SmartZone 3.5

Release Notes

Part Number: 800-71305-001
Published: 30 March 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

Copyright Notice and Proprietary Information.....2

1 New and Changed Features in Release 3.5

What's New In Release 3.5.....5
Changed Features in This Release.....11

2 Hardware/Software Compatibility and Supported AP Models

Hardware and Software Compatibility.....16
Release Information.....16
Supported and Unsupported Access Point Models.....17

3 Caveats, Limitations, and Known Issues

AVC Known Issues.....19
AP Known Issues.....20
AP KPI Known Issues.....24
Autonomous AP Known Issues.....24
Bonjour Fencing Known Issues.....24
Cassandra Known Issues.....25
Visual Connection Diagnostics Known Issues.....25
Client Whitelist Isolation Known Issues.....25
Control Communicator Known Issues.....25
Control Domain Known Issues.....25
Control CLI Known Issues.....26
Control Platform Known Issues.....27
Data Plane Known Issues.....27
Hotspot Known Issues.....28
MSP Known Issues.....28
Scalability, Stability, and Performance Known Issues.....28
Public API Known Issues.....28
RAC Known Issues.....29
Reporting Known Issues.....29
Session Manager Known Issues.....30
SNMP Known Issues.....30
Syslog Known Issues.....30
System Known Issues.....30
UI/UX Known Issues.....32

vSZ Known Issues....34
vSZ-D Known Issues....35
Wireless Clients Known Issues....36
WISPr Known Issues....36
ZoneDirector to SmartZone Migration Known Issues....36

4 Resolved Issues

5 Upgrading to This Release
Virtual SmartZone Recommended Resources....39
Supported Upgrade Paths....41
Upgrading With Unsupported APs....41
Multiple AP Firmware Support in the SCG200....43
EoL APs and APs Running Unsupported Firmware Behavior....44

6 Interoperability Information
AP Interoperability....45
Redeploying ZoneFlex APs with SmartZone Controllers....46
Converting Standalone APs to SmartZone....46
ZoneDirector Controller and SmartZone Controller Compatibility....47
Client Interoperability....48

New and Changed Features in Release 3.5

1

What's New In Release 3.5

This topic provides a high-level overview of several key features that are introduced in the SmartZone (SZ) software release 3.5. For detailed descriptions of these features and configuration help, refer to the respective 3.5 documentation guides.

The SZ release 3.5 is applicable to the Ruckus Wireless SmartZone 300, SmartCell Gateway 200, SmartZone 100, vSZ-H, and vSZ-E controller platforms. In this release, the SmartZone controller has a completely new UI with enhancements to visibility and troubleshooting as well as streamlined monitoring and configuration workflows as well as several UI-related features. Behind the new UI are many architectural enhancements that improve scalability, operations, and data access. 3.5 also introduces native support for three new AP models (R610, T610, and C110). For a complete list of supported access point models, see Supported and Unsupported Access Point Models on page 17.

New APs

SZ 3.5 adds native support for three new AP models (T610, R610, and C110).

- R610 – Indoor 802.11ac Wave2 3x3:3 AP with aggregate rates up to 1,900 Mbps. Features BeamFlex+, MU-MIMO, 160MHz channels, and 802.3af PoE.
- T610 – Outdoor 802.11ac Wave2 4x4:4 AP with aggregate rates up to 2,533 Mbps. Features BeamFlex+, MU-MIMO, and IoT support.
- C110 – Wall-plate 802.11ac 2x2:2 AP with DOCSIS 3.0 8x4 cable modem backhaul. Features BeamFlex+, matched band radio coverage, additional in-room Ethernet ports, and IoT readiness.

New Controller Model – SZ300

With the release of 3.5, we are introducing a new SmartZone appliance called the SmartZone 300 (SZ300). SZ300 is designed as the next generation carrier-grade controller with performance exceeding the SCG200. With separate control, management, and data planes, each SZ300 has 2x 10Gbps data planes, as well as 6x 1Gbps ports for management, control, and cluster support.

Redesigned UI

Along with system architecture changes, 3.5 has a completely redesigned and optimized UI experience. Look and feel have been modernized, menus have been consolidated to simplify monitoring and configuration actions, and many of the workflows are streamlined

with contextual information and profile linking. Along with the new look and feel, there are a number of new features highlighted by the new UI, like mapping, health and traffic analysis, troubleshooting, spectrum analysis, and much more.

Client Connectivity Analysis

This feature is a troubleshooting tool that allows an administrator to focus on a specific client device and its connectivity status. It starts by detecting APs near the client or where the client is already connected and evaluating AP environmental health (e.g. channel, airtime utilization, client SNR, connection failure %, etc). The tool then tracks the step-by-step progress of the client's connection, through 802.11 stages, RADIUS, EAP authentication, captive portal redirects, encryption key setup, DHCP, roaming, and more (depending on WLAN type). Admins can identify information in each step, like EAP type or IP assigned to the UE, and then can pinpoint where/if a failure occurs during the process.

AP Health Analysis

Along with the new UI, AP health analysis is a central theme in 3.5. On the dashboard, AP status is categorized based on health/performance thresholds defined by an administrator. On a map, APs are color-coded based on this status. We also list the top APs based on key health metrics, like interface latency, airtime utilization, and connection failures—this allows the administrator to focus his/her attention on troubleshooting. From the AP context, admins can analyze specific zones, AP groups, or APs to view historical health trends and compare individual APs against others in its group to look for isolated trouble spots or broader patterns.

Map Enhancements

Prior to 3.5, SmartZone had Google maps for outdoor APs. In 3.5, we've dramatically enhanced our mapping functionality to display both sites/floorplans as well as APs on the map. Admins can choose an AP to view details like health status, IP address, or other operational metrics, or admins can view a floorplan to see AP status and details across that floorplan. APs are color-coded by status, and administrators can overlay operational data—like operating channel, traffic, client count, airtime utilization—for each AP on the map.

Multi-Zone Support in SZ100/vSZ-E

Prior to 3.5, SCG200 and vSZ-H had a system hierarchy with domains, subdomains, and zones. In 3.5, we're introducing zones to the SZ100 and vSZ-E platforms. Zones allow administrators to segment the network into distinct operational groups. This allows for separation of profiles like WLANs and policies. Admins can also upgrade AP zones independently from the controller software and utilize AP releases going back N-2

releases. Zones can operate in different firmware versions and with different country codes.

MSP Domain Enhancements

This releases introduces a new domain concept called a “partner domain.” MSP use cases often dictate that each of the MSP’s tenants/customers has a siloed set of configurations, profiles, and system objects, which are not shared with other tenants. In prior releases, we had either system-level or zone-level objects; with the introduction of operator domains, we have moved the majority of system-level objects into the operator domain so as to provide segmentation, privacy, scalability, and flexibility in implementations. This change alleviates some of the operational requirements of MSPs.

Enhanced Admin Role-based Access Control

The 3.5 administrative role-based access control has been refined to improve usability and simplify the creation of function-specific administrative roles. It is now easier to create administrators and attach them to predefined or custom admin roles, and it is easier to define limited-permission roles like modify or read-only.

vSZ-D Enhancements

In this release, we continue to improve scale and flexibility of our virtual data plane (vSZ-D). We’re scaling up to 10 vSZ-Ds per vSZ and increasing the cluster count to 40. Admins will also be able to configure zone affinities, steering individual zones to one or more specific vSZ-Ds. We have also added vSZ-D support for DHCP/NAT, northbound L2oGRE tunneling, CALEA monitoring, and L3 roaming using Ruckus GRE tunnels.

DHCP/NAT in AP

In highly distributed environments, particularly those with only a few APs per site, we’re introducing the ability for an AP or a set of APs to provide DHCP/NAT support to local client devices. This simplifies deployment by providing all-in-one functionality on the AP, which eliminates the need for a separate router and DHCP server for each site. It also eases site management by providing central control and monitoring of the distributed APs and their clients.

ZD to SZ Migration

The 3.5 release has a built-in ZD-to-SZ migration tool that simplifies the process of migrating ZD-managed APs to the SmartZone. This migration toolset is focused on migrating the APs and preserving operational configurations necessary to maintain AP connectivity, such as IP settings, mesh configuration, management VLAN, and more. It does not provide full migration of ZD configuration into SZ. This tool is initially designed to support SZ and ZD on the same site and may not support every deployment architecture without additional configuration of firewalls and/or port forwarding rules.

DPSK Enhancements

DPSK progress continues with new features, scale, and flexibility. In SCG200, vSZ-H, and SZ300, the number of DPSKs has increased from 20,000 to 50,000, with up to 10,000 per zone. SZ100 and vSZ-E are also increased from 10,000 to 20,000, with up to 10,000 per zone. We're also introducing the concept of group DPSKs, which allows a single DPSK to be reused by many devices. There can be up to 64 Group DPSKs in a zone. In 3.5, we also now allow the admin to specify the passphrase for a given DPSK; this is supported both in CSV import as well as manual generation from the UI. Admins can also specify a number-only DPSK, which makes guest scenarios or other "easy entry" scenarios a little more user-friendly. Finally, the CSV format and admin-defined password will now allow for ZD DPSK migration, starting with ZD 10.0, when admins can export the ZD's DPSK.

CALEA Support

Utilizing the data plane of vSZ-D, we're introducing support for lawful traffic intercept, which allows some traffic to flow centrally to a CALEA server for investigation by law enforcement or government agencies. For some network operators, this allows them to abide by local regulations required to operate a network as a service.

Operational Enhancements

Several operational enhancements have been made, including:

- Improved stats granularity (measurement and reporting intervals)
- New counters/KPIs have been added for better troubleshooting and stats review
- SNMP polling is supported for real-time AP/client stats snapshots

Public API Enhancements

Continued expansion of public API support, including:

- Retrieving zone and WLAN details
- AP group override settings
- AP override settings

AP Performance Enhancements

Low-level AP performance enhancements have been made to improve speed in tunnel mode WLANs. AP IPsec hardware acceleration has also been implemented to improve IPsec performance.

ChannelFly Enhancements

In 3.5, we continue to enhance ChannelFly by adding a cost metric to the channel change logic. The "cost" metric allows the AP to automatically adjust channel change

aggressiveness based on client count (before and after a channel change) as well as traffic load patterns.

Topology Network View

As a part of the UI enhancement, we have added a topology health view, which allows administrators to view the system hierarchy (domain, subdomain, zone, apgroup) as a tree and to identify nodes in the tree with offline APs or APs that have crossed admin-defined performance/health thresholds.

Manual Client Isolation Whitelist

Prior versions of SmartZone allows client isolation whitelist, but the functionality was automatic. The AP would snoop DHCP offers to determine a UE's IP gateway. Then APs would only allow traffic to that destination. In 3.5, we've also added the ability for an admin to configure a manual whitelist entry, either to add non-gateway devices (e.g. printer) or to configure additional gateway MAC addresses that may be required for load balancing or other gateway architectures. The isolation whitelist can be auto only, manual only, or auto and manual.

Role-Based Policy Enhancements

In SZ 3.5, role policies have been enhanced with new functionality. When a UE/device is assigned to a role, you can now apply role-specific VLANs or VLAN pools. You can also apply a UTP to the role—UTPs in 3.5 have been enhanced with some L7 application policies as well as rate limiting based on L3/4 rules (note that role-based L7 policies will be enforced in a short-term release after 3.5.0). All WLAN types with ProxyAAA authentication now support role-based policy assignment. Admins can also change the precedence of WLAN, device OS, and role policies, which adds flexibility for different use cases.

Application Control (Rate Limit and QoS)

L7 application control has been expanded to include both rate limiting and QoS actions. Prior releases supported application deny policies. The L7 policy has now been integrated into User Traffic Profiles (UTP) for a more cohesive point of policy configuration.

Spectrum Analysis

3.5 introduces spectrum analysis to the SmartZone platforms. In this release, we support 11n as well as 11ac APs (both Wave1 and Wave2). Spectrum visibility includes real-time amplitude and utilization (i.e. duty cycle) graphs, a spectrum density view, and a swept spectrogram (waterfall) view. The utilization view allows the administrator to define a signal amplitude threshold. For dual-radio APs, when a radio is placed in spectrum mode, it will prevent clients from connecting; however, for APs with three radios, the 3rd radio

can provide spectrum analysis of both 2.4 and 5 GHz bands without impacting client connectivity.

Bonjour Fencing

This release introduces a new Bonjour management feature called Bonjour Fencing. Fencing allows the admin to control the physical area in which a given Bonjour-based service is discoverable. This is accomplished by mapping devices advertising Bonjour services to nearby APs and allowing only that AP or its neighbors to advertise the Bonjour record. Effectively, this prevents users/devices from discovering Bonjour services that are not nearby, and thus are not relevant to their search.

Real-Time Client Health

Alongside all the other UI and health-related enhancements in 3.5, admins can view real-time client SNR and data rate, as well as historical traffic, to help troubleshoot connectivity problems.

Block UE After Repeat Auth Failures

As a Denial-of-Service (DoS) prevent measure, 3.5 introduces a feature to temporarily block a UE if it fails authentication too many times in a short period. The feature thresholds (number of failures, span of time to measure failures, and duration of block) are configurable by the administrator. This effectively prevents many authentication cracking attacks or other DoS attacks that consume AP resources.

LDAP over SSL

As straightforward as it sounds, 3.5 introduces the ability to support LDAPS, or “LDAP over SSL” connections. In this mode, the LDAP client and server initiate an encrypted session before any LDAP messages are transferred, thus providing an additional layer of data privacy.

Manually Block Client

This feature is a workflow improvement that allows administrators to select one or more wireless clients/devices and create a system/zone-wide block on them. This block prevents the UE from connecting to any AP on the system. This can be useful in situations where devices have been stolen or compromised, or in situations where a user has violated some acceptable use policies.

Test AAA Role Assignment

The Test AAA function has been enhanced to help the administrator determine which role attributes the AAA server is providing and how that maps to local roles on the

SmartZone. This simplifies the deployment testing process by confirming that a user will be assigned to the proper role and policy.

Mark Rogues as Known

This functionality gives administrators more control over rogue classification. Some APs that are detected as “rogue,” may not actually be rogue. They may be known neighbors or lab equipment with similar settings. For this reason, admins can now mark detected rogues as known (i.e. safe), which prevents the AP from taking action against these discovered APs.

IPv6 Support for WSON

WSON (Wireless Self Optimization Network) is an architectural enhancement introduced in SZ 3.4 that allows for fast roaming and load balancing by sharing data between APs. In 3.5, SmartZone adds support for WSON in APs using IPv6 addressing—in 3.4, WSON supported IPv4 only.

Additional Enhancements

Many other enhancements have been made as well, including:

- Customized NAS-IP-Address in SCG-Radius
- Support Acct-Session-ID as a session key in COA/DM
- EPON/GPON status display on SZ UI
- WISPr with MAC bypass and DVLAN
- Protocol support for the Multiband Operation specification

Changed Features in This Release

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

ARC

User Defined and Port Mapping Profiles

- The User Defined Profile page has been moved from the zone level to the domain level to support MSP. [SCG-56370]
- The Port Mapping Profile page has been merged with the User Defined Profile. [SCG-56563]

Denial Policy Profile vs Application Policy Profile

- The Denial Policy has been integrated into the Application Policy Profile. Because the design has changed, the denial policy profile configuration created in the previous releases cannot be migrated. The customer will need to recreate Denial Rules (Application) by choosing from “System Defined” profiles.

- The Application Policy Profile is now at the domain level to support MSP. [SCG-49933]
- The Application Policy Profile is also used by the User Traffic Profile. [SCG-49936]

Public API and CLI

- A new public API (v5) is available for AVC. The old public API for AVC is no longer supported. [SCG-49931]
- Creating or configuring Application Control Profiles using the CLI is no longer supported. [SCG-53476]
- The following CLI commands have been removed in this release:
  - show rogue-aps rogue-mac <ap-mac>
  - show rogue-aps rogue-type {type}

AVC

In this release, the user-defined application name text box is no longer available on the UI. To define a denial policy for a user-defined application, use the pre-defined signature pack.

VLAN Pooling

The VLAN pooling page has been moved from the zone level to the domain level.

WISPr

Requests to the northbound interface from freshly installed controllers and partner-created domain users now include the "user name" field.

Cluster-wide KSP Framework

KSPs are now uploaded to the entire cluster, as opposed to individual nodes. This change makes it easier for users to deploy KSPs.

Upgrade Flow Optimization

The enhanced upgrade process provides user-friendly progress diagrams and enhanced debugging information.

Certificate Encryption Update

Certificate migration is now supported, allowing users to replace the default certificate encrypted with MD5. SHA256, a more secure hash algorithm, is used instead.

NOTE Because the encryption algorithm has changed, the autoredirect mechanism, which redirects users to the logon page after the upgrade process is completed, no longer works.

Auto Cluster-wide Restore Local

- The "restore local" command has been merged with the "restore" command.
- if any node in the cluster is out of service, the cluster-wide restore local command is now supported.

User Role Policy Enhancements

The following changes to the user role policy have been made:

- A user can now be assigned to a role in all WLAN types and for all proxy AAA authentication mechanisms.
- A user-defined VLAN has been added to role assignment, allowing role-based VLANs to be defined and to override WLANs.
- VLAN pool is now supported in role assignment, allowing a role-based VLAN pool to override a WLAN.
- The administrator can now change the precedence policy.

LDAP Over TLS

SmartZone supports LDAP over TLS only when proxy is selected as the authentication service. The TLS client certificate is unsupported.

SCI Settings

- Authentication with SCI's MQTT broker by the security protocol of TLS 1.2 with Pre-Shared Key is now supported. This allows a user to provide a username and a password to connect to SCI version 2.3 (or later), which supports SmartZone's push mode operation.
- After SmartZone is upgraded from release 3.2 or 3.4, SCI is disabled. This is because earlier SmartZone releases do not support the authentication information required in the SCI settings for release 3.5.

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 SCG-200, 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 dataplane 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: 3.5.0.0.808
- Control Plane Software Version: 3.5.0.0.561
- Data Plane Software Version: 3.5.0.0.808
- AP Firmware Version: 3.5.0.0.1333

SCG200

- Controller Version: 3.5.0.0.808
- Control Plane Software Version: 3.5.0.0.561
- Data Plane Software Version: 3.5.0.0.448
- AP Firmware Version: 3.5.0.0.1333

SZ100

- Controller Version: 3.5.0.0.808
- Control Plane Software Version: 3.5.0.0.561
- Data Plane Software Version: **3.5.0.0.216**
- AP Firmware Version: 3.5.0.0.1333

vSZ-H and vSZ-E

- Controller Version: 3.5.0.0.808

- Control Plane Software Version: 3.5.0.0.561
- AP Firmware Version: 3.5.0.0.1333

vSZ-D

- vSZ-D software version: : 3.5.0.0.808

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

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

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.

AVC Known Issues

The following are the known issues related to AVC.

- Applying an application-based rate limiting rule could cause the AP to stop responding (kernel panic). [SCG-66174]
- 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]
- AVC is unable to apply policies consistently to apps that cannot be identified by Deep Packet Inspection (DPI). [SCG-60339]
- 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]
- When a system-defined application (AVC feature) -- for which a rate limiting rule (Rate Limiting feature) has been configured -- generates a high volume of traffic, it could cause the AP to stop responding (kernel panic). This issue only occurs when AVC and Rate Limiting are used together.

  WORKAROUND: Use the AVC and Rate Limiting features separately. [SCG-66174]

AP Known Issues

The following are the known issues related to access points.

- The controller displays the top 10 APs, when the web interface is configured to display the top 20 APs.

  WORKAROUND: After you configure the web interface to display the top 20 APs, refresh the web interface. [SCG-65144]

- The initial spectrum scan takes around 20 to 30 seconds. [SCG-65034]
- After the 2.4GHz radio is disabled, some wireless clients that are connected to the 5GHz radio may get disconnected or lose their IP addresses. [SCG-65026]
- The value for Power Source on the AP information page for the R720 is incorrect. [SCG-64998]
- Some of the interoperability clients may disconnect and reconnect after a fast roam if both APs are on adjacent or the same channels. [SCG-64665]
- In high density environments with heavy congestion, transmission timeouts may happen on an AP's 2.4GHz radio. This may cause packet loss and/or clients to get disconnected temporarily.

  WORKAROUND: Move clients to the 5GHz radio using the band balancing feature. [SCG-64153]

- The web interface may show that spectrum analysis is still running long after the actual spectrum analysis process on the AP has already stopped. This issue occurs when spectrum analysis runs for five hours or more.

  WORKAROUND: Stop and then restart the spectrum analysis process. [SCG-63494]

- The web interface displays a warning message when an AP disconnects from and reconnects to the controller while a spectrum analysis scan is running. [SCG-63323]
- If a spectrum scan is running and the AP is disconnected from the controller (for example, due to power cycling or network issues), the web interface shows that the spectrum scan is still running. Only when the AP is reconnected to the controller does the spectrum scan stop. [SCG-63322]
- When scan debug logs are enabled, the R610 AP may stop responding.

  WORKAROUND: Avoid enabling radio-level debug logs. If you must enable them, make sure they are enabled on only one WLAN at the time and only for short periods of time. [SCG-63062]

- CALEA mirroring of unicast packets between clients connected to the same AP is not happening. [AP-3822]

- When a wired service that is anchored by an AP is removed, the AP does not update its service list. [AP-3255]
- When receiving multicast traffic at a high rate, the filtering algorithm on the AP does not drop packets as precisely as intended. [AP-4707]
- ARC does not support clients that are assigned IPv6 addresses. [AP-4835]
- If the user changes the Ethernet connection between eth0 and eth1 after a DHCP/NAT configuration is applied successfully, the gateway AP needs to be rebooted. Otherwise, ARP beacons are not sent on the eth1 interface. [AP-4429]
- Multicast IGMP join requests from a local subnet are not forwarded to the WAN. As a result, any streaming on the WAN side cannot be accessed from the local subnet. [AP-4303]
- If the channel on the root AP changes continuously, BEACON-MISS may be observed on the wlan63 interface of mesh APs. [SCG-49635]
- 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]

- Client frame IP addresses are sometimes sent as 0.0.0.0 in AP-initiated accounting messages. [SCG-47164]
- H510 802.1X enabled Ethernet interface configured for MAC-based authentication fails to authenticate supplicants. [SCG-51986]
- 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]
- 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]

- 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]
- 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]
- On the controller's web interface, the LAN port status for the C110 is mislabeled. Additionally, LAN1/LAN2 mapping is incorrect. [SCG-58332]

- 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]
- AP SNMPv3 displays INFORM when the notification type is set to TRAP. [SCG-56994]
- 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]
- 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]

- Some cable modem termination systems (CMTSs) may show the "Reset CM" button on the user interface. Clicking this button only resynchs the signal and does not actually reboot the CM. [SCG-57683]
- 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. [SCG-51975]
- 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 R710 and R510 APs do not support the RTS packet size threshold when operating in 11ac 20 Mhz mode. [SCG-45294]
- The R710 and T710 APs do not honor the idle timeout setting as received in the RADIUS access accept message. [SCG-48133]
- The cable modem-related status LEDs on the C110 AP cannot be disabled from the controller's web interface. [SCG-56903]
- The total rate will be higher than the SSID rate limit because to each STA rate limit cannot be lower than 100kbps. Based on the current implementation, the minimum rate limit per station is 100kbps. As a result, the total rate (station number * 100kbps) will be more 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. [SCG-43697]

- When 11w is set to capable, the throughput goes down to less than 1Mbps after the channel is changed. [SCG-47051]
- 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 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]
- 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 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]
- Changing the UTP association in a user role takes effect after the next UE connection. [SCG-63835]
- Configuring static link speed on the R720's 2.5G Ethernet port using Ruckus AP CLI command is not supported. The port will auto-negotiate to 2.5Gbps/1000Mbps/100Mbps rates. [SCG-63519]
- When rogue AP detection is enabled on ac wave1/2 APs, sometimes deauth packets cannot be sent when a malicious AP is detected on the network. [SCG-61871]
- The H510 AP does not support PoE operating mode. [SCG-64376]
- When a controller-managed or standalone AP is moved to a new SmartZone cluster, the AP's configuration (including its WLANs) will remain the same if it was not factory-reset before it was moved to the new cluster. If the AP has WLANs, it will continue broadcasting the SSIDs. [SCG-59390]
- Sometimes, a target assert error occurs on the AP after the AP is migrated from a ZoneDirector controller to a SmartZone controller. [SCG-63749]
- An AP assigned an IPv6 address loses its IPv6 address after it connects to an SCG200 controller. This is design intent. [SCG-54582]
- 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 configuring walled garden entries, Ruckus Wireless recommends using IP addresses (not DNS names) to help ensure that the walled garden rules are applied consistently. [SCG-61183]
- 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]
- 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]
- Multicast traffic is always directed as unicast traffic, even when the AP has more than five clients associated with it. [SCG-46967]
- Mesh operation over 80+80/160MHz for R610 will be enabled in a future release.
- When the primary authentication server is unavailable, wired clients do not use the secondary authentication server that has been configured. [SCG-52194]
- A softlock sometimes occurs on an AP when it is in the process of being migrated from a ZoneDirector controller to a SmartZone controller. [SCG-63771]

- 11ac APs have limited target memory. To efficiently utilize the target memory, the 5GHz recovery SSID interface has been disabled on 11ac APs, as well as on the R710 APs. [SCG-44242]
- Multicast/unicast communication still occurs even after client isolation is enabled for an APLBO WLAN. [SCG-64652]

AP KPI Known Issues

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

- The AP capacity value increases after all traffic going through the AP ceases. [SCG-61611]
- When the AP sends bidirectional traffic, the estimated AP capacity shown on the web interface is incorrect. [SCG-57964]

Autonomous AP Known Issues

The following are the known issues related to autonomous AP.

- 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]

Bonjour Fencing Known Issues

The following are the known issues related to Bonjour Fencing.

- Bonjour Fencing is not yet supported for Google Chromecast. [SCG-63732]
- 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]
- Bonjour Fencing is not yet supported on mesh APs. [AP-4115]
- Bonjour Gateway does not support the gateway functionality for APs behind NAT, therefore Bonjour Fencing is also unsupported. [AP-4635]
- Bonjour Fencing is not supported for Tunnel WLANs. [AP-3842]
- Bonjour Fencing is not supported for DHCP/NAT GW AP. [SCG-64346]
- Bonjour Fencing of wired devices (wired fencing) requires wireless fencing to also be enabled for the same Bonjour Service Type.

Cassandra Known Issues

The following are the known issues related to Bonjour Fencing.

- WISPr authentication may fail if the CNR receives an invalid home server type. [SCG-52520]

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]
- 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]

Client Whitelist Isolation Known Issues

The following are the known issues related to Client Whitelist Isolation.

- A UE is able to access a mismatched whitelist after it has been connected to the WLAN for five minutes. [SCG-62531]

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]
- The web interface becomes blank when the administrator clicks a release 3.2.1 zone on the **Configuration** tab of the **Access Points** page .

  Workaround: Reapply the zone configuration. [SCG-64621]

- Only one AVP (either Filter-Id or Ruckus-User Groups) is supported in Access-Accept from AAA. [SCG-60630]
- If VLAN pooling is enabled for a legacy zone running 3.1.1, then DVLAN is always enabled and cannot be disabled. [SCG-61669]
- 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 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 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]

- IPv6 stateless addresses are unsupported. [SCG-59194]
- The SZ300 and vSZ-H support IPv6 zones with RuckusGRE tunnels, but the SZ100 and vSZ-E do not. [SCG-61781]
- CALEA
  - vDP will be given a MAC list (blacklist) for monitor all NB and SB traffic. Any packet with the matched MAC will be duplicated and sent to CALEA server through Ruckus secured tunnel.
  - vDP will build a high performance lookup tree or table from the MAC list. The lookup of this table will be conducted at the flow engine to avoid packet latency delay. Any subsequent packet of the same flow will consult only the flow entry for packet duplication to achieve no impact CALEA operation.
  - Local vDP conducting CALEA monitor will be given remote (data center) vDP address for Ruckus secured tunnel establishment. The remote (data center) vDP will be given all local vDPs addresses for tunnel establishment and CALEA server address for forwarding the CALEA packets to this ultimate destination. The CALEA packets come in from the Ruckus secured tunnels from all connected local vDPs.
  - The Ruckus secured tunnel is built through the TLS protocol between the tunnel managers inside each vDP. The TLS transaction only authenticates each other and provide the key if needed. It does not provide tunnel id or any other info as seen in tunnel connection between AP and vDP.

- There are keep-alive messages exchanged between vDPs for keeping the tunnel up. The messages are encrypted and contain vDP MAC, tunnel MTU, key info if needed, and other info.
- Tunnel MTU discovery is performed between the vDP peers.

Hotspot Known Issues

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

- 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]

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.

Scalability, Stability, and Performance Known Issues

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

- A high number of TX timeouts may occur in the presence of multi AC traffic streams. [SCG-49373]
- A SmartZone backup file exported from release 2.x cannot be imported to a controller running release 3.x. [SCG-50908]

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

- 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]

RAC Known Issues

The following are the known issues related to RAC.

- Ruckus Wireless recommends using additional session identification AVP, such as accounting-session-id/callingstationid, along with username for COA/DM. [SCG-48959]
- 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]

Reporting Known Issues

The following are the known issues related to reports.

- The SZ300, SCG200, and vSZ-H now only support four report types:

  1. Client Number
  2. Continuously Disconnected APs
  3. System Resource Utilization
  4. Tx/Rx Bytes

  Also, only hourly time intervals are supported, with a maximum duration of 24 hours. [SCG-63444]

- 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.

Session Manager Known Issues

The following are the known issues related to the session manager.

- When a client that is associated with a legacy AP running release 3.2.1 moves from one SSID to another SSID, and then sends DM from the AAA, the DM response will not be received from controller. [SCG-63947]
- The session manager process does not handle the session timeout of WISPr clients after a UE roams from one AP to another. [SCG-52369]
- WISPr login/logout won't change session start time and total session time. Following the same behavior of other WLAN type. [SCG-61369]

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]
- When tunnel mode is enabled on a WLAN, the controller is unable to query SNMP information on APs, radios, WLANs, and clients. [SCG-66157]

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]

System Known Issues

The following are the known issues related to the system.

- In a system configured with multiple domains, a report generated using a management domain as the filter does not have all the domain statistics. [SCG-62155]
- 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 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 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]
- 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]
- The default behavior of "Upload Patch Scripts" has been changed to to cluster-wide. This means that the uploaded script will automatically synchronize across nodes. [SCG-60218]
- 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 the SZ300 is managing at least 10K APs and 100K UEs, Ruckus Wireless strongly recommends avoiding generating a daily Client Number report at System domain level between 22:00 and 23:59 UTC. Doing so could impact system performance and cause the controller application to restart. Ruckus Wireless recommends generating this type of report after 00:00 UTC. [SCG-65954]
- Restoring an SCG200 configuration backup to the SZ300 will apply the SCG200 temperature threshold settings to the SZ300. This could cause the node's status to change to "Flagged." To clear this "Flagged" status, reset the temperature threshold on the SZ300. [SCG-65620]

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]
- After the idle session timeout mechanism automatically logs off an administrator from the web interface, the logon page appears. However, after every minute that passes, the Dashboard page reappears for a split second, and then changes back to the logon page again. [SCG-63725]
- On the Bonjour Gateway page, the Create button remains enabled after you select an existing policy. [SCG-54420]
- Administrators who do not have the privilege to manage alarms may be able to clear or acknowledge alarms in bulk. [SCG-34126]

- If the administrator changes the channelization setting for the 5GHz radio, the channel settings for the 2.4 GHz radio will be displayed as "Auto." However, the actual channel settings are unaffected; this is only a display bug.

  Workaround: Reconfigure the 2.4GHz radio settings after changing the 5GHz radio settings, and the 2.4GHz settings will remain the same. [SCG-52152]
- 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]
- 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]
- 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]
- 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 web interface only supports the following web browsers: Chrome 47+, Firefox 44+, Safari 7+ (Mac), Internet Explorer 11+, and Microsoft Edge. [SCG-63092]
- During a TTG call flow, the DHCP server stats under Diagnostics are not updated. [SCG-62316]
- On the Create User Group page, the selected domains are displayed in reverse order. [SCG-58403]
- The server name is overridden by a ladder diagram in Internet Explorer 11. [SCG-63365]
- The AP traffic graph does not fit into the legacy AP report. [SCG-62327]

- The FTP export functionality is only available on the SZ300, SCG200, and vSZ-H. Also, the "Daily" interval option for statistics has been removed and the default option is now "Hourly." [SCG-57099]
- When the SZ100 is upgraded from R3.2/R3.4 to R3.5, the AP firmware of zones are upgraded to R3.5 automatically. The AP firmware cannot be downgraded from R3.5 to R3.2/R3.4. [SCG-55911]
- 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]
- For the best user experience and optimum screen resolution, the web interface does not support zooming in or out. [SCG-56236]
- 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]
- The channel background application sends the channel number without checking whether the current channel mode supports the channel number. [SCG-60820]
- The list of AP models to which a patch applies is truncated on the AP Patch page. [SCG-62421]
- The zone template for auto-channel selection cannot be applied.

  WORKAROUND: Import or extract the zone template from the zone with auto-channel selection enabled (default value) and apply it to the specified zone. [SCG-65783]

- 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]
- If the web interface does not display elements correctly (for example, if the Dashboard icons do not load), Ruckus Wireless recommends refreshing the web browser manually. [SCG-65179, SCG-65180]
- 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]
- The "Enable on Each AP" option for DHCP configuration is not allowed in a mesh-enabled zone. However, the web interface does not prevent the user from selecting this option. [SCG-65486]
- 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]

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]

- 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]
- Static routes in vSZ cannot be added in bulk. To add multiple static routes, you need to add each static route individually. [SCG-49186]

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]
- 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]
- 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]

Wireless Clients Known Issues

The following are the known issues related to wireless clients

- On the web interface, the client fingerprinting feature displays "N/A" under "OS type" for connected clients running Android 7.0. [SCG-56991]

WISPr Known Issues

The following are the known issues related to WISPr.

- WISPr does not support IPv6 clients. [SCG-61036]
- When the primary AAA server is unreachable, authentication messages are not forwarded to the secondary AAA server. [SCG-49493]

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 where the controller behind NAT enhancement was incompatible with AP firmware download. [SCG-58191]
- Resolved an issue where, in mesh mode, if the root AP was set to 80MHz channelization and the mesh AP was set to 40/20MHz, the mesh AP failed to obtain an IP address. [SCG-57479]
- Resolved an issue where querying of history of clients with IPv6 addresses was unsupported. [SCG-57445]
- Resolved an issue where if the administrator performed a configuration restore via the CLI after a failed upgrade on the SZ100, the image upgrade failure state could not be reset. [SCG-52344]
- Resolved an issue where the both IPv4 and IPv6 syslog servers in a dual stack AP zone are enabled, APs did not send any syslogs to the IPv6 syslog server. [SCG-51777]
- Resolved an issue where vSZ logs displayed an "update failed" error message when updating the configuration of the R710 APs for the first time. [SCG-51436]
- Resolved an issue where Tunnel Termination Gateway (TTG) and PMIP were supported only when the controller was in standalone mode (not in cluster mode). [SCG-38585]
- Resolved an issue where the controller behind NAT enhancement was incompatible with AP firmware download. [SCG-58191]
- Resolved an issue where, in mesh mode, if the root AP was set to 80MHz channelization and the mesh AP was set to 40/20MHz, the mesh AP failed to obtain an IP address. [SCG-57479]
- Resolved an issue where querying of history of clients with IPv6 addresses was unsupported. [SCG-57445]
- Resolved an issue where if the administrator performed a configuration restore via the CLI after a failed upgrade on the SZ100, the image upgrade failure state could not be reset. [SCG-52344]
- Resolved an issue where when both IPv4 and IPv6 syslog servers in a dual stack AP zone are enabled, APs did not send any syslogs to the IPv6 syslog server. [SCG-51777]
- Resolved an issue where vSZ logs displayed an "update failed" error message when updating the configuration of the R710 APs for the first time. [SCG-51436]
- Resolved an issue where traffic from authorized UEs connected to a WISPr hotspot with web proxy enabled was no longer proxied to the controller. As a result, UEs connected to an AP running legacy firmware (3.4, 3.2 and 3.1) were unable to connect to the network. [SCG-50608]
- Resolved an issue where Tunnel Termination Gateway (TTG) and PMIP were supported only when the controller was in standalone mode (not in cluster mode). [SCG-38585]

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
SCG200	3.2.1.0.163
SZ100	3.2.1.0.253
vSZ (vSCG)	3.2.1.0.193
vSZ-D	3.2.1.0.217
	3.2.1.0.245
	3.4.0.0.976
	3.4.1.0.208
	3.4.2.0.152

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

In the SCG200, 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 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. In contrast, the SZ100 and vSZ-E automatically upgrade both the controller firmware and AP firmware when the system is upgraded.

Up to Three Previous Major AP Releases Supported

Each SCG200 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 will retain depend on the SCG200 release version from which you are upgrading.

- If you are upgrading the SCG200 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 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 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.

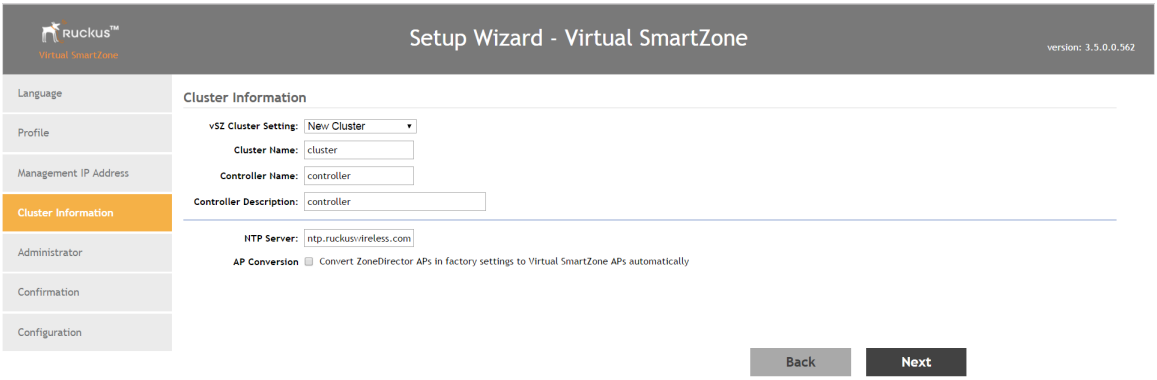
Follow these steps to convert standalone ZoneFlex APs to the SmartZone controller firmware so that they can be managed by the SZ300, SCG200, SZ100, or vSZ.

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