Ruckus
Simply Better Wireless.

SmartZone 3.4.2 Patch 1

Release Notes

Copyright Notice and Proprietary Information

Contents

New Features and Enhancements

This section lists the new features and enhancements in this release.

New Features

- Added a feature to modify **Adaptive Noise Immunity** on per zone per AP model. [FR-2591]

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

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

  These commands persist on AP after reboots.

  On the SmartZone CLI:

  1. CLI command name: 'ani-ofdm-level <AP Model> <Radio>'

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

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

  On the AP CLI:

  - CLI command name: 'set ani-ofdm-level <wifix> [0..9]'

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

NOTE   This feature is only available for Wave-2 APs

Hardware/Software Compatibility and Supported AP Models

<div style="text-align:right;">2</div>

This document provides release information about the SmartCell Gateway 200 (SCG-200), SmartZone 100 (SZ-100), Virtual SmartZone (vSZ), and Virtual SmartZone Data Plane (vSZ-D) features with notes on known issues, caveats, and workarounds.

- The SCG-200, 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 SZ-100, 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 SZ-100 models: the SZ-104 and the SZ-124.
- 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

- 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.

SCG200

- Controller version: 3.4.2.0.169
- Control plane software version: 3.4.2.0.89
- Data plane software version: 3.4.2.0.114
- AP firmware version: 3.4.2.0.373

SZ100

- Controller version: 3.4.2.0.169
- Control plane software version: 3.4.2.0.89
- Data plane software version: 3.4.2.0.41
- AP firmware version: 3.4.2.0.373

vSZ-H and vSZ-E

- Controller version: 3.4.2.0.169
- Control plane software version: 3.4.2.0.89
- AP firmware version: 3.4.2.0.373

vSZ-D

- vSZ-D software version: 3.4.2.0.169

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.

NOTE

APs preconfigured with the SCG200/SZ100/vSZ AP firmware may be used with the SCG200/SZ100/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.

Supported AP Models

This release supports the following Ruckus Wireless AP models.

- C110
- C500
- R300
- R310
- R500
- R500E
- R510
- R600
- R610
- R700
- R710
- T300
- T300E
- T301N
- T301S
- T504
- T610
- T610s
- T710
- T710S
- H500
- H510
- ZF7055
- ZF7352
- ZF7372
- ZF7372-E
- ZF7781CM
- ZF7782

- ZF7782-E
- ZF7782-N
- ZF7782-S
- ZF7982

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

Related Documentation and SNMP MIBs

This section describes the documentation and SNMP MIBs that are available for this release.

Related Documentation

NOTE   The SmartZone 3.4.2 Patch 1 release adds support for new AP models and includes fixes for some issues. No new features were introduced in this release, therefore the documentation remains the same as the 3.4.1 release.

To download the available documentation for this release, go to https://support.ruckuswireless.com/documents?query=smartzone+3.4.1.

SNMP MIBs

To download the SNMP MIBs for this release, click the following links:

- SCG200 and vSZ-H SNMP MIBs
- SZ100 and vSZ-E SNMP MIBs

Caveats, Limitations, and Known Issues

<div style="text-align:right">3</div>

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

Access Points

- If 802.11R roaming is enabled and when a client roams from AP1 to AP2, the *Class* and *Chargeable-User-Identity* attributes are missing in the Interim-Update packet sent by AP2. [SCG-70831]
- 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]
- 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 consistent. [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]
- The cable modem-related status LEDs on the C110 AP cannot be disabled from the controller's web interface. [SCG-56903]
- AP SNMPv3 displays INFORM when the notification type is set to TRAP. [SCG-56994]
- 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]
- On the controller's web interface, the LAN port status for the C110 is mislabeled. Additionally, LAN1/LAN2 mapping is incorrect. [SCG-58332]
- BEACON-MISS may be observed on the wlan63 interface of mesh APs if the channel on the root AP changes continuously. [SCG-49635]
- 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 802.11ac 20MHz mode. [SCG-45294]
- Based on the current design, the minimum rate limit per station is 100kbps. As a result, the total rate (station number * 100kbps) will be higher than the SSID rate limit -- this is design intent. For example, if the rate limit for downlink is 10Mbps for one

SSID, when an AP has 200 STAs associated with that SSID, the total rate will be 200 * 100kbps = 20,000kbps = 20 Mbps > 10Mbps.

WORKAROUND: Limit the maximum clients number per WLAN. Using the above example, you can set the maximum clients per WLAN to 100. [SCG-43697]

- H510 802.1X enabled Ethernet interface configured for MAC-based authentication fails to authenticate supplicants. [SCG-51986]
- 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]
- WISPr client session statistics are not properly moved to historical data after logout. [SCG-52507]
- 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 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]
- AVC with Trend Micro is unsupported on the following AP models:

  - ZF7982
  - ZF7782/ZF7782-S/ZF7782-N/ZF7782-E
  - ZF7781CM
  - SC8800-S/SC8800-S-AC
  - R300
  - ZF7372/ZF7372-E
  - ZF7352
  - ZF7055
  - H500 [SCG-50596]

- 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]
- The R710 and T710 APs do not honor the idle timeout setting as received in the RADIUS access accept message. [SCG-48133]
- 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 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]
- The 5GHz recovery SSID interface has been disabled on the T710 and R710 APs. [SCG-44242]
- Under high channel utilization (>90%), a high number of TX timeouts may occur in the presence of multi AC traffic streams. [SCG-49373]
- After the accounting service is disabled for a particular WLAN, Accounting Off messages are not initiated. [SCG-47772, SCG-40827]
- Solo APs are unable to discover the controller via Option 52. This is because DHCPv6 solicit messages from solo APs do not include Option 52 information. [SCG-34885]
- If 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]

Application Visibility and Control (AVC)

- If a wireless client roams from AP1 to AP2, AP1 can update all AVC statistics successfully, but AP2 may lose some AVC recognition updates. [SCG-43267]
- AVC is unable to identify BitTorrent traffic accurately. [SCG-43336]
- The Trend Micro engine that is used by AVC recognizes TFTP traffic based on port 69. Since only the first packet of TFTP traffic uses port 69, only the first packet is detected as 'tftp'. [SCG-44064]
- When AVC cannot determine the application that a device is using, the controller displays the device's IP address as the application name. [SCG-47746]
- The AVC denial policy requires both the user-defined app and app port mapping, instead of only the user-defined app name. [SCG-44724]
- If a Skype P2P tunnel is set up before the Application Denial Policy is applied, the controller cannot identify the traffic and will allow the call through. [SCG-52257]
- AVC is unable to identify Vindictus traffic accurately. [SCG-43487]
- When configuring a denial policy in AVC, take note of the following limitations:

  - When "google.com" is set as the AVC denial policy, traffic to the Google website may not be blocked because most Google traffic is encrypted. Google traffic is marked "Google(SSL)" or "SSL/TLS," which does not match the policy, so traffic is not denied.

- When "music.baidu.com" is set as the AVC denial policy, traffic to the Baidu web site may not be blocked because most Baidu traffic is marked as "BaiduMusic" or "baidu", which does not match the policy, so traffic is not denied.
- BitTorrent download traffic may be difficult to block unless the app IDs, such as "BitTorrent Series", "BBtor","eDonkey Series", "SoMud", etc, are specified in the policy. If you set the denial policy to "xxx. net", " xxx.cn", "xxx.org" , etc., AVC will be unable to block such traffic because Trend Micro recognizes the app name without the domain extension.
- To block Sina mail traffic, deny traffic to both "sina mail" and "sina.com."In the denial policy, the space character is taken into consideration. For example, if you block "qq game" or "sina video", users will still be able to access "qqgame" or "sinavideo" (no space character). Conversely, if you block "baidumusic" (no space character), traffic to "baidu music" will not be blocked.
- When blocking Hotmail or Outlook.com traffic, set the denial policy to "live" or "live.com". If you block "hotmail" or "outlook.com", user will still be able to access Outlook.com. [SCG-44384]

- When the authentication type is set to webauth, an application that has been configured to be denied sometimes still passes data through the AP. [SCG-61444]

Cassandra

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

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 SZ-100, the DNS IP address has to be configured manually because DNS IP address assignment via DHCP cannot be completed. [SCG-38184]

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

- When testing an IPv6 accounting server, the NAS IP4 attribute is sent in the accounting message. [SCG-61667]
- If VLAN pooling is enabled for a legacy zone running 3.1.1, then DVLAN is always enabled and cannot be disabled. [SCG-61669]
- Network tunnel statistics are not displayed for dual stack APs when queried with an IPv6 address. [SCG-57446]

- The forwarding service is unsupported on the SZ-100, 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]
- When rate limits are modified, the new limits are not applied to clients that are in the grace period. [SCG-51422]
- 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]

- 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. To resolve this issue, Ruckus Wireless recommends assigning a static IP address to the SZ-100 network interface. [SCG-41046]
- 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]
- TTG Session Summary is not as part of associated clients for TTG sessions established using a TTG+WISPr profile. [SCG-32706]

Control Public API

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

RAC

- 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]
- COANAK/DMNAK is received if COA/DM messages are sent to the node that does not have the corresponding WISPr/WebAuth session. [SCG-48959]
- When the primary authentication server is unavailable, wired clients do not use the secondary authentication server that has been configured. [SCG-52194]
- When the primary AAA server is unreachable, authentication messages are not forwarded to the secondary AAA server. [SCG-49493]

- The Ethernet port-based profile selection feature was added along with AD/LDAP enhancements. However, the related settings are unavailable on the web interface. [SCG-39032]
- 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]

Scaling/Performance

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

SCG200

- 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]

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]
- Client frame IP addresses are sometimes sent as 0.0.0.0 in AP-initiated accounting messages. [SCG-47164]
- The session manager process does not handle the session timeout of WISPr clients after a UE roams from one AP to another. [SCG-52369]

SNMP

- The event type and SNMP trap for Event 518 do not match. [SCG-49689]

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]
- Syslog servers that are using IPV6 addresses are currently unsupported. [SCG-53679]

System

- 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. This is design intent. [VSCG-1509]

- When vSZ is upgraded from release 3.2 to a newer release, the web interface cannot be accessed using the Microsoft Internet Explorer 11 browser. [SCG-48747]
- 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 SZ-100 and vSZ are unsupported. Only accounting servers on the SCG-200 can be assigned IPv6 addresses. [SCG-46917]
- With this release, SmartZone to SCI communications can be enabled through the web interface using the new SCI Management setting in the SZ web interface. However, this feature only works for SCI version 2.0 (and later). If you are using an older version of SCI (1.x), you will still need to execute the "ap-sci enable" command to allow SZ-SCI communications, even after upgrading the SZ to 3.4. [SCG-51832]
- After the accounting service is disabled for a particular WLAN, Accounting Off messages are not initiated. [SCG-47772]
- 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]
- 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]

- 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]

- 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 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]

- The controller may be unable to renew its DHCP server-assigned IP address, which may cause all controller services to go down. [SCG-40383]
- 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]
- The controller's management interface IP address may not be changed from DHCP to static IP address mode. [SCG-35281]
- 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 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]
- When the SMTP settings on the controller are configured and the outbound firewall is enabled, the SMTP packets are dropped. [SCG-64695]
- When AP Subnet discovery is enabled on the controller and the outbound firewall is enabled, the port 5353 related to subnet discovery packets are dropped. [SCG-64701]

UI/UX

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

- When the AP bundle is applied to SZ100 or vSZ-E, 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]

- When the Device Policy feature is enabled, the host name Chrome devices and PlayStation appear as "N/A" on the web interface. This occurs because "DHCP option 12" does not exist in DHCP Discover and DHCP Request. [SCG-50595]
- The SZ-100 Setup Wizard does not validate the IPv6 address if the IPv6 prefix is not configured. [SCG-40257]
- Administrators who do not have the privilege to manage alarms may be able to clear or acknowledge alarms in bulk. [SCG-34126]
- Some of the options for the Certificate Store page may not show up on the Safari web browser. [SCG-34971]

vSZ

- When the controller is behind a NAT server, APs are assigned both public and private IP addresses. [SCG-46949]
- Static routes in vSZ cannot be added in bulk. To add multiple static routes, you need to add each static route individually. [SCG-49186]
- 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]
- 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]

- 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]
- 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]
- 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]

- vSZ does not generate syslog messages about the number of free licenses left. [ER-4896]

  WORKAROUND: Set the log level of Scheduler to Info.

Resolved Issues 4

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

- Resolved an LLDP MAC address issue. Now, APs use *br0 MAC address* for LLDP packets. [ER-5228/AP-4919]
- Resolved an issue where TCP MSS synchronization failed between the AP and server. [ER-4042]
- Resolved an issue where, if Force DHCP was enabled, clients would be de-authenticated after roaming to another AP if the VLAN was the same as the previous VLAN after roaming. [ER-4992]
- Resolved a device fingerprinting issue where Ubuntu clients failed to be categorized as Linux OS clients. [ER-5121]
- Resolved an issue of excessive AP-to-AP ARP traffic, which caused network congestion in high-density settings. Resulting in port isolation usage rather than fast roaming. [ER-5138]
- Resolved an issue, where the cloud license server was unreachable when the firewall was enabled. [ER-5168]
- 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 guest pass configuration could not import the alphabets *i, I,l,L,o,O* and numbers *0 and 1*. [ER-5260]
- Resolved an issue where the AP kernel panic reboot was caused on receiving malformed BTM response frame from certain type of clients. [ER-5386]
- Resolved an issue of failed login attempt logs were not sent to the remote syslog server. [ER-5443]
- Resolved issues, by:
    - Adding IP source guard entries at relaying DHCP offer from TTG to virtual DHCP server
    - Adding IP source guard entry on Gateway IP
    - Resolving the browsing issue when roaming from Bridge WLAN to TTG WLAN
    - Setting the DHCP lease time to 3600 seconds on TTG WLAN to prevent IP to MAC binding ION datablade prematurely aging out
    - Avoiding potential packet access after it is free
    - Avoiding potential memory corruption on 3rd Party AP configuration
    - Dropping DNS packets which uses GTP port which causes the core to hang.
    - Eliminating core dump utility in the controller SCG200 which caused the core to hang. This was caused by logging problematic packets. [SCG-68035/ER-5358/ER-5222/ER-5009/]
- Resolved an issue of load balancing in tunnel manager. [SCG-68531/SCG-68532/ SCG-68530/ER-5245]

- Resolved an issue where the code logic is fixed to get the latest tunnel information for both access and core sides. [ER-5311]
- Resolved an issue where Northbound/Core process did not retry socket connection towards MsgDist after the first failure, which caused login failure of WISPr clients. [ER-5382]
- Resolved an issue where AP could fail to stay on a statically configured channel. [ER-5074]
- Resolved vDP logging issue in order to manage the amount of logs to be archived. [ER-5092]
- Resolved issues on the vDP side by:

  - Adding validation of tunnel keepalive packet to avoid receiving false packet which cause MTU size spike.
  - Adding validation of MAC address in the tunnel keepalive message to avoid duplicate tunnel identifiers. [ER-5424/ER-5476]

- Resolved an issue where the Guest Pass expiration validation was invalid on authentication failure after the expiration time. [ER-5399]
- Resolved an issue where migration of guestpass configuration from ZD (9.13.0.0 build 232) failed and required support of alphabets *i, I,l,L,o,O* and numbers *0 and 1*. [ER-5334]
- Resolved an issue where message digest and Java were consistently spiking. [ER-5128]
- Resolved an issue where the log showed that the AP was reset to factory defaults.[ER-4282]
- Resolved an issue where one of the data plane's rebooted after data plane´s core dead. [ER-3902]
- Resolved a memory leak issue which caused R510s to target assert. [ER-5383]
- Resolved an issue of LWAPP2SCG crash due to checking of nullpointers. [ER-5018]
- Resolved an issue on QoS classification. [ER-5319]
- Resolved an issue where incorrect traffic counter values were included in Accounting Stop for a TTG client, which roamed across different data planes and control planes in quick succession. [ER-5372]
- For resolution of CVE-2004-2761, refer to the security advisory (https://www.ruckuswireless.com/security). [ER-4478]

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.

NOTE

- In pre-3.2 releases, AP firmware download from the controller is performed over an HTTP connection on port 91 in the clear.
- In release 3.2, the controller uses an HTTPS connection and an encrypted path for the firmware downloads. The port used for AP firmware downloads was also changed from port 91 to 11443 to distinguish between the two methods.
- In release 3.4, the controller uses port 443 for AP firmware downloads. To ensure that all APs can be upgraded successfully to release 3.4, open ports 443, 11443 (for cluster restore to release 3.2), and 91 in the network firewall.

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.

IMPORTANT   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. Apply SCG47455_WorkAround_RP_OS_433930.ksp, which fixes SCG-47455.
2. Adjust the system resources allocated to the virtual machine on which vSZ is installed (see the recommended resource tables below).
3. Upgrade vSZ to this release.

Table 1: High Scale profile configuration: Recommended system resources

Nodes per Cluster	AP Count per Cluster		Client Count	Disk Size	vCPU	RAM	Preserved Events	Resource Level
	Min	Max	Max	GB	Core	GB	Max	
3-4	10,001	30,000	300,000	600	24	48	3M	8
1-2	5,001	10,000	100,000	600	24	48	3M	7
1-2	2,501	5,000	50,000	300	12	24	2M	6.5
1-2	1,001	2,500	50,000	300	6	19	1.5M	6
1-2	501	1,000	20,000	100	4	15	600k	5
1-2	101	500	10,000	100	4	14	300k	4
1-2	1	100	2,000	100	2	13	60k	3

Table 2: Essentials profile configuration: Recommended system resources

Nodes per Cluster	AP Count per Cluster		Client Count	Disk Size	vCPU	RAM	Preserved Events	Resource Level
	Min	Max	Max	GB	Core	GB	Max	
3-4	1,025	3,000	60,000	250	8	23	10k	3
1-2	101	1,024	25,000	250	8	23	10k	2
1-2	1	100	2,000	100	2	15	1k	1

Using the "Extend Upload Precheck Timeout" Script

Whenever you upload an upgrade image to the controller, the controller starts a timer to monitor the status of the upload process at set intervals. If the upload process is not completed within 10 minutes, the controller terminates the upload process and aborts the upgrade attempt.
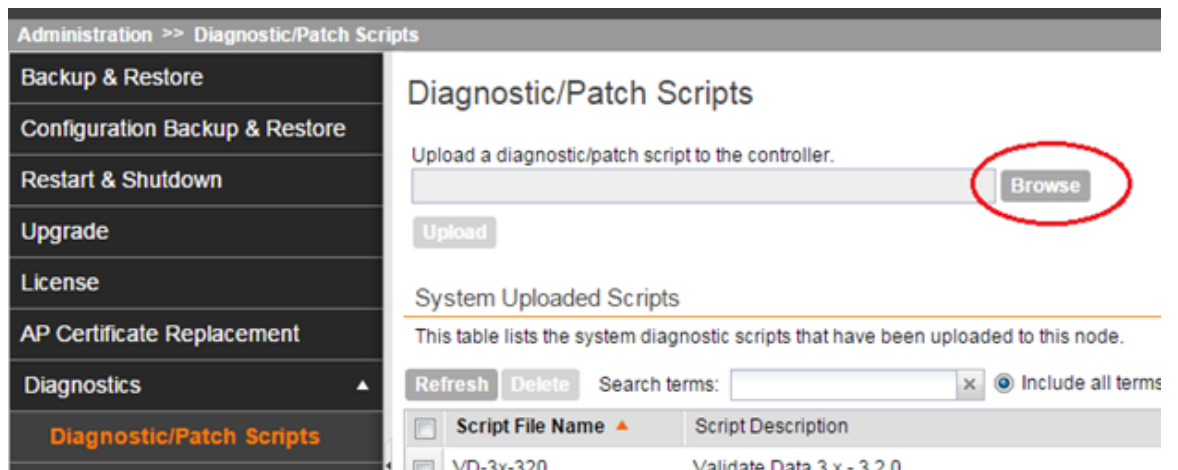
In release 3.2.1, Ruckus Wireless introduces a data migration precheck process that must be completed *before* the upgrade process can start. When you upload an upgrade image, the controller will first check the database for issues before it starts the upgrade process. This new pre-check increases the duration of the image upload process and could potentially cause the upload timer to time out and the upgrade attempt to fail.

To ensure that the upload timer does not time out, apply the extend upload precheck timeout KSP (script file).

IMPORTANT   Apply the KSP before you upload the upgrade image file.
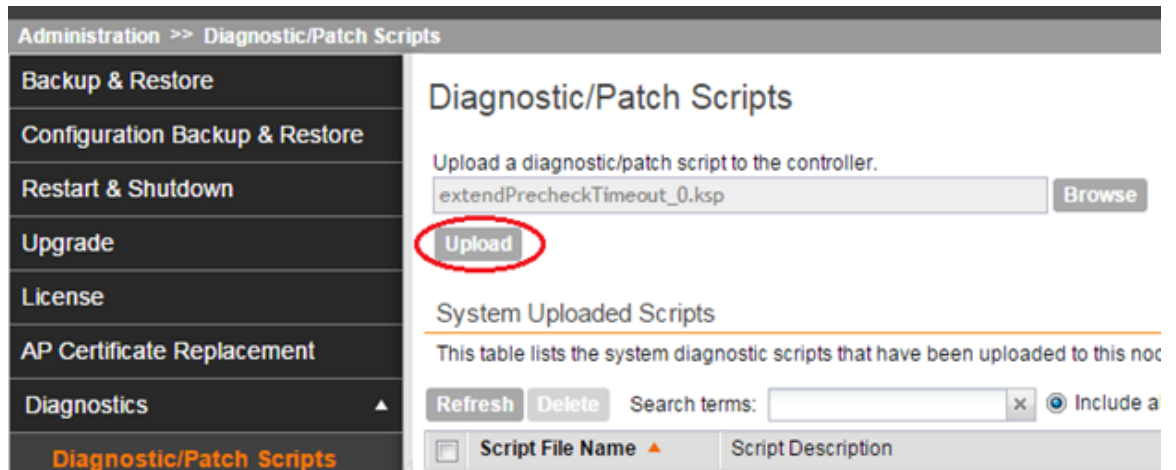

IMPORTANT   The precheck process requires at least 2GB of available system memory to proceed with the upgrade. If the system has less than 2GB of available system memory, the precheck process will abort the upgrade attempt.

---

1. Download the KSP file from the Support website to your computer. The file name is `extendPrecheckTimeout_0.ksp.`

2. Log on to the controller, and then go to **Administration** > **Diagnostics** > **Diagnostic/Patch Scripts**.

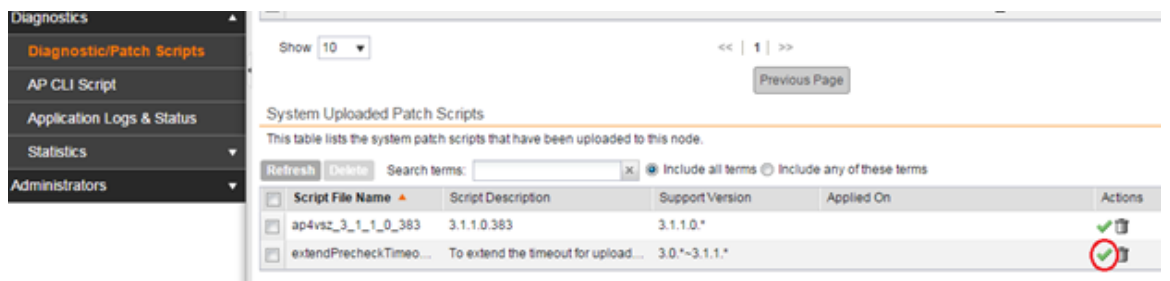3. Click **Browse**, and select the KSP file that you downloaded.

4. Click **Upload**.

5. When the KSP file appears on the list of available scripts, click the green check mark under the **Actions** column.

After the KSP script is applied, upload the upgrade image file, and then upgrade the controller to this release.

Performing Preupgrade Validation

Another enhancement to the upgrade process that Ruckus Wireless added in this release is preupgrade validation.
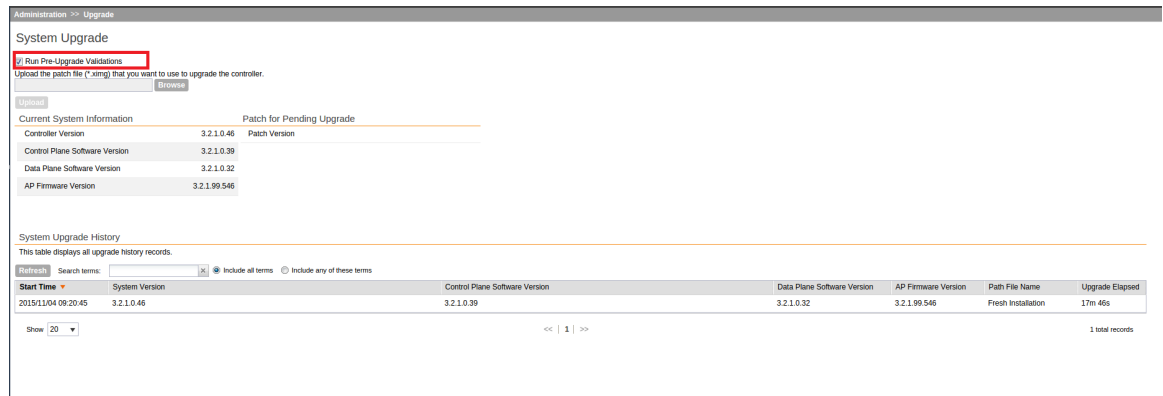
Preupgrade validation automatically runs if you are upgrading from release 3.2 or earlier. However, if you are upgrading from an earlier 3.2.1 release, you need to manually enable preupgrade validation by going to **Administration** > **Upgrade**, and then selecting the **Run Pre-Upgrade Validations** check box.

Preupgrade validation checks for data migration errors before performing the upgrade. If data migration was unsuccessful, this error message is displayed: `Exception occurred during the validation of data migration. Please apply the system configuration backup and contact system administrator.` If this occurs, take a backup of the system configuration and contact Ruckus Wireless to resolve the issue.

To access the logs of the validation process, log on to the web interface, and then navigate to **Administration** > **Diagnostics** > **Application Logs** > **Datamanager** > **datamanager.log**.

Figure 1: Pre-upgrade validation

NOTE If data migration validation fails due to insufficient memory, the following error message appears: `Insufficient memory. The system requires at least 2 GB of available memory to complete data validation.` Therefore, Ruckus Wireless recommends the following:

- If you are upgrading a physical controller, restart the controller to free up memory.
- If you are upgrading a virtual controller, allocate additional memory to the virtual machine, and then restart the virtual machine instance.
- Alternatively, clear the check box above to upgrade the controller to the new release without completing data validation.

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 the previous releases that can be upgraded to this release.

Table 3: Previous release builds that can be upgraded to this release

Platform	Release Build	Release Build
SCG200	3.1.0.0.236	3.2.0.0.790
SZ100	3.1.0.0.249	3.2.1.0.134
vSZ (vSCG)	3.1.1.0.442	3.2.1.0.139
vSZ-D	3.1.1.0.450	3.2.1.0.163
	3.1.1.0.474	3.2.1.0.193
	3.1.1.0.476	3.2.1.0.217
	3.1.2.0.95	3.2.1.0.245
	3.1.2.0.513	3.2.1.0.247
	3.1.2.0.520	3.2.1.0.253
	3.1.2.0.536	3.4.0.0.659
	3.1.2.0.1015	3.4.0.0.745
	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 SZ-100 or SCG-200 is managing APs that have reached EoL and the possible workarounds for each issue. [SCG-42511, SCG-43360]

Table 4: Issues and workarounds for upgrading the SZ-100 with EoL APs

Release Version	Issue	Workaround
3.1, 3.1.1	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 following is an example of the warning message: Your current system cannot be upgraded. Reason:The system cannot be upgraded, because the following AP model(s) will be unsupported: ZF7343 * 1" Despite this limitation, the **Upgrade** and **Backup & Upgrade** buttons remain visible and clickable, which seem to indicate that the controller can still be upgraded. However, when you click **Upgrade** or **Backup & Upgrade**, the upgrade attempt fails because of the unsupported APs.	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.
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.	

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 5: Issues and workarounds for upgrading the SCG-200 with EoL APs

Release Version	Issue	Workaround
3.1, 3.1.1	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 following is an example of the warning message: Your current system cannot be upgraded. Reason:The system cannot be upgraded, because the following zone(s) will be unsupported: v1.1.2.0.93 * 1 Despite this limitation, the **Upgrade** and **Backup & Upgrade** buttons remain visible and clickable, which seem to indicate that the controller can still be upgraded. However, when you click **Upgrade** or **Backup & Upgrade**, the upgrade attempt fails because of the unsupported APs.	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.
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.	

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.

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 SCG-200 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, 3.1 and 3.1.1 are considered part of the same major release version, which is 3.1.

The following releases can be upgraded to release 3.4:

- 3.2.x
- 3.2
- 3.1.x
- 3.1

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 3.2, then the AP firmware releases that it will retain after the upgrade will be 3.4 and 3.2.
- If you are upgrading the SCG200 from release 3.1, then the AP firmware releases that it will retain after the upgrade will be 3.4, 3.2, and 3.1.

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

- 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.

Compatibility with 64MB APs

Ruckus Wireless APs with 64MB memory have reached end-of-life (EoL) status and are no longer supported in this and later releases. If you have 64MB APs that are being managed by the controller and you want to keep using these APs to provide Wi-Fi services to users, ensure that these APs belong to zones running release 3.1.x or earlier.

Table 6: To continue managing 64MB APs, they must belong to zones running release 3.1.x or earlier

Release	Compatible Release as a Zone	64MB AP Support
3.4	3.1 3.1.x 3.2 3.2.x	64MB APs must belong to a zone running release 3.1.x or earlier.

Interoperability Information

<div style="text-align: right; font-size: 3em;">6</div>

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 higher.

The AP base image is optimized for controller-discovery compatibility to support all Ruckus Wireless controller products including ZoneDirector, SCG-200, vSZ, SZ- 100, and SAMs.

Once the AP discovers and joins a controller (for example, the SZ-100), 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

The information in this section applies to standalone ZoneFlex APs (those that are not managed by ZoneDirector), in factory default configuration, to the SCG- 200/SZ-100/vSZ.

Follow these steps to convert standalone ZoneFlex APs to the SCG-200/SZ-100/ vSZ firmware so that they can be managed by the SCG-200, SZ-100, or vSZ.

1. When you run the SCG-200, SZ-100, or vSZ 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 SCG-200 Setup Wizard. If you are setting up SZ-100 or vSZ, the check box description may be slightly different
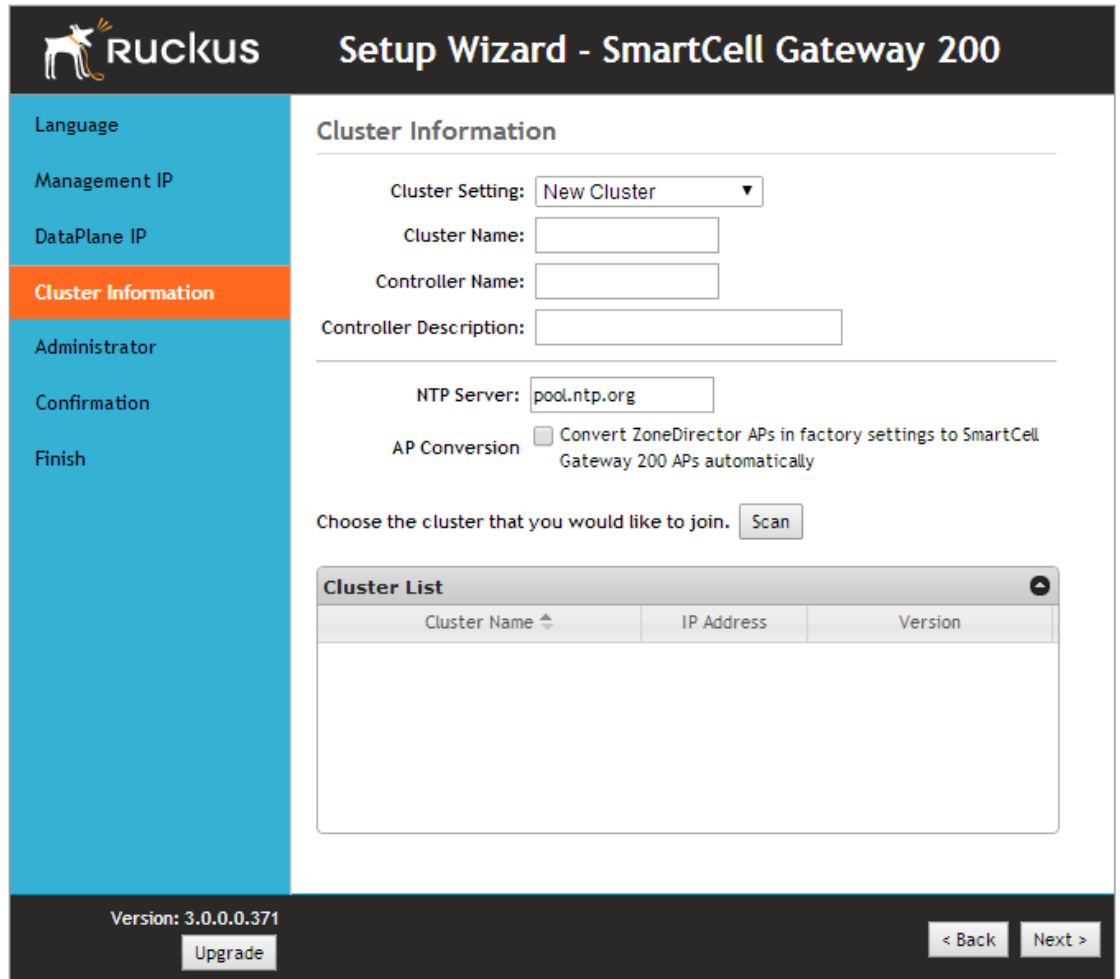
Figure 2: Select the AP Conversion check box to convert standalone ZoneFlex APs to SCG-200/SZ-100/vSZ APs

2. After you complete the Setup Wizard, connect the APs to the same subnet as the SCG-200/SZ-100/vSZ.
   When the APs are connected to the same subnet, they will detect the SCG-200/SZ-100/vSZ on the network, and then they will download and install the AP firmware from SCG-200/SZ-100/vSZ. After the SCG-200/SZ-100 firmware is installed on the APs, the APs will automatically become managed by the SCG-200/SZ-100/vSZ 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.