RELEASE NOTES

# Ruckus SmartZone 5.1 Release Notes

## Supporting SmartZone 5.1

*Part Number: 800-71940-001 Rev H*
*Publication Date: October 2019*

# Contents


**Document History** ..... **5**

**New Features and Changed Behavior** ..... **7**

New Features ..... 7

ICX Switch Management ..... 7

Cluster Geo-Redundancy Phase3 ..... 7

IPv6 Support ..... 8

GDPR Enhancements ..... 9

VMware vSphere (ESXi) 6.7 Support ..... 9

AP M510 Enhancements ..... 9

AP DPI Engine ..... 9

SCI Data Enhancements ..... 9

URL Filtering Enhancements ..... 10

AP Split Tunneling ..... 10

AAA Admin Enhancements ..... 10

Rogue AP Enhancements ..... 10

Captive Portal Detection and Suppression ..... 10

Increased DPSK Scale ..... 11

Client Isolation Redesign ..... 11

Anti-spoofing ..... 11

Ekahau Blink and Aeroscout RTLS (Real Time Location Systems)Support ..... 12

SmartZone100 Data Plane Appliance ..... 12

vSZ-D Statistics Enhancement ..... 12

Adaptive Client Load Balancing ..... 12

Additional Enhancements ..... 13

Pre-paid Wi-Fi ..... 13

Changed Behavior ..... 14

Geo Redundancy ..... 14

**Hardware/Software Compatibility, Supported AP Models and Switches** ..... **17**

Overview ..... 17

Release Information ..... 17

SZ300 ..... 17

SZ100 ..... 18

vSZ-H and vSZ-E ..... 18

vSZ-D ..... 18

SZ Google Protobuf (GPB) Binding Class ..... 18

**Switch Management License** ..... 18

Supported and Unsupported Access Point Models ..... 19

Supported AP Models ..... 19

Unsupported AP Models ..... 20

Supported Switch Models ..... 20

**Caveats, Limitations, and Known Issues in this Release** ..... **21**

Bonjour Gateway Limitations ..... 53

**Resolved Issues** ..... **55**

**Upgrading to This Release** ..... **63**

Before Upgrading to This Release ..... 63
Data Migration Recommendations ..... 64
Upgrade Considerations ..... 64
Virtual SmartZone Required Resources ..... 65
Maximum Supported AP and Switch Management ..... 67
SmartZone Upgrade Paths ..... 67
Supported SmartZone and Data Plane Platform ..... 68
Multiple AP Firmware Support in the SZ100/vSZ-E/SCG200-C/SZ300/vSZ-H ..... 69
Up to Three Previous Major AP Releases Supported ..... 69
EoL APs and APs Running Unsupported Firmware Behavior ..... 70
**Interoperability Information ..... 71**
AP Interoperability ..... 71
Enabling ZoneFlex AP Discovery to a SmartZone Controller Using DHCP Option 43 ..... 71
Enabling ZoneFlex AP Discovery to a SmartZone Controller Using DNS ..... 71
Redeploying ZoneFlex APs with SmartZone Controllers ..... 72
Converting Standalone APs to SmartZone ..... 72
ZoneDirector Controller and SmartZone Controller Compatibility ..... 73
Client Interoperability ..... 73

# Document History

| Revision Number | Summary of changes | Publication date |
|---|---|---|
| E | Added a note on *VMware VMotion*in the Release Information section | February 12, 2019 |
| F | Added caveat **SCG-101748** | March 27, 2019 |
| G | Added a note on M510 support | June 10, 2019 |
| H | Modified text for SCG-49689 | October 14, 2019 |

# New Features and Changed Behavior


- New Features ..... 7
- Changed Behavior ..... 14


# New Features

This section provides a high-level overview of several key features that are introduced in the SmartZone (SZ) software release 5.1.

The SZ release 5.1 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.

> **NOTE**
> For detailed descriptions of these features and configuration help, refer to the respective 5.1 documentation guides available at https://www.ruckuswireless.com

## ICX Switch Management

The 5.0 release of SmartZone adds management and monitoring support for Ruckus ICX 7000 switches. Similar to wireless control and management of APs, the SmartZone will begin providing management functionality for switches. The first step focuses on monitoring, status, usage visibility, and some basic management, including configuration backups and firmware management. In this release, we are taking the next step towards a full-featured wired/wireless integration plan.

For this release, the following functionality is provided:

- **ICX switch management licensing**
- **Improve scaling limits**
- **ICX Client Troubleshooting** - Allows users to locate the wired or wireless client within a given network using the MAC address. AP to switch connectivity information is also presented in the case of wireless clients.
- **ICX Custom Events** - Custom Events enables creation of threshold based events or alarms against CPU and memory utilization. In addition, text patterns contained in the existing ICX Syslogs can also be used to define these Custom Events.
- **Remote Ping and Traceroute** - Simplifies checking connectivity of switches to external networks. PING or Traceroute can be initiated to an external network from the switch without the user having to login to the switch.

## Cluster Geo-Redundancy Phase3

The SZ Cluster Geo-Redundancy feature was introduced (Phase1) in the SmartZone 3.6.0 release and (Phase2) was introduced in the 5.0 release. Geo-redundancy addresses datacenter disaster recovery use cases for large customers, such as SPs and Large Enterprises. As such, it is only supported on the High-Scale SmartZone platforms, namely SZ300 and vSZ-H. It is not supported on SZ100 nor vSZ-E.

The functional highlights of Phase3 include:

1. (Legacy) Multi-cluster failover support
2. SZ300 clusters backup to vSZ-H cluster
3. vSZ-D support for Geo-Redundant vSZ-H clusters

4. License portability
5. GUI enhancements for better visibility of Geo-Redundancy status
6. Improve configuration restore operation time
7. API Enhancements

# IPv6 Support

Several IPv6 related enhancements have been carried out in this release

In an IPv6 network, hosts accomplish address resolution by sending Neighbor Solicitation (NS) message that asks the target node to return its link-layer address. NS messages are multicast to the solicited-node multicast address of the target address (TA). The target host returns its link-layer address in a unicast Neighbor Advertisement (NA) message. A single request-response pair of packets is sufficient for both the initiator and the target to resolve each other's link-layer addresses as the initiator includes its link-layer address in the NS. NS messages can also be used to determine if more than one node has been assigned the same unicast address with a process called Duplicate Address Detection (DAD). Ruckus supports DAD detection as a requirement for auto-configuration of IPv6 addresses.

Apart from NS and NA, there are another set of multicast messages being exchanged in a IPv6 network called Router Solicitation (RS) and Router Advertisement (RA). RA contain information, which is used by hosts to configure their interfaces. This information includes address prefixes, the MTU of the link and information about default routers. When an interface on a host comes up and an RA is received (either an unsolicited/periodic RA or a reply to a router solicitation), the host can configure an address on the interface by using the prefix and appending the EUI-64 identifier derived from the hardware address (mac address). The host can also choose a default router by examining the RA. The rest works automatically.

As NS, RS and RA messages are multicast and once received on AP Linux bridge, it will copy them to all the interfaces (WLANs and Ethernet) in a broadcast domain which unnecessarily creates too much airtime utilization. Apart from that, multicast frame in WLANs are unreliable and are sent with the minimal supported rates. They can be further delayed due to power saving mechanism usually enabled in APs.

To avoid unnecessary burden on the airtime utilization and other reasons mentioned above, Ruckus has implemented support of ND and RA proxy set up in AP. ND proxy maintains a mapping of IPv6 address and MAC addresses for each associated STA by snooping NS and NA messages. It updates the mapping when the IPv6 address of any of the associated STA changes. When IPv6 address being resolved with NS packet belongs to one of the associated STA (and also mapping is available in the cache) the ND proxy service responds on behalf of the STA (replies with an NA).

Similarly, RA proxy caches router information and replies on behalf of the router to a solicited RS. We are also trying to limit the number of RS and RA being propagated in a wireless medium by guarding them.

In Client Isolation (CI) there are three types of filtering: manual whitelisting, auto-whitelisting and hybrid for IPv4, IPv6 and dual stack networks (IPv6 & IPv4). The CI for IPv6 feature is to support Client Isolation auto-whitelist for IPv6 enabled clients in unicast and multicast scenarios.

In this release, Ruckus officially supports Portal-based WLAN UE with IPv6 address. Those WLANs include tunnel or non-tunnel WISPr, Web Auth, Guest Access, and HS2.0.

# GDPR Enhancements

To support requirements for GDPR (General Data Protection Regulation), we are adding several dimensions of admin account security and controls.

The following GDPR features are added.

- **GDPR Right To View** :
  - Search tool via API and CLI
  - Ability to store search output to an external FTP server
- **GDPR Right To Be Forgotten** :
  - Ability to delete PII (Personally Identifiable Information) data (by MAC address)
  - Ability to generate logs in case of PII delete

# VMware vSphere (ESXi) 6.7 Support

The vSZ-H and vSZ-E virtual appliances now support VMware vSphere ESXi 6.7

# AP M510 Enhancements

The following features are supported:

- **LTE Stats in SZ GUI**: Increased statistics are available under M510 in SZ GUI - RSCP/EcNO/SNR
- **GUI Enhancements to change the connectivity health check sites**: User can choose through GUI which sites to use for **connectivity** check
- **AP GPS Position display in Google Maps with Auto-refresh**: The M510 can be displayed on SmartZone GUI on maps with auto refresh functionality.

  **NOTE**
  M510 JP SKU is supported in release 5.1.1

# AP DPI Engine

In this release the AP DPI Engine has been updated to include the Qosmos DPI Engine. The following feature is now supported.

- L7 policy enforcement by App Category

# SCI Data Enhancements

Following additional data are now available for SCI.

- AP data for CPU, RAM and disk usage
- Report actual traffic transmit rate for AP and Client

# URL Filtering Enhancements

In this release, there are two major improvements.

1. **URL Filtering Blocked Page**: Wireless users accessing HTTP website in blocked categories are redirected to a blocked page hosted at the AP. This page clearly communicates the reason why the user is seeing the blocked page instead of the originally requested page.
2. **Robust and Granular Blocking with Latest DPI Engine**: URL filtering leverages new AP DPI engine to resolve several issues found in the past releases. Granular blocking is more pronounced with sites hosting a mix of allowed and denied categories on servers with same IP address. For example: *explicit.bing.net* can be blocked while allowing *bing.com/maps*

# AP Split Tunneling

In prior Ruckus WLAN architecture, users on a WLAN can either be all tunneled to a gateway/Ruckus data plane or Local Break Out (LBO) to AP's WAN interface. Such solution limits deployment options where customers require UE traffics on a WLAN to be able to do both LBO (connect to local printers) and tunnel (to office IT systems) at the same time. This feature is to address that and adding selective LBO/R-GRE/S-GRE tunneling capabilities for a UE on same WLAN.

Split Tunnel profile enabled on a WLAN enables users to access both local and tunnel network simultaneously. This is based on ACL's (Access Control List) mapped to Split Tunnel profile.

The ACL's mapped in Split Tunnel profile help AP to differentiate between local and remote traffic, and enables AP to use session ACL's to forward the corporate traffic destined for tunnel or local network.

# AAA Admin Enhancements

In this release, it is now possible to allow the administrator to assign AAA-authenticated administrators to a default SmartZone role without requiring any special attributes from the RADIUS server.

# Rogue AP Enhancements

In this release, to make Rogue AP Detection more efficient, we have introduced the three minutes quick report mechanism to speed the process of protecting the network ASAP, and Rogue AP Detection keeps updating the rogue information to the controller every 15 minutes, as before.

# Captive Portal Detection and Suppression

Android and iOS use some form of captive portal detection to detect whether or not they are behind a captive portal. iOS actually aggressively kicks the UE off from the network if it determines the captive portal login has not been completed. Usually these agents perform an HTTP request to particular domain and URL and verify that they receive an expected response. If they do not, they determine you are behind a captive portal.

This poses challenges for a service provider (that has a walled garden services that they would like their users to stay in while being authenticated) where a subscriber might have access to the walled garden, but the captive portal agent kicks you off the network since it cannot access its well-known URL. So, this feature implements a mechanism for captive portal detection suppression to solve the issue.

# Increased DPSK Scale

In this release the DPSKs supported on the SmartZone are increased as per the below table.

| DPSK Type | System Maximum | Domain Maximum | Zone Maximum | Comment |
|---|---|---|---|---|
| Unbound | 50,000 | 25,000 | 500 | Only Unbound DPSK in system. No Bound/Group DPSK |
| Bound | 50,000 | 25,000 | 25,000 | Only Bound DPSK in system. No Unbound/ Group DPSK |
| Group | 50,000 | 25,000 | 500 | Only Group DPSK in system. No Unbound/ Bound DPSK |
| **Total** | **50,000** | **25,000** | **25,000** | |

# Client Isolation Redesign

In 5.1 release the Client Isolation feature has been redesigned to aid in better scale and manageability. In addition, the following new capabilities are supported. Refer to the User Guide and Release notes to understand the network design implementations as well as caveats.

- Allows/drops multicast traffic between isolated clients
- Allows for adding wireless client MAC addresses to the manual whitelist
- Supports client isolation in VRRP (Virtual Router Redundancy Protocol) deployment
- Supports client isolation for IPv6 clients
- Supports auto/manual/hybrid whitelisting for IPv6
- Supports client isolation in HSRPv2 deployments

# Anti-spoofing

In 5.1 release, anti-spoofing feature support is introduced. The primary use case is to address ARP (Address Resolution Protocol) cache poisoning (or other ARP based attacks) in situations where client isolation is not enabled. For example, Universities allow wireless devices to communicate with each other but need protections in the network to avoid malicious behavior related to ARP cache poisoning. Following features are supported.

- Dynamic ARP inspection and protection
- Wireless and wired client support (DHCP clients only)
- One IP address to MAC address mapping
- DHCP request packet snooping is supported
- ARP and DHCP request rate limiting is supported

**Limitations specific to wired clients when anti-spoof is enabled**

- Anti-spoof feature will not be useful when enabled on WAN port (port providing access to network) of AP, since hosts connected to a network switch will not send DHCP packets through the AP and therefore the AP will not have MAC-IP binding for such hosts.

**Observations and Recommendations**

ARP rate limit value of 35 is recommended in general deployment to account for ARP request loss and prevent sluggishness in accessing network. The default 15 is also fine, given that during the experiments, most of the clients were fine to network access with the default value, and only a few clients faced sluggishness, which in turn was solved by setting the ARP rate limit value to 35. This recommended value could be further fine tuned to suit the needs to different network conditions and deployments.

# Ekahau Blink and Aeroscout RTLS (Real Time Location Systems)Support

Release 5.1 introduces RTLS support for Ekahau Blink and Aeroscout RTLS tags. A new sub-menu is created in the GUI in Services and Profiles named RTLS where these configurations can be managed. This feature can be enabled on a per Zone basis.

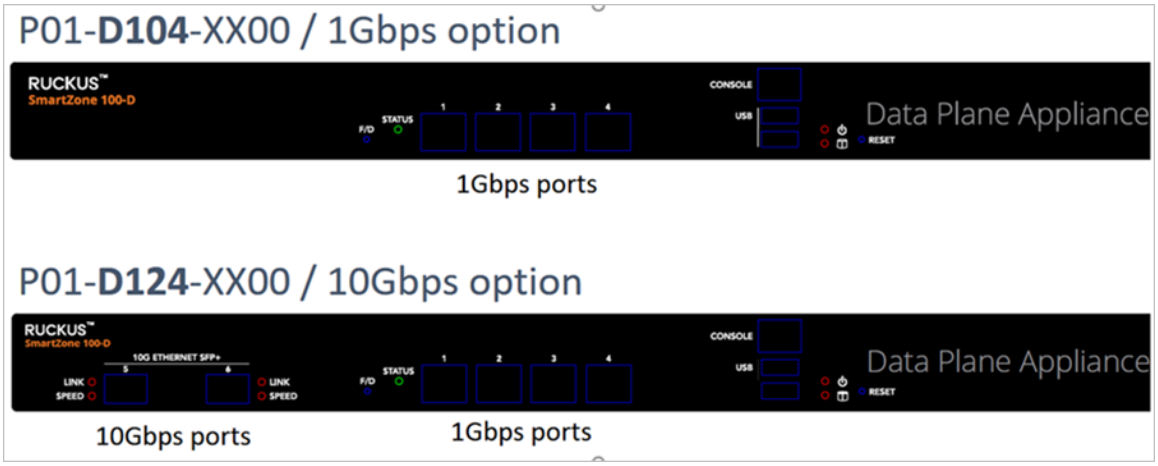
# SmartZone100 Data Plane Appliance

New data plane product is now available along with 5.1 release, SmartZone100 data plane (SZ100-D) appliance. In the same manner as well-known virtual data plane vSZ-D. The SZ100-D is managed by vSZ controller or cluster. SZ100-D is a lean IT friendly product.

SZ100-D uses the same data plane services licenses, such as L3 Roaming, Flexi-VPN, CALEA etc. From a deployment perspective, both SZ100-D and vSZ-D can be managed by the same vSZ cluster with up to 40 instances all together.

SZ100-D has two product SKUs

1. P01-D104-XX00 (1Gbps throughput)
2. P01-D124-XX00 (10Gbps throughput)




# vSZ-D Statistics Enhancement

In 5.1 release, there are new vSZ-D specific statistics that are enhanced and available in the vSZ GUI for better troubleshooting and network management.

# Adaptive Client Load Balancing

Adaptive Client Load Balancing (ACLB) is a natural evolution to the pre-R5.1 band balancing and client load balancing technology.

First, ACLB adds to the traditional station-count load metric with a throughput based **capacity metric**. The new capacity option is suited to balance the RF capacity of AP radios while providing optimal service to individual stations. Network administrator may now choose between these two methods to balance the Wi-FI network.

Second, ACLB adds complete support of 11k and BTM support to all load balancing features. This means all load balancing features use both passive (probe withholding) and active (BTM steering) techniques to balance load.

# Additional Enhancements

The following additional enhancements have been made in the 5.1 release:

- Application Whitelist
- Improvement of diagnostic snapshot performance
- Supports Optimized Connectivity Experience (OCE)
- GUI enhancements
- vSZ-D Backup/Restore enhancements
- CLI show command - *show running-config-all* Exports all configurations to the external FTP server
- Data retention time - The maximum data retention time on the controllers are:
  - High-scale products (vSZ-H/SZ-300) - One day
  - Low-scale products (vSZ-E/SZ-100) - 14 days

**NOTE**
This release does not support three interface mode in GCE.

# Pre-paid Wi-Fi

**Pre-paid Wi-Fi** feature supports pre-paid Wi-Fi architecture around existing Commercial Off-the-Shelf (COTS) network components. This service is provided for WISPr+MAC authentication WLAN. With this feature, volume based prepaid solution is provided to operators, where AAA server provides the required quota information to Ruckus AP/Controller, to consumers connected with XWF SSID provided by the vendor.

**Traffic Class Policy Object**: Using this feature provides a way to perform WISPr WLAN session control using RADIUS rather than the REST Portal API. A Traffic Class is a set of predefined access list based on Domains, IP Address or Subnets. When deploying a WISPr/Hotspot WLAN, it is possible to assign one or more Traffic Classes to a client (up to 4) via RADIUS Access-Accept or CoA along with a volume quota (Uplink+Downlink). For instance a traffic class can implement a Walled Garden. A special Traffic Class named *Internet* provides access to the whole Internet when assigned to a client (for instance after clearing authentication). Accounting of bytes and packets is done on a per Traffic Class basis. For packages purchased by end customer, the AAA server sends traffic class AAA attribute in Radius Access Request. Each traffic class is a set of predefined access lists based on Domains, IP addresses, Subnets. Each traffic class can be assigned a Quota (UL + DL or Unlimited).

**Token Based URL Enrichment**: Many nations have implemented tight regulations regarding exporting of Personal Identifiable Information out side the country physical borders. This feature provides a mechanism to replace the traditional redirect URL attributes, that include IP and MAC address information with a token provided during MAC address authentication in a WISPr/Hotspot WLAN.

**Internal Node**: In WISPr WLAN it is impossible for a subscriber portal to identify the context of a request if a client implicitly browses the portal URL (not as a result of a redirect). Configuring an Internal Node IP address that resides on the AP will allow the portal to redirect such request to that node IP address, resulting on the AP redirecting the client back to the portal (including the redirect parameters or token). Ruckus AP reports the quota consumption to AAA server and provides the required to captive

portal to purchase Internet usage or quota. It includes secured URL redirection, where user identification is encrypted while redirecting to external portal. Token exchanged while authentication, is signed with pre-shared key (SHA1 HMAC).

# Changed Behavior

## Geo Redundancy

The following are the changed behavior issues related to Geo Redundancy.

### *Active-Active Geo Redundancy*

1. For all active clusters in Active-Active geo redundancy to make sure configuration consistency between all clusters, it is recommended that only **One** cluster is enabled as *Schedule Configuration Sync*
2. The options *Schedule Configuration Sync* and *Configuration Schedule Backup* need to be set to a time gap longer than 20 minutes.
3. Active-Active type geo redundancy can only be enabled in same model clusters (SZ300 or vSZ-H)
4. Following configurations will be disabled after the configuration is restored in a target active cluster:
   - Configuration FTP export
   - Configuration schedule backup
   - Schedule configuration synchronization
5. After configuration restores in target active cluster, the user account that applies custom security may get locked. If an account is locked and unable to use in target active cluster, do unlock it before proceeding to the next step.

### *Active-Standby Geo Redundancy Enhancement*

1. vSZ-H can be the standby cluster while active clusters can either be SZ300 or vSZ-H
2. Following license types can only be applied to the standby cluster:
   - CAPACITY_AP_HA
   - SUP_SZ300_HA_EU
   - SUP_SZ300_HA_PTNR
   - SUPPORT_HA_EU
   - SUPPORT_HA_PTNR
3. Following license types are unable to be applied to standby cluster:
   - CAPACITY_AP
   - CAPACITY_AP_BUNDLED
   - CAPACITY_AP_DEFAULT
4. When the standby becomes the backup model of a certain active cluster, standby cluster leverages all the licenses from its backup active cluster except the license types mentioned in points 2 and 3
5. To enable Active-Standby geo redundancy, standby cluster should be able to access the control interface of active cluster through its own control interface

6. The interface number is not necessary the same between active and standby cluster
7. After configuration restores in target active cluster, the user account that applies custom security may get locked. If an account is locked and unable to use in target active cluster, do unlock it before proceeding to the next step

## *Data Plane Redundancy*

1. Only vSZ-D and SZ100-D are supported
2. In release 5.1, both Active-Active and Active-Standby geo redundancy support Data Plane failover mechanism
3. In Active-Standby geo redundancy, Data Planes automatically failover to standby cluster once active cluster is unreachable for a while and users can *rehome* all Data Planes and access points after active cluster is back in-service
4. In Active-Active geo redundancy, Data Planes automatically failover to target active clusters with round robin according to their priority once original active cluster is unreachable for a while. User can *switchover* Data Planes that already failed over to target active cluster fallback to original cluster after original active cluster is back in-service
5. The number of Data Planes that standby cluster or target active cluster can take over is still limited to Data Plane license number of that cluster

## *Access Point/Data Plane Switchover*

1. Supports Data Plane switchover in this release
2. Supports *Predefined Destination* in Active-Active geo redundancy
3. User can decide to retain or delete Access Point/Data Plane after switching over by choosing the option in the controller web interface
4. Access Points with following attributes are unable to switch over
   a. Firmware version older than 5.0.0.0.0

      AP mesh mode

# Hardware/Software Compatibility, Supported AP Models and Switches


- Overview....17
- Release Information....17
- Supported and Unsupported Access Point Models....19


## 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

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

**ATTENTION**
VMware VMotion is not supported.

### SZ300

- Controller Version: **5.1.0.0.496**
- Control Plane Software Version: **5.1.0.0.447**

- Data Plane Software Version: **5.1.0.0.496**
- AP Firmware Version: **5.1.0.0.595**

## SZ100

- Controller Version: **5.1.0.0.496**
- Control Plane Software Version: **5.1.0.0.447**
- Data Plane Software Version: **5.1.0.0.209**
- AP Firmware Version: **5.1.0.0.595**

## vSZ-H and vSZ-E

- Controller Version: **5.1.0.0.496**
- Control Plane Software Version: **5.1.0.0.447**
- AP Firmware Version: **5.1.0.0.595**

## vSZ-D

- vSZ-D software version: **5.1.0.0.496**

## 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

**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.

## Switch Management License

Switch management licences are now enforced from SmartZone release 5.1. Release 5.0 customers can manage switches from SmartZone without purchasing any Switch Management licenses (*part number L09-0001-SGCX*), if they upgrade to release 5.1 but 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.

# Supported and Unsupported Access Point Models

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

APs preconfigured with the SmartZone AP firmware may be used with 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.

When connecting solo APs running releases 104.x and higher, the LWAPP2SCG service running on the controller must be disabled. To disable the LWAPP2SCG service, log on to the controller's CLI, and then go to enable mode **config** > **lwapp2scg** > **policy deny-all**. Enter **Yes** to save your changes. > 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

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

**NOTE**
**M510 JP SKU is supported in release 5.1.1**

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

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

# Unsupported AP Models

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

**TABLE 2** Unsupported AP Models

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

# Supported Switch Models

This release supports the following Ruckus switch models running ICX FastIron software version 08.0.80 or higher.

**TABLE 3** Supported Switch Models

| | |
|---|---|
| 7150 | 7250 |
| 7450 | 7650 |
| 7750 | |

# Caveats, Limitations, and Known Issues in this Release

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

| Component/s | AP |
|---|---|
| **Issue** | SCG-101748 |
| **Description** | The upgrade to 5.1 enables AP certificate check by data plane, but the AP certificate is valid only for one year. This can cause the tunnel to go down as soon as the certificate validity expires.<br><br>**NOTE**<br>Clients using data plane for tunneling user traffic will have an impact. There is no Impact for LBO (Local Break Out) |
| **Workaround** | Apply the KSP to disable AP Certificate check by Data Plane<br><br>Visit the Ruckus support site to download and apply the KSP (https://support.ruckuswireless.com//software/1996-smartzone-5-1-ga-cluster-data-plane-certificate-check-patch-ksp) |

| Component/s | AP |
|---|---|
| **Issue** | AP-9989 |
| **Description** | APs will not be able resolve DNS queries and all functions related to DNS, **if (and only if)** management VLAN of the APs are configured other than default VLAN (vlan1). |
| **Impacted Areas/ Features** | Following features are impacted due to this issue, however, the extent of impact varies and depend on the feature configuration.<br>• DHCP-NAT<br>– Without per pool DNS (Domain Name System)configuration (Single AP, Multiple AP and Hierarchical)<br>– DWPD (Drive Write Per Day) (Single AP, Multiple AP case and Hierarchical Case)<br>• URL Filtering<br>• Wi-Fi Calling<br>• Pre-paid Wi-Fi<br>• Qosmos (DNS fallback)<br>• DNS based AP discovery<br>• WISPr (with external captive portal redirection)<br>• Generic impact on functions where AP uses it DNS configuration to resolve the DNS queries |
| **Workaround** | DNS configuration for the AP is not saved during the DHCP transaction in the *DHCP-ACK* for the non-default VLAN. As a workaround, DNS IP addresses on all the APs with non-default VLAN should be set manually using the below CLI command. You can also login to remote CLI from the controller user interface.<br><br>`set dns x.x.x.x`<br><br>or via remote CLI feature from the UI |

| Component/s | AP |
|---|---|
| **Issue** | SCG-95164 |
| **Description** | Mesh link flaps and reboots automatically after the controller is not reachable. This issue observed when the configuration is a manual uplink selection and the mesh state changes with auto selection<br><br>A Mesh AP which has ACS (Auto Cell Size) enabled will not reduce its Tx power (not to destabilize the Mesh tree), but it will exchange ACS information with its neighboring APs so that those neighboring APs can reduce Tx Power to help reduce interference |

| Component/s | AP |
|---|---|
| **Issue** | SCG-96444 |
| **Description** | AP fails to generate the accounting packets after VLAN ID is changed in WLAN |

| Component/s | AP |
|---|---|
| **Issue** | SCG-93473 |
| **Description** | AP R720 displays 80MHz channelization with channel 165 when it can only support 20 MHz on that channel |

| Component/s | AP |
|---|---|
| **Issue** | AP-9659 |
| **Description** | Fragmented packets are getting dropped by AP in the downlink direction with DHCPNAT |

| Component/s | AP |
|---|---|
| **Issue** | AP-8909 |
| **Description** | The default IP address currently used for IPv6 is *fc00::1/7* similar to 192.168.0.1 as IPv4. Changing the default IP address to an unique local address will be fixed in future release |

| Component/s | AP |
|---|---|
| **Issue** | AP-9049 |
| **Description** | Pinging with a hostname from an AP in an IPv6 zone prefers the IPv4 address rather than IPv6 address |

| Component/s | AP |
|---|---|
| **Issue** | AP-9319 |
| **Description** | For the traffic flows where the uplink and downlink ports used are different for example, TFTP, the split tunnel feature does not work |

| Component/s | AP |
|---|---|
| **Issue** | AP-9549 |
| **Description** | Split tunnel is not supported with portal redirection enabled WLANs, therefore the below combinations will not work.<br>• Split tunnel with WISPr<br>• Split tunnel with Web authentication |

| Component/s | AP |
|---|---|
| **Issue** | SCG-93034 |
| **Description** | AP does not try to join the data plane within the DP Group after the losing the tunnel, rather fails over to data plane on another data plane group<br>. |

| Component/s | AP |
|---|---|
| **Issue** | SCG-94395 |
| **Description** | IPv6 packets processing goes through a slow path and has performance limitation |

| Component/s | AP |
|---|---|
| **Issue** | SCG-89373 |
| **Description** | AP packet capture shows PHY type as *11n* under 802.11 radio information though the capture is for *11ac* mode. |

| Component/s | AP |
|---|---|
| **Issue** | SCG-92611 |
| **Description** | Ruckus LACP/LAG Implementation follows LACP 802.3ad specification where:<br>• LAG slaves must be configured at same port speed and duplicity<br>• Administrator user, enabling LAG must make sure that the above requirement is met before adding AP Ethernet ports as LAG slaves<br>• While LAG is ON, changing one or more slave port speed/duplicity is not supported and if it is done the AP will malfunction<br>• On AP R720, changing Ethernet port speed is not supported due to system limitation. AP ports must be configured in auto mode of operation to follow switch, speed and duplicity configuration |

| Component/s | AP |
|---|---|
| **Issue** | SCG-81497 |
| **Description** | R720 has limitation on interface eth1 where it is NOT able to update logical link state in on removal of physical link from port. The port is non-auto negotiating port. It will work in follow mode to switch side speed configurations (100/1000/2500 FD). Functionality is unaffected in presence of active link on eth1 port. |

| Component/s | AP |
|---|---|
| **Issue** | SCG-93183 |
| **Description** | AP R300 slows down considerably when both radios are enabled, along with kernel panic and does not respond to SSH requests. If the radios are disabled, the AP functions normal |

| Component/s | AP |
|---|---|
| **Issue** | SCG-94547 |
| **Description** | Client running latest IOS version 12 and MAC OS version 10.14 fails to establish TLS tunnel during EAP authentication with server supporting only TLS 1.0. Whereas, the same works fine if the server support higher TLS version like TLS 1.2 |

| Component/s | AP |
|---|---|
| Issue | SCG-94545 |
| Description | When APs are moved in a dual zone, the APs use IPv6 address for SSH tunnel formation but for GRE tunnel formation IPv4 address is used. Previously APs used IPv4 address for SSH and GRE tunnel formation in dual zone |

| Component/s | AP |
|---|---|
| Issue | ER-3433 |
| Description | When an AP is assigned the default static IP of 192.168.0.1 is rebooted, it is unable to establish a tunnel with the controller |

| Component/s | AP |
|---|---|
| Issue | ER-5493 |
| Description | Currently if AP-DHCP profile is enabled with DNS override, AP-DHCP profile settings take precedence. Workaround: Change the settings of AP-DHCP profile to reflect the same as DNS override, to override the issue |

| Component/s | AP |
|---|---|
| Issue | SCG-34299 |
| Description | If APs are discovering the controller on the network using DNS discovery and the DNS server address on the DHCP server is updated, solo APs will continue to use the previous DNS server address, which could result in their inability to discover the controller again on the network. Workaround: To resolve this issue, reboot solo APs after the DNS server address on the DHCP server is updated |

| Component/s | AP |
|---|---|
| Issue | SCG-34885 |
| Description | Solo APs are unable to discover the controller via Option 52. This is because DHCPv6 solicit messages from solo APs do not include Option 52 information |

| Component/s | AP |
|---|---|
| Issue | SCG-34981 |
| Description | If only Option 52 (no DNS server address) is configured on the DHCPv6 server, APs are unable to obtain the controller's IP address from the Option 52 information and, therefore, are unable to discover the controller on the network |

| Component/s | AP |
|---|---|
| Issue | SCG-43697 |
| Description | Based on the current design, the minimum rate limit per station is 100kbps. As a result, the total rate (station number * 100kbps) will be higher than the SSID rate limit -- this is design intent. For example, if the rate limit for downlink is 10Mbps for one SSID, when an AP has 200 STAs associated with that SSID, the total rate will be 200 * 100kbps = 20,000kbps = 20 Mbps > 10Mbps. Workaround: Limit the maximum clients number per WLAN. Using the above example, you can set the maximum clients per WLAN to 100 |

| Component/s | AP |
|---|---|
| Issue | SCG-44242 |
| Description | The 5GHz recovery SSID interface has been disabled on the T710 and R710 APs |

| Component/s | AP |
|---|---|
| Issue | SCG-45294 |
| Description | The R710 and R510 APs do not support the RTS packet size threshold when operating in 802.11ac 20MHz mode |

| Component/s | AP |
|---|---|
| Issue | SCG-46967 |
| Description | Multicast traffic is always directed as unicast traffic, even when the AP has more than five clients associated with it |

| Component/s | AP |
|---|---|
| Issue | SCG-48133 |
| Description | The R710 and T710 APs do not honor the idle timeout setting as received in the RADIUS access accept message |

| Component/s | AP |
|---|---|
| Issue | SCG-48792 |
| Description | When wireless clients based on Intel Dual Band Wireless AC-7256 and Intel Centrino N 6300 AGN, and Samsung S5 mobile devices fail to perform Opportunistic Key Caching (OKC) roaming, they go through full 802.1x authentication instead |

| Component/s | AP |
|---|---|
| Issue | SCG-48895, SCG-89397 |
| Description | The following are the Zero touch mesh limitations.<br>• Zero-touch mesh only supports 5Ghz<br>• Zero-touch mesh only supports Solo AP 110+ and SZ AP 5.0+<br>• When Solo AP upgrades from previous release (for example 104 or 106) to 110, AP needs a set factory option to activate zero-touch mesh<br>• When Solo AP has the updated configuration (for example, WLAN configuration update), the AP needs a set factory option to activate zero-touch mesh |

| Component/s | AP |
|---|---|
| Issue | SCG-49635 |
| Description | BEACON-MISS may be observed on the wlan63 interface of mesh APs if the channel on the root AP changes continuously |

| Component/s | AP |
|---|---|
| Issue | SCG-51422 |
| Description | When rate limits are modified, the new limits are not applied to clients that are in the grace period |

| Component/s | AP |
|---|---|
| **Issue** | SCG-51529 |
| **Description** | Beginning with ZoneFlex standalone AP version 104.0, APs will delay joining a ZoneDirector in favor of joining a SmartZone controller for 30 seconds, if both controllers exist on the same L2 subnet. However, in some situations, the AP can still potentially join the ZD instead of the SZ when both controllers are set to auto approve. Workaround: Do not deploy both ZD and SZ controllers on the same L2 subnet, or there will be potential for APs to join the ZD instead of the SZ |

| Component/s | AP |
|---|---|
| **Issue** | SCG-51790 |
| **Description** | The Ethernet port on the H510 AP does not auto negotiate the data transmission rate when the port speed is changed from 10Mbps to 100Mbps |

| Component/s | AP |
|---|---|
| **Issue** | SCG-51975 |
| **Description** | The 802.1X Ethernet port (supplicant) on the H510 AP does not reply to EAP identity requests when the link is disconnected, and then reconnected |

| Component/s | AP |
|---|---|
| **Issue** | SCG-51986 |
| **Description** | H510 802.1X enabled Ethernet interface configured for MAC-based authentication fails to authenticate supplicants |

| Component/s | AP |
|---|---|
| **Issue** | SCG-53376 |
| **Description** | When the Ethernet port on the H510 AP is configured to use either MAC-based or port-based authentication, MAC authentication bypass cannot be enabled using the CLI |

| Component/s | AP |
|---|---|
| **Issue** | SCG-54202 |
| **Description** | Client events are not shown by default on the **Monitor** > **Events** page. To view client events, set the *Category* filter to *Clients*, and click *Load Data* |

| Component/s | AP |
|---|---|
| **Issue** | SCG-54682 |
| **Description** | Rebooting the H510 AP using the CLI causes the AP to log a 'Kernel Panic' event. No operational effect is observed beyond the log message during reboot process |

| Component/s | AP |
|---|---|
| **Issue** | SCG-56903 |
| **Description** | The cable modem-related status LEDs on the C110 AP cannot be disabled from the controller's web interface |

| Component/s | AP |
|---|---|
| Issue | SCG-56994 |
| Description | AP SNMPv3 displays INFORM when the notification type is set to TRAP |

| Component/s | AP |
|---|---|
| Issue | SCG-57683, SCG-56905 |
| Description | Some cable modem termination systems (CMTSs) may show the "Reset CM" button on the user interface. Clicking this button only resyncs the signal and does not actually reboot the CM |

| Component/s | AP |
|---|---|
| Issue | SCG-58332 |
| Description | On the controller's web interface, the LAN port status for the C110 is mislabeled. Additionally, LAN1/LAN2 mapping is incorrect |

| Component/s | AP |
|---|---|
| Issue | SCG-59255 |
| Description | When the C110 AP is using an Ethernet backhaul (instead the CM), the cable modem serial number cannot be displayed on the access point detail page on the controller's web interface |

| Component/s | AP |
|---|---|
| Issue | SCG-60852 |
| Description | In a two-node cluster, Smart Monitor causes APs to lose connection with the controller. When an AP resumes its connection with the controller, the AP sends Accounting-On message to the controller, but the controller never forwards the same Accounting-On message to the AAA server |

| Component/s | AP |
|---|---|
| Issue | SCG-60865 |
| Description | The valid management traffic rates for the 5GHZ radio are 6Mbps, 12Mbps, and 24Mbps. Ruckus Wireless recommends restricting the management traffic rates to these values using the rate limiting features |

| Component/s | AP |
|---|---|
| Issue | SCG-61183 |
| Description | When configuring walled garden entries, it is recommended to use IP addresses (not DNS names) to help ensure that the walled garden rules are applied consistent |

| Component/s | AP |
|---|---|
| Issue | SCG-62866, SCG-63990 |
| Description | When a mesh is formed in 80+80 MHz mode, wireless clients are unable to send and receive traffic reliably |

| Component/s | AP |
|---|---|
| **Issue** | SCG-63519 |
| **Description** | Configuring static link speed on the 2.5GHz Ethernet port of the R720 AP using the Ruckus AP CLI is unsupported. The port will auto negotiate to 2.5Gbps/1000Mbps/ 100Mbps |

| Component/s | AP |
|---|---|
| **Issue** | SCG-63990, SCG-62866 |
| **Description** | When a mesh is formed in 80+80 MHz mode, wireless clients are unable to send and receive traffic reliably |

| Component/s | AP |
|---|---|
| **Issue** | SCG-65754 |
| **Description** | Client isolation across different WLANs mapped to different VLANs is not supported |

| Component/s | AP |
|---|---|
| **Issue** | SCG-67161 |
| **Description** | The PoE injector detection mechanism may be unreliable. Ruckus strongly recommends manually configuring the PoE injector to use 802.3at mode |

| Component/s | AP |
|---|---|
| **Issue** | SCG-67412 |
| **Description** | LACP does not work on H320 |

| Component/s | AP |
|---|---|
| **Issue** | SCG-68042 |
| **Description** | The force power modes (at+, at or af) are designed for interoperability with PoE injectors. No LLDP Power over MDI TLV is advertised by the AP. If, for any reason, forced at+ or at mode is configured when the AP is connected to a switch port, then the appropriate static power must be configured on the switch port. The switch port power static allocation must be higher than AP port (PD). – AF: Force AP to run at 802.3af power, 12.95W at PD – AT: Force AP to run at 802.3at power, 25W at PD – AT +: Force AP to run at 802.3at+ power, 35W at PD |

| Component/s | AP |
|---|---|
| **Issue** | SCG-68405 |
| **Description** | When an R720 AP is downgraded from release 3.5.1 to 3.5, it remains in AF mode and is unable to transition to AT power mode |
| **Description** | Reset the R720 to factory default settings. - Perform LLDP set via RKS CLI, and then reset the AP to *set LLDP power 25000* |

| Component/s | AP |
|---|---|
| **Issue** | SCG-69227 |
| **Description** | The "Mesh Mode" and "Mesh Role" columns incorrectly display "Auto," when they should display "Not Applicable" as the H320 AP does not support mesh |

| Component/s | AP |
|---|---|
| Issue | SCG-69945 |
| Description | On an abrupt shutdown (power down) of the AP and the Single Accounting Session ID is enabled, the accounting start is seen instead of interim update after the UE roams to another AP |

| Component/s | AP |
|---|---|
| Issue | SCG-70971 |
| Description | VLAN-ID value has zero (0) as the default value when the option Subopt-1 is selected for DHCP Relay under DHCP Option 82 |

| Component/s | AP |
|---|---|
| Issue | SCG-74976 |
| Description | It is recommended to use MDNS enabled when you deploy tunneled WLAN with Apple TV and airplay support. Just make sure that the Apple TV is not connected to the Ethernet tunneled port on the AP but on the WLAN tunnel or on the network Local Breakout in the core network |

| Component/s | AP |
|---|---|
| Issue | SCG-78247 |
| Description | The AP E510 will be automatically rebooted when external antenna gain setting is modified |

| Component/s | AP |
|---|---|
| Issue | SCG-78457 |
| Description | AP does not auto negotiate with switch ports when the switch is configured with half duplex |

| Component/s | AP |
|---|---|
| Issue | SCG-81588 |
| Description | An AP reboot is required when enabling and disabling the non-Beamflex antenna (Part Number: 911-0505-DP01) |

| Component/s | AP |
|---|---|
| Issue | SCG-81705 |
| Description | AP Tx power is not reverting to default values after applying non-Beamflex antenna (Part Number: 911-0505-DP01) gain and switching back to a Beamflex antenna (Part Number: 902-2101-0000). [SCG-81705] |
| Workaround | Set 3 dBi for 2.4 GHz and 5 dBi for 5 GHz, apply the configuration and disable the non-Beamflex antenna (Part Number: 911-0505-DP01). Another option is to factory reset the AP |

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

| Component/s | AP |
|---|---|
| Issue | SCG-82513 |
| Description | AP-to-AP communication in M510 does not work when the backhaul is LTE (Long Term Evolution). This may impact features like Fast Roaming, Bonjour Fencing and 11r |

| Component/s | AP |
|---|---|
| Issue | SCG-84194 |
| Description | The controller web user interface does not have the option to upgrade LTE firmware |
| Workaround | Use the AP CLI to upgrade LTE firmware |

| Component/s | AP |
|---|---|
| Issue | SCG-67394 |
| Description | LACP does not work on R510 |

| Component/s | AP |
|---|---|
| Issue | SCG-67512 |
| Description | The R710 AP stops responding because of memory leak and *Target Fail Detected* error. This issue occurs when the AP's MTU size for LAN1/LAN2 is set to a value greater than 1978 bytes |

| Component/s | AP |
|---|---|
| Issue | SCG-67593 |
| Description | Application of DiffServ values is not preserved on downlink IPv6 Tunnel header when the inner packet is also IPv6 is not supported |

| Component/s | AP |
|---|---|
| Issue | SCG-84002 |
| Description | Configuring SmartCast L2 and L3 IPv6 filters on WLAN interface drops all traffic from the UE |

| Component/s | AP |
|---|---|
| Issue | SCG-67158 |
| Description | Rogue AP detection does not work if the rogue AP's channel is not on the list of Ruckus AP operating channels |

| Component/s | AP |
|---|---|
| Issue | SCG-63561 |
| Description | The AP starts ChannelFly for the 5GHZ radio 30 minutes later than the 2.4GHz radio |

| Component/s | AP |
|---|---|
| Issue | SCG-70949 |
| Description | This is a client limitation affecting devices MotoXStyle (6.0), Samsung Note4 (5.0.1), Samsung Alpha (5.0.2), Samsung S7 X, Samsung S8 where they are unable to move to |

| Component/s | AP |
|---|---|
| | 5G band from 2.4G when the channel in use is an outdoor one. This happens when Band Balancing is enabled with Proactive or Strict options. |

| Component/s | AP |
|---|---|
| **Issue** | SCG-81340 |
| **Description** | AP does not allow association of more than 200 clients per WLAN when transient client MGMT is enabled though AP supports clients per radio of 256 |

| Component/s | AP |
|---|---|
| **Issue** | SCG-51385 |
| **Description** | Microsoft Surface 3 Pro does not respond to ADDBA request frames with Action frames, which can cause the AP to send frames to the client without AMPDU |

| Component/s | AP |
|---|---|
| **Issue** | AP-7201 |
| **Description** | AP model ZF-7372 (128 MB RAM) should not be used in high density environment |

| Component/s | AP |
|---|---|
| **Issue** | AP-7387 |
| **Description** | When WAN link of one of the GAP (Gateway AP) goes down the clients connected to those APs do not get any service |

| Component/s | AP |
|---|---|
| **Issue** | AP-5480 |
| **Description** | Any change in ARC policy resets the pre-existing policy to null. R710/R610/R510 APs are not affected while other or the rest of the AP models are affected |

| Component/s | AP |
|---|---|
| **Issue** | SCG-69178 |
| **Description** | APs may not be balanced or distributed equally among the virtual data planes, when zone affinity is mapped to AP zones |

| Component/s | AP |
|---|---|
| **Issue** | SCG-81050 |
| **Description** | M510 does not support SIM hot plug. It does not detect the SIM installation on the secondary SIM |

| Component/s | AP |
|---|---|
| **Issue** | SCG-73119 |
| **Description** | SmartZone controller can only accept COA (Change of Authorization) or DM (Disconnect Message) to control the wireless client after the wireless client gets the IP address |

| Component/s | AP |
|---|---|
| Issue | SCG-64376 |
| Description | The H510 AP does not support PoE operating mode |

| Component/s | AP |
|---|---|
| Issue | SCG-80309 |
| Description | APs and Controllers report on SCI still shows configuration details of the disabled partner domains and zones |

| Component/s | AP |
|---|---|
| Issue | SCG-64543 |
| Description | If multiple zones or AP groups exist in a domain or zone, it might take at least 30 seconds to expand the AP Status tree on the Health Dashboard screen |

| Component/s | ARC |
|---|---|
| Issue | SCG-43487 |
| Description | ARC is unable to identify Vindictus traffic accurately |

| Component/s | ARC |
|---|---|
| Issue | SCG-50596 |
| Description | ARC with ARC / DPI engine is unsupported on the following AP models= 128 MB RAM platforms)<br>• ZF7982<br>• ZF7782/ZF7782-S/ZF7782-N/ZF7782-E<br>• ZF7781CM<br>• R300<br>• ZF7372/ZF7372-E<br>• ZF7352<br>• ZF7055<br>• H500 |

| Component/s | ARC |
|---|---|
| Issue | AP-3869 |
| Description | When the uplink QoS is marked with DSCP, it marks both Dot1p and DSCP for clients configured with a static IP address |

| Component/s | ARC |
|---|---|
| Issue | AP-4065 |
| Description | Configuring a rate limit rule for a single direction impacts both the directions for clients configured with a static IP address |

| Component/s | ARC |
|---|---|
| Issue | AP-4835 |
| Description | ARC does not support clients that are assigned IPv6 addresses |

| Component/s | ARC |
|---|---|
| Issue | SCG-44064 |
| Description | The ARC engine that is used by ARC recognizes TFTP traffic based on port69. Since only the first packet of TFTP traffic uses port 69, only the first packet is detected as 'tftp' |

| Component/s | ARC |
|---|---|
| Issue | SCG-44384 |
| Description | When configuring a denial policy in ARC, take note of the following limitations:<br>• When "google.com" is set as the ARC denial policy, traffic to the Google website may not be blocked because most Google traffic is encrypted. Google traffic is marked "Google(SSL)" or "SSL/TLS," which does not match the policy, so traffic is not denied.<br>• When "music.baidu.com" is set as the ARC denial policy, traffic to the Baidu web site may not be blocked because most Baidu traffic is marked as "BaiduMusic" or "baidu", which does not match the policy, so traffic is not denied.<br>• BitTorrent download traffic may be difficult to block unless the app IDs, such as "BitTorrent Series", "BBtor","eDonkey Series", "SoMud", etc, are specified in the policy. If you set the denial policy to "xxx. net", " xxx.cn", "xxx.org" , etc., ARC will be unable to block such traffic because ARC engine recognizes the app name without the domain extension.<br>• To block Sina mail traffic, deny traffic to both "sina mail" and "sina.com."In the denial policy, the space character is taken into consideration. For example, if you block "qq game" or "sina video", users will still be able to access "qqgame" or "sinavideo" (no space character). Conversely, if you block "baidumusic" (no space character), traffic to "baidu music" will not be blocked.<br>• When blocking Hotmail or Outlook.com traffic, set the denial policy to "live" or "live.com". If you block "hotmail" or "outlook.com", user will still be able to access Outlook.com. |

| Component/s | ARC |
|---|---|
| Issue | SCG-47746 |
| Description | When ARC cannot determine the application that a device is using, the controller displays the device's IP address as the application name |

| Component/s | ARC |
|---|---|
| Issue | SCG-52257 |
| Description | If a Skype P2P tunnel is set up before the Application Denial Policy is applied, the controller cannot identify the traffic and will allow the call through |

| Component/s | ARC |
|---|---|
| Issue | SCG-60339 |
| Description | ARC is unable to apply policies consistently to apps that cannot be identified by Deep Packet Inspection (DPI) |

| Component/s | ARC |
|---|---|
| Issue | SCG-65933 |

| Component/s | ARC |
|---|---|
| Description | ARC rate limiting for user-defined applications does not work on fragmented packets |

| Component/s | Bonjour Fencing |
|---|---|
| Issue | SCG-59625 |
| Description | The Bonjour service is unable to establish a fence using the fencing neighbor's RSSI |

| Component/s | Bonjour Gateway |
|---|---|
| Issue | SCG-90604 |
| Description | Bonjour Gateway feature does not work for tunnel enabled WLANs on vSZ-D. Multicast DNS (mDNS) has been added in the SZ100 to support multicast forwarding of the vSZ-D service. Currently mDNS is not supported on a vSZ-D managed by vSZ |

| Component/s | Bonjour Gateway |
|---|---|
| Issue | SCG-73134 |
| Description | **Limitation in Bonjour Gateway Rule**<br>• Each Bonjour Gateway rule is configured to advertise per service from one VLAN (VLAN-X) to another VLAN (VLAN-Y). This is a limitation because the To VLAN (VLAN-Y) is just a single VLAN ID and does not allow configuration of a range (like VLAN100-VLAN164) or comma separated values (like VLAN100, VLAN119, VLAN140). A maximum of only 32 rules are allowed in a Bonjour Gateway Policy. This adds a limitation that only a specific service can span up to 32 other VLANS. Also, if service-1 spans to 32 different VLANS then you cannot have other bonjour services [there are 20 such bonjour services present in R3.6 excluding Chromecast service] to span to other VLANS (due to maximum 32 rule limit). |

| Component/s | CLI |
|---|---|
| Issue | SCG-89899 |
| Description | New feature added after release 3.5 is not supported in the CLI command - *show running-config all* |

| Component/s | CLI |
|---|---|
| Issue | SCG-38184 |
| Description | When setting up the SZ-100, the DNS IP address must be configured manually because DNS IP address assignment via DHCP cannot be completed |

| Component/s | CLI |
|---|---|
| Issue | SCG-52077 |
| Description | The CLI configuration logic differs between configuring individual APs and configuring model-specific settings from the AP group context |

| Component/s | CLI |
|---|---|
| Issue | SCG-64943 |
| Description | When the SMTP settings on the controller are configured and the outbound firewall is enabled, the SMTP packets are dropped |

| 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 | Control Plane |
|---|---|
| **Issue** | SCG-95928 |
| **Description** | Solo AP in pure IPv6 mode fails to join the controller using L2 Discovery. However it works fine with *set scg* command |

| Component/s | Data Plane |
|---|---|
| **Issue** | SCG-64571 |
| **Description** | Data plane's DHCP ladder diagram is out of sequence. Visual Connection Diagnostics will perform a best-effort correction of the sequence, but it's not guaranteed |

| Component/s | Data Plane |
|---|---|
| **Issue** | SCG-78044 |
| **Description** | Data plane's DHCP ladder diagram is out of sequence. Visual Connection Diagnostics will perform a best-effort correction of the sequence, but it's not guaranteed |

| Component/s | Public API |
|---|---|
| **Issue** | SCG-52111 |
| **Description** | Creating an AAA service for AP zones that are managed by MVNO using the Public API is currently unsupported |

| Component/s | Public API |
|---|---|
| **Issue** | SCG-53762 |
| **Description** | Every SmartZone release is compatible with the three most recent major Public API versions. SmartZone release 3.5 is compatible with v3_0 (including v3_1), v4_0, and v5_0 of the public API |

| Component/s | Public API |
|---|---|
| **Issue** | SCG-62513 |
| **Description** | When wireless clients are associated with the AP, the average client count may be displayed as in a non-integer value (for example, a decimal number) |

| Component/s | Public API |
|---|---|
| **Issue** | SCG-94214 |
| **Description** | The AP field of data scope within *Data-Streaming Profiles* performs the regular expression validation with the correct format of the IEEE MAC address. It is required to remove the double quotation marks in the HTTP body message to configure null AP via Public API administrative interface |

| Component/s | SPoT |
|---|---|
| **Issue** | SCG-93224 |

| Component/s | SPoT |
|---|---|
| Description | LBS server supports open SSL TLSv1.0 and not TLSv1.1 and TLSv1.2 |

| Component/s | Switch Management |
|---|---|
| Issue | SCG-82184 |
| Description | Substring search does not work when using search boxes |

| Component/s | Switch Management |
|---|---|
| Issue | SCG-82509 |
| Description | Cluster support Geo-redundancy feature does not support ICX switches |

| Component/s | System |
|---|---|
| Issue | SCG-50883 |
| Description | The WLAN scheduler closes a WLAN one hour ahead of schedule because the AP does not take into consideration daylight saving time (DST) |
| Workaround | Make sure that the *Daylight Saving Time* check box on the **Access Points** > **System** > **Select the Zone** > **Configuration** page is not selected |

| Component/s | System |
|---|---|
| Issue | SCG-53518 |
| Description | Nessus reported "Database Reachable from the Internet" vulnerability on port 11311. Memproxy will access the memcache on the cluster interface via port 11311. For data synchronization across the cluster, it needs to be enabled on the cluster interface |

| Component/s | System |
|---|---|
| Issue | SCG-47863 |
| Description | After UEs that are using Internet Explorer are authenticated, they are sometimes redirected to hotspot logon page |

| Component/s | System |
|---|---|
| Issue | SCG-67370 |
| Description | Bypass CNA is not supported on MAC Air Book when the web proxy is enabled |

| Component/s | System |
|---|---|
| Issue | SCG-88998 |
| Description | The controller does not have a backup captive portal status, so it cannot redirect to the backup login page for logging out. This is a limitation for SZ ZD hotspot API (logout) |

| Component/s | System |
|---|---|
| Issue | SCG-76058 |
| Description | When primary DHCP server is recovered, lease file copied from the secondary DHCP server may expire if it is copied prior to time synchronization |

| Component/s | System |
|---|---|
| Issue | SCG-41046 |
| Description | When Virtual Router Redundancy Protocol (VRRP) is used to set up redundant SZ-100 controllers and one of the controller is rebooted, it may be unable to obtain an IP address from the DHCP server |
| Workaround | To resolve this issue, it is recommended to assign a static IP address to the SZ100 network interface |

| Component/s | System |
|---|---|
| Issue | SCG-41960 |
| Description | When you restore the system using a cluster backup, configuration backup files may get deleted. Ruckus strongly recommends that you configure an FTP server to which you can automatically export configuration backups that you generate manually or using the backup scheduler |

| Component/s | System |
|---|---|
| Issue | SCG-45440 |
| Description | The forwarding service is unsupported on the SZ100, therefore related options are automatically removed when the controller software is newly installed. However, if forwarding service profiles were created in release 3.1.2 and the controller is upgraded to a newer release, these profiles are not automatically removed and can still be configured in the WLAN settings, but the settings are not applied |

| Component/s | System |
|---|---|
| Issue | SCG-57260 |
| Description | A UE can log on to a hotspot WLAN on one partner domain using the credentials of a local user on different partner domain |

| Component/s | System |
|---|---|
| Issue | SCG-61667 |
| Description | When testing an IPv6 accounting server, the NAS IP4 attribute is sent in the accounting message |

| Component/s | System |
|---|---|
| Issue | SCG-69261 |
| Description | Rebalance AP feature is not available for single node cluster |

| Component/s | System |
|---|---|
| Issue | SCG-73259 |
| Description | When you configure an internal DPSK name with full length, you may see the username truncated in the clients page |

| Component/s | System |
|---|---|
| Issue | SCG-47886 |

| Component/s | System |
|---|---|
| Description | APs running earlier releases (for example, release 2.5) are unable to join the controller to upgrade their firmware. This issue occurs because of SSL incompatibility in earlier SmartZone releases |

| Component/s | System |
|---|---|
| Issue | SCG-61160 |
| Description | When the data plane receives the first DHCP message, it suppresses other DHCP messages for 180 seconds to prevent message flooding |

| Component/s | System |
|---|---|
| Issue | SCG-62440 |
| Description | The data plane does not support WISPr to SP messages |

| Component/s | System |
|---|---|
| Issue | SCG-63193 |
| Description | The connection failure counter does not increment when EAP fails |

| Component/s | System |
|---|---|
| Issue | SCG-63199 |
| Description | Retransmission of physical layer packets, such as EAPOL, is not displayed on the Visual Connection Diagnostics live troubleshooting page |

| Component/s | System |
|---|---|
| Issue | SCG-78053 |
| Description | The sequence RADIUS Access Accept (AP to client) should be in front of Authentication Success of proxy web authentication tunnel WLAN<br><br>**NOTE**<br>As there are many modules involved in reporting the messages, CCD (Client Connection Diagnostics) module collects all messages (from various modules) and tries to correct sequences if the messages are arrived out of sequence. However, it has been observed that under some special cases, messages may arrive at CCD way out of sequence and CCD cannot correct them. So, the sequence correction is a best effort approach and it's not guaranteed |

| Component/s | System |
|---|---|
| Issue | SCG-67041 |
| Description | The Apple Captive Network Assistant (CNA) is not a fully functional browser. Therefore, it may not work with the controller's portals |

| Component/s | System |
|---|---|
| Issue | SCG-50908 |
| Description | A SmartZone backup file exported from release 2.x cannot be imported to a controller running release 3.x |

| Component/s | System |
|---|---|
| Issue | SCG-39032 |
| Description | The Ethernet port-based profile selection feature was added along with AD/LDAP enhancements. However, the related settings are unavailable on the web interface |

| Component/s | System |
|---|---|
| Issue | SCG-40729 |
| Description | If LDAP authentication is used to authenticate hotspot (WISPr) users, the full path to the LDAP server must be configured. Otherwise, users will be unable to log on to the hotspot using LDAP |

| Component/s | System |
|---|---|
| Issue | SCG-47816 |
| Description | The controller does not support the Chargeable-User-Identity (CUI) attribute through WISPr accounting messages |

| Component/s | System |
|---|---|
| Issue | SCG-62289 |
| Description | When the controller initiates a RADIUS Accounting Off message to an IPv6 Accounting server, the value of Ruckus-control plane- IP address in the message is zero '0'. This issue occurs when an AP abruptly goes offline and does not come back online within a certain period |

| Component/s | System |
|---|---|
| Issue | SCG-50595 |
| Description | When the Device Policy feature is enabled, the host name Chrome devices and Play Station appears as "N/A" on the web interface. This occurs because "DHCP option 12" does not exist in DHCP Discover and DHCP Request |

| Component/s | System |
|---|---|
| Issue | SCG-34801 |
| Description | To help ensure that the cluster firmware upgrade process can be completed successfully, the cluster interfaces of all nodes must be connected and up |

| Component/s | System |
|---|---|
| Issue | SCG-35281 |
| Description | The controller’s management interface IP address may not be changed from DHCP to static IP address mode |

| Component/s | System |
|---|---|
| Issue | SCG-38338 |
| Description | To protect the virtual controller against denial-of-service (DoS) and other forms of network attacks, it strongly recommends installing it behind a firewall |

| 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 |

| Component/s | System |
|---|---|
| Issue | SCG-41756 |
| Description | When an AP switches to another cluster, authorized hotspot (WISPr) clients are unable to log off from the original portal page |

| Component/s | System |
|---|---|
| Issue | SCG-46917 |
| Description | IPv6 addresses for accounting servers on the SZ100 and vSZ are unsupported. Only accounting servers on the SZ300/vSZ-H can be assigned IPv6 addresses |

| Component/s | System |
|---|---|
| Issue | SCG-47946 |
| Description | On iOS 8.x devices, EAP-FAST does not work without a RADIUS server certificate configured in Wi-Fi profile for the device |

| Component/s | System |
|---|---|
| Issue | SCG-48747 |
| Description | When vSZ is upgraded from release 3.2 to a newer release, the web interface cannot be accessed using the Microsoft Internet Explorer 11 |

| Component/s | System |
|---|---|
| Issue | SCG-49736 |
| Description | Cluster formation fails if nodes that are up and running are not syncing time with the configured upstream NTP server |

| Component/s | System |
|---|---|
| Issue | SCG-50826 |
| Description | In a cluster, if the controller to which an AP is connected gets rebooted, the AP moves to another controller in the same cluster. When the controller node that was rebooted comes up, the WISPR sessions on the AP will get terminated. This is a corner case and is not always observed |

| Component/s | System |
|---|---|
| Issue | SCG-56879 |
| Description | Some 802.11w-capable (Protected Management Frames) devices (for example, Samsung and Nexus) may experience interoperability issues when the option 802.11w required is enabled |

| Component/s | System |
|---|---|
| Issue | SCG-58804 |

| Component/s | System |
|---|---|
| Description | The ZoneDirector to SmartZone migration process uses IPv4 addresses. SmartZone currently does not support the migration of APs that are using only IPv6 addresses |

| Component/s | System |
|---|---|
| Issue | SCG-61661 |
| Description | After upgrading the controller from 3.2.x to 3.5 successfully, the web interface does not redirect to the logon page automatically. After the upgrade, it still shows the upgrade process page because of encryption enhancements in release 3.5 |

| Component/s | System |
|---|---|
| Issue | SCG-64679 |
| Description | The migration results might not be up-to-date if web session times out or the web browser is refreshed before the migration process is completed |

| Component/s | System |
|---|---|
| Issue | SCG-65453 |
| Description | Mesh is not applicable to the DHCP NAT on Each AP case because, in this scenario, there is only one AP and no root AP. If a mesh AP is set up, clients connecting to it will be unable to obtain an IP address from a root AP |

| Component/s | System |
|---|---|
| Issue | SCG-66832 |
| Description | The WLAN group override of a VLAN can only be applied if the WLAN and WLAN group are of the same type (for example, both are configured with VLAN tags or both are configured for VLAN pooling) |

| Component/s | System |
|---|---|
| Issue | SCG-71699 |
| Description | iMAC, MAC pro, MAC book pro (model 9,2) MAC air (model6,2) and MAC mini clients are not able to associate with Z2 country code |

| Component/s | System |
|---|---|
| Issue | SCG-80538 |
| Description | Outbound firewall If cluster redundancy and outbound firewall are both necessary, enable cluster redundancy first and then outbound firewall |

| Component/s | System |
|---|---|
| Issue | SCG-57263 |
| Description | When the primary syslog server is down, syslogs are sent to the secondary server. However, syslogs still show the IP address of the primary syslog server (instead of the secondary server) |

| Component/s | System |
|---|---|
| Issue | SCG-52369 |

| Component/s | System |
|---|---|
| Description | The session manager process does not handle the session timeout of WISPr clients after a UE roams from one AP to another |

| Component/s | System |
|---|---|
| Issue | SCG-94778 |
| Description | It is recommended use static resolution of GGSN (Gateway GPRS Support Node) for access point name option rather than using DNS (Domain Name System) resolution |

| Component/s | System |
|---|---|
| Issue | SCG-90606 |
| Description | APs allow ICMP packets though ICMP is blocked in UTP traffic access control list |

| Component/s | System |
|---|---|
| Issue | SCG-94719 |
| Description | Avoid configuring domains in block list of URL filtering, which is a part of XWF traffic classes |

| Component/s | System |
|---|---|
| Issue | SCG-91887 |
| Description | This release does not support IPv6 for RADIUS, TACACS+, AD and LDAP on the Admin AAA page |

| Component/s | System |
|---|---|
| Issue | SCG-89454 |
| Description | If the system fails to obtain DHCP IPv6 address during boot, it will not display IPv6 address in GUI as it is not auto updated. However, the same can be seen through CLI if it got DHCP IPv6 address post boot |
| Workaround | Restart the system to display the DHCP IPv6 address in the management IP address |

| Component/s | System |
|---|---|
| Issue | SCG-93369 |
| Description | Schedule backup in **Backup & Restore** > **Configuration** is not triggered on restoring a configuration backup |
| Workaround | Disable the feature and enable it for the configuration to be applied properly |

| Component/s | System |
|---|---|
| Issue | SCG-93096 |
| Description | The exported CSV report for APs and Clients carry a null entry in the last row |

| Component/s | System |
|---|---|
| Issue | SCG-91940 |
| Description | IPv6 address configuration is not seen for dual mode AP Zone and on system level when dual stack on vSZ is enabled. |

| Component/s | System |
|---|---|
| Issue | SCG-90693 |
| Description | When cluster redundancy settings on the controller is configured and the outbound firewall is enabled, the packets are dropped at Active controller |
| Workaround | Configure the outbound firewall rule for TCP port 8443 |

| Component/s | System |
|---|---|
| Issue | SCG-90479 |
| Description | The order of execution of the scheduled AP CLI script is not guaranteed and the execution might be terminated due to timeout constraints. Clients should be aware this constraint before planning the scheduled execution |

| Component/s | System |
|---|---|
| Issue | SCG-93359 |
| Description | The default *Captive Portal* detection uses *Android-Wi-Fi* to detect Android CNA. It may not support all Android devices if different user agents are used. New customized rules must be created to cover such user agents |

| Component/s | System |
|---|---|
| Issue | SCG-93363 |
| Description | The default CPDS rules cannot detect with the default user-agent Microsoft Phone user equipment |

| Component/s | System |
|---|---|
| Issue | SCG-93556 |
| Description | The default CPDS profile uses .*Microsoft NCSI.* to detect Microsoft Windows devices. It may not support all Microsoft Windows devices if different user agents are used. New customized rules must be created to cover such user agents |

| Component/s | System |
|---|---|
| Issue | SCG-97508 |
| Description | The issue only happens in the controller enabled active-active Geo-Redundancy mode. AP does not re-join the controller when user joins AP to a non-source active cluster and the non-source active cluster is restored by source active cluster, which does not include this AP entry |

| Component/s | System |
|---|---|
| Issue | SCG-94282 |
| Description | The logs of message drop counters with data streaming to UniversalExporter is displayed as *mqttAgentReceivingChannel* as it leverages the same receiving channels as KafkaAgent |

| Component/s | System |
|---|---|
| Issue | ER-3948 |
| Description | The controller does not support multiple LDAP AAA server profiles that use the same IP address and port number |

| Component/s | System |
|---|---|
| **Issue** | SCG-97442 |
| **Description** | Three or four nodes cluster running on version 5.0.0.0.676 with 22500 APs and above will fail to upgrade to version 5.1.0.0.496, causing an unexpected restart of the failed node |
| **Workaround** | **ATTENTION**<br>This KSP patch is applicable only for controller vSZ-H.<br><br>Visit the Ruckus support site to download and apply the KSP (https://support.ruckuswireless.com/software/1906-smartzone-5-0-to-5-1-multi-node-cluster-upgrade-ksp-file) on each node of cluster running 5.0.0.0.676 prior to the upgrade. Refer to https://support.ruckuswireless.com/articles/000003818 for KSP installation instructions.<br><br>The KSP patch will protect the controller not to accept an overload of APs which causes the system crash during the upgrade. |

| Component/s | System |
|---|---|
| **Issue** | SCG-61369 |
| **Description** | WISPr client session statistics are moved to historical data after client terminates layer 2 connection with AP, and not after logout |

| Component/s | System |
|---|---|
| **Issue** | SCG-66362 |
| **Description** | Only one VLAN can be assigned to the Ethernet interface. If the first client is assigned to one VLAN, the second client must use the same VLAN |

| Component/s | System |
|---|---|
| **Issue** | SCG-67708 |
| **Description** | In a wired guest VLAN implementation, the wired client is authorized with a different VLAN even if the client fails wired 802.1X authentication. It can use the Ethernet profile's guest VLAN number to check whether the client is a guest or a normal user |

| Component/s | System |
|---|---|
| **Issue** | AP-4115 |
| **Description** | Bonjour fencing does not work on a mesh network. |

| Component/s | System |
|---|---|
| **Issue** | SCG-67987 |
| **Description** | Wired client is seen as authorized after the AP upgrades or reboots |

| Component/s | System |
|---|---|
| **Issue** | SCG-96854 |
| **Description** | CPU and memory usage approximately reached 90% when the MAC address pooling is enabled in *Sim-Tool* |

| Component/s | System |
|---|---|
| Issue | SCG-87235 |
| Description | If the NAT IP address is configured on the controller, the external subscriber portal (SP) can communicate with the control interface but not with the management interface |

| Component/s | System |
|---|---|
| Issue | SCG-66092 |
| Description | Rate limiting affects fragmented traffic by 50% even when the configured threshold has not been reached |

| Component/s | System |
|---|---|
| Issue | SCG-52507 |
| Description | WISPr client session statistics are not properly moved to historical data after logout |

| Component/s | System |
|---|---|
| Issue | SCG-63167 |
| Description | Bonjour Fencing might not work as expected with Apple TV 3 Rev. A (model A1469) and later versions. This is a known issue and will be fixed in upcoming releases |

| Component/s | System |
|---|---|
| Issue | SCG-49689 |
| Description | The event type and SNMP trap for Event 518 do not match |

| Component/s | System |
|---|---|
| Issue | SCG-80988 |
| Description | In this release onwards, when WLAN with proxy authentication mode, only CCD (Client Connection Diagnostics) message on AAA radius proxy is supported. If AD (Active Directory) or LDAP (Lightweight Directory Access Protocol) server is selected as the authentication server in proxy mode, CCD message are not supported |

| Component/s | System |
|---|---|
| Issue | SCG-64377 |
| Description | When migrating APs from ZoneDirector to SmartZone, if you want all APs to be in same zone, migrate all APs at the same time |

| Component/s | System |
|---|---|
| Issue | SCG-49493 |
| Description | When the primary AAA server is unreachable, authentication messages are not forwarded to the secondary AAA server |

| Component/s | System |
|---|---|
| Issue | SCG-57518 |
| Description | A partner administrator can obtain the status of a client on a different partner domain through the northbound interface |

| Component/s | System |
|---|---|
| Issue | SCG-61036 |
| Description | WISPr does not support IPv6 clients |

| Component/s | UI/UX |
|---|---|
| Issue | SCG-63365 |
| Description | The server name is overridden by a ladder diagram in Internet Explorer 11 |

| Component/s | UI/UX |
|---|---|
| Issue | SCG-54420 |
| Description | On the Bonjour Gateway page, the Create button remains enabled after you select an existing policy |

| Component/s | UI/UX |
|---|---|
| Issue | SCG-62316 |
| Description | During a TTG call flow, the DHCP server stats under Diagnostics are not updated |

| Component/s | UI/UX |
|---|---|
| Issue | SCG-59160 |
| Description | To support WISPr for MSP partners, the "username" attribute was added in the northbound interface query in this release. Customers who upgraded the controller from a previous release do not need to enable the northbound interface unless they intend to use the MSP feature. All requests from an external subscriber portal without a user name specified will still be accepted and considered as an MSP user |

| Component/s | UI/UX |
|---|---|
| Issue | SCG-90059 |
| Description | Zone templates get created with more than the allowed characters while importing |

| Component/s | UI/UX |
|---|---|
| Issue | SCG-91885 |
| Description | Unable to display the AP information when the UE switches to another SSID, Radio or AP in troubleshooting page |

| Component/s | UI/UX |
|---|---|
| Issue | SCG-88854 |
| Description | When URL Filtering policy is created and applied to UTP, which is mapped to a WLAN, the blacklisted sites in the URL policy are not blocked. The URL filtering settings has to be enabled at WLAN level along with UTP. UTP policy will take precedence over WLAN level |

| Component/s | UI/UX |
|---|---|
| Issue | SCG-34971 |
| Description | Some of the options for the Certificate Store page may not show up on the Safari web browser |

| Component/s | UI/UX |
|---|---|
| **Issue** | SCG-47704 |
| **Description** | The local DB option for the authentication and accounting server is used in earlier releases for the ZeroIT feature. Although Zero IT has been removed in release 3.4, the local DB option is still visible on the web interface |

| Component/s | UI/UX |
|---|---|
| **Issue** | SCG-48255 |
| **Description** | The AP management VLAN of legacy APs (for example, APs running release 3.1.1 or 3.1.2) cannot be configured from the controller's web interface. As a result, the AP Management VLAN field on the AP Monitor page cannot display the correct information |
| **Workaround** | If you have APs in legacy AP zones, you can view the correct AP management VLAN from the AP CLI. Alternatively, upgrade the legacy AP zones to this release to resolve this issue. |

| Component/s | UI/UX |
|---|---|
| **Issue** | SCG-56905, SCG-57683 |
| **Description** | Some cable modem termination systems (CMTSs) may show the "Reset CM" button on the user interface. Clicking this button only resyncs the signal and does not actually reboot the CM |

| Component/s | UI/UX |
|---|---|
| **Issue** | SCG-58881 |
| **Description** | On the controller's web interface page for individual access points, the **Restart Cable Modem** button on the **Restart** tab is not functional |

| Component/s | UI/UX |
|---|---|
| **Issue** | SCG-61522 |
| **Description** | The APs on Google Maps sometimes appear off the map. This is a known issue with Google Maps for markers in high latitudes |

| Component/s | UI/UX |
|---|---|
| **Issue** | SCG-61677 |
| **Description** | After an AP is moved from one zone to another, its historical data from its previous zone no longer appears on the web interface |

| Component/s | UI/UX |
|---|---|
| **Issue** | SCG-61779 |
| **Description** | After a backup configuration (from release 3.2 or 3.4) is restored, the web interface does not redirect automatically to the logon page. This issue occurs because of changes in the security certificates |

| Component/s | UI/UX |
|---|---|
| **Issue** | SCG-65236 |

| Component/s | UI/UX |
|---|---|
| Description | If a global filter is applied to a zone, the Access Points page does not correctly display the APs that match the filter |

| Component/s | UI/UX |
|---|---|
| Issue | SCG-66143 |
| Description | Modifying the settings of multiple APs in the same AP zone is not supported |

| Component/s | UI/UX |
|---|---|
| Issue | SCG-76181 |
| Description | If a zone that has been added to a report is deleted, the corresponding report will fail to be completed because the zone is missing |

| Component/s | UI/UX |
|---|---|
| Issue | SCG-77032 |
| Description | When the system boots it does not display the IPv6 address since DHCP IPv6 address in the management IP address is not auto updated |
| Workaround | Restart the system for it to display the DHCP IPv6 address in the management IP address |

| Component/s | UI/UX |
|---|---|
| Issue | SCG-80455 |
| Description | Even after a WISPr client has signed out, the controller web interface continues to show the client in an authorized state. Manually de-authorizing the client does not change the status |

| Component/s | UI/UX |
|---|---|
| Issue | SCG-68696 |
| Description | The SZ300's web interface shows inaccurate vSZ-D network usage |

| Component/s | UI/UX |
|---|---|
| Issue | SCG-63576 |
| Description | Visual Connection Diagnostics does not work if a user opens two simultaneous user interface (UI) sessions (for example, by opening two browser tabs that both show the controller's web interface) |

| Component/s | UI/UX |
|---|---|
| Issue | SCG-64346 |
| Description | Bonjour Fencing is not supported for DHCP/NAT GW AP |

| Component/s | UI/UX |
|---|---|
| Issue | SCG-65376 |
| Description | When the AP sends bidirectional traffic, the estimated AP capacity shown on the web interface is incorrect |

| Component/s | UI/UX |
|---|---|
| Issue | SCG-76950 |
| Description | The search text allows users to search text from the beginning of the string. For example, if the string is RuckusWirelesss, you should search for Ruckus instead of Wireless |

| Component/s | UI/UX |
|---|---|
| Issue | SCG-76953 |
| Description | Special characters are used as tokenizers for indexed texts in the system, and, when performing a search, special characters are used to separate search terms into smaller segments before performing a search. Therefore, search terms with special characters are not supported and is ignored |

| Component/s | UI/UX |
|---|---|
| Issue | SCG-77639 |
| Description | After creating an Ethernet profile for an Ethernet port and adding VLAN tag, the Ethernet profile is not available for AP T811 Lan3 and Lan4 Ethernet ports. The created profile is available for other APs |

| Component/s | Virtual SmartZone |
|---|---|
| Issue | ER-4896 |
| Description | vSZ does not generate syslog messages about the number of free licenses that available |

| Component/s | Virtual SmartZone |
|---|---|
| Issue | SCG-39957 |
| Description | After nodes in a vSZ cluster running on Microsoft Azure are set to factory settings, the nodes are assigned the same host name, instead of their instance names. When nodes in a cluster have duplicate host names, the vSZ cluster cannot be established |

| Component/s | Virtual SmartZone |
|---|---|
| Issue | SCG-42367 |
| Description | When the controller is installed on Microsoft Azure hypervisor and dynamic mode is enabled on the hypervisor, the controller's private and public IP addresses may change if the hypervisor is shut down. This will disconnect APs from the controller, as well as disconnect nodes that form the cluster. |
| Workaround | • Do not shut down the Azure hypervisor<br>or<br>• Set a static IP address for the controller on the Azure hypervisor. |

| Component/s | Virtual SmartZone |
|---|---|
| Issue | SCG-46949 |
| Description | When the controller is behind a NAT server, APs are assigned both public and private IP addresses |

| Component/s | Virtual SmartZone |
|---|---|
| Issue | SCG-49186 |
| Description | Static routes in vSZ cannot be added in bulk. To add multiple static routes, you need to add each static route individually |

| Component/s | Virtual SmartZone Data Plane |
|---|---|
| Issue | SCG-64605 |
| Description | The alarm messages that appear on the dashboard do not disappear until an administrator clears them. Also, it is normal for the physical interface to be down as the controller is rebooting |

| Component/s | Virtual SmartZone Data Plane |
|---|---|
| Issue | SCG-89292, SCG-89276 |
| Description | vSZ-D assigns the earlier IP address based on UE VLAN to client DHCP request instead of matching the DHCP pool received in Option82 |

| Component/s | Virtual SmartZone Data Plane |
|---|---|
| Issue | SCG-89015 |
| Description | vSZ-D does not assign the IP address when DHCP packets are relayed by another vSZ-D with Option82 and sub options |

| Component/s | Virtual SmartZone Data Plane |
|---|---|
| Issue | SCG-85554 |
| Description | In vSZ-D DHCP/NAT feature, when Tunnel NAT is enabled and Tunnel DHCP is disabled in a multi-VLAN deployment, user has to enable DHCP relay to forward the DHCP packets |

| Component/s | Virtual SmartZone Data Plane |
|---|---|
| Issue | SCG-73030 |
| Description | The current release does not support L3 roaming for multicast traffic, so multicast video streaming will not work when the UE roams from vSZ-D2 to vSZ-D1 or when UE initializes the connection to vSZ-D1 and subscribes the multicast video stream |

| Component/s | Virtual SmartZone Data Plane |
|---|---|
| Issue | SCG-91615 |
| Description | When vSZ-D or /SZ100-D backup process starts, the previous backup image will be erased |

| Component/s | Virtual SmartZone Data Plane |
|---|---|
| Issue | SCG-93691 |
| Description | After vSZ-D upgrades to build 3.6.2.0.73 from 3.4.2.0.176, it takes 15 to 20 minutes to come back online |

| Component/s | Virtual SmartZone Data Plane |
|---|---|
| Issue | SCG-59194 |

| Component/s | Virtual SmartZone Data Plane |
|---|---|
| Description | Only static and stateful DHCPv6, IPv6 addressing is supported |

| Component/s | Virtual SmartZone Data Plane |
|---|---|
| Issue | SCG-59772 |
| Description | When the internal DHCP server in vSZ-D is enabled, vSZ-D ignores DHCP requests from non-matched VLANs and does not forward these requests to Local Breakout |

| Component/s | Virtual SmartZone Data Plane |
|---|---|
| Issue | SCG-66426 |
| Description | If the primary and backup destination vSZ-Ds belong to the same vSwitch/ESXi server, Flexi-VPN UEs receive replies twice after the primary vSZ-D comes back online |

| Component/s | Virtual SmartZone Data Plane |
|---|---|
| Issue | SCG-67016 |
| Description | UE IPv4 traffic fails when the destination vSZ-D for Flexi-VPN is unavailable |

| Component/s | Virtual SmartZone Data Plane |
|---|---|
| Issue | SCG-62285 |
| Description | Modifying the data plane network configuration from the vSZ High Scale web interface can enable the IPv6 function to support IPv6 connections on vSZ-D release 3.5 |

| Component/s | Virtual SmartZone Data Plane |
|---|---|
| Issue | SCG-66850 |
| Description | When both Flexi-VPN and NAT DP are enabled and the DHCP server is not running on the vSZ-D server, Ruckus recommends enabling DHCP relay and using that as the forwarding profile |

| Component/s | Virtual SmartZone Data Plane |
|---|---|
| Issue | SCG-68163 |
| Description | The two-NIC architecture for the data traffic of vSZ-D does not work if one NIC is configured for vSwitch and the other NIC is configured for DirectIO |

| Component/s | Virtual SmartZone Data Plane |
|---|---|
| Issue | SCG-68535 |
| Description | Users may experience unexpected drop in packets when the vSZ-D data interface is configured with Direct I/O and features based on inter-vSZ-D tunnels (such as Flexi-vpn/L3 Roaming/CALEA) are used |
| Workaround | Do not deploy both vSZ-D peers with Direct I/O on same Intel NIC (having multiple ports) or Intel NIC with consecutive MAC addresses |

| Component/s | Virtual SmartZone Data Plane |
|---|---|
| Issue | SCG-84658 |
| Description | IPv6 multicast traffic fails for RGRE wireless station |

| Component/s | Virtual SmartZone Data Plane |
|---|---|
| **Issue** | SCG-72610 |
| **Description** | vSZ-D CLI can only support one user to login to view DHCP and NAT information |

| Component/s | Virtual SmartZone Data Plane |
|---|---|
| **Issue** | SCG-72649 |
| **Description** | vSZ-D external syslog messages of *DHCP/NAT_Released* are not supported in this release |

| Component/s | Virtual SmartZone Data Plane |
|---|---|
| **Issue** | SCG-72776 |
| **Description** | If a client connects to a WLAN that uses Radius profile based DHCP/NAT service, Web UI UE entry will report VLAN where NAT IP address belongs instead of the private one assigned by Radius server |

| Component/s | 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/s | Virtual SmartZone Data Plane |
|---|---|
| **Issue** | SCG-72991 |
| **Description** | If generated syslog events in vSZ-D are greater than 8,000 per second, there will be events dropped and not reaching external syslog server |

| Component/s | Virtual SmartZone Data Plane |
|---|---|
| **Issue** | SCG-76345 |
| **Description** | NAT IP and port configuration is only used by AP, therefore when it is configured by the controller, this configuration does not move it to the data plane. Data plane always reports the NAT information, which is configured through virtual data plane CLI |

| Component/s | Virtual SmartZone Data Plane |
|---|---|
| **Issue** | SCG-63511 |
| **Description** | There are no statistics for vSZ-D DHCP/NAT feature in vSZ |

| Component/s | Virtual SmartZone Data Plane |
|---|---|
| **Issue** | SCG-71118 |
| **Description** | When NAT service is enabled in vSZ-D core side L2-GRE does not work though it is configurable |

# Bonjour Gateway Limitations

The following requirements and limitations should be taken into consideration before enabling the Bonjour Gateway feature:

- Bonjour policy deployment to an AP takes effect after the AP joins the controller.
- Some APs of one local area link must be in one subnet. The switch interfaces connected to these APs must be configured in VLAN-trunk mode. Only by doing so can the designated AP receive all the multicast Bonjour protocol packets from other VLANs.
- Dynamic VLANs are not supported.

# Resolved Issues

The following are the resolved issues related to this release.

| Component/s | AP Configuration |
|---|---|
| **Issue** | SCG-91442 |
| **Description** | Resolved an issue where the AP broadcasted tunnel WLAN SSID when the GRE tunnel without vSZ-D was not yet established |

| Component/s | AP Configuration |
|---|---|
| **Issue** | SCG-93112 |
| **Description** | If user changes the DNS settings from AP RKSCLI command, the cubic will be affected. The DNS setting should be reloaded by cubic |
| **Workaround** | Execute the commands:<br>• set scg disable<br>• set scg enable |

| Component/s | AP Configuration, AP Control Plane, SoftGRE |
|---|---|
| **Issue** | SCG-92111 |
| **Description** | APs with Kernel version 2.6 do not renew the IP addresses on receiving the periodic RAs<br>This is very important for the APs having Kernel version 2.6 (R700, R600, R500, R310, P300, T504, T301s, T300, T300e) |
| **Workaround** | The value of preferred and valid lifetime for the RA needs to be configured as a big value (preferably in months) to avoid frequent regeneration of the IP addresses and re-establishment of the RGRE and SSH tunnels<br>Alternatively, if the customers do not want to change the preferred and valid lifetimes in the RAs then you would need to disable the privacy extensions using AP CLI or remote AP CLI on the AP models mentioned above by executing the command<br>`set privacy-extension disable` |

| Component/s | AP Data Plane |
|---|---|
| **Issue** | SCG-89553 |
| **Description** | Resolved an issue where when PMTU (Path Maximum Transmission Unit) for a SoftGRE profile is set to 1238, the br8 interface of AP had the MTU (Maximum Transmission Unit) as 1200. On sending traffic with data size greater than 1200, the packets did not get fragmented |

| Component/s | AP Data Plane |
|---|---|
| **Issue** | SCG-74011 |
| **Description** | Resolved an issue where URL filtering needed to do a reverse lookup of domain names from destination IP address in APs DNS cache |

| Component/s | AP Data Plane |
|---|---|
| **Issue** | AP-5226 |
| **Description** | In order to deny Google+ application, clients would need to configure the deny policy on the below Google applications.<br>• Google Plus<br>• Web - Google Accounts<br>However, blocking *Google Accounts* will impact other Google applications. This issue exist for Google applications, where most of the applications use standard Google APIs. Google Apps follow *google_gen* or similar protocols internally. Therefore, we cannot simply block the Google API specific flows. |

| Component/s | AP Others |
|---|---|
| **Issue** | SCG-64652 |
| **Description** | Resolved an issue where multicast/unicast communication occurred even after client isolation was enabled for an AP LBO WLAN |

| Component/s | AP Others |
|---|---|
| **Issue** | SCG-84897 |
| **Description** | Resolved an issue where after rebooting the M510, USB power and GPS stayed enabled even after disabling it from controller web user interface and the power mode was set as 802.11AT |

| Component/s | AP Others |
|---|---|
| **Issue** | SCG-81036 |
| **Description** | Resolved an issue where channel mismatch occurred between the AP and controller |

| Component/s | AP Others |
|---|---|
| **Issue** | SCG-80218 |
| **Description** | Resolved an issue where ARC did not work properly when user defined ARC was created but it is was not associated with any UTP profile. |

| Component/s | AP Platform |
|---|---|
| **Issue** | AP-8738 |
| **Description** | Resolved an issue where SoftGRE tunnel re-establishment did not get re-initiated post fail over when both primary and secondary SoftGRE gateways are down. |

| Component/s | AP Platform |
|---|---|
| **Issue** | AP-5347 |
| **Description** | Resolved an issue where clients were able to access eBay services though the deny rule is set |

| Component/s | AP Platform, AP Others |
|---|---|
| **Issue** | SCG-89036 |
| **Description** | Resolved an issue where the power LED kept blinking after the AP M510 failed over from Ethernet to LTE |

| Component/s | AP Platform, System |
|---|---|
| **Issue** | SCG-88902 |
| **Description** | Resolved an issue where when the power mode is auto, and power injector is used, the AP power mode was automatically set to 802.11AF mode |

| Component/s | ARC |
|---|---|
| **Issue** | SCG-70636 |
| **Description** | Resolved an issue where R600 AP detected Instagram as Facebook traffic. |

| Component/s | ARC |
|---|---|
| **Issue** | SCG-70027 |
| **Description** | Resolved an issue where AP R600 was unable to detect and deny the four shared applications running on an Android device |

| Component/s | ARC, DHCP |
|---|---|
| **Issue** | SCG-70475 |
| **Description** | Resolved an issue where AP R710 in non gateway AP mode was not able to deny the TFTP traffic |

| Component/s | Captive/Proxy |
|---|---|
| **Issue** | SCG-93438 |
| **Description** | Resolved an issue where bypass CNA was not working |

| Component/s | Control Domain |
|---|---|
| **Issue** | SCG-93105 |
| **Description** | Resolved an issue where in controllers vSZ or SZ300 web user interface *Traffic & Health* tab showed the CPU and memory information but had no data to show |

| Component/s | Control Domain |
|---|---|
| **Issue** | SCG-93114 |
| **Description** | Resolved an issue where TACACS test script was successful though the administrator user was not configured. |

| Component/s | Control Domain |
|---|---|
| **Issue** | SCG-93104 |
| **Description** | Resolved an issue where IPv6 stations are not displayed in the **Wireless**> **Clients** view |

| Component/s | Switch Management |
|---|---|
| **Issue** | SCG-91096 |
| **Description** | Resolved an issue by adding the admin activity log after creating or modifying switch custom event |

| Component/s | Switch Management |
|---|---|
| **Issue** | SCG-85353 |
| **Description** | Search based on POE (Power Over Ethernet) value is now supported |

| Component/s | Switch Management |
|---|---|
| **Issue** | SCG-85322 |
| **Description** | When firmware upgrade and configuration backup/restore is triggered simultaneously, firmware upgrade is given priority<br><br>**NOTE**<br>The web user interface displays a note for the user regarding the priority |

| Component/s | Switch Management |
|---|---|
| **Issue** | SCG-89019 |
| **Description** | Only super administrators with system domain can upload ICX firmware. Network or super admin or full access ICX management administrators can only view the ICX firmware list |

| Component/s | Switch Management |
|---|---|
| **Issue** | SCG-88979 |
| **Description** | Resolved an issue on cluster support where when adding a new node to the existing cluster on the controller did not result in auto load of switch firmware in the controller cluster |

| Component/s | Syslog |
|---|---|
| **Issue** | SCG-89372 |
| **Description** | Resolved an issue where event 117 (AP configuration get failed) failed to be generated |

| Component/s | System |
|---|---|
| **Issue** | SCG-93368 |
| **Description** | On restoring the configuration backup with syslog server disabled, messages are sent after restoration |
| **Limitation** | Due to restore mechanism, the syslog server setting might be delayed by a maximum of 10 minutes after configuration restore is complete |

| Component/s | Security, System |
|---|---|
| **Issue** | SCG-50060, SCG-92188, SCG-50060, EET-387 |
| **Description** | The new set of GET and SET APIs are now available for controlling the TLS versions at the AP.<br><br>SmartZone (5.1+) and Solo (112.x) firmware releases will have TLS versions controlled by AP CLI for version 1.0, 1.1 and 1.2. By default, the minimum TLSv1.0 will be the default version which can be accessed via AP CLI *get tls-version*. Users can change the TLS version as per their convenience and security requirements using AP CLI "*set tls-version*.<br><br>**ATTENTION** |

| Component/s | Security, System |
|---|---|
| | Reboot is needed after any change. |

| Component/s | SZ SNMP |
|---|---|
| **Issue** | SCG-77981 |
| **Description** | Resolved an issue where SNMPv1 was enabled on the AP when enabling SNMPv2 |

| Component/s | UI/UX |
|---|---|
| **Issue** | SCG-89427 |
| **Description** | Resolved an issue where AP reported the value as zero or not applicable to the controller when the connection failure bar was not displayed in the specified color codes on the web user interface. |

| Component/s | vSZ |
|---|---|
| **Issue** | SCG-73427 |
| **Description** | Resolved an issue where Flexi-VPN option was not compatible with Dynamic VLAN setting in WLAN configuration |

| Component/s | vSZ |
|---|---|
| **Issue** | SCG-65463 |
| **Description** | Resolved the issue, where the user can configure the static route when retaining the original configuration is set but function does not work.<br>*Static Routes* tab is greyed when the interface mode is set to *Keep original configuration*. The user is not allowed to configure static route under this condition |

| Component/s | vSZ-D |
|---|---|
| **Issue** | SCG-89292, SCG-89276 |
| **Description** | Resolved an issue where vSZ-D assigned the earlier IP address based on UE VLAN to client DHCP request instead of matching the DHCP pool received in Option82 |

| Component/s | vSZ-D |
|---|---|
| **Issue** | SCG-89214 |
| **Description** | Resolved an issue where when multiple features deployed to vSZ-D, upgrade process executed from vSZ web user interface failed |

| Component/s | vSZ-D |
|---|---|
| **Issue** | SCG-63511 |
| **Description** | Resolved an issue where there were no statistics for vSZ-D DHCP/NAT feature in vSZ |

| Component/s | UI/UX |
|---|---|
| **Issue** | SCG-91670 |
| **Description** | Resolved an issue where retrieving the saved map scale data when accessing the controller through the user interface failed |

| Component/s | UI/UX |
|---|---|
| **Issue** | SCG-82984, SCG-64238 |
| **Description** | Resolved an issue where overlapping L3 roaming subnet/VLAN settings on multiple vSZ-D is allowed but can impact UE connectivity. Therefore, this configuration should be avoided |

| Component/s | UI/UX |
|---|---|
| **Issue** | ER-6853 |
| **Description** | Resolved an issue where the customer SIM card did not register in roaming network |

| Component/s | UI/UX |
|---|---|
| **Issue** | ER-6830 |
| **Description** | Resolved an issue where the client experienced low throughput if the rate limit was configured and then removed |

| Component/s | UI/UX |
|---|---|
| **Issue** | ER-6743 |
| **Description** | Enhanced the login message from *Identifiant* to *Se Connecter* on the French Hotspot login page |

| Component/s | vSZ |
|---|---|
| **Issue** | ER-6710 |
| **Description** | Resolved an issue where the auto cell sizing failed to be deleted properly when the value is null<br>. |

| Component/s | AP Platform |
|---|---|
| **Issue** | ER-6684 |
| **Description** | Resolved an issue where the redirection URL created by AP used the question mark (?) incorrectly, which resulted in a failed redirection request |

| Component/s | System |
|---|---|
| **Issue** | ER-6682 |
| **Description** | Resolved an issue where the node was out of service since Mosquitto service was offline |

| Component/s | AP Platform |
|---|---|
| **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/s | System |
|---|---|
| **Issue** | ER-6649 |
| **Description** | Resolved an issue where the UE was unable to associate to the unbound DPSK (Dynamic Pre-Shared Key) WLAN post initial connection |

| Component/s | System |
|---|---|
| Issue | ER-6648 |
| Description | Resolved an issue where the cluster application stopped on the node |

| Component/s | AP Platform |
|---|---|
| Issue | ER-6627 |
| Description | Resolved an issue where the client was unable to obtain the IP address |

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

| Component/s | vSZ |
|---|---|
| Issue | ER-6611 |
| Description | Resolved an issue where the AP statistics command did not work on the controller |

| Component/s | System |
|---|---|
| Issue | ER-6587 |
| Description | Resolved an issue where the SCI stopped showing any data after upgrading the controller to release version 5.0 |

| Component/s | System |
|---|---|
| Issue | ER-6582 |
| Description | Resolved an issue where the AP MAC address is incorrect in the terminated tunnel from the AP event |

| Component/s | System |
|---|---|
| Issue | ER-6569 |
| Description | Resolved an issue where the local data base username was case sensitive |

| Component/s | AP Platform |
|---|---|
| Issue | ER-6567, ER-6576 |
| Description | Resolved an issue of poor upload speed with R720 AP's |

| Component/s | AP Platform |
|---|---|
| Issue | ER-6517 |
| Description | Resolved an issue of poor speed experiences with R720 AP's |

| Component/s | vSZ |
|---|---|
| Issue | ER-6510 |

| Component/s | vSZ |
|---|---|
| Description | Resolved an issue where it was unable to create a Zone with a France country code if global country code was United Kingdom |

| Component/s | vSZ |
|---|---|
| Issue | ER-6425 |
| Description | Resolved an issue where high latency was noticed on th **Samsung SM-T113NU tablets (android 4.4.4, b/g/n)** when connecting with the R610 AP's |

| Component/s | vSZ-D |
|---|---|
| Issue | ER-6393 |
| Description | Resolved an issue where the AP was unable to connect to the vSZ-D after rebooting vSZ-D |

| Component/s | vSZ |
|---|---|
| Issue | ER-6369 |
| Description | Resolved an issue where vSZ approved the new AP join request even though the *automatic approval* was disabled on the vSZ |

| Component/s | vSZ |
|---|---|
| Issue | ER-63639 |
| Description | Resolved an issue where the graph of average throughput estimate for client was not working on the SCI |

| Component/s | vSZ |
|---|---|
| Issue | ER-6290 |
| Description | Resolved an issue where clients using Samsung Chromebooks in their networks were unable to manage the controller using the Chrome browsers on those laptops |

| Component/s | vSZ-D |
|---|---|
| Issue | ER-6118 |
| Description | Resolved an issue where the UR experienced a slow response time in fetching the IPv6 global address |

| Component/s | vSZ-D |
|---|---|
| Issue | ER-6234 |
| Description | Resolved an issue where the UE packets sometimes dropped due to the race condition |

| Component/s | vSZ-D |
|---|---|
| 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)* |

# Upgrading to This Release


- Before Upgrading to This Release ..... 63
- Virtual SmartZone Required Resources..... 65
- Maximum Supported AP and Switch Management..... 67
- SmartZone Upgrade Paths..... 67
- Supported SmartZone and Data Plane Platform..... 68
- Multiple AP Firmware Support in the SZ100/vSZ-E/SCG200-C/SZ300/vSZ-H..... 69
- EoL APs and APs Running Unsupported Firmware Behavior..... 70


# Before Upgrading to This Release

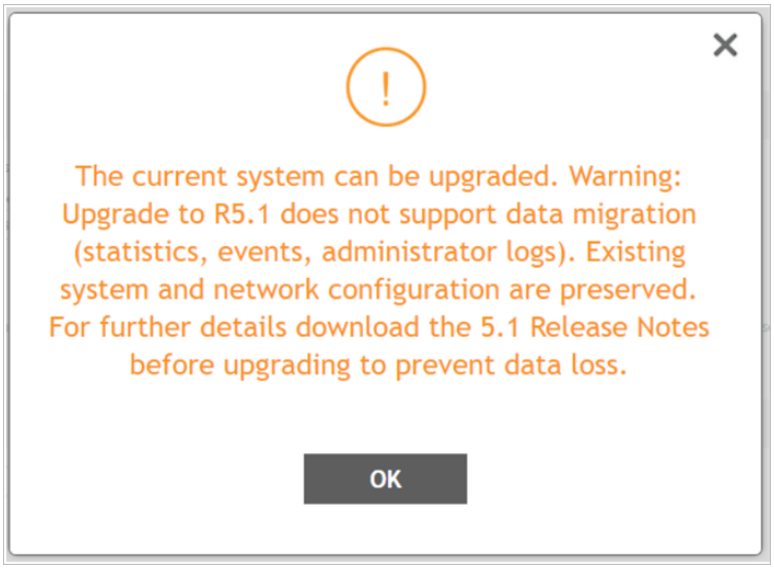
Due to underlying changes of the database in this release, data will be dropped during the upgrade. It is recommended that you read the following content carefully before upgrading to this release.

**IMPORTANT**
Data migration from SmartZone (SZ) 5.0 to 5.1 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 or to release 5.1 by SmartZone (SZ) release 5.0 and 5.1 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 releases can be upgraded to 5.1.
- When upgrading to the release 5.1 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.




# 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.

# 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 and wireless clients 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 4** vSZ High Scale required resources

| AP Count Range | | Max Clients | Nodes per Cluster | AP Count per Node (without switch) | AP/Switch Capacity Ratio | Switch Per Node(without AP) |
|---|---|---|---|---|---|---|
| **From** | **To** | | | **Max** | | **Max** |
| 10,001 | 30,000 | 300,000 | 4 | 10,000 | 8 : 1 | 1,250 |
| | 20,000 | 200,000 | 3 | | 8 : 1 | 1,250 |
| 5,001 | 10,000 | 100,000 | 1-2 | 10,000 | 8 : 1 | 1,250 |
| 2,501 | 5,000 | 50,000 | 1-2 | 5,000 | 8 : 1 | 625 |
| 1,001 | 2,500 | 50,000 | 1-2 | 2,500 | 8 : 1 | 312 |
| 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 5** 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][3] | **GB** [3] | **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 |

**TABLE 5** vSZ High Scale required resources (continued)

| AP Count Range | | vCPU | RAM | Disk Size | Preserved Events | Concurrent CLI Connection | Resource Level |
|---|---|---|---|---|---|---|---|
| 1,001 | 2,500 | 6 | 22 | 300 | 1.5 M | 2 | 6 |
| 501 | 1,000 | 4 | 18 | 100 | 600 K | 2 | 5 |
| 101 | 500 | 4 | 16 | 100 | 300 K | 2 | 4 |
| 1 | 100 | 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 6** vSZ Essentials required resources

| AP Count Range | | Maximum Clients | Nodes per Cluster | AP Count per Node | AP/Switch Capacity Ratio | Switch Per Node (without AP) |
|---|---|---|---|---|---|---|
| **From** | **To** | | | **Max** | | **Max** |
| 1025 | 3,000 | 60,000 | 4 | 1,024 | 5 : 1 | 200 |
| | 2,000 | 40,000 | 3 | | 5 : 1 | 200 |
| 501 | 1,024 | 25,000 | 1-2 | 1,024 | 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 Essentials required resources

| AP Count Range | | vCPU | RAM | Disk Size | Preserved Events | Concurrent CLI Connection | Resource Level |
|---|---|---|---|---|---|---|---|
| **From** | **To** | **Logic Processor** [1][2][3] | **GB** [3] | **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 | 13 | 100 | 1 K | 2 | 1 |

**NOTE**

Logic Processor [1] vCPU requirement is based on Intel Xeon CPU E5- 2630v2 @2.60 GHz.

Logic Processor [2] Azure with low CPU throughput unsupported. The vSZ with the lowest resource plan (2 core CPU, 13 GB memory) can NOT be supported due to the low CPU throughput on Azure.

Logic Processor [3] 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.

# Maximum Supported AP and Switch Management

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

This release supports dynamic (linear) AP/Switch capacity based on capacity ratio. No AP/Switch mode and AP/Switch support numbers are based on the total connect of AP/Switch capacity. The capacity ratio is either low footprint profile with higher switch support capacity ratio such as *1:5* or high footprint profile enhancement to *1:8*.

For example, for the profile ***SZ100/vSZ-E/vSZ-H L1 ~ L5*** the ratio is 5:1, which means 1000 APs to 200 Switches and for the profile *vSZ-H L6 ~ L8* the ratio is 8:1, which means 10000 APs to 1250 Switches

**Calculating the Total Capacity**

- If you have a setup of 200 APs and 100 Switches, where the capacity ratio is 1:5. The total capacity would be 200 x 1 + 100 x 5 = 700. This requirement could use L5, since the total capacity is smaller than 1000.
- If you have a setup of 200 APs and 180 Switches, where the capacity ratio is 1:8. The total capacity would be 200 x 1 + 180x 8 = 1640. This requirement could use L6, since the total capacity is smaller than 2500.
- If you have a setup of 400 APs and 10 Switches, where the capacity ratio is 1:5. The total capacity would be 400 x 1 + 10 x 5 = 450. 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 8** AP and Switch resource table for 1 and 2 nodes

| Profile | 1 and 2 Nodes | | | | 1 /2 Nodes |
|---|---|---|---|---|---|
| Capacity | AP Mode | | Switch Mode | | AP/Switch Capacity Ratio |
| SZ100 | 1024 | 0 | 0 | 204 | 5:1 |
| SZ300 | 10,000 | 0 | 0 | 1250 | 8:1 |

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

**TABLE 9** 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 | 2500 | 8:1 | 30,000 | 0 | 0 | 3750 | 8:1 |

# 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 10 Previous release builds**

| Platform | Release Build |
|---|---|
| SZ300 | 3.6.0.0.510 |
| SZ100 | 3.6.1.0.227 |
| vSZ | 3.6.2.0.78 |
| 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 |
|---|---|---|---|---|
| **Controller** | | | | |
| SZ300 | ✓ | ✓ | ✓ | ✓ |
| SZ100 | ✓ | ✓ | ✓ | ✓ |
| vSZ-High Scale | ✓ | ✓ | ✓ | ✓ |
| vSZ-Essential | ✓ | ✓ | ✓ | ✓ |
| SCG200 | ✗ | ✗ | ✗ | ✗ |
| SCG200-C | ✓ | ✓ | ✗ | ✗ |
| **Data Plane** | | | | |
| D104 | ✗ | ✓ by vSZ (POC) | N/A | ✓ by vSZ |
| D124 | ✗ | ✓ by vSZ (POC) | N/A | ✓ by vSZ |
| vDP | ✓ | ✓ | ✓ | ✓ |

# Multiple AP Firmware Support in the SZ100/vSZ-E/SCG200-C/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.

**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, 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:

- 5.0
- 3.6
- 3.6.x

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

- 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 and 5.0.
- If you are upgrading the controller from release 3.6.2, then the AP firmware releases that it will retain after the upgrade will be 5.1 and 3.6.2 (and 3.6.1 if this controller was previously in release 3.6.1).
- If you are upgrading the controller from release 3.6.1, then the AP firmware releases that it will retain after the upgrade will be 5.1 and 3.6.1.

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

# EoL APs and APs Running Unsupported Firmware Behavior

Understanding how the 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 ZoneFlex Indoor AP and ZoneFlex Outdoor AP product pages on the Ruckus Support website. The icons for EoL APs appear with the *END OF LIFE* watermark.

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 3.5 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....71
- Redeploying ZoneFlex APs with SmartZone Controllers....72
- Converting Standalone APs to SmartZone....72
- ZoneDirector Controller and SmartZone Controller Compatibility....73
- Client Interoperability....73


# 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

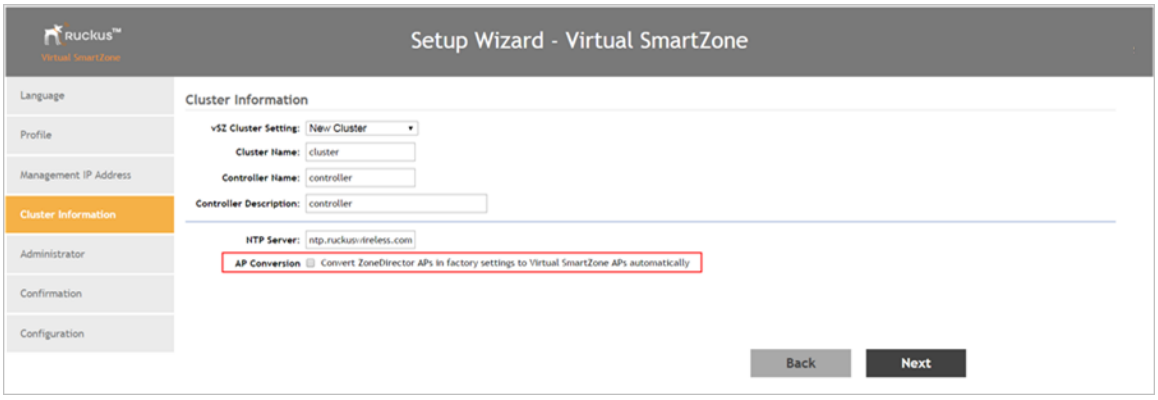
You can convert standalone ZoneFlex APs (those that are not managed by ZoneDirector) in factory default configuration to be managed by a SmartZone controller.

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