SmartZone 3.5 GA Refresh

Release Notes

Part Number: 800-71617-001 Rev A
Published: 26 May 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

1 Hardware/Software Compatibility and Supported AP Models

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: 3.5.0.0.832
- Control Plane Software Version: 3.5.0.0.564
- Data Plane Software Version: 3.5.0.0.832
- AP Firmware Version: 3.5.0.0.1444

SCG200

- Controller Version: 3.5.0.0.832
- Control Plane Software Version: 3.5.0.0.564
- Data Plane Software Version: 3.5.0.0.453
- AP Firmware Version: 3.5.0.0.1444

SZ100

- Controller Version: 3.5.0.0.832
- Control Plane Software Version: 3.5.0.0.564
- Data Plane Software Version: 3.5.0.0.219
- AP Firmware Version: 3.5.0.0.1444

vSZ-H and vSZ-E

- Controller Version: 3.5.0.0.832

- Control Plane Software Version: 3.5.0.0.564
- AP Firmware Version: 3.5.0.0.1444

vSZ-D

- vSZ-D software version: : 3.5.0.0.832

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*
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		

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

2

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

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]

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 does not work with DHCP/NAT on APs. [SCG-64358]
- 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]
- 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]

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.
- The Bonjour service is unable to establish a fence using the fencing neighbor’s RSSI. [SCG-59625]

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]

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 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]
- 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 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]

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.

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]

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]

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 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.

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]

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]

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]
- 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]

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]
- No UI/API for DHCP/NAT on vSZ-D. [SCG-63511]

- 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]
- 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]

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 3

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, SCG-61150]
- 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 an AP reboot due to a kernel panic issue that occurred when rate limiting with AVC was applied. [SCG-66174]
- 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 [SCG-68095]:
  - 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.

- Enhanced AP-to-AP communication to share the PMKR1 keys to all neighbor APs in peerlist, whether or not all the BSSIDs are in the neighbor table. This helps ensure that 11r feature functions normally. [ZF-17171]
- Resolved an LLDP MAC address issue. Now, APs use br0 MAC address for LLDP packets. [ER-5228]

Upgrading to This Release 4

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	3.2.1.0.163
SCG200	3.2.1.0.253
SZ100	3.2.1.0.193
vSZ (vSCG)	3.2.1.0.217
vSZ-D	3.2.1.0.245
	3.2.0.0.790
	3.4.0.0.976
	3.4.1.0.208
	3.4.2.0.152
	3.5.0.0.808

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 5

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.

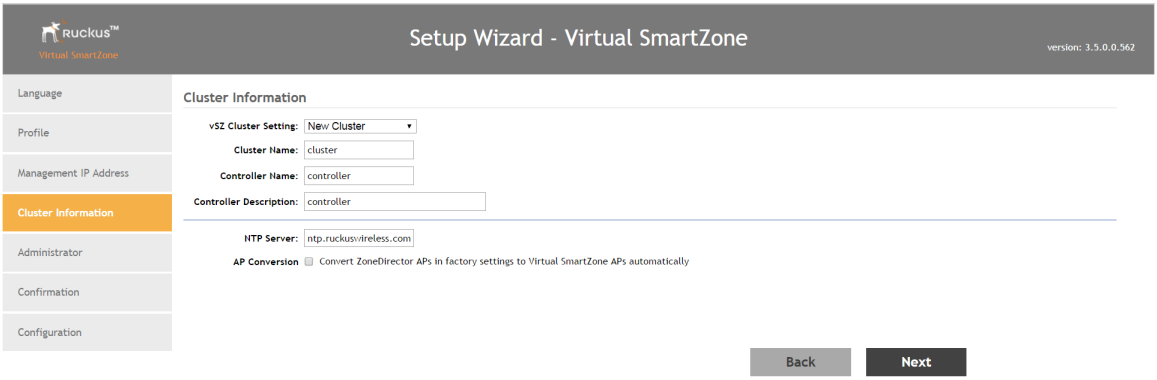
Follow these steps to convert standalone ZoneFlex APs to the SmartZone controller firmware so that they can be managed by the SZ300, SCG200, SZ100, or vSZ.

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