RELEASE NOTES

Ruckus SmartZone 5.1.2 Release Notes

Supporting SmartZone 5.1.2

Part Number: 800-72360-001 Rev A
Publication Date: September 2019

Contents

Document History

Revision Number	Summary of changes	Publication date
A	Initial release notes	13, September 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 5.1.2

The SZ release 5.1.2 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 5.1.2.

> **NOTE**
> For detailed descriptions of these features and configuration help, refer to the respective 5.1.2 documentation guides available at https://support.ruckuswireless.com/

Federal Information Processing Standards

The following are enhancements in Federal Information Processing Standards (FIPS) mode.

Administrator Login Enhancements

- **RadSec Support**: With 5.1.2, administrator Radius authentication to an external Radius server is now protected through a RadSec tunnel. When any external Radius server is configured for administrator authentication that support RadSec, the controller initiates the RadSec session with it to protect the keys exchanged during authentication.
- **Admin Role Assignment through External Radius**: When external Radius server is used for admin authentication, roles can be assigned through VSA for AAA admin user role mapping. Role need to be manually created on the controller before assigning it through an external AAA server.
- **Personal Identity Verification (PIV) or Common Access Card (CAC) Login**: The controller now supports admin authentication via CAC/PIV card or smart card. Admin users are authenticated through the certificate loaded on a CAC/PIV card. OCSP (Online Certificate Status Protocol) and user PIN (two factor) validation is supported as well.
- **Admin Session Timer with Session Lock**: For admin users both active and inactive session monitoring is now supported. Admin user's session can be automatically logged off when the active or inactive session timer configured is reached. Users can re-login when the logout event due to session time out occurs.
- **Customizable Login Banner**: With 5.1.2, the controller now supports a customizable login banner in web user interface. The login banner can be configured by the admin to be displayed at every login in the login/authentication page.
- **Concurrent Session Limit**: Administrator can now configure maximum allowed concurrent admin sessions.
- **Password Complexity Restrictions**: Enhanced password complexity restrictions are now available to enforce more stringent new and old password reuse requirements.

Wireless Intrusion Prevention System (WIPS)/Wireless Intrusion Detection System (WIDS)

Controller managed APs now also support a *Monitoring Group*. When APs are in monitoring group, they will stop serving clients in access mode and assume the role of full time monitoring APs for WIPS/WIDS functions. APs in monitoring group will be continuously scanning the air and report Rogue APs and clients to the controller. Access APs can also perform background scanning function in addition to full time monitoring APs. Configuration options for channels to be scanned and the scan interval can be configured within the monitoring group.

IPSec - Controller to Third Party

Controller now support IPSec connectivity for northbound connections primarily to protect NTP, Syslog and other administrative functions,

IPSec - AP to Controller

In addition to GRE and Ruckus encrypted GRE, IPSec is also supported as a tunneling option for data traffic between AP and controller or vSZ-D.

Backup NTP

NTP configuration on controller now allows configuration of a backup NTP sever alongside authentication.

Open API

Ruckus's Public APIs development style now integrates Public APIs related information to generate documents that conform to Open API specification. Users can use Swagger tools to meet their requirement.

Open API Specification (OAS) - The Open API is the official name of the specification. The development of the specification is fostered by the Open API Initiative, which involved more the 30 organizations from different areas of the tech world - including Microsoft, Google, IBM, and CapitalOne. Smartbear Software, which is the company that lead the development of the Swagger tools, is also a member of the Open API Initiative, helping lead the evolution of the specification.

SmartBear launched Open API Initiative and Open API 3.0 was the first official release of the specification. It was donated to the Open API Initiative by SmartBear software and renamed from Swagger Specification to Open API specification in 2015.

Swagger is the name associated with some of the most well-known, and widely used tools for implementing the Open API specification. The Swagger tool set includes a mix of open source, free, and commercial tools, which can be used at different stages of the API life cycle.

Swagger vs Open API: The easiest way to understand the difference is:

- Open API = Specification.
- Swagger = Tools for implementing the specification.

Ruckus uses version **2.0** and **JSON** format for the Open API.

Limitation of the Ruckus's Open API :

- The login API only supports one API **POST:/serviceTicket** for authorization through CAS server.
- Open API document only supports current Public API version.

Nutanix Hypervisor Support

In this release, we added Nutanix Hypervisor support for vSZ and vSZ-D. Please refer to Nutanix official site for their hardware resource requirements to run the Hypervisor itself. The resource requirements to run vSZ and vSZ-D will be same as the other Hypervisors we support.

SmartZone Admin Authentication with RadSec

SmartZone Admin login has been authenticated over non secure RADIUS interface accessing external AAA in prior releases. With this feature, the admin authentication can be secured by using RadSec. SZ controller already has the capability to provide secure interface where RADIUSD process uses TLS (Transport Layer Security) to communicate AAA server, so this feature is an extension to make SZ Admin authenticated via a secured RadSec interface.

Switch Management

SmartZone 5.1.2 adds usability enhancements related to switch management and visibility in to all the devices that are connected to ICX switches.

- **Switch Client Visibility**: Provides detailed information about the devices that are connected to ICX switches including end user devices as well as Ruckus Access Points.
- **Simplified Default Group for SZ100/vSZ-E** : Users are no longer mandated to move switches to a user defined group. Switches can be managed from the default group directly.
- **New switch models supported**: SmartZone 5.2 supports management of these latest switch models:
  - ICX7150-C08P
  - ICX7150-C10ZP
  - ICX7150-24F

Changed Behavior

Changed Behavior

The following are the changed behavior issues.

- Port details are now seen when a user hovers mouse over a port icon on the switch front panel view.
- LACP configuration on APs R720, R710 and R610 is now available though the controller web user interface. It is recommended not to use CLI to configure LACP on these APs. Using CLI may result in inconstant behavior since the controller will push and overwrite the CLI configuration. **[SCG-104445]**

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: **5.1.2.0.302**
- Control Plane Software Version: **5.1.2.0.260**
- Data Plane Software Version: **5.1.2.0.302**
- AP Firmware Version: **5.1.2.0.373**

SZ100

- Controller Version: **5.1.2.0.302**
- Control Plane Software Version: **5.1.2.0.260**
- Data Plane Software Version: **5.1.2.0.64**
- AP Firmware Version: **5.1.2.0.373**

vSZ-H and vSZ-E

- Controller Version: **5.1.2.0.302**
- Control Plane Software Version: **5.1.2.0.260**
- AP Firmware Version: **5.1.2.0.373**

vSZ-D

- vSZ-D software version: **5.1.2.0.302**

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/software/2169-smartzone-5-1-2-mr2-gpb-proto-google-protobuf-image-for-gpb-mqtt

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		
		T305e		
		T305i		

NOTE
R750 AP is not supported in Japan for this release.

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.
H510 and T310C APs do not support PoE operating mode.

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 5.1	SZ 5.1.1	SZ 5.1.2
FastIron 08.0.80	Y	Y	N
FastIron 08.0.90a	N	Y	Y
Fastiron 08.0.91	N	Y	Y
Fastiron 08.0.92 *	N	N	Y

NOTE

Fastiron 08.0.92 * is planned to be released in December 2019.

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
Change Default Switch Group Behavior	5.1.2 and above	08.0.92 and above
ICX Wired Client Visibility	5.1.2 and above	08.0.92 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				

Unsupported Features for all 11ax AP's

1. ATF/BSSP
2. 160Mhz and 80+80Mhz
3. Spectrum Analysis
4. LACP (bonding of Eth1 and Eth0)

5. MESH

NOTE
The full scope of the 11ax features will be fully realized in subsequent software releases.

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 5.1.1 release notes are also applicable to this release.

NOTE
R750 AP is not supported in Japan for this release

Component	AP R730
Issue	SCG-84849
Description	At times false radar detection on DFS enabled channels causes AP R730 to change channel. User can expect to see one false detect per day per AP in a typical enterprise environment

Component/s	Wi-Fi Client AP R750
Description	Windows laptops with Intel wireless card do not show SSID of APs advertising 11ax capability in their scan report. Therefore, users cannot connect to any 11ax capable AP

Workaround	If users encounter any interoperability issue with AP operating in 11ax (default mode). AP can be re-configured via RKSCLI to operate in 11ac mode. This mode can stay persistent across reboots.
	`Use the below RKSCLI command to configure 5G radio to 11ac mode:`
	`set mode wifi1 11ac`
	`Use the below RKSCLI command to configure 2.4G radio to 11ng mode:`
	`set mode wifi0 11ng”`

Solution	Latest Intel wireless driver has addressed this problem and Ruckus recommends a driver upgrade. Refer to https://www.intel.com/content/www/us/en/support/articles/000054799/network-and-i-o/wireless-networking.html

Component/s	AP R750
Issue	SCG-105384
Description	Following QOS classification on R750 is not supported • Voice classification based on L2/L3/L4 • Voice/video classification based on VLAN • Voice/video classification based on dot1p

Component/s	AP R750
Issue	SCG-104362

Component/s	AP R750
Description	With 2.4g connected Chrome book running software version 71 and lower can cause low throughput issue on the radio

Component/s	AP R750
Issue	SCG-107270
Description	2.4Ghz air time utilization can go over 75% due to new reporting mechanisms, but this has no performance impact

Component/s	AP R750
Issue	SCG-105751
Description	Controller web user interface incorrectly always displays MCS Rate (Tx) as *zero (0)*

Component/s	AP R750
Issue	SCG-107013
Description	Speedflex application on Wi-Fi client device when connected to R750 radio inaccurately shows uplink speed is lower than downlink speed

Component/s	AP R750
Issue	SCG-93197
Description	Airtime details tab does not show up for R750 in the controller

Component/s	AP R750
Issue	SCG-106484
Description	Controller web user interface incorrectly displays radio type as *an/ac/ax* instead of *a/n/ac/ax* for Wi-Fi 6 connected clients

Component/s	AP R750
Issue	SCG-108833
Description	Reducing power in the web user interface by more than -10 dB causes the transmit power to reduce even further
Workaround	Do not reduce power more than -10 dB

Component/s	AP R750
Issue	SCG-107712
Description	When the countries of Bangladesh, Bahrain, Costa Rica, El Salvador are selected, allowing the channelization to be *Auto* or *80MHz* in the Zone can cause issues in the R750 behavior
Workaround	For the above countries, select channelization at the zone level or AP level where R750 will be deployed explicitly to *Auto* or *20MHz*to make sure this issue does not occur

Component/s	AP R750
Issue	SCG-109216

Component/s	AP R750
Description	R750 Historical Client Connection Diagnostic (HCCD) fails to create *CCD_REASON_AUTH_FILTERED_BY_ACL* log when L2 ACL is configured.

Component/s	AP R750
Issue	SCG-105847
Description	AP PoE interface fails to connect when the switch port is set to 100-full duplex speed
Workaround	It is recommended to set the configuration to auto negotiation

Component/s	AP
Issue	SCG-107433
Description	C-Band channels 169 and 173 are blocked when changing channel width mode from 80 to 20 MHz by RKSCLI for outdoor AP T310d

Component/s	AP
Issue	SCG-104614
Description	Console port has LEDs meant for Ethernet port

Component/s	AP
Issue	SCG-104603
Description	The LED status is displayed as red with slow blinking when AP D124 was managed by the controller

Component/s	AP
Issue	SCG-104650
Description	802.11r Fast BSS Transition association fails with Windows 10 and Intel adapter 7265 (driver : 19.51.18.1) and Windows 10 and Intel 11ac 8260

Component/s	AP
Issue	SCG-105750
Description	Get station WLAN statistics under Ruckus CLI is missing *tx_kbps* statistics

Component/s	AP
Issue	SCG-106434
Description	Remote IP address output is empty on RKSCLI when executing the AP capture from the controller web user interface for capture mode as stream to wire shark

Component/s	AP
Issue	IOTC-2592
Description	IOT fails to detect and apply the 40Mhz channel width for the bluetooth coexistence in R750 AP

Component/s	AP
Issue	SCG-94006
Description	Using EAP-SIM profile Sony Xperia Z5, Sony Xperia Z3, LG G3 stylus do not connect to AP R730 successfully. This is due to client limitation

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

Component	AP
Issue	SCG-97876
Description	When the Windows Deployment Services (WDS) clients connects behind a Customer-Premises Equipment (CPE) in a series, the accounting stop is sent and No Change of Authorization (CoA) or Disconnect Message (DM) requests can be initiated to that CPE. But, if all WDS clients and CPE are attached to the AP at the same time, accounting stop is not sent for the CPE

Component	AP
Issue	SCG-105318
Description	When only Customer-Premises Equipment (CPE) connects with the AP and if a client behind it is not connected, then CoA/DM for the CPE is still served and fails to be ignored

Component	AP
Issue	SCG-105851
Description	AP loose the IP address and goes offline when downgrading the AP firmware from release 5.1.2 to 3.6.1 from AP Zone

Component	AP
Issue	SCG-109306
Description	Split tunnel feature does not work when AP is in dual zone

Component	AP
Issue	SCG-106272
Description	Modification of client certificates results in RADIUS process restart

Component	AP
Issue	SCG-109262
Description	AP initiates accounting on/off message when using WLAN edit option but without saving any modifications to existing WLAN and the Radius vendor specific attribute profile is associated to the WLAN

Component/s	Control Plane
Issue	SCG-109040

Component/s	Control Plane
Description	TACACS and test AAA server connection is successful though it is mapped to an incorrect service

Component/s	Control Plane
Issue	SCG-107101
Description	Accounting test AAA server with TLS enabled does not check Client Certificate or CN/SAN or OCSP in the received certificate. Test AAA with TLS is only for checking the reachability of the RadSec server

Component/s	Control Plane
Issue	SCG-106932
Description	Accounting ON/OFF is a proprietary feature so this is not supported for TLS handshake

Component/s	Control Plane
Issue	SCG-106322
Description	RAC fails to match UTP identifier when the user role is modified under authentication profile

Component/s	Control Plane
Issue	SCG-98894
Description	Upgrade from 3.6.0.3.290 is not supported for AP, controller or data plane due to: 1. Change in *XIMG* format for controller or data plane image to be in compliance with CC 2. Increase in SSH key sizes on AP, controller to be in compliance with CC. An intermediate image will be provided to enable customers to migrate from 3.6.0.3.290 to 5.1.2

Component/s	Control Plane
Issue	SCG-101649
Description	RAC fails to send the dynamic VLAN from role to the AP

Component/s	Control Plane
Issue	SCG-93304
Description	ACL in UTP policy will not take effect in Express Wi-Fi WLAN whereas ARC policy and URL filtering in UTP policy will work without any issue

Component/s	Data Plane
Issue	SCG-103688
Description	Created tunnel WLAN could trigger the alarm of data plane configuration update failed

Component	Switch Management
Issue	SCG-109929

Component	Switch Management
Description	When ICX7150-C12 and ICX7150-C10ZP are placed in one switch group the deployed VLAN tags or untags the ports for these two models under the same group level, which causes an error since the controller fails to distinguish these two models
Workaround	It is recommended to configure the two models in two different groups

Component/s	System
Issue	SCG-107110
Description	Controller does not prompt to change the password on first login to FIPS/JITC
Workaround	As per the JITC guidance document as soon as the password complexity is enabled, the administrator of last resort or the default super administrator must change their password

Component/s	System
Issue	SCG-104680
Description	Due to Rogue policy naming rule, the name cannot be the same and the controller cannot clone the Rogue policy with the duplicate name
Workaround	It is recommended that the user creates the Rogue policy

Component/s	System
Issue	SCG-106985
Description	OCSP (Online Certificate Status Protocol) IP address in server certificates validates first for CAC/PIV (Common Access Card/Personal Identity Verification Card) login where as user interface configured OCSP server will be validated in system IPSEC configuration
Workaround	Administrator should make sure the web interface is configured and details in certificates should be the same otherwise it will cause the discrepancy

Component/s	System
Issue	SCG-106541
Description	CAC (Common Access Card) or PIV (Personal Identity Verification Card) configuration is not available for MVNO account

Component/s	System
Issue	SCG-106752
Description	CAC (Common Access Card) user login fails irrespective of user role password expiry in the controller
Workaround	It is recommended to have separate security profile accounts for CAC/PIV (Personal Identity Verification Card) users and not to enable password expiry for these users

Component/s	System
Issue	SCG-108894
Description	Mismatch in protocol type in primary and secondary configuration as the controller AAA server always takes the primary protocol type
Workaround	The same protocol type should be configured on both primary and secondary AAA server configuration

Component/s	System
Issue	SCG-108213
Description	Authentication AD server fails to return non Ruckus WSG (Wireless Service Gateway) user information
Workaround	Only one Ruckus WSG user can be set on AAA server. Multiple roles should not be mapped

Component/s	System
Issue	SCG-109354
Description	In the controller AAA admin configuration for RADIUS with primary and secondary configuration the *ngnx* engine has a timeout for retry requests that are greater than 60 seconds
Workaround	Configure the request timeout to be less than 60 seconds

Component/s	System
Issue	SCG-40383
Description	The controller may be unable to renew its DHCP server-assigned IP address, which may cause all controller services to go down
Workaround	It is highly recommended to assign static IP addresses to the controller's interfaces

Component/s	System
Issue	SCG-105633
Description	Last two column headers are missing when historical client statistics log is exported as a CSV file

Component	System
Issue	SCG-105741
Description	Nexus 5x clients may not be able to connect using SIM authentication profile if the EAP SIM attributes are *AT_VERSION_LIST* and *AT_FULLAUTH_ID_REQ*

Component/s	UI/UX
Issue	SCG-100495
Description	Option button fails to display when change the Geo-Redundancy mode from active-standby to active-active

Component	UI/UX
Issue	SCG-104246
Description	Legacy known issue when the SZ time is moved to backward than current controller time

Component	UI/UX
Issue	SCG-104742
Description	Change the password through configuration setting does not provide the old password for comparing the change in password characters

Component	UI/UX
Workaround	1. Disable updating self-password by modifying the administrator account page 2. Update self-password through the change password page of account setting

Component	UI/UX
Issue	SCG-105302
Description	The entry list of the controller administrative on the web user interface page may not sufficiently be displayed when the browser zoom (Mozilla Firefox or any other browser) is above 90 percent due to the current design limitation
Workaround	Re-configure the zoom-level of the browser to below 90 percent.

Component/s	UI/UX
Issue	SCG-107500
Description	While creating Zone or AP Group the scroll bar does not work properly at times
Workaround	Make sure that the screen height should be greater than 570 pixels

Component/s	UI/UX
Issue	SCG-106659
Description	SpeedFlex wireless performance test from client web user interface fails with the error, *SmartZone is not responding to the SpeedFlex request. Verify the testing device is connected, and then try again* though the client is connected

Component/s	UI/UX
Issue	SCG-105519
Description	On the AP page, some columns that have the option to sort fail to sort

Component/s	UI/UX
Issue	SCG-105451
Description	Default AP Group entry did not show up within that AP Zone as soon as a new AP Group was created

Component/s	UI/UX
Issue	SCG-109646
Description	Rogue client table displays AP MAC(BSSID) in SSID field

Resolved Issues

The following are the resolved issues related to this release.

Component	AP
Issue	ER-7429
Description	Resolved an issue where AP create tunnel failed because SFP port did not initialize in NSS model with AP T710 plugged to SFP port

Component	AP
Issue	ER-7426
Description	This fix will stop the *send interim* report when the configured interval is zero

Component	AP
Issue	ER-7399
Description	Resolved an issue where AP failed to connect to the data plane due to *fail to authenticate*

Component	AP
Issue	ER-7395
Description	Resolved an issue where 802.1x clients failed to login to the local data base authentication

Component	AP
Issue	ER-7391
Description	Resolved an issue where HTTP redirection failed when it is blocked using URL filtering

Component	AP
Issue	ER-7379
Description	Resolved an issue where the AP Client SSID did not encode as UTF-8

Component	AP
Issue	ER-7331
Description	Resolved an issue in rogue AP detection where certain SSIDs were wrongfully classified as rogue SSID.

Component	AP
Issue	ER-7304
Description	Resolved an issue where AP SNMP could not get the updated device name

Component	AP
Issue	ER-7286
Description	Resolved an issue where R710 APs showed two MAC addresses and R720 APs showed three MAC addresses on switch port when NSS offload was enabled

Component	AP
Issue	ER-7282
Description	Resolved an issue where resubmitting DHCP NAT HN configuration with DWPD (drive writes per day) would override model specific options on gateway APs.

Component	AP
Issue	ER-7276
Description	Resolved an issue where Smart Monitor option failed to be enabled on each AP configuration

Component	AP
Issue	ER-7261
Description	Resolved an issue where AP could not move from Staging Zone with the option *wlanService50Enabled* as true by Public API

Component	AP
Issue	ER-7260
Description	The issue resulted from a NULL pointer encountered at Mesh mode AP, and AP ended in reboot. By checking the NULL point resolves the issue

Component	AP
Issue	ER-7259
Description	The issue is that R300/R500 APs in many aspect violates the DHCP backoff Algorithm described in RFC 2131. The resolution is that the existing design has been made compliant to RFC 2131, section 4.1

Component	AP
Issue	ER-7252
Description	Resolved an issue where AP rebooted with kernel panic reason

Component	AP
Issue	ER-7247
Description	Resolved an AP issue with *Singapore* country code where DFS channels were not listed in the supported channel list for certain AP models

Component	AP
Issue	ER-7204
Description	Resolved an issue where MAP randomly disassociated from RAP using ChannelFly

Component	AP
Issue	ER-7079
Description	Resolved an issue where excessive RPM had caused the error *wsgclient/timezone value too big* in support file

Component	AP
Issue	ER-7047
Description	Resolved an issue where the CSV header was missing on FTP statistics

Component	AP
Issue	ER-6857
Description	Resolved an issue where AP (R710 or R720) sent keepalive with MAC address of Ethernet 0 rather than bridge 0 when offload was enabled

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

Component	AP
Issue	ER-6461
Description	Resolved an issue where AP broadcasted in WLAN even though if WLAN scheduler was set to *Always Off*

Component	AP
Issue	SCG-104967
Description	Resolved an issue where the AP failed to login after the AP joined the staging zone for more than 12 hours

Component	AP
Issue	SCG-104323
Description	Resolved an issue where client data rate in client health tab did not show the correct downlink rate

Component	AP
Issue	SCG-101202
Description	Resolved an issue where flows failed to get tagged with ARC- RL and Qos markings for the application such as Google video

Component	Control Plane
Issue	ER-7204
Description	Resolved an issue where duplicate AP MAC address were in the ES and caused the SCI data display failure

Component	ARC
Issue	SCG-104145
Description	Resolved an issue where at times, YouTube detection failed for iPAD with iOS 12.2, iPhone 12.1.4 and MacBook Air 10.14.4. f.

Component	ARC
Issue	SCG-103307
Description	Resolved an issue where Amazon music and Pokemon game failed to get denied as per the ARC configured policy

Component	CLI
Issue	SCG-103274
Description	Resolved an issue where a user can now modify vSZe network setting on CLI

Component	CLI
Issue	ER-7145
Description	Resolved an issue where the set password by CLI *config-support-admin* function was displayed in some logs

Component	Control Plane
Issue	ER-7410
Description	Resolved an issue where the guest pass export data time was not synchronized with the web user interface time

Component	Control Plane
Issue	ER-7365
Description	Resolved an issue where the Radius proxy process crashed while processing third party VSAs with identifier one from AAA server during authentication procedure

Component	Control Plane
Issue	ER-7358
Description	Resolved an issue where the SZ100 could not change DNS server and returned the error an value is null

Component	Control Plane
Issue	ER-7285
Description	Resolved an issue where few of the AP zones created using the Zone template could not be deleted because of the incorrect creator UUID in the AP zone

Component	Data Plane
Issue	ER-7415
Description	Resolved an issue where a user lost Internet access suddenly on tunneled WLANs

Component	Data Plane
Issue	ER-7254
Description	Until this issue was fixed, the SZ300 only accepted the STP packets when the whole destination MAC address, 01:80:C2:00:00:00, was present in BPDU (Bridge Protocol Data Units)packet. However, for any other destination MAC address (e.g. 01:80:C2:00:00:08), the BPDU packet will be dropped. The fix will let data plane handle all BPDU type packets with last octet of MAC address to be of any value (e.g. 01:80:C2:00:00:XX)

Component	Switch Management
Issue	SCG-103623
Description	Resolved an issue where ICX switch (ICX 8.0.90a) failed to delete the TACACS+ and Radius AAA servers when pushed from the controller if SNMP query was not enabled in the switch

Component	Switch Management
Issue	ER-7242
Description	Resolved an issue where switch configuration backup failed due to unclosed Telnet connections

Component	System
Issue	SCG-103962
Description	Resolved an issue where DNS address of IPv4 or IPv6 become strange where only IPv6 was displayed on modification of IP address of data interface

Component	System
Issue	ER-7508
Description	Resolved an issue where FQDN (fully qualified domain name) validation failed for valid domain name in Traffic Class configuration

Component	System
Issue	ER-7490
Description	Resolved an issue where: • Change Zone, AP Group, and AP LACP configuration to *Keep AP Setting* by default • When the controller upgrades from 5.1.1 to 5.1.2, Zone LACP configuration option of *Disabled* will be migrated to *Keep AP Setting*

Component	System
Issue	ER-7434
Description	Resolved an issue where Radius proxy process crashed while processing third party VSAs with identifier one from AAA server during accounting messages

Component	System
Issue	ER-7421
Description	Resolved an issue due to a typo on the switch firmware upgrade window

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

Component	System
Issue	ER-7211
Description	When configuring an AP zone on a SZ100, which reporting an error *Unable to update configuration of AP Zone*, it has been fixed by ensuring that an error handling is properly done in a scenario where ethernet port related data is not available in data base at that instance

Component	System
Issue	ER-7066
Description	Resolved an issue where duplicate entries are found in *client.csv*file

Component	System
Issue	ER-6991
Description	Resolved an issue where SNMPD crashed frequently

Component	System
Issue	ER-6980
Description	Resolved an issue where when *Access&Core Separation* feature was enabled, and a static route was defined on Control Plane for Location Based Service, this traffic did not use the specified gateway

Component	Virtual SmartZone Data Plane
Issue	ER-7508
Description	Resolved an issue where AP RGRE tunnel failed to form because SZ100-D did not enable MTU probing on the Linux server

Component	Zone Director
Issue	ER-6248
Description	Resolved an issue that Rogue Device reporting does not work properly when SSID name is configured as a none English name

Upgrading to This Release

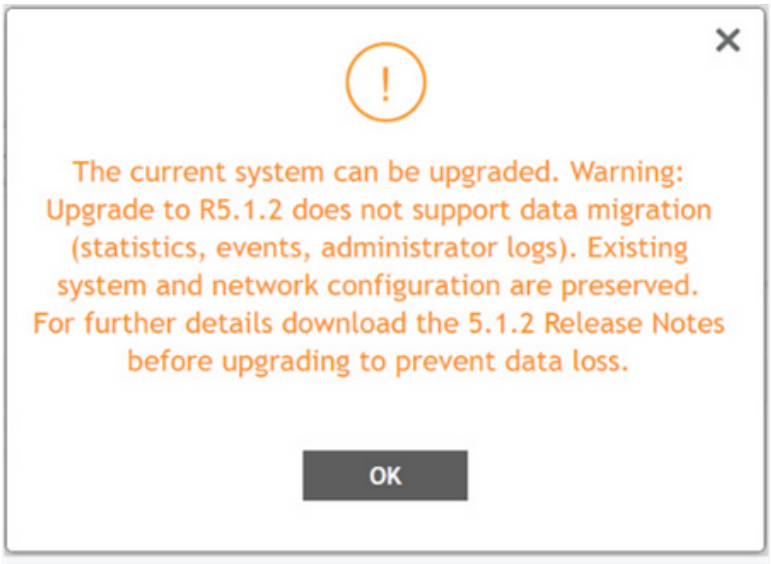
Before Upgrading to This Release

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 or 5.1.1 to 5.1.2 is supported.

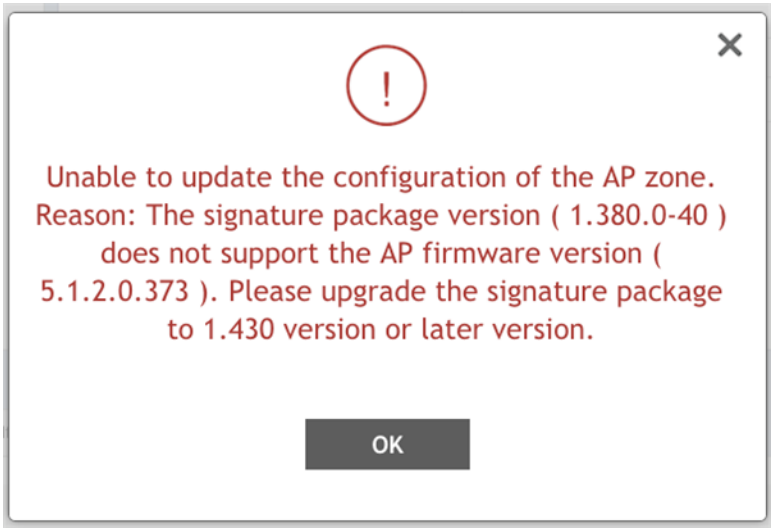
CAUTION
Data migration is not supported if system upgrades from release 3.6.0 or 3.6.1 or 3.6.2 to release 5.0, 5.1 5.1.1 or 5.1.2 by SmartZone (SZ) release 5.0, 5.1, 5.1.1 and 5.2 upgrade. Existing system and network configuration is preserved, but data such as status and statistics, alarms or events, administrator logs, and mesh uplink history is not migrated to the new release. Contact Ruckus support for concerns or additional clarifications. [SCG-73771]

- 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 or 5.1.1 releases can be upgraded to 5.1.2 release.
- When upgrading to the release 5.1.2 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 APs

AP DPI feature uses an Application Signature Package that in general it can be optionally updated when a new version is available. But in this case, previous packages are not compatible with 5.1.2 AP firmware, and upgrading zone firmware is blocked until the corresponding signature package (**RuckusSigPack-v2-1.430.1.tar.gz**) is installed.



Do follow this mandatory process before upgrading AP zone firmware:

1. Download Signature package by visiting the Ruckus support site https://support.ruckuswireless.com/software/2194-smartzone-5-1-2-sigpack-1-430-1-application-signature-package
2. Manually upgrade the signature package by navigating to **Services & Profiles** > **Application Control** > **Signature Package**. (more details can be found in Administrator Guide, in section *Working with Application Signature Package*)

Once this is done, AP zones can be upgraded. **[SCG-108730]**

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.
  6. Disable the secondary port from the switch.

Virtual SmartZone Required Resources

Hypervisor Hardware Performance Requirements

vSZ requires enough hardware resources to sustain the service. vSZ cannot support deployment in low performance hypervisor.

- vSZ needs to be deployed on dedicated hardware resource to avoid different VM instance grabbing CPU or IO resources, which can impact vSZ stability in a hypervisor, especially in a scenario where thousands of APs per node are deployed.
- vSZ needs to reach both CPU and IO requirement. Measure the hypervisor hardware performance before deploying vSZ.
- Disks IO is most important in vSZ cluster. Disk IO is the slowest subsystem in a server, which means that write-heavy clusters can easily saturate their disks, which in turn become the bottleneck of the cluster. Avoid network-attached storage (NAS). People routinely claim their NAS solution is faster and more reliable than local drives. NAS is often slower, displays larger latencies with a wider deviation in average latency, and is a single point of failure.
- Virtual Disk - Preallocated, Eager Zeroed and Fixed Size are required to provide good performance and low latency for IO.

  Avoid using **Thin Provision Lazy Zeroed** or **Dynamic Expanding** to impact IO performance. If virtual platforms need it, as a workaround, skip the following setup validation which involves a risk user must understand. High AP deployment environment requires high IO performance.

```
CLI # debug
CLI(debug)# debug-tools
(debug tool-set) system $ use sz
(debug tool-set) sz $ skip-setup-capability-check
```

The following table lists the minimum network requirement for the controller's cluster interface.

TABLE 6 Minimum Network Requirement

Model	SZ300	vSZ-H	SZ100	vSZ-E
Latency	85ms	68ms	77ms	77ms
Jitter	10ms	10ms	10ms	10ms

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 7 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 8 vSZ High Scale required resources

AP Count Range		vCPU	RAM	Disk Size	Disk IO Requirement	Preserved Events	Concurrent CLI Connection	Resource Level
From	**To**	**Logic Processor** [1][2]	**GB** [1]	**GB**	MiB/s	**Max**	**Max** (per node not per cluster)	
10,001	30,000	24	48	600	45	3 M	4	8

TABLE 8 vSZ High Scale required resources (continued)

AP Count Range		vCPU	RAM	Disk Size	Disk IO Requirement	Preserved Events	Concurrent CLI Connection	Resource Level
	20,000							
5,001	10,000	24	48	600	45	3 M	4	7
2,501	5,000	12	28	300	30	2 M	2	6.5
1,001	2,500	6	22	300	25	1.5 M	2	6
501	1,000	4	18	100	20	600 K	2	5
101	500	4	16	100	15	300 K	2	4
1	100	2-4[2]	13	100	15	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 9 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 10 vSZ Essentials required resources

AP Count Range		vCPU	RAM	Disk Size	Disk IO Requirement	Preserved Events	Concurrent CLI Connection	Resource Level
From	**To**	**Logic Processor**	**GB** [1]	**GB**	MiB/s	**Max**	**Max** (per node not per cluster)	
1025	3,000	8	18	250	20	10 K	2	3
	2,000							
501	1,024	8	18	250	20	10 K	2	2
101	500	4	16	100	15	5 K	2	1.5
1	100	2-4[2]	13	100	15	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] - For trial and development deploy purposes only.
[3] - 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).

Public Cloud Platform - Instance Resource Type

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 11 vSZ High Scale

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

TABLE 12 vSZ High Scale

AP Count Range		Minimum vCPU	Minimum RAM	Minimum Disk Size	Recommended Machine Type for AWS	Recommended Machine type for GCP	Recommended Machine type for AZure	Disk IO Requirement	Resource Level
From	**To**	**Logic Processor**	**GB [1]**	**GB**					
10,001	30,000	24	48	600	c4.8xlarge	Custom Machine Type w/ Skylake or later. Follow the vCPU/ Memory number based managed AP number.	F32s_v2	45	8
	20,000								
5,001	10,000	24	48	600	c4.8xlarge		F32s_v2	45	7
2,501	5,000	12	28	300	c4.4xlarge		F16s_v2	30	6.5
1,001	2,500	6	22	300	m4.2xlarge		D8s_v3	25	6
501	1,000	4	18	100	r4.xlarge		E4s_v3	20	5
101	500	4	16	100	m4.xlarge		D4s_v3	15	4
1	100	2-4[3]	13	100	r4.large		DS11_v2/ D4s_v3	15	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 13 vSZ Essentials required resources

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

TABLE 13 vSZ Essentials required resources (continued)

AP Count Range		Maximum Clients	Nodes per Cluster	AP Count per Node	Maximum Switch (w/o AP)
1	100	2,000	1-2	100	20

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

TABLE 14 vSZ Essentials required resources

AP Count Range		Minimum vCPU	Minimum RAM	Minimum Disk Size	Recommended Machine Type for AWS	Recommended Machine type for GCP	Recommended Machine type for AZure	Disk IO Requirement	Resource Level
From	**To**	**Logic Processor**	**GB** [1]	**GB**		Custom Machine Type w/ Skylake or later.			
1025	3,000	8	18	250	m4.2xlarge		D8s_v3	20	3
	2,000								
501	1,024	8	18	250	m4.2xlarge	Follow the vCPU/ Memory number based managed AP number.	D8s_v3	20	2
101	500	4	16	100	m4.xlarge		D4s_v3	15	1.5
1	100	2-4[3]	13	100	r4.large		DS11_v2/ D4s_v3	15	1

Maximum Supported AP and Switch Management

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

SmartZone 5.1.2 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 x 1) + (100 x 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 x 1) + (10 x 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 15 AP and Switch resource table for 1 and 2 nodes

Profile	1 and 2 Nodes				1 or 2 Nodes
Capacity	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 L7	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 16 AP and Switch resource table for 3 and 4 nodes

Profile	3 Nodes					4 Nodes				
Capacity	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 17 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
	5.1.1.0.598

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.

TABLE 18 Upgrade matrix and backward compatibility

Controller Platforms (SZ100, SZ300, Virtual SmartZone and Virtual Data Plane) Upgrade/Restore Matrix	
Base build	Target Build (SZ 5.1.2)
SmartZone 3.6	Yes
SmartZone 3.6.1	Yes
SmartZone 3.6.2	Yes
SmartZone 5.0	Yes
SmartZone 5.1	Yes
SmartZone 5.1.1	Yes

Switch Backward Compatibility Matrix	
Target Build (SmartZone 5.1.2)	Switch Version
SmartZone 5.1.2	8.0.90
	8.0.91
	8.0.92*

NOTE
Switch version 8.0.92* is planned to be released in December 2019.

NOTE
Upgrade from 3.6.0.3 FIPS (GA) to 5.1.2 is not supported.

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 5.1.2. 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 5.1.2, the AP Zone firmware remains the same.

NOTE
The changes made with new firmware version is automatically reverted when downgrading to old firmware version, as the changes might contain the configuration that is not supported by old firmware version.

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 5.1.2:

- 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
5.1.1 > 5.1.2	5.1.1, 5.1.2

All other AP firmware releases that were previously available on the controller will be deleted automatically. For example: retain after the upgrade will be 5.1.2.

- 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

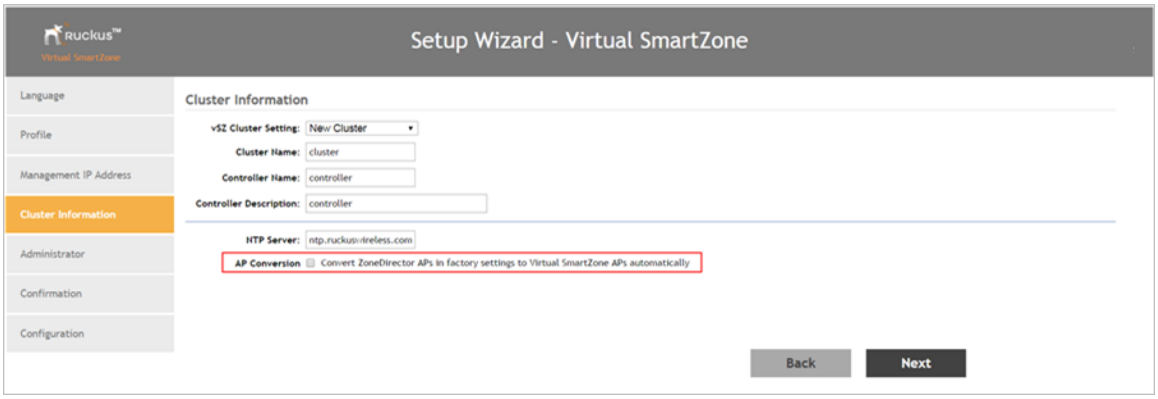
You can convert standalone ZoneFlex APs (those that are not managed by ZoneDirector) in factory default configuration to be managed by a SmartZone controller.

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



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

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