SmartZone 3.5.1 GA

Release Notes

Part Number: 800-71627-001 Rev B
Published: 28 June 2017

www.ruckuswireless.com

Copyright Notice and Proprietary Information

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader’s responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN (“MATERIAL”) IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless, Ruckus, the bark logo, BeamFlex, ChannelFly, Dynamic PSK, FlexMaster, Simply Better Wireless, SmartCell, SmartMesh, SmartZone, Unleashed, ZoneDirector and ZoneFlex are trademarks of Ruckus Wireless, Inc. in the United States and other countries. All other product or company names may be trademarks of their respective owners.

Contents

New and Changed Features in Release 3.5.1

1

New Features in Release 3.5.1

This topic provides an overview of the different features and capabilities introduced in the 3.5.1 release of the SmartZone Controller platforms. For detailed descriptions of these features and configuration help, refer to the SmartZone 3.5.1 documentation.

The SmartZone 3.5.1 release is applicable to the Ruckus SmartZone 300, SmartCell Gateway200, SmartZone 100, vSZ-H, and vSZ-E controller platforms. Although considered a minor release, this SmartZone release incorporates a number of new features, enhancements, and bug fixes.

Monitoring for Wired Clients

The purpose of this feature set is to improve the visibility of client devices that are connected to the Ethernet ports of APs that are managed by SmartZone. Up to 16 wired clients can be connected to an AP. However, the maximum number of supported clients remains the same at 512 clients per AP.

Wired Port Disconnect

This feature enables customers to send a Disconnect Message (DM) from a RADIUS server to disconnect a client device that was previously authorized and connected to an Ethernet port of an AP.

Scalable DPSK with RADIUS

This feature is an enhancement to the built-in Dynamic PSK architecture that allows the customer to utilize an external RADIUS server for scalable storage of DPSKs.

In prior releases, the DPSK database was stored directly on the AP or SZ, which hindered some very large networks from achieving scale and/or workflow processes necessary for their deployment. By utilizing RADIUS servers and exchanges during the authentication, the DSPK count can scale up into the hundreds of thousands, without sacrificing the benefits of individual PSKs.

In this “external” DPSK operating mode, customers still receive many of the benefits of DPSK, including per-device and per-user credential control, simplicity for end-users, ubiquitous support by all devices types (even headless devices), role-based policy on a per-DPSK basis, and fast roaming without the need for specific 802.11 enhancements.

This feature requires a significant amount of RADIUS server development effort. This effort is unique to each customer or partner to differentiate their onboarding workflow and services.

Flexi-VPN on vSZ-D

Flexi-VPN feature builds on the Inter vSZ-D Tunnels that have been supported on the vSZ-D since 3.5 release. This feature enables flexible and configurable overlay networks by allowing WLAN traffic that has been tunneled to a vSZ-D to be securely tunneled to another vSZ-D that is connected (usually) to a different network segment (remote site, data center, regional tunnel aggregator, etc.).

Role-Based Application Policies

The role-based policy enhancements from 3.5 have been expanded in 3.5.1 with application policies. Customers can now set application policies to deny, rate limit, or reprioritize (QoS) applications based on the user/device role. For example, the network admin can provision different L7 app privileges for students, teachers, staff, and administrators. When the user/device is assigned to a role, that policy will automatically be applied to the traffic.

NAS-ID Formatting for Wired Clients

This feature enables customers to configure the format of NAS identifier for AP's wired clients so that AP can send this info in its RADIUS request.

Disable HTTPS Redirect for WISPr WLAN

When using Hotspot (WISPr) networks, the client device's HTTP requests are redirected to the captive portal page. With HTTP networks, this functionality works fine. However, with HTTPS, there are different redirect handling behaviors that we can employ.

Prior to 3.5.1, when an HTTPS request is sent from the client device, the SZ redirected this request to the portal page; however, because the SZ's web certificate did not match the client's requested web page, the browser would show a certificate error, which often causes users to back away from the page instead of clicking through and accepting the certificate — for security best practices, we do not want to encourage users to click through certificate errors unless they know what they are doing.

With this new feature, the network administrator has the choice to disable redirect for HTTPS webpages, which will cause the request to timeout. The client's browser will not have a certificate error, but the user will not have an opportunity to hit the captive portal. They will have to browse to an HTTP page in order to be properly redirected. In 3.5.1, we are making this a configurable option for the administrator. HTTPS Redirect will still be enabled by default.

SCI Push for SZ Alarms

With this enhancement, the SZ-SCI API interface (utilizing GPB) has added messaging for the creation and clearing of SZ alarms. This allows both SCI as well as 3rd party systems that are integrating with SZ's APIs to support a centralized, aggregate, and/or multi-cluster view of alarms happening on the SmartZone.

Client Isolation Whitelist for Tunneled WLANs

In the 3.5 release, the SmartZone added the ability for an administrator to specify whitelist (i.e. exceptions) to the client isolation functionality. These are approved wired network destinations that should be allowed for wireless clients that are connected to a WLAN with isolation whitelist enabled. In 3.5.1, we are adding support for this functionality in tunneled WLANs.

Filter Application Data by Radio Band

In the 3.4 and 3.5 releases, we added and improved the built-in L7 application visibility tools. In 3.5, the administrator could filter the view by zone/group, AP, or time. In the 3.5.1 release, we are adding a WLAN dimension, so the administrator can view application consumption for specific WLANs.

IPv6 Support for RADIUS Proxy

The 3.5.1 release adds IPv6 support for IP communication with RADIUS servers, when the RADIUS server is configured as a "proxy" server. In other words, when the SmartZone controller acts as the RADIUS client (AAA authenticator), IPv6 is supported.

GRE Tunnel Status Enhancements

Additional SNMP MIBs have been added to enable polling of GRE status, which enables 3rd party systems to determine the connectivity status of RuckusGRE and SoftGRE tunnels.

Changed Features in Release 3.5.1

Some features that existed in earlier releases have been updated in this release.

RADIUS Proxy Support for Validating All attributes in CoA/DM (RFC 5176 Compliance) [FR-2067]

In previous releases, SmartZone RAC does not honor the following CoA/DM attributes as session identification attributes:

- NAS-Port
- Framed-IP-Address

- Called-Station-Id
- Acct-Multi-Session-Id
- NAS-Port-Id
- Framed-Interface-Id
- Framed-IPv6-Prefix

Also, SmartZone RAC does not support the NAS-IPv6-Address attribute.

In this release, SmartZone RAC honors the above mentioned attributes in CoA/DM as session identification attributes. If any of these attributes are received in CoA/DM and validation fails, SmartZone RAC sends NAK with error-cause as “Session Not Found” to the AAA server.

Configuration of the s2a or s5/s8 Interface Towards PGW [FR-1851]

This feature has been added to the pre-existing advanced gateway configuration and to the public API.

SNMP Temp Sensor Output for the T710 AP [SCG-59065]

The OID 1.3.6.1.4.1.25053.1.1.2.1.1.1.10.0 (ruckusHwInfoTemperature) has been added to report the T710 AP temperature.

Configuration of Adaptive Noise Immunity (ANI) via the SmartZone CLI [FR-2591, SCG-65676]

In previous releases, the only way to change the ANI receive sensitivity on the R710 (and potentially other future APs) is to have root shell access to AP and manually execute the "iwprivwifi1 ani_ofdm_level 7" command. This command, however, does not persist between AP reboots.

In this release, commands have been added to configure ANI via the CLI:

- On the SmartZone CLI, a command is now available for configuring the ANI level per AP-Group.
- On the AP CLI, a command is now available for configuring the ANI level.

These commands persist on AP after reboots.

On the SmartZone CLI:

1. CLI command name: 'ani-ofdm-level <AP Model> <Radio>'
    a. Auto-complete supports the AP model list
    b. Auto-complete supports values 0 to 9
    c. 'no ani-ofdm-level' command removes this configuration from current AP-Group setting. After executing this command and updating the ap-group, the new configuration that is pushed to APs does not include any ani-ofdm-level configuration. APs will keep their current ani-ofdm-level configuration.

2. 'show running-config zone <zone name> ap-group <ap-group name>' command displays ANI-OFMD-Level value if it is overridden.

On the AP CLI:

- CLI command name: 'set ani-ofdm-level <wifix> [0..9]'
  - The AP CLI command is set per radio interface (wifi0/wifi1) and levels can be specified from 0 to 9.
  - 'get ani-ofdm-level <wifix>' command retrieves the configured level and displays it.

Adjusted CPU and Memory Threshold to 90% [SCG-65490]

In release 3.4 and earlier, SmartZone has different CPU and memory thresholds for the different SmartZone platforms (SZ100, SCG200, vSZ-E, and vSZ-H). This sometimes results in the leader node getting flagged for high memory utilization.

In release 3.5 and later, the CPU and memory thresholds have both been adjusted to 90% to address the high memory utilization issue in earlier releases.

mDNS [SCG-67681]

Multicast DNS (mDNS) has been added in the SZ100 to support multicast forwarding of the vSZ-D service.

Hardware/Software Compatibility and Supported AP Models

2

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

- The SZ300 Flagship Large Scale WLAN Controller is designed for Service Provider and Large Enterprises, which prefer to use appliances. The Carrier Grade platform supports N+1 Active/Active clustering, comprehensive integrated management functionality, high performance operations and flexibility to address many different implementation scenarios.
- The SCG200, developed for the service provider market, combines a WLAN access controller with Wi-Fi traffic aggregation, along with a built-in carrier-grade element management system in a 2U rack-mountable, all-in-one hardware form factor.
- The SZ100, developed for the enterprise market, is the next generation midrange, rack-mountable WLAN controller platform for the enterprise and service provider markets. There are two SZ100 models: the SZ104 and the SZ124.
- The vSZ, which is available in *High Scale* and *Essentials* versions, is a Network Functions Virtualization (NFV) based WLAN controller for service providers and enterprises that desire a carrier-class solution that runs in the cloud. It supports all of the WLAN controller features of the industry leading SCG200, while also enabling the rollout of highly scalable and resilient wireless LAN cloud services.
- The vSZ-D offers organizations more flexibility in deploying the SZ data plane as needed in an NFV architecture-aligned fashion. Deploying vSZ-D offers secured tunneling of user data traffic that encrypts payload traffic, maintains flat network topology, enables mobility across L2 subnets, supports POS data traffic for PCI compliance, and offers differentiated per site policy control and QoS, etc.

NOTE

By downloading this software and subsequently upgrading the controller and/or the AP to release 2.5.1.0.177 (or later), you understand and agree that:

- The AP may send a query to Ruckus Wireless 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 Wireless 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.

Hardware and Software Compatibility

This release is compatible with the following controller hardware and software.

Compatible Hardware

- SmartZone 300 (SZ300)
- SmartCell Gateway 200 (SCG200)
- SmartZone 100 (SZ100)

Compatible Software

- Virtual SmartZone High Scale (vSZ-H)
- Virtual SmartZone Essentials (vSZ-E)
- Virtual SmartZone Data Plane (vSZ-D)

Release Information

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

SZ300

- Controller Version: 3.5.1.0.296
- Control Plane Software Version: 3.5.1.0.205
- Data Plane Software Version: 3.5.1.0.296
- AP Firmware Version: 3.5.1.0.419

SCG200

- Controller Version: 3.5.1.0.296
- Control Plane Software Version: 3.5.1.0.205
- Data Plane Software Version: 3.5.1.0.86
- AP Firmware Version: 3.5.1.0.419

SZ100

- Controller Version: 3.5.1.0.296
- Control Plane Software Version: 3.5.1.0.205
- Data Plane Software Version: 3.5.1.0.95
- AP Firmware Version: 3.5.1.0.419

vSZ-H and vSZ-E

- Controller Version: 3.5.1.0.296

- Control Plane Software Version: 3.5.1.0.205
- AP Firmware Version: 3.5.1.0.419

vSZ-D

- vSZ-D software version: 3.5.1.0.296

Supported and Unsupported Access Point Models

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

APs preconfigured with the SmartZone AP firmware may be used with the SZ300, SCG200, SZ100, or vSZ in their native default configuration. APs factory-configured with the ZoneFlex-AP firmware may be used with the SCG200/SZ100/vSZ when LWAPP discovery services are enabled.

On solo APs running release 104.x, the LWAPP2SCG service must be disabled. To disable the LWAPP2SCG service on an AP, log on to the CLI, and then go to **enable mode** > **config** > **lwapp2scg** > **policy deny-all**. Enter **Yes** to save your changes.

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

Supported AP Models

This release supports the following Ruckus Wireless AP models.

Table 1: AP models supported in SmartZone 3.5 and 3.5.1

11ac-Wave2		**11ac-Wave1**		**11n**	
Indoor	*Outdoor*	*Indoor*	*Outdoor*	*Indoor*	*Outdoor*
R720	T710	R700	T504	R300	ZF7782
R710	T710s	R600	T300	ZF7982	ZF7782-E
R610	T610	R500	T300E	ZF7372	ZF7782-N
R510		C500	T301N	ZF7372-E	ZF7782-S
H510		H500	T301S	ZF7352	ZF7781CM
C110		R310	FZM300	ZF7055	
			FZP300		

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

Note that when the R720, R710, T610, or R610 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.

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

Caveats, Limitations, and Known Issues

3

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

AAA Known Issues

The following are the known issues related to AAA.

- The number of accounting messages that the AAA server on the network may receive could significantly increase in this release. This is because this release introduces event-triggered accounting, which generates additional interim messages when an IPv6 address is assigned to an IPv4 client (and vice versa).
- 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. [SCG-40729]
- The controller does not support multiple LDAP AAA server profiles that use the same IP address and port number. [ER-3948]
- When the controller initiates a RADIUS Accounting Off message to an IPv6 Accounting server, the value of Ruckus-SCG-CBlade-IP 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 of time. [SCG-62289]
- The Ethernet port-based profile selection feature was added along with AD/LDAP enhancements. However, the related settings are unavailable on the web interface. [SCG-39032]
- The controller does not support the Chargeable-User-Identity (CUI) attribute through WISPr accounting messages. [SCG-47816]
- When the primary authentication server is unavailable, wired clients do not use the secondary authentication server that has been configured. [SCG-52194]
- The R710 and T710 APs do not honor the idle timeout setting as received in the RADIUS access accept message. [SCG-48133]

AP KPI Known Issues

The following are the known issues related to access point KPI.

- When the AP sends bidirectional traffic, the estimated AP capacity shown on the web interface is incorrect. [SCG-65376]

AP Known Issues

The following are the known issues related to APs.

- A UE can access a mismatched whitelist (valid MAC address but invalid IP list) after it has been connected to the WLAN for five minutes. [SCG-62531]
- 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. [SCG-34885]
- 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. [SCG-34981]
- 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 number of clients per WLAN. Using the above example, you can set the maximum clients per WLAN to 100. [SCG-43697]

- The 5GHz recovery SSID interface has been disabled on the T710 and R710 APs. [SCG-44242]
- The R710 and R510 APs do not support the RTS packet size threshold when operating in 802.11ac 20MHz mode. [SCG-45294]
- When an AP that is assigned the default static IP of 192.168.0.1 is rebooted, it is unable to establish a tunnel with the controller. [ER-3433]
- Multicast traffic is always directed as unicast traffic, even when the AP has more than five clients associated with it. [SCG-46967]
- Client frame IP addresses are sometimes sent as 0.0.0.0 in AP-initiated accounting messages. [SCG-47164]
- Solo APs running release 100.x may be unable to obtain firmware from the controller's captive portal if the captive portal is behind NAT.

  WORKAROUND: Disable NAT IP translation if the captive portal is behind NAT. On the CLI, run the command "no nat-ip-translation" in the config > lwapp2scg context. [SCG-47518]

- 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. [SCG-48792]
- BEACON-MISS may be observed on the wlan63 interface of mesh APs if the channel on the root AP changes continuously. [SCG-49635]

- 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. [SCG-51385]
- 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. [SCG-51529]

- 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. [SCG-51790]
- The 802.1X Ethernet port (supplicant) on the H510 or R510 AP does not reply to EAP identity requests when the link is disconnected, and then reconnected. [SCG-51975]
- H510 802.1X enabled Ethernet interface configured for MAC-based authentication fails to authenticate supplicants. [SCG-51986]
- 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. [SCG-53376]
- Client events are not shown by default on the Monitor > Events page. To view client events, set the Category filter to Clients, and then click Load Data. [SCG-54202]
- 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. [SCG-54682]
- On the controller's web interface, the LAN port status for the C110 is mislabeled. Additionally, LAN1/LAN2 mapping is incorrect. [SCG-58332]
- On the controller's web interface page for individual access points, the Restart Cable Modem button on the Restart tab is not functional. [SCG-58881]
- 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. [SCG-60852]
- 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. [SCG-60865]
- When the 7273 AP starts downloading the latest firmware from a legacy zone and the controller control IP is unreachable, the AP stops responding. [SCG-61448]
- When a mesh is formed in 80+80 MHz mode, wireless clients are unable to send and receive traffic reliably. [SCG-62866, SCG-63990]

- Configuring static link speed on the 2.5GHz Ethernet port of the R720 AP using the Ruckus AP CLI is unsupported. The port will autonegotiate to 2.5Gbps/1000Mbps/100Mbps. [SCG-63519]
- The H510 AP does not support PoE operating mode. [SCG-64376]
- Client isolation across different WLANs mapped to different VLANs is not supported. [SCG-65754]
- Client isolation is not supported when a client roams from one AP to another in the same WLAN. [SCG-66077]
- 802.1x operation of the Eth1 (PoE) interface may not operate in supplicant or authenticator mode. [SCG-67078, SCG-67079]
- Rogue AP detection does not work if the rogue AP's channel is not on the list of Ruckus AP operating channels. [SCG-67158]
- The PoE injector detection mechanism may be unreliable. Ruckus strongly recommends manually configuring the PoE injector to use 802.3at mode. [SCG-67161]
- The R710 AP stops responding as a result 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. [SCG-67512]
- When the SoftGRE IPv4 MTU value is set between 850 and 1279 bytes in a SoftGRE tunnel profile attached to dual mode zone, configuration push to APs fails. [SCG-67583]
- The R710 AP stops responding after the AP's Ethernet port speed is configured to 100 full duplex and its ports are connected to the Netgear Switch M4100. [SCG-67707]
- 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 [SCG-68042]
- Clients are still able to access eBay services even if a DENY rule has been set for these service. [AP-5347]
- When CoA is used to apply a rate limit to a user's webauth session, the subsequent webauth session of the same user uses the same rate limit as the first. [SCG-68381]
- 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.

WORKAROUNDS:

- Reset the R720 to factory default settings, or;
- Perform LLDP set via RKSCLI, and then reset the AP to “set LLDP power 25000”. [SCG-64805]

- When an AP is moved from one zone to another zone that is using a whitelist with a high number of entries (for example, 10 WLANs with 64 entries), the AP is unable to obtain the correct WLAN list for the new zone. [SCG-68407]
- In 80+80 MHz mode, when configuring static channel 36 as primary and 132-144 as secondary and upgrading from release 3.5 to 3.5.1, the user will run into state where release 3.5.1 zone settings will show "no-data" in the secondary channel and the user will not be able to apply any configuration changes in the zone.

  WORKAROUND: Edit the secondary channel field with available channels, and then apply the configuration. [SCG-68602]

- 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.

  WORKAROUND:

  - Reset the R720 to factory default settings.
  - Perform LLDP set via RKSCLI, and then reset the AP to “set LLDP power 25000”.

- The temperature and packet-per-second (PPS) cost metric drops for an indeterminate amount of time. [SCG-61247]
- On a WLAN where both the tunnel and proxy ARP services are enabled, the proxy ARP service stops working if the tunnel service is disabled.

  WORKAROUND: If you change a WLAN from a tunneled to non-tunneled (or vice versa), disable and then re-enable the proxy ARP service. [SCG-68987]

- The IPv6 SoftGRE MTU is incorrect when the MTU for a dual stack zone is set to 1500 bytes. [SCG-67497]
- Malicious devices are still shown as "SSID spoofing" on the Rogue AP/Malicious AP list after the same SSID is removed on the Ruckus AP. [SCG-67332]
- The AP starts ChannelFly for the 5GHZ radio 30 minutes later than the 2.4GHz radio. [SCG-63561]
- 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 Configuration > Common Settings page is not selected. [SCG-50883]

- Multicast/unicast communication still occurs even after client isolation is enabled for an APLBO WLAN. [SCG-64652]

AVC Known Issues

The following are the known issues related to AVC.

- AVC rate limiting for user-defined applications does not work on fragmented packets. [SCG-65933]
- AVC is unable to identify Vindictus traffic accurately. [SCG-43487]
- AVC with Trend Micro is unsupported on the following AP models (<= 128 MB RAM platforms) [SCG-50596]:
  - ZF7982
  - ZF7782/ZF7782-S/ZF7782-N/ZF7782-EZF
  - 7781CM
  - R300
  - ZF7372/ZF7372-E
  - ZF7352
  - ZF7055
  - H500
- The Trend Micro engine that is used by AVC recognizes TFTP traffic based on port 69. Since only the first packet of TFTP traffic uses port 69, only the first packet is detected as 'tftp'. [SCG-44064]
- When AVC cannot determine the application that a device is using, the controller displays the device's IP address as the application name. [SCG-47746]
- Sometimes, an application that has been configured to be denied still passes data through the AP. [SCG-61444]
- AVC is unable to identify BitTorrent traffic accurately. [SCG-43336]
- Strange traffic flows with inconsistent uplink and downlink are displayed on the AVC page in release 3.4. [SCG-44169]
- When configuring a denial policy in AVC, take note of the following limitations:
  - When "google.com" is set as the AVC 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.
  - When "music.baidu.com" is set as the AVC 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.
  - 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., AVC will be unable to block such traffic because Trend Micro recognizes the app name without the domain extension.
  - 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.
    - 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. [SCG-44384]

- The AVC denial policy requires both the user-defined app and app port mapping, instead of only the user-defined app name. [SCG-44724]
- 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. [SCG-52257]
- When the uplink QoS is marked with DSCP, it marks both Dot1p and DSCP for clients configured with a static IP address. [AP-3869]
- Configuring a rate limit rule for a single direction impacts both the directions for clients configured with a static IP address. [AP-4065]
- On the Applications page, when a user selects a specific app, all clients that have used this app in different domains are displayed on the page. [SCG-64735]
- AVC does not support clients that are assigned IPv6 addresses. [AP-4835]
- In AVC GPB streams for external systems, the Application category field is reported as zero. [SCG-65936]
- The AVC deny rule does not work on proxied YouTube streaming traffic. This issue occurs because the signature package and DNS do not recognize this type of traffic as YouTube traffic. [AP-5122]
- AVC identifies YouTube as "googlevideo.com." [SCG-61150]
- AVC does not work with DHCP/NAT on APs. [SCG-64358]
- AVC is unable to apply policies consistently to apps that cannot be identified by Deep Packet Inspection (DPI). [SCG-60339]

Bonjour Fencing Known Issues

The following are the known issues related to Bonjour Fencing.

- Bonjour Fencing of wired devices (wired fencing) requires wireless fencing to also be enabled for the same Bonjour Service Type.
- If AirPlay Services are configured for hop0 fence, they may still be discoverable on an AppleTV outside hop0. [AP-4455]
- Bonjour Fencing is unsupported for Google Chromecast Services in release 3.5. [SCG-63732] and 3.5.1. [SCG-65552]
- Bonjour Fencing is not supported for DHCP/NAT GW AP. [SCG-64346]
- 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. [SCG-63167]
- The Bonjour service is unable to establish a fence using the fencing neighbor's RSSI. [SCG-59625]

- Bonjour Fencing is not yet supported on mesh APs. [AP-4115]
- Bonjour Fencing is not supported for tunnel WLANs. [AP-3842]

Control CLI Known Issues

The following are the known issues related to Control CLI.

- The CLI configuration logic differs between configuring individual APs and configuring model-specific settings from the AP group context. [SCG-52077]
- When setting up the SZ100, the DNS IP address has to be configured manually because DNS IP address assignment via DHCP cannot be completed. [SCG-38184]
- When the SMTP settings on the controller are configured and the outbound firewall is enabled, the SMTP packets are dropped. [SCG-64943]

Control Communicator Known Issues

The following are the known issues related to Control Communicator.

- 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. [SCG-47886]

Control Domain Known Issues

The following are the known issues related to Control Domain.

- After the controller is restored from release 3.2 to 2.6, mesh network on the R700 cannot disabled and its 5GHz radio is unable to support 16 WLANs.

  Workaround: Before restoring the controller from release 3.2 to 2.6, disable mesh networking on the controller. [SCG-39742]

- 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. [VSCG-1509]
- Network tunnel statistics are not displayed for dual stack APs when queried with an IPv6 address. [SCG-57446]
- TTG Session Summary is not as part of associated clients for TTG sessions established using a TTG+WISPr profile. [SCG-32706]
- 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, Ruckus Wireless recommends assigning a static IP address to the SZ100 network interface. [SCG-41046]

- When rate limits are modified, the new limits are not applied to clients that are in the grace period. [SCG-51422]
- When you restore the system using a cluster backup, configuration backup files may get deleted. Ruckus Wireless 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. [SCG-41960]
- When testing an IPv6 accounting server, the NAS IP4 attribute is sent in the accounting message. [SCG-61667]
- 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. [SCG-45440]
- When a two-node cluster is freshly installed, the default node affinity profile is created for only one node, not for both nodes. [SCG-46655]

Control Platform Known Issues

The following are the known issues related to Control CLI.

- The ZoneDirector to SmartZone migration process uses IPv4 addresses. SmartZone currently does not support the migration of APs that are using only IPv6 addresses. [SCG-58804]

Data Plane Known Issues

The following are the known issues related to the data plane.

- On the SCG200 with core network gateways (such as L2oGRE), configuration of host routes to these core network gateways could result in route lookup failure.

  WORKAROUND: Configure the subnet routes. [ER-4329]

- The SZ300 and vSZ-H support IPv6 zones with RuckusGRE tunnels, but the SZ100 and vSZ-E do not. [SCG-61781]
- IPv6 stateless addresses are unsupported. [SCG-59194]

MSP Known Issues

The following are the known issues related to the MSP feature.

- A UE can log on to a hotspot WLAN on one partner domain using the credentials of a local user on different partner domain. [SCG-57260]
- A partner administrator is able to obtain the status of a client on a different partner domain through the northbound interface. [SCG-57518]
- The MSP and MVNO features are mutually exclusive.

Private API Known Issues

The following are the known issues related to the Private API.

- RESTful APIs (https://SCG_ManagementIP:8443/wsg/api/rest/) are not supported in release 3.5. [SCG-64370]

Public API Known Issues

The following are the known issues related to the Public API.

- Creating an AAA service for AP zones that are managed by MVNO using the Public API is currently unsupported. [SCG-52111]
- 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. [SCG-53762]

Rate Limiting Known Issues

The following are the known issues related to rate limiting.

- Rate limiting affects fragmented traffic by 50% even when the configured threshold has not been reached. [SCG-66092]

Reporting Known Issues

The following are the known issues related to reports.

- The SZ300, SCG200, and vSZ-H now only support PDF output format.
- When generating reports on the SZ100 or vSZ-E, take note of the following:
  - The maximum hourly time interval that can be configured is 168 hours (or 7 days).

  - The maximum daily time interval that can be configured is 14 days.
  - The reports in this release do not support monthly time intervals.
- After the system is upgraded to this release, take note of the following:
  - Previously configured CSV/PDF outputs for report types that are no longer supported in this release will be dropped.
  - Any reports in SCG200 and vSZ-H configured to produce a CSV output (which is unsupported in SZ300, SCG200, and vSZ-H) will be converted to PDF output automatically.
  - If the time filter configured in the previous release exceeds the allowed time filter in this release, the time filter will be set to the maximum that this release allows.

Scalability, Stability, and Performance Known Issues

The following are the known issues related to scalability, stability, and performance.

- A SmartZone backup file exported from release 2.x cannot be imported to a controller running release 3.x. [SCG-50908]

SNMP Known Issues

The following are the known issues related to SNMP.

- The event type and SNMP trap for Event 518 do not match. [SCG-49689]
- AP SNMPv3 displays INFORM when the notification type is set to TRAP. [SCG-56994]

Syslog Known Issues

The following are the known issues related to syslog.

- 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). [SCG-57263]
- vSZ does not generate syslog messages about the number of free licenses that available. [ER-4896]

System Known Issues

The following are the known issues related to the system.

- Cluster formation fails if nodes that are up and running are not syncing time with the configured upstream NTP server. [SCG-49736]

- IPv6 addresses for accounting servers on the SZ100 and vSZ are unsupported. Only accounting servers on the SCG200 can be assigned IPv6 addresses. [SCG-46917]
- In a cluster, if the SCG to which an AP is connected gets rebooted, the AP moves to another SCG in the same cluster. When the SCG 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.

  WORKAROUND: Do nothing. Subsequent calls will work fine. [SCG-50826]

- When vSZ is upgraded from release 3.2 to a newer release, the web interface cannot be accessed using the Microsoft Internet Explorer 11. [SCG-48747]
- 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]
- Syslog servers that are using IPV6 addresses are currently unsupported. [SCG-53679]
- The controller may be unable to renew its DHCP server-assigned IP address, which may cause all controller services to go down. [SCG-40383]
- The controller's management interface IP address may not be changed from DHCP to static IP address mode. [SCG-35281]
- To protect the virtual controller against denial-of-service (DoS) and other forms of network attacks, Ruckus Wireless strongly recommends installing it behind a firewall. [SCG-38338]
- When an AP switches to another cluster, authorized hotspot (WISPr) clients are unable to log off from the original portal page. [SCG-41756]
- When the Device Policy feature is enabled, the host name Chrome devices and PlayStation appears as "N/A" on the web interface. This occurs because "DHCP option 12" does not exist in DHCP Discover and DHCP Request. [SCG-50595]
- When the controller is added to the SCI, the Monitor > Administrator Activities page may show that an administrator (SCI) is logging on to the controller every five minutes. [SCG-35320]
- When the location information of a zone is configured, this information is inherited by APs that belong to the zone (unless AP-specific location information is configured). If the location information of the zone is cleared (deleted), this absence of location information is propagated to the APs. As a result, the APs retain the location information previously configured for the zone, which may no longer be valid.

  WORKAROUND: To clear or update the location information on APs, do it at the AP level (instead of the zone level). [SCG-39848]

- SmartZone to SCI communications can be enabled through the web interface using the new SCI Management setting in the SZ web interface. However, this feature only works for SCI version 2.0 (and later). If you are using an older version of SCI (1.x), you will still need to execute the "ap-sci enable" command to allow SZ-SCI communications, even after upgrading the SZ to 3.4. [SCG-51832]

- After the accounting service is disabled for a particular WLAN, Accounting Off messages are not initiated. [SCG-47772, SCG-40827]
- On iOS 8.x devices, EAP-FAST does not work without a RADIUS server certificate configured in Wi-Fi profile for the device. [SCG-47946]
- 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. [SCG-34299]

- 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. [SCG-53518]
- The cable modem-related status LEDs on the C110 AP cannot be disabled from the controller's web interface. [SCG-56903]
- 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. [SCG-56905, SCG-57683]
- Downloading the SCG200 snapshot log and AP support log may fail if multiple attempts are performed in quick succession. [SCG-61855]
- 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). [SCG-66832]
- When rate limiting is enabled, the throughput for voice traffic is restricted to around 128kbps (128kbps in case of UTP rate-limit and 100kbps for SSID rate-limit). If a higher throughput is needed for voice traffic, disable rate limiting. [SCG-51924]
- When the IPv6 tunnel is configured for a WLAN, the WLAN's SSID may not be advertised from the AP. Also, performing an IPv6 ping from another host on the same network to the vSZ-D interface also fails.

  WORKAROUND: On the vSZ web interface, go to **System** > **Cluster**, change the current IPv6 gateway to a different address, and then click **OK**. After a few minutes, go back to the same configuration page, type the correct IPv6 address, and then click **OK**. [SCG-69363]

- 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. [SCG-65453]
- When Sub-Option 1 Type 4 is selected under Option 82, vSZ-D does not forward Sub-Option 1 inside Option 82 in a DHCP Relay scenario. [SCG-68497]

- The 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. [SCG-64571]
- 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. [SCG-65453]
- 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. [SCG-61661]
- The APs on Google Maps sometimes appear off the map. This is a known issue with Google Maps for markers in high latitudes. [SCG-61522]
- 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. [SCG-56879]

UI/UX Known Issues

The following are the known issues related to the UI/UX.

- The current client count may not be consistent with the client count that appears in the Traffic Analysis section. [SCG-60424]
- After client fingerprinting is enabled, the OS Type field on the Wireless Clients page no longer shows the IPv6 client's operating system. [SCG-48886]
- Administrators who do not have the privilege to manage alarms may be able to clear or acknowledge alarms in bulk. [SCG-34126]
- Some of the options for the Certificate Store page may not show up on the Safari web browser. [SCG-34971]
- 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. [SCG-48255]

- The SZ100 Setup Wizard does not validate the IPv6 address if the IPv6 prefix is not configured. [SCG-40257]
- 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. [SCG-47704]

- When the AP bundle is applied, there is no warning message to warn users that applying the bundle will upgrade and reboot all APs, resulting in a temporary service outage. [SCG-55178]
- During a TTG call flow, the DHCP server stats under Diagnostics are not updated. [SCG-62316]
- The channel background application sends the channel number without checking whether the current channel mode supports the channel number. [SCG-60820]
- If a global filter is applied to a zone, the Access Points page does not correctly display the APs that match the filter. [SCG-65236]
- After an AP is moved from one zone to another, its historical data from its previous zone no longer appears on the web interface. [SCG-61677]
- 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 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. [SCG-59160]
- 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. [SCG-59255]
- 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). [SCG-62513]
- The current implementation of L3 roaming does not allow users to select VLAN-based roaming for one set of vSZ-D, while using subnet-based roaming for another set of vSZ-D on same vSZ system. [SCG-64729]
- Modifying the settings of multiple APs in the same AP zone is not supported. [SCG-66143]
- Sometimes, icons on the Dashboard do not load in Google Chrome. [SCG-65180]
- Sometimes, when the Dashboard is reloaded, an HTML script appears, instead of the Dashboard. [SCG-65179]
- 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. [SCG-64543]
- The server name is overridden by a ladder diagram in Internet Explorer 11. [SCG-6336]
- Predictive search on the user traffic and VLAN polling pages only shows results if the first three characters in the search string find a match. [SCG-62718]
- The AP traffic graph does not fit into the legacy AP report. [SCG-62327]
- 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. [SCG-61779]
- On the Bonjour Gateway page, the Create button remains enabled after you select an existing policy. [SCG-54420]

Visual Connection Diagnostics Known Issues

The following are the known issues related to Visual Connection Diagnostics.

- The data plane does not support WISPr to SP messages. [SCG-62440]
- 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). [SCG-63576]
- Retransmission of physical layer packets, such as EAPOL, is not displayed on the Visual Connection Diagnostics live troubleshooting page. [SCG-63199]
- The connection failure counter does not increment when EAP fails. [SCG-63193]
- Even if an AP does not support Visual Connection Diagnostics, messages at the RAC can still be used to help identify potential issues associated with RADIUS connections. [SCG-61281]
- When the data plane receives the first DHCP message, it suppresses other DHCP messages for 180 seconds to prevent message flooding. [SCG-61160]

vSZ Known Issues

The following are the known issues related to vSZ.

- Added a default route for IPv6 via the control interface on vSZ when Control Access-Core Separation is enabled on the web interface. [ER-3843]
- 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. [SCG-39957]
- Clients are unable to use DPSK when using Hyper-V with dynamic MAC since vSZ's br0 MAC address does not match its base board MAC address. Workaround: Set the br0 MAC address using Hyper-V's static configuration. [ER-4806]
- WISPr client session statistics are not properly moved to historical data after logout. [SCG-52507]
- When the controller is behind a NAT server, APs are assigned both public and private IP addresses. [SCG-46949]
- 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, or;
  - Set a static IP address for the controller on the Azure hypervisor. [SCG-42367]

- Static routes in vSZ cannot be added in bulk. To add multiple static routes, you need to add each static route individually. [SCG-49186]
- Client isolation is only supported on clients that are using IPv4 (not IPv6) addresses. [SCG-64581]
- A static route will not work if the network configuration is set to "Keep-Original." [SCG-65463]
- The Apple Captive Network Assistant (CNA) is not a fully functional browser. Therefore, it may not work with the controller's portals. [SCG-67041]
- A zone affinity profile cannot be deleted if it is in use by a SoftGRE zone. [SCG-68651]

vSZ-D Known Issues

The following are the known issues related to vSZ-D.

- When vSZ is deployed with vSZ-D, APs running firmware release 3.1.1 (or earlier) cannot obtain the correct vSZ-D IP address and port number and are unable to establish tunnel manager connections. This is because vSZ-D is unsupported in release 3.1.1 and the data plane IP address formats in releases 3.1.1 and 3.2 are different. [SCG-42325]
- vSZ-D only supports IPv4. If the AP IP mode on vSZ is set to IPv6 only, managed APs will be unable to establish tunnels with vSZ-D. [SCG-39206]
- 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. [SCG-64605]
- When the internal DHCP server in vSZ-D is enabled, the DHCP discover/request messages from UEs are not forwarded to Local Breakout if no matching DHCP profile is found. This is design intent. To override this behavior, enable DHCP relay in the WLAN configuration. [SCG-64664]
- 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. [SCG-68535]

- 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. [SCG-66426]
- 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. [SCG-66850]
- UE IPv4 traffic fails when the destination vSZ-D for Flexi-VPN is unavailable. [SCG-67016]

- The set-factory command on the vSZ-D CLI does not completely reset the vSZ-D to the default settings. The logon and enable passwords are not reset to the default password 'admin' and the vSZ-D setup status is still 'Done,' which results in the 'setup' command still disabled on the CLI.

  WORKAROUND: Execute the set-factory command one more time. After the command is executed successfully, vSZ-D will be reset to the default state. [SCG-68228]

- 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. [SCG-68163]
- The SZ300's web interface shows inaccurate vSZ-D network usage. [SCG-68696]
- Overlapping L3 roaming subnet/VLAN settings on multiple vSZ-D can impact UE bootp and ARP packets when vSZ-D runs the DHCP/NAT service. [SCG-64238]
- When upgrading vSZ-D from 3.2.x to 3.5, the upgrade status may appear as "Firmware Upgrade Failed", even when vSZ-D was upgraded successfully. [SCG-64177]
- No UI/API for DHCP/NAT on vSZ-D. [SCG-63511]
- 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. [SCG-62285]
- 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. [SCG-59772]

Wired Clients Known Issues

The following are the known issues related to wired clients.

- Only one VLAN can be assigned to the Ethernet interface. If the first client is assigned to one VLAN, the second client has to use the same VLAN. [SCG-66362]
- 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. [SCG-67708]

WISPr Known Issues

The following are the known issues related to WISPr.

- When the primary AAA server is unreachable, authentication messages are not forwarded to the secondary AAA server. [SCG-49493]

- If the WISPr user rate limit is throttled by CoA, then the same CoA rate limit will be applied to the same user at the next logon. [SCG-68309]
- When configuring walled garden entries, Ruckus Wireless recommends using IP addresses (not DNS names) to help ensure that the walled garden rules are applied consistent. [SCG-61183]
- WISPr authentication may fail if the CNR receives an invalid home server type. [SCG-52520]
- If the external portal is using HTTPS and a private/self-signed certificate, the pop-up login window does not appear on iOS devices, even if bypass CNA is disabled. [SCG-65321]
- The session manager process does not handle the session timeout of WISPr clients after a UE roams from one AP to another. [SCG-52369]
- Bypass CNA is unsupported on MacBook Air when the web proxy is enabled. [SCG-67370]
- After UEs that are using Internet Explorer are authenticated, they are sometimes redirected to hotspot logon page. [SCG-47863]
- WISPr client session statistics are not properly moved to historical data after logout. [SCG-61369]
- WISPr does not support IPv6 clients. [SCG-61036]

ZoneDirector to SmartZone Migration Known Issues

The following are the known issues related to ZD to SZ migration.

- When migrating APs from ZoneDirector to SmartZone, if you want all APs to be located in same zone, migrate all APs at the same time. [SCG-64377]
- 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. [SCG-64679]

Resolved Issues 4

This section lists previously known issues and internally-found issues that have been resolved in this release.

- Resolved an issue on the R610 AP that resulted in reboot due to kernel panic. [AP-3685]
- Resolved an issue where when the AP's settings were configured from the controller's CLI, some other AP settings were modified incorrectly. [ER-5208]
- Resolved an issue where the controller's web interface did not support network and broadcast IP addresses in different IP configuration fields. [ER-5224]
- Resolved an issue where the guest pass configuration could not be migrated from the ZoneDirector to a SmartZone controller because of a limitation in the characters that SmartZone supports. [ER-5260, ER-5334]
- Resolved an issue where the guest pass printout from the controller did not display the correct WLAN information and expiration time. [ER-5269]
- Resolved an issue that could cause vSZ-D to reboot due to accessing an incorrect flow. [ER-5296, ER-5306]
- Resolved an issue where a user was unable to log on to a hotspot if the user's password contained the ampersand sign. [ER-5302]
- Resolved an issue where APs that have their management network VLAN ID manually configured to a tagged VLAN ID (something other than “VLAN 1”) can become stranded after the controller was upgraded from release 3.2/3.4 to 3.5. [ER-5305]
- Resolved an issue where an application that had been configured to be denied still passed data through the AP. [SCG-60277]
- Resolved an issue where when tunnel mode was enabled on a WLAN, the controller was unable to query SNMP information on APs, radios, WLANs, and clients. [SCG-66157]
- Resolved a race condition during upgrade in vSZ-D that could cause vSZ-D to lose its IP address. [SCG-67396]
- Resolved an issue in vSZ-D that could result in an incorrect MAC address during bootup causing communication issues. [SCG-67548]
- Integrated the following fixes in the SCG200 data plane:
  - Corrected the handling of DNS packets for port 512499 to avoid core crash
  - Avoided memory corruption by accessing the meta info after a packet becomes free
  - Eliminated extra logs
  - Enhanced the debug logs for 3rd party APs and WISPr
  - Enabled the gateway source guard. [SCG-68095]
- Enhanced AP-to-AP communication to share the PMKR1 keys to all neighbor APs on the peer list, whether or not all the BSSIDs are in the neighbor table. This helps ensure that the 11r feature functions normally. [ZF-17171]

- Resolved an LLDP MAC address issue. Now, APs use br0 MAC address for LLDP packets. [ER-5228]

+++ NEW RESOLVED ISSUES IN 3.5.1 START HERE +++

- Resolved an issue where in 80+80 channelization mode, Channel 138 could not detect radar so it was removed from the list of supported AP channels. [SCG-66704]
- Resolved an issue where the Cloud license server could not be reached when the network firewall was enabled. [SCG-65720, ER-5168]
- Resolved an issue where the DHCP/NAT feature could be enabled on individual APs but could not work on mesh APs. Clients that were connected to mesh APs (on which the DHCP/NAT feature was enabled) could not obtain an IP address or access the Internet. [SCG-65486]
- Resolved an issue where the web interface only displayed the top 10 APs, even when it was configured to display the top 20 APs. [SCG-65144]
- Resolved an issue where when an LDAP authentication service was created with the TLS option enabled, the TLS option could only be disabled using the Public API (not through the web interface). [SCG-64717]
- Resolved an issue where when a client that was associated with a legacy AP running release 3.2.1 moved from one SSID to another SSID and then sent DM from the AAA, the DM response was not received from controller. [SCG-63947]
- Resolved an issue where the list of AP models to which a patch applies was truncated on the AP Patch page. [SCG-62421]
- Resolved an issue where, on the web interface, the client fingerprinting feature displayed "N/A" under "OS type" for connected clients running Android 7.0. [SCG-56991]
- Resolved an issue where, under high channel utilization (>90%), a high number of TX timeouts occurred in the presence of multi AC traffic streams. [SCG-49373]
- Added the "HTTPS Redirect" option on the hotspot portal profile page for enabling or disabling HTTPS redirection in WISPr WLANs. [SCG-60823]
- Resolved an issue where applying an application-based rate limiting rule caused the AP to stop responding (kernel panic). [SCG-66174]
- Resolved a msgdist memory leak issue that occurred in two-node clusters. [ER-5128]
- Resolved an issue where when the AP was rebooted, wired clients were unable to complete 802.1x authentication and, as a result, ended up joining the guest VLAN. [ER-3379]
- Resolved the security issue described in the following advisory: 91572-CVE-2016-2107. For more information, visit https://www.ruckuswireless.com/security. [ER-4892]
- Resolved an issue where when the controller was configured in dual stack mode, wired clients that were using IPv4 addresses could not browse the Internet. [SCG-68547]
- Resolved an issue where a user was unable to log on to a hotspot if the user's password contained the ampersand sign. [SCG-67792]

- Resolved an issue where UDP/ICMP fragmentation occurred from a wired client to a wireless client. This issue occurred when the MTU size for the Ruckus GRE tunnel for APs was set to a value between 850 and 1001 bytes. [SCG-67487]
- Resolved an issue where changes to the table settings of a cluster were not applied immediately to other nodes in the cluster. [SCG-67434]
- Resolved an issue where when the default AP group was not selected on the web interface, the value for "Total APs" appeared as zero (0). [SCG-67421]
- Resolved an issue where when the Override check box for Smart Monitor was selected, the parameters did not appear. [SCG-67006]
- Resolved an issue where the controller sent a CoA NAK when CoA was received on a different cluster node. [SCG-48959]
- Resolved an issue where when the management IP or control IP of vSZ had the same first octet as one of the configured DHCP pool VLANs, AP connectivity to the controller could be broken. [SCG-65729]
- Resolved an issue where when an SCG200 configuration backup was restored to the SZ300, the SCG200 temperature threshold settings were also applied to the SZ300. [SCG-65620]
- Resolved an issue where customers were able to send Disconnect Message (DM) to a specific authorized wired client. [SCG-63914]
- Resolved an issue where the incorrect event "AP rebooted due to IP change" was being reported when, in reality, the AP was rebooted due to a country code change. [SCG-63899]
- Added help information on web interface to save the zone first before creating a Bonjour fencing profile. [SCG-63897]
- Added the Create Ethernet Port Profile button on the AP and AP Group pages of the web interface. [SCG-63893]
- Resolved an issue where the NAS-IPV6-ADDRESS of the AP was not saved in memory. [SCG-62645]
- Resolved an issue where users could not create unsupported function profiles in IPv6 zones. [SCG-62286]
- Added the capability to search for domains and zone names in the global filter. [SCG-61414]
- Resolved an issue where when the SZ300 was managing at least 10K APs and 100K UEs, generating a daily Client Number report at System domain level between 22:00 and 23:59 UTC caused the controller application to restart. [SCG-65954]
- Resolved an issue where the zone template for auto-channel selection could not be applied. [SCG-65783]
- Resolved an issue where the web interface became blank when the administrator clicked a release 3.2.1 zone on the AP page > Configuration tab. [SCG-64621]

Upgrading to This Release 5

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

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

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

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

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

Virtual SmartZone Recommended Resources

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

See the tables below for the virtual machine system resources that Ruckus Wireless recommends.

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

WARNING! If you are upgrading from an earlier release, you will likely need to upgrade the system resources allocated to the virtual machine on which vSZ is installed. However, changing the system resources could result in an issue where the vSZ cluster goes out of service [SCG-47455]. To prevent this issue from occurring, you must do the following:

1. Contact Ruckus Wireless Support and obtain SCG47455_WorkAround_RP_OS_433930.ksp.
2. Apply SCG47455_WorkAround_RP_OS_433930.ksp, which fixes SCG-47455.

3. Adjust the system resources allocated to the virtual machine on which vSZ is installed (see the recommended resource tables below).
4. Upgrade vSZ to this release.

Table 2: vSZ High Scale recommended resources

Nodes per Cluster	AP Count per Node	AP Count per Cluster		Client Count per Cluster	Disk Size	vCPU	RAM	Max Preserved Events	Resource Level
	Max	Min	Max	Max	GB	Core[1]	GB	Max	
3-4	10,000	10,001	30,000	300,000	600	24	48	3M	8
1-2	10,000	5,001	10,000	100,000	600	24	48	3M	7
1-2	5,000	2,501	5,000	50,000	300	12	28	2M	6.5
1-2	2,500	1,001	2,500	50,000	300	6	22	1.5M	6
1-2	1,000	501	1,000	20,000	100	4	18	600K	5
1-2	500	101	500	10,000	100	4	16	300K	4
1-2	100	1	100	2,000	100	2	13	60K	3

Table 3: vSZ Essentials recommended resources

Nodes per Cluster	AP Count per Node	AP Count per Cluster		Client Count per Cluster	Disk Size	vCPU	RAM	Max Preserved Events	Resource Level
	Max	Min	Max	Max	GB	Core[2]	GB	Max	
3-4	1,024	1,025	3,000	60,000	250	8	18	10K	2
1-2	1,024	101	1,024	25,000	250	8	18	10K	2
1-2	100	1	100	2,000	100	2	13	1K	1

1 Azure with low CPU throughput unsupported

2 Azure with low CPU throughput unsupported

Supported Upgrade Paths

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

The table below lists previous releases that can be upgraded to this release.

Table 4: Previous release builds that can be upgraded to this release

Platform	Release Build
SZ300	3.2.0.0.790
SCG200	3.2.1.0.163
SZ100	3.2.1.0.193
vSZ (vSCG)	3.2.1.0.217
vSZ-D	3.2.1.0.245
	3.2.1.0.253
	3.4.0.0.976
	3.4.1.0.208
	3.4.2.0.152
	3.5.0.0.808
	3.5.0.0.832

Upgrading With Unsupported APs

If the controller is currently managing APs that are unsupported in this release, here are a few issues that you may encounter when you upgrade to this release and their workarounds.

AP models that have already reached End-of-Life (EoL) status (for example, the 2942) are unsupported in this release. If you currently have AP models that are unsupported, you will be able to upgrade the controller to this release but not the AP zones to which the EoL APs belong.

- After you upload the upgrade (.ximg) file the **Administration** > **Upgrade** page of the web interface, the web interface will inform you that the upgrade cannot be started because the controller is managing at least one AP that is unsupported by this release.
- If you click **Upgrade** or **Backup & Upgrade** on the **Administration** > **Upgrade** page, the upgrade process will start, but it will eventually fail. [SCG-41229]

Issues and Workarounds for Upgrading Unsupported APs to This Release

The following tables summarize some of the upgrade issues that you may encounter if the SZ100 or SCG200 is managing APs that have reached EoL and the possible workarounds for each issue. [SCG-42511, SCG-43360]

Table 5: Issues and workarounds for upgrading the SZ100 with EoL APs

Release Version	Issue	Workaround
3.2	When you attempt to upgrade the controller, a warning message appears and informs you that the system cannot be upgraded because there are APs that are unsupported in the new release. The message identifies these unsupported APs. The **Upgrade** and **Backup & Upgrade** buttons are hidden to prevent you from attempting to upgrade the system before one of available workarounds to the issue is applied.	To be able to upgrade the system, do one of the following: • On the web interface, clear the Automatically approve all join requests from APs check box. • Delete any unsupported APs from the controller. • Before running the upgrade, apply the KSP file for this issue. Contact Ruckus Wireless Support for more information.

When you attempt to upgrade the SCG200 to this release, the upgrade script will check if the controller has any AP zones using AP firmware releases that are unsupported in this release. If the upgrade script finds at least one AP zone that is using an unsupported AP firmware release, the upgrade process will aborted.

Table 6: Issues and workarounds for upgrading the SCG200 with EoL APs

Release Version	Issue	Workaround
3.2	When you attempt to upgrade the controller, a warning message appears and informs you that the system cannot be upgraded because there are APs that are unsupported in the new release. The message identifies these unsupported APs. The **Upgrade** and **Backup & Upgrade** buttons are hidden to prevent you from attempting to upgrade the system before one of available workarounds to the issue is applied.	To be able to upgrade the system, do one of the following: • Move the EoL APs to the *Staging Zone*. • Upgrade the AP zones to the latest available AP firmware release. • Before running the upgrade, apply the KSP file for this issue. Contact Ruckus Wireless Support for more information.

Multiple AP Firmware Support in the SCG200/vSZ-H

In the SCG200/vSZ-H, the AP firmware releases that APs use are configured at the zone level. This means that APs that belong to one zone could use a different AP firmware release from APs that belong to another zone.

NOTE Some earlier AP models can only support AP firmware 3.1.x and earlier. If you have these AP models, note that they cannot be upgraded to this release.

NOTE If you have AP zones that are using 3.1.x and the AP models that belong to these zones support AP firmware 3.2 (and later), change the AP firmware of these zones to 3.2 (or later) to force these APs to upgrade their firmware. After you verify that all of the APs have been upgraded to AP firmware 3.2 (or later), proceed with upgrading the controller software to release 3.5.

In the current release and earlier releases, when the SCG200/vSZ-H software is upgraded to a newer release, the upgrade mechanism does not require the administrator to upgrade the AP firmware releases that managed APs are using.

NOTE In contrast, in 3.5 and earlier releases, the SZ100/vSZ-E automatically upgrade both the controller firmware and AP firmware when the system is upgraded. In release 3.5.1, however, the concept of "zones" is introduced, which slightly changes the upgrade workflow. The system and the AP zones in SZ100/vSZ-E are now upgraded independently. The administrator must now proactively upgrade the AP zones (and thus, the APs in them) after upgrading the system to the new firmware.

Up to Three Previous Major AP Releases Supported

Every SCG200/vSZ-H release can support up to three major AP firmware releases, including (1) the latest AP firmware release and (2) two of the most recent major AP firmware releases. This is known as the *N-2* (n minus two) firmware policy.

NOTE A major release version refers to the first two digits of the release number. For example, 3.4 and 3.4.1 are considered part of the same major release version, which is 3.4.

The following releases can be upgraded to release 3.5:

- 3.4.x
- 3.4
- 3.2.x
- 3.2

The AP firmware releases that the SCG200/vSZ-H will retain depend on the SCG200/vSZ-H release version from which you are upgrading.

- If you are upgrading the SCG200/vSZ-H from release 3.4, then the AP firmware releases that it will retain after the upgrade will be 3.5 and 3.4.
- If you are upgrading the SCG200/vSZ-H from release 3.2, then the AP firmware releases that it will retain after the upgrade will be 3.5, 3.4, and 3.2.

All other AP firmware releases that were previously available on the SCG200/vSZ-H will be deleted automatically.

EoL APs and APs Running Unsupported Firmware Behavior

Understanding how the SCG200 handles APs that have reached EoL status and AP running unsupported firmware can help you design an upgrade plan that will minimize impact on wireless users in your organization.

EoL APs

NOTE To check if an AP that you are managing has reached EoL status, visit the ZoneFlex Indoor AP and ZoneFlex Outdoor AP product pages on the Ruckus Wireless Support website. The icons for EoL APs appear with the `END OF LIFE` watermark.

- An EoL AP that has not registered with the SCG200 will be moved to the **Staging Zone** and its state set to `Pending`. This AP will be unable to provide WLAN service to wireless clients.
- If an EoL AP is already being managed by the SCG200 and you attempt to upgrade the controller, the firmware upgrade process will be unsuccessful. The web interface

may or may not display a warning message (see Upgrading With Unsupported APs). You will need to move the EoL AP to the **Staging Zone** to upgrade the controller successfully.

APs Running Unsupported Firmware Releases

- APs running AP firmware releases that are unsupported by the SCG200 release can still connect to the controller.
- Once connected to the controller and assigned to a zone, the AP will be upgraded to the AP firmware assigned to the zone to which it belongs.

Interoperability Information 6

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 Wireless controller products including ZoneDirector, SCG200, vSZ, SZ- 100, and SAMs.

Once the AP discovers and joins a controller (for example, the SZ100), the AP is updated to the compatible controller-specific AP firmware version. The updated AP firmware version becomes the factory-default image. The updated AP firmware version (for example, vSZ AP 100.x) will remain persistent on the AP after reset to factory defaults.

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

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

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

Enabling ZoneFlex AP Discovery to a SmartZone Controller Using DNS

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

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

Redeploying ZoneFlex APs with SmartZone Controllers

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

Once the AP firmware is updated, the AP will no longer be able to communicate with its old ZoneDirector controller. The AP must be reset to factory default setting before attempting to configure the AP from the SmartZone controller.

NOTE There are established ZoneDirector to SmartZone controller migration tools and procedures. Contact `support.ruckuswireless.com` for the latest available procedures and utilities.

Converting Standalone APs to SmartZone

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

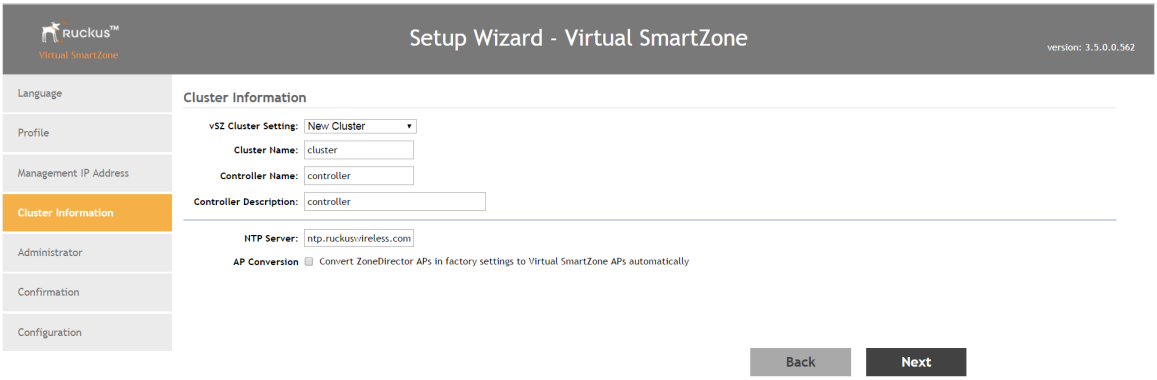
Follow these steps to convert standalone ZoneFlex APs to the SmartZone controller firmware so that they can be managed by the SZ300, SCG200, SZ100, or vSZ.

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, SCG200, or SZ100 the check box description may be slightly different

---

Figure 1: Select the AP Conversion check box to convert standalone ZoneFlex APs to SCG 200/SZ100/vSZ APs



2. After you complete the Setup Wizard, connect the APs to the same subnet as the SmartZone controller.
   When the APs are connected to the same subnet, they will detect the SmartZone controller on the network, and then they will download and install the AP firmware from SmartZone controller. After the SmartZone firmware is installed on the APs, the APs will automatically become managed by the SmartZone controller on the network.

ZoneDirector Controller and SmartZone Controller Compatibility

If you have a ZoneDirector controller on the same network, take note of this important information.

To ensure reliable network operations, it is recommended that ZoneDirector controllers and SmartZone controllers (SCG, SZ, vSZ, SAMs controllers) not be deployed on the same IP subnet or in such a way as the controllers share the same DHCP address scopes and domain name servers (DNS) as there may be limitations or restrictions in AP controller discovery capabilities. An effective network segmentation strategy should be developed when ZoneDirector and SmartZone controllers coexist on the same network.

Client Interoperability

SmartZone controllers and ZoneFlex APs use standard protocols to interoperate with third party Wi-Fi devices. Ruckus Wireless qualifies its functionality on the most common clients.

350 West Java Drive, Sunnyvale, CA

www.ruckuswireless.com