Self-signed or default certificates used in the controller internal subscriber portal has interoperability issues at times with Android devices when using the Google Chrome browser
Workaround	It is strongly recommended to use public key certificates [rather than self-signed or default certificates] for both external and internal HTTPS based subscriber portal

Component	IoT
Issue	SCG-100868
Description	AP R730 IoT only works from one radio at a time. If external I100 is connected to the USB, it takes precedence, else the internal IoT is in use
Workaround	Re-enable the R730 internal IoT radio by disconnecting the I100 module

Component	Switch Management
Issue	SCG-103623
Description	ICX switch (ICX 8.0.90a) fails to delete the TACACS+ and Radius AAA servers when pushed from the controller if SNMP query is not enabled in the switch or if this is a pre-configured switch before joining the controller
Workaround	Turn the SNMP query flag in Switch.

Component	Switch Management
Issue	SCG-104260
Description	In this release only forming a LAG through the controller web user interface is supported. The system does not support configuring LAG interface detail through the controller web user interface
Workaround	To configure detail settings for LAG after form it, you need to configure it through ICX console directly

Component	Switch Management
Issue	SCG-103158
Description	In the current design, the controller does not support operators other than <i>equal to</i> . If the user configures ACL rules on switch using operators like <i>greater than</i> , <i>less than</i> , it will be transferred to <i>equal to</i> in the controller

Component	Switch Management
Issue	SCG-98589
Description	The maximum configurable limit of OSPF areas is four on ICX7150
Workaround	OSPF area needs to deleted by the user if it creates L3 interfaces with different OSPF areas

Component	Switch Management
Issue	SCG-97629
Description	Brand new ICX switch joining the controller with SZ having AAA authentication setting disabled cannot login to console
Workaround	Enable AAA authentication with local username password on the controller for the switches

Component	Switch Management
Issue	SCG-98182
Description	Not able to assign VLAN untagged/tagged ports to ICX stack switches (7150) in family group
Workaround	Update validate rules for VLAN tagged and untagged port. Group level <ul style="list-style-type: none"> • Check basic port string (supported) : <ul style="list-style-type: none"> - For example, for 7450-24P the valid port range is from 1/1/1 to 1/1/24 - If the user enters the port as 1/1/26 as either tagged or untagged port, the controller rejects it • Skip additional module checking (not supported) <ul style="list-style-type: none"> - For example, for 7450-24P if the user enters the port as 1/2/1 or 1/5/1, the controller does not throw any error because the controller does not know what modules the customers is going to use • It is recommended that users should not use values like 1/5/1 for 7450-24P.

Caveats, Limitations, and Known Issues in this Release


Component	Switch Management
Issue	SCG-101555
Description	Sometimes ICX Switch does not reload automatically on completion of firmware upgrade
Workaround	If this happen, wait the job to timeout (fail). Re-trigger the upgrade job again

Component	Switch Management
Issue	FI-197298 and FI197300
Description	Online configuration from the controller causes memory leak on the switch and can lead to crash NOTE Recommended to stop the configuration from the controller if the switch memory reaches 80% until the memory is recovered by a reboot.

Component	Switch Management
Issue	FI-197045
Description	Sometimes configuration backup fails

Component	Switch Management
Issue	FI-196937
Description	Connection to the controller fails after <i>stack switch-over</i>

Component	Syslog
Issue	SCG-88903
Description	AP M510 stops sending LTE related event after disabling LTE when using the below RKSCCLI command: <code># set lte-state</code>

Component	System
Issue	SCG-90627
Description	AP's running below firmware can no longer talk directly to SZ/vSZ for firmware upgrade using LWAPP even if LWAPP2SCG is enabled
Workaround	 <p>CAUTION This workaround is not recommend.</p> <p>If you still want to upgrade firmware using <i>LWAPP2SCG</i> manually login to each AP and execute the below AP CLI commands.</p> <pre>set scg disable reboot set scg enable (after upgrade) reboot</pre>

Component	System
Issue	SCG-75792
Description	Host name is not displayed in client finger printing for Nexus 5x,Google Pixel and 6P Android 8.0.0 or 8.1.0 devices

Component	System
Issue	SCG-99945
Description	If a user configures the logon URL parameter as <i>Internal</i> in the Hotspot Portal profile, a valid CA signed certificate should be uploaded to the controller for Hotspot usage as well. Otherwise the UE's using Microsoft Edge 40+ browser will fail on post-authentication redirect to user intended URL or configured fixed URL

Component	UI/UX
Issue	SCG-104138
Description	Controller fails in creating SCI when the server host is set as FQDN. Server host only accepts IP address and not hostname

Component	UI/UX
Issue	SCG-104307
Description	Client data rate in client health tab does not show the correct downlink rate

Component	UI/UX
Issue	SCG-98310
Description	Real time connection failure rate chart fails to update any value

Component	Virtual SmartZone Data Plane
Issue	SCG-100910
Description	UE traffic drops to 95% when IPSec debug log level 4 or above is enabled on the data plane

Component	Virtual SmartZone Data Plane
Issue	SCG-72793
Description	When using tunneled WLAN with vSZ-D DHCP/NAT feature with Radius-based profile, clients connected to the same WLAN will be able to see each other Multicast/Broadcast traffic even if they are in different subnets

Component	Virtual SmartZone Data Plane
Issue	SCG-102179
Description	Multicast forwarding feature is only supported on SZ100 for IPv4 only, and not on any other platform including SZ100-D in this release. This results in failure of exchange of MDNS request and response across SoftGRE tunnels. Therefore, Bonjour Service, Bonjour Gateway and Bonjour Fencing is not supported for IPv6 SoftGREGRE

Caveats, Limitations, and Known Issues in this Release

Component	Virtual SmartZone Data Plane
Issue	SCG-98848
Description	Currently vSZ-D or SZ100-D does not have CLI command to display IPSec configuration or status

Component	Virtual SmartZone Data Plane
Issue	SCG-98238
Description	Communication between AP and data plane always uses self signed certificate from the controller

Component	Virtual SmartZone Data Plane
Issue	SCG-97558
Description	vSZ-D remains connected to the controller even after deleting the valid CA chain from the web user interface

Component	Virtual SmartZone
Issue	SCG-97924
Description	Hyper-V requires power shell to run some setting for VM to support VLAN trunk
Workaround	Refer to https://docs.microsoft.com/en-us/powershell/module/hyper-v/set-vmnetworkadapervlan?view=win10-ps

Component	Virtual SmartZone
Issue	SCG-103404
Description	vSZ-E 100 AP profile requires 2 CPU Cores. However, based on CPU performance, If vSZ-E setup fails, Ruckus strongly recommends increasing the core numbers to a maximum of 4 CPUs

Component	Virtual SmartZone
Issue	SCG-104432
Description	<p>For Transient Client Management (TCM) feature, administrator should reconfigure the TCM parameters under WLAN profile on upgrading the controller from releases 3.4.2 > 3.6.2 > 5.1.1</p> <p>In release 3.4.2, TCM was AP centric feature where the user configures this feature using AP CLI. Starting from release 3.6.2, TCM is configurable through the controller user interface WLAN with default disabled and is no longer AP centric.</p> <p>Due to this new feature support, if you configured TCM in AP in 3.4.2 and then upgrade to 3.6.2 or later versions TCM will become disabled.</p>
Workaround	Enable TCM and reconfigure TCM parameters <i>rsssi_threshold/ drop_random_prbs/ auth</i> and <i>assoc rssi threshold</i> in WLAN profile

Resolved Issues

The following are the resolved issues related to this release.

Component	AP
Issue	ER-6606
Description	This enhancement allows configurable <i>Multicast Airtime</i> in percentage on Wave 1 APs. The default value is 25%

Component	AP
Issue	ER-6607
Description	Resolved an issue where the AP now reports the statistics to SZ resulting in the display of the current information

Component	AP
Issue	ER-6008
Description	Resolved an issue where APs using SoftGRE over IPv6 went into a GRE inactive state and closed their SSIDs.

Component	AP
Issue	ER-6665
Description	Resolved a target fail detected issue on APs

Component	AP
Issue	ER-6664
Description	Resolved an issue where the APs selected the channels 149-161 though they were not visible in the Zone/AP Group

Component	AP
Issue	ER-6781
Description	<p>Resolved an issue where the user can download and use the AP certificate to log in the controller.</p> <p>IMPORTANT Refer to the below pointers for upgrading to 3.6.2 Patch1</p> <ul style="list-style-type: none"> This issue will be present on 3.6.2 Patch-1 if upgrade path of 3.2.0 > 3.4.2 > 3.6.2 Patch-1 is followed. Issue will be not be present on 3.6.2 Patch-1 if upgrade path of 3.2.0 > 3.4.2 > Apply KSP for ER7881 > 3.6.2 Patch-1 is followed

Component	AP
Issue	ER-6901
Description	<p>Resolved an issue where the switch reports two MAC addresses of AP R720. This is valid for virtual controllers running on release 3.5 version.</p> <p>Users have to manually disable NSS offload in release 3.6 or later versions.</p>

Resolved Issues

Component	AP
Issue	ER-6969
Description	Resolved an issue where the R310 AP at times failed to transmit in 20MHz bandwidth mode

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

Component	AP
Issue	ER-6724
Description	The issue was caused by handling pseudo random number (shifting) incorrectly on WPA encryption, such that certain type of device fails to de-crypt the frames. The issue is resolved with the correct PN shifting is used.

Component	AP
Issue	ER-7091
Description	Resolved an issue where on editing a created Zone the channel information was not correct if the browser was Google Chrome

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

Component	AP
Issue	ER-7018
Description	Resolved an issue where the error in rate control algorithm of Wave 1 AP using unsupported data rate in 5 GHz radio for the first data packet to the client is corrected

Component	AP
Issue	SCG-93649
Description	Resolved an issue where DHCP/NAT AP listed the wrong type name on sorting the column by AP type

Component	AP
Issue	SCG-104740
Description	Resolved an issue where AP M510 failed to connect to LTE using the APN default setting

Component	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	DHCP-Server
Issue	SCG-76058
Description	Resolved an issue where primary DHCP server AP is recovered, lease file copied from the secondary DHCP server AP may expire if it is copied prior to time synchronization

Component	Data Plane
Issue	ER-7130, SCG -102178
Description	Resolved an issue where SZ100-D consumed data plane capacity license

Component	IoT
Issue	SCG-104659
Description	Resolved an issue where the AP at times got disconnected if AP name, location, or floor was changed

Component	IoT
Issue	IOTC-2230
Description	Resolved an issue where the IoT process continuously restarted when the process (<i>iotg-process</i>) was disabled with Zigbee Wi-Fi Co-existence being disabled or enabled.

Component	IoT
Issue	IOTC-2271
Description	Resolved an issue where IoT was unable to change the Zigbee channel with Wi-Fi Co-existence being disabled.

Component	System
Issue	ER-6619
Description	Resolved an issue where mapping VLAN pools using the VLAN override option from WLAN Group failed

Component	System
Issue	ER-7029
Description	Resolved an issue where the permission settings for API is not right

Component	System
Issue	ER-7031
Description	Resolved an issue where the user was unable to configure Client Isolation Whitelist with zero as second or third octet

Component	System
Issue	ER-6965
Description	Resolved an issue where the password failed to contain characters like "%"

Resolved Issues

Component	System
Issue	ER-6630
Description	Resolved an intermittent connectivity issue in a WLAN with DPSK (Dynamic Pre-Shared Key) enabled due to an internal race condition in the controller

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

Component	UI/UX
Issue	ER-6449
Description	Resolved an issue where AP name was displayed incorrectly in several menus in Web user interface

Component	Virtual SmartZone
Issue	ER-6584
Description	Resolved an issue where Radius proxy process would go offline intermittently.

Component	Virtual SmartZone
Issue	ER-6552
Description	Resolved an issue where Novell LDAP authentication now passes in absence of dictionary group information response. This makes the controller version in par with ZoneDirector version

Component	Virtual SmartZone
Issue	ER-6742
Description	Resolved an issue where there was a performance issue of the vSZ user interface

Component	Virtual SmartZone
Issue	SCG-91127
Description	Resolved an issue where Rogue Access points did not display any rogue detected AP. User is given option to select rogue profile in modify Zone/Zone template

Component	Virtual SmartZone Data Plane
Issue	ER-6997
Description	Resolved an issue where the MDNS packets were blocked in the queue causing a delay in processing the other packets. Clients experienced delayed response time when using the Internet.

Upgrading to This Release

Before Upgrading to This Release

Due to underlying changes of the database in this release, data will be dropped during the upgrade. It is recommended that you read the following content carefully before upgrading to this release.

IMPORTANT

Data migration from SmartZone (SZ) 5.0 or 5.1 to 5.1.1 is supported.



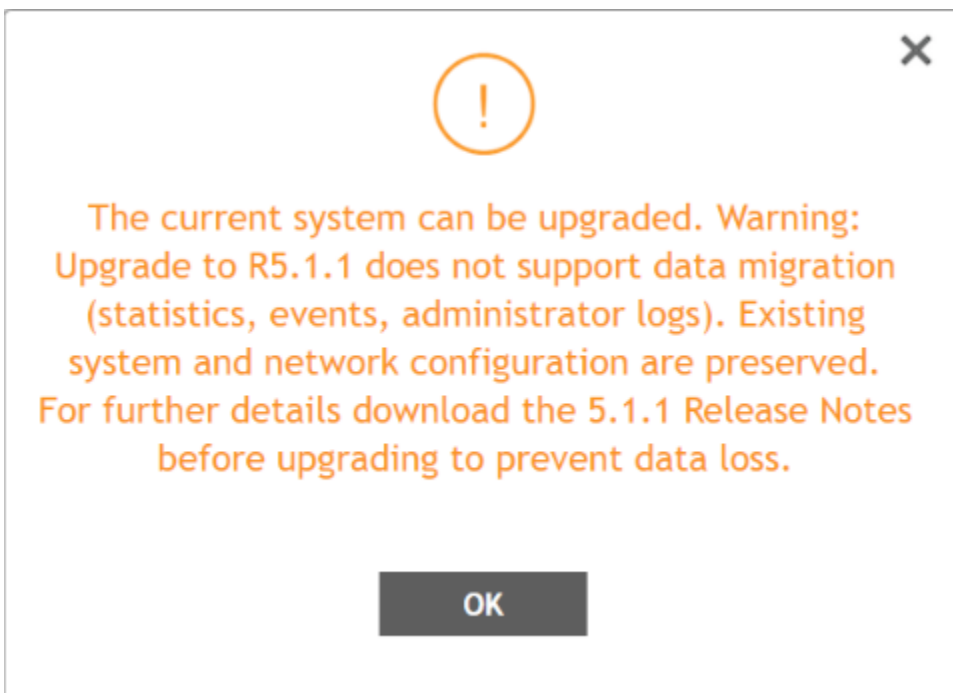
CAUTION

Data migration is not supported if system upgrades from release 3.6.0 or 3.6.1 or 3.6.2 to release 5.0, 5.1 or 5.1.1 by SmartZone (SZ) release 5.0, 5.1, and 5.1.1 upgrade. Existing system and network configuration is preserved, but data such as status and statistics, alarms or events, administrator logs, and mesh uplink history is not migrated to the new release. Contact Ruckus support for concerns or additional clarifications. [SCG-73771]

ATTENTION

If you are upgrading with a three or four nodes cluster running on version 5.0.0.0.676 with 22500 APs and above refer to caveat [SCG-97442].

- The upgrade path is changed and is now limited to N-2 support. Only 3.6.0 or 3.6.1 or 3.6.2 or 5.0 or 5.1 releases can be upgraded to 5.1.1 release.
- When upgrading to the release 5.1.1 image from release 3.6.0 or 3.6.1 or 3.6.2, the system displays the following warning message about not supporting data migration (statistics, events, administrator logs) during the upgrade process.



Upgrading ICX Switches

Ruckus ICX switches starting from 08.0.90 releases supports unified images which require two step process from prior releases. The two step process is:

1. **Step 1** - Upgrade from **08.0.80 (non- Unified FastIron Image (UFI) or UFI) > 08.0.90 UFI**
2. **Step 2** - Upgrade from **08.0.90 UFI > 08.0.90a UFI**

NOTE

Refer to Ruckus FastIron Software Upgrade Guide, 08.0.90 for details.

Data Migration Recommendations

If you need to preserve your data or reports, consider the following recommended options before upgrading:

- Leverage an existing SCI platform to send statistics and reports to SCI before the upgrade.

NOTE

SCI comes with a free 90-day evaluation.

- Backup and export existing statistics and reports using Export tools or Streaming API before the upgrade.
- Ruckus will be able to provide the Data Migration Tool to interested customers (only available to Essential controllers), and the Data Migration Tool Guide is downloadable from the support site.

NOTE

Use of the Data Migration Tool is not recommended for high-scale users running SZ300 or vSZ-H.

Upgrade Considerations

Before upgrading, consider these additional points.

- 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.
- 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.
- 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.



WARNING

LAG users must go through the following process before upgrade to avoid losing IP connectivity:

1. Disable secondary port of the LAG in the AP.
2. Disable Bonding on the AP using AP CLI.
3. Upgrade the AP Zone.
4. Enable LAG using controller GUI.
5. Enable secondary port on the AP.

Virtual SmartZone Required 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, wireless clients and ICX Switches that you plan to manage. See the tables below for the **required** virtual machine system resources.

The values for vCPU, RAM, and Disk Size are linked together and cannot be changed individually. When changing one of these parameters, all three values need to **match exactly** with an existing Resource Level. Taking vSZ-H Resource Level 5 as an example: when adjusting the number of vCPU from 4 to 6, the amount of RAM needs to be adjusted to 22GB and the Disk Size needs to be adjusted to 300GB, thereby matching all the values of Resource Level 6.



WARNING

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

NOTE

When initially building up the network it can use a higher Resource Level than needed for the number of APs first deployed, if all the three parameters (vCPU, RAM and Disk Size) **match exactly** with that higher Resource Level.

ATTENTION

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

In the following tables the high scale resources are broken into two tables for easy readability. These tables are based on the *AP Count Range*.

TABLE 6 vSZ High Scale required resources

AP Count Range		Max Clients	Nodes per Cluster	AP Count per Node (without Switch)	AP/Switch Capacity Ratio	Maximum Switch (w/o AP)
From	To			Max		Max
10,001	30,000	300,000	4	10,000	5 : 1	6,000
	20,000	200,000	3		5 : 1	4,000
5,001	10,000	100,000	1-2	10,000	5 : 1	2,000
2,501	5,000	50,000	1-2	5,000	5 : 1	1,000
1,001	2,500	50,000	1-2	2,500	5 : 1	500
501	1,000	20,000	1-2	1,000	5 : 1	200
101	500	10,000	1-2	500	5 : 1	100
1	100	2,000	1-2	100	5 : 1	20

TABLE 7 vSZ High Scale required resources

AP Count Range		vCPU	RAM	Disk Size	Preserved Events	Concurrent CLI Connection	Resource Level
From	To	Logic Processor ^{[1][2]}	GB ^[1]	GB	Max	Max (per node not per cluster)	
10,001	30,000	24	48	600	3 M	4	8
	20,000						
5,001	10,000	24	48	600	3 M	4	7
2,501	5,000	12	28	300	2 M	2	6.5
1,001	2,500	6	22	300	1.5 M	2	6

TABLE 7 vSZ High Scale required resources (continued)

AP Count Range		vCPU	RAM	Disk Size	Preserved Events	Concurrent CLI Connection	Resource Level
501	1,000	4	18	100	600 K	2	5
101	500	4	16	100	300 K	2	4
1	100	2-4 ^[2]	13	100	60 K	2	3

In the following tables the essential scale resources are broken into two tables for easy readability. These tables are based on the *AP Count Range*.

TABLE 8 vSZ Essentials required resources

AP Count Range		Maximum Clients	Nodes per Cluster	AP Count per Node	AP/Switch Capacity Ratio	Maximum Switch (w/o AP)
From	To			Max		Max
1025	3,000	60,000	4	1,024	5 : 1	600
	2,000	40,000	3		5 : 1	400
501	1,024	25,000	1-2	1,024	5 : 1	204
101	500	10,000	1-2	500	5 : 1	100
1	100	2,000	1-2	100	5 : 1	20

NOTE

The recommended vCPU core for the vSZ-E with **AP Count Range** 1 through 100 is 2-4.

TABLE 9 vSZ Essentials required resources

AP Count Range		vCPU	RAM	Disk Size	Preserved Events	Concurrent CLI Connection	Resource Level
From	To	Logic Processor ^{[1][2]}	GB ^[1]	GB	Max	Max (per node not per cluster)	
1025	3,000	8	18	250	10 K	2	3
	2,000						
501	1,024	8	18	250	10 K	2	2
101	500	4	16	100	5 K	2	1.5
1	100	2-4 ^[2]	13	100	1 K	2	1

NOTE

[1] - vSZ-H and vSZ-E have different report interval. For example, AP sends the status to vSZ-E every 90 seconds but to vSZ-H it is sent every 180 seconds, which means that vSZ-E need more CPU in scaling environment based on the resource level.

[2] - 4 logic processors requested in Hyper-V environment or Azure with low CPU throughput. If vSZ setup failed because Azure with low CPU throughput, it is strongly recommended to increase core numbers or migrate to other family of Azure that provides better ACU (Azure Compute Unit), for instance, at least better than (D1 family, ACU = 160).

Maximum Supported AP and Switch Management

The tables below list the maximum supported resources between APs and switches.

SmartZone 5.1.1 support dynamic (linear) AP/Switch capacity based on capacity ratio. No AP/Switch mode, only mix mode and AP/Switch support number base on total amount connect AP/Switch capacity.

Capacity Ratio

High scale profile with higher switch support capacity to 5:1 from 8:1

vSZ-H L6 ~ L8

5:1 (10000 AP : 1250 switches)

Example: Calculating the Total Capacity

- 200 APs + 100 switches (1:5)
 $(200 \times 1) + (100 \times 5) = 700$ (Total Capacity) This requirement could use L5, since the total capacity is smaller than 1,000.
- 400 APs + 10 switches (1:5)
 $(400 \times 1) + (10 \times 5) = 450$ (Total Capacity) This requirement could use L4, since the total capacity is smaller than 500.

NOTE

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

TABLE 10 AP and Switch resource table for 1 and 2 nodes

Profile	1 and 2 Nodes				1 or 2 Nodes
	AP Mode		Switch Mode		AP/Switch Capacity Ratio
SZ100	1,024	0	0	204	5:1
SZ300	10,000	0	0	2,000	5:1
vSZ-E L1	100	0	0	20	5:1
vSZ-E L1.5	500	0	0	100	5:1
vSZ-E L3	1,024	0	0	204	5:1
vSZ-H L3	100	0	0	20	5:1
vSZ-H L4	500	0	0	100	5:1
vSZ-H L5	1,000	0	0	200	5:1
vSZ-H L6	2,500	0	0	500	5:1
vSZ-H L6.5	5,000	0	0	1,000	5:1
vSZ-H L8	10,000	0	0	2,000	5:1

In the following tables for three and four nodes are broken into two tables for easy readability.

TABLE 11 AP and Switch resource table for 3 and 4 nodes

Profile	3 Nodes					4 Nodes				
	AP Mode		Switch Mode		AP/Switch Capacity Ratio	AP Mode		Switch Mode		AP/Switch Capacity Ratio
SZ100	2,000	0	0	400	5:1	3,000	0	0	600	5:1
SZ300	20,000	0	0	4,000	5:1	30,000	0	0	6,000	5:1
vSZ-E L3	2,000	0	0	400	5:1	3,000	0	0	600	5:1
vSZ-H L8	20,000	0	0	4,000	5:1	30,000	0	0	6,000	5:1

SmartZone Upgrade Paths

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

To help ensure that the cluster firmware upgrade process can be completed successfully, the cluster interfaces of all nodes must be connected and up. **[SCG-34801]**

TABLE 12 Previous release builds

Platform	Release Build
SZ300	3.6.0.0.510
SZ100	3.6.1.0.227
vSZ	3.6.2.0.222
vSZ-D	5.0.0.0.675
SZ100-D	5.1.0.0.496

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.

Supported SmartZone and Data Plane Platform

The below table lists the supported platform for each controller and data plane.

Controller	SmartZone 3.6	SmartZone 3.6.1	SmartZone 5.0	SmartZone 5.1	SmartZone 5.1.1
Controller					
SZ300	✓	✓	✓	✓	✓
SZ100	✓	✓	✓	✓	✓
vSZ-High Scale	✓	✓	✓	✓	✓
vSZ-Essential	✓	✓	✓	✓	✓
SCG200	✗	✗	✗	✗	✗
SCG200-C	✓	✓	✗	✗	✗
Data-Plane					
D104	✗	✓ by vSZ (POC)	N/A	✓ by vSZ	✓ by vSZ
D124	✗	✓ by vSZ (POC)	N/A	✓ by vSZ	✓ by vSZ
vDP	✓	✓	✓	✓	✓

Multiple AP Firmware Support in the SZ100/vSZ-E/SZ300/vSZ-H

The AP firmware releases that APs use are configured at the zone level. This means that APs that belong to one zone could use a different AP firmware release from APs that belong to another zone.

ATTENTION

SZ300/SZ100/vSZ-E/vSZ-H is referred as **controller** in this section.

REMEMBER

If you have AP zones that are using 3.4.x or 3.5.x and the AP models that belong to these zones support AP firmware 3.6 (and later), change the AP firmware of these zones to 3.6 (or later) to force these APs to upgrade their firmware. After you verify that all the APs have been upgraded to AP firmware 3.6 (or later), proceed with upgrading the controller software to release 5.1.1. All other AP firmware releases that were previously available on the controller will be deleted automatically during the upgrade.

ATTENTION

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 5.1.1, the AP Zone firmware remains the same.

Up to Three Previous Major AP Releases Supported

Every platform release can support up to three major AP firmware releases, including (1) the latest AP firmware release and (2) two of the most recent major AP firmware releases. This is known as the N-2 (n minus two) firmware policy.

NOTE

A major release version refers to the first two digits of the release number. For example, 3.6.1 and 3.6.2 are considered part of the same major release version, which is 3.6.

The following releases can be upgraded to release 5.1.1:

- 5.1
- 5.0
- 3.6.x

The AP firmware releases that the controller will retain depends on the controller release version from which you are upgrading:

Upgrade path	AP firmware releases in controller
5.1 > 5.1.1	5.1, 5.1.1
5.0 > 5.1 > 5.1.1	5.0, 5.1, 5.1.1
5.0 > 5.1.1	5.0, 5.1.1
3.6.x > 5.0 > 5.1 > 5.1.1	3.6.x, 5.0, 5.1, 5.1.1
3.6.x > 5.0 > 5.1.1	3.6.x, 5.0, 5.1.1
3.6.x > 5.1 > 5.1.1	3.6.x, 5.1, 5.1.1
3.6.x > 5.1.1	3.6.x, 5.1.1

All other AP firmware releases that were previously available on the controller will be deleted automatically. For example:

- If you are upgrading the controller from release 5.1, then the AP firmware releases that it will retain after the upgrade will be 5.1.1 and 5.1 (and 5.0 and/or 3.6.x if this controller was previously in these releases).
- If you are upgrading the controller from release 5.0, then the AP firmware releases that it will retain after the upgrade will be 5.1.1 and 5.0 (and 3.6.x if this controller was previously in release 3.6).
- If you are upgrading the controller from release 3.6.x, then the AP firmware releases that it will retain after the upgrade will be 5.1.1 and 3.6.x.

EoL APs and APs Running Unsupported Firmware Behavior

Understanding how the 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

SZ300/vSZ-H is referred as **controller** in this section.

EoL APs

To check if an AP that you are managing has reached EoL status, visit the Ruckus support website. The icons for EoL APs appear with the *END OF LIFE* watermark.

1. An EoL AP that has not registered with the controller will be moved to the Staging Zone and its state set to Pending. This AP will be unable to provide WLAN service to wireless clients.
2. The EoL AP affects the upgrade only in the following conditions. Otherwise, the upgrade be successful.
 - a. Upgrade should be prior to 3.6 release
 - b. This is applicable in SZ100 or vSZ-E controllers

APs Running Unsupported Firmware Releases

- APs running AP firmware releases that are unsupported by the controller release can still connect to the controller.
- Once connected to the controller and assigned to a zone, the AP will be upgraded to the AP firmware assigned to the zone to which it belongs.

Interoperability Information

AP Interoperability

APs with ordering number prefix 901- (example 901-T300-WW81) may now be supplied with an AP base image release 100.0 or later (including 104.0).

The AP base image is optimized for controller-discovery compatibility to support all Ruckus controller products including ZoneDirector, vSZ and SZ100.

Once the AP discovers and joins a controller (for example, the SZ100), the AP is updated to the compatible controller-specific AP firmware version. The updated AP firmware version becomes the factory-default image. The updated AP firmware version (for example, vSZ AP100.x) will remain persistent on the AP after reset to factory defaults.

An AP configured with base image release 100.0 may be managed by the FlexMaster management tool or may be used in standalone controller-less operation if controller discovery is disabled on the AP web interface.

Enabling ZoneFlex AP Discovery to a SmartZone Controller Using DHCP Option 43

To ensure reliable discovery of ZoneFlex APs to SmartZone controllers, the DHCP server must be configured to support DHCP Option 43 settings as outlined in the Getting Started Guide for your controller. DHCP option 43 sub codes 03 and 06 IP address assignments must both point to the SmartZone controller's control plane IP address to ensure reliable discovery services.

Enabling ZoneFlex AP Discovery to a SmartZone Controller Using DNS

To ensure reliable discovery of ZoneFlex APs to SmartZone controllers using DNS resolution, the DNS server must be configured to have two DNS entries. The first DNS entry must use the "RuckusController" prefix and the second entry the "zonedirector" prefix.

Refer to the *Getting Started Guide* for your SmartZone controller for instructions on how to connect the AP to the controller using DNS.

Redeploying ZoneFlex APs with SmartZone Controllers

NOTE

A supported ZoneFlex AP configured to operate with ZoneDirector will require an upgrade to a compatible SmartZone controller approved software release prior to interoperating with an SZ or vSZ 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.

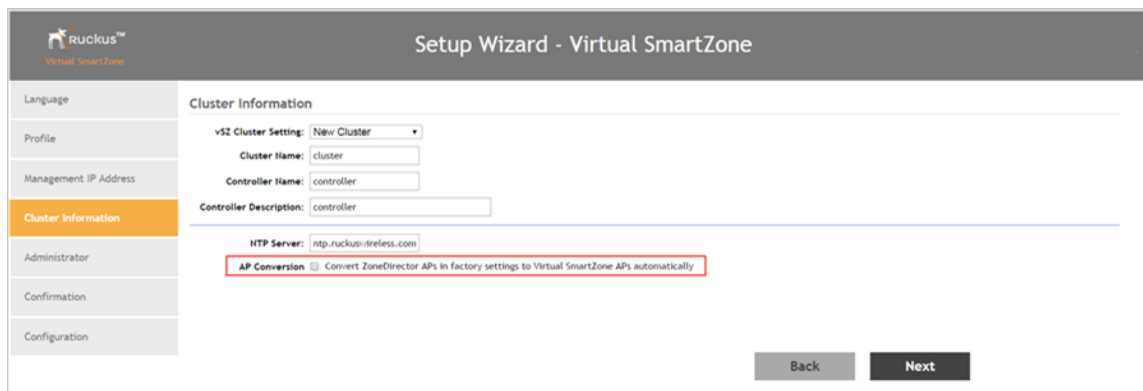
Follow these steps to convert standalone ZoneFlex APs to the SmartZone controller firmware so that they can be managed by the SZ300, SZ100, or vSZ

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 'Cluster Information' selected. The main area is titled 'Cluster Information' and contains the following fields:

- vSZ Cluster Setting: New Cluster (dropdown)
- Cluster Name: cluster (text input)
- Controller Name: controller (text input)
- Controller Description: controller (text input)
- HTP Server: ntp.ruckuswireless.com (text input)

At the bottom, there is a checkbox labeled 'AP Conversion' with the description 'Convert ZoneDirector APs in factory settings to Virtual SmartZone APs automatically'. This checkbox is highlighted with a red rectangular box. Below the form 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 (SZ or vSZ 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.

Users will not be redirected to WISPr Internal Logon URL with Chrome browser 65. This is the behavior of Chrome browser version starting from 63. **[SCG-85552]**

Workaround: Add the following URLs in Walled Garden list for WISPr redirection to work.

- connectivitycheck.gstatic.com
- clients3.google.com
- connectivitycheck.android.com
- play.googleapis.com
- gstatic.com

For details refer to <https://www.chromium.org/chromium-os/chromiumos-design-docs/network-portal-detection>



© 2019 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