SmartZone 3.4

Release Notes

Copyright Notice and Proprietary Information

Contents

1 What's New in This Release

2 Hardware/Software Compatibility and Supported AP Models

3 Caveats, Limitations, and Known Issues

4 Resolved Issues

5 Resolved Customer Reported Issues

6 Upgrading to This Release

7 Interoperability Information

What's New in This Release 1

This section provides a high-level overview of several key features that are introduced in the SmartZone (SZ) software release 3.4. For detailed descriptions of these features and configuration help, refer to the SmartZone 3.4 documentation set.

IMPORTANT The ZeroIT feature has been removed in this release. The suggested alternative to ZeroIT is to use Cloudpath.

The SZ release 3.4 is applicable to the RuckusWireless SmartCell Gateway 200, SmartZone 100, vSZ-H, and vSZ-E controller platforms. In this release, RuckusWireless introduces support for two new AP models (T710 and R510) and adds the ability to support new APs without upgrading the software on the controller. For a complete list of supported access point models, see Supported and Unsupported Access Point Models.

New AP Model

This new feature allows new AP models to be supported, without upgrading the controller software on SZ. In the future, new APs with new firmware can be released without upgrading the software on the controller. With this feature, SZ firmware releases and AP firmware releases are de-coupled and each of them can be upgraded, independent of each other. An example of this will be to upgrade AP firmware to fix a bug on AP without upgrading the controller software.

New APs

- *T710*: The T710 is a carrier grade dual-band concurrent 802. 11ac Wave 2 outdoor access point with 4x4: 4 antennas, dual GbE ports and an SFP fiber interface. The T710 supports PoE in, PoE out, Ethernet port aggregation, and hot swappable SFP fiber optic module.
- *T710s*: The T710s is the 120-degree sector antenna variant of the T710. It includes all of the same features as the T710.
- *R510*: The R510 is a new midrange 2x2: 2 dual-band 802. 11ac Wave 2 indoor access point with dual GbE ports, 802.3af/ at PoE in, USB port for BLE (Bluetooth Low Energy) module or 3G/LTE backhaul dongle, and flexible mounting options including wall, ceiling and t-bar mounting.

Cluster Name Change Using the CLI

The cluster name can now be changed using the command "`cluster-name <new-name>`" on the CLI.

AWS Support

The vSZ can be deployed on AWS with this release. An OVA image will be available to deploy vSZ on AWS.

Dynamic Pre-Shared Key (DPSK)

DPSK eliminates tedious and time-consuming manual installation of encryption keys, passphrases or user credentials needed to securely access a wireless network. Dynamic PSK changes this model by dynamically generating strong, unique security keys for each authenticated user, automatically installing these encryption keys on end user devices with little or no human intervention.

Following are few example deployment scenarios, where DPSK can be deployed:

- IOT (Headless devices)
- Deployments, where there are no RADIUS servers
- Legacy devices which does not support 802.1X
- Mobile devices

DPSK can be manually generated or through automated onboarding process (through Cloudpath).

Per SSID Rate Limiting

This feature allows you to perform rate limiting on per-SSID basis. The amount of bandwidth consumed by an SSID can be configured with upload limit, download limit, or both. With this feature, for example, you can apply a rate limit on the guest SSID, but not on the SSIDs used by employees.

Enhancements to SZ behind NAT

With this new enhancements, APs can be located outside of NAT or on the internal network. This deployment model is supported with the new enhancements. This enhancement allows SZs and APs to be deployed in wide variety of deployment scenarios, with respect to deploying SZ and APs behind NAT.

Support for 802.11r/k (WSON)

WSON (Wireless Self Optimization Network) is a set of enhancements on SZ and APs, which allows for fast roaming of clients between APs, by exchanging and sharing of load and other performance data between APs. A few other enhancements to authentication and authorization have been implemented to make roaming between APs faster.

Mesh Support for Wave2 APs

This release adds support for mesh on Wave2 APs (for example, R710).

Application Recognition Enhancements

A new Trend Micro based Application Recognition Engine has been introduced. This new engine recognizes 2000+ applications. This new engine also detects applications better and more efficiently. Note that this feature is only available for certain AP models (specifically, those with 128MB or higher RAM).

Secure Firmware Upgrade (Using 443 Port)

This feature allows for securely upgrading firmware through port 443 (the standard port used for SSL traffic) and this enhancement allows the firmware to be downloaded securely.

DNS Override

This feature allows configuration of customizable DNS servers. This will allow to override the default DNS used. This will allow the users to connect to different servers, based on configuration in different DNS servers. Using this feature, DNS based content filtering can be enforced.

SmartCell Insight (SCI) Interface Enhancements for AVC

Application usage (AVC) data will be sent to SmartCell™ Insight, starting with this release. This will allow generation of Application Visibility reports on SCI. For applications data to be sent from SZ to SCI, the SCI server details have to be configured on SZ.

Smart Positioning Technology (SPoT) Interface Enhancements

Smart Positioning Technology, a cloud-based Smart Wi-Fi location-based services (LBS) user positioning technology suite from Ruckus Wireless, relies on the time synchronization. To allow for efficient synchronization of time and ability to query time, new APIs have been added to query and synchronize time between SPoT, controllers and APs.

Public API Enhancements

A set of new public APIs has been added to improve the programmable interface of SZ. The following are few examples of new APIs:

- Enhancement to AP rules API
- API for cluster backup and restore
- API to identify user role

These are just a sample of the APIs that have been added. Complete set and detailed documentation is available in user and API guides.

Test AAA Functionality Enhancements

PAP and CHAP options have been added to the web interface.

802.3at

Support for 802.3at power mode has been added. 802.3at mode will be used, when auto mode is selected. User has option to select other power modes.

AP Image Security Enhancements

AP images will be signed when AP image is created. APs will verify the AP image signature before storing and loading the image.

Hardware/Software Compatibility and Supported AP Models

2

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 (SCG-200)
- SmartZone 100 (SZ-100)

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.

- Controller version: 3.4.0.0.976
- Control plane software version: 3.4.0.0.494
- Data plane software version: 3.4.0.0.548
- AP firmware version: 3.4.0.0.1306

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 SCG-200/SZ-100/vSZ AP firmware may be used with the SCG-200/SZ-100/vSZ in their native default configuration. APs factory-configured with the ZoneFlex-AP firmware may be used with the SCG-200/SZ-100/vSZ when LWAPP discovery services are enabled.

Supported AP Models

This release supports the following Ruckus Wireless AP models.

- C500
- FZM300
- FZP300
- H500

- R300
- R310
- R500
- R500E
- R600
- R700
- R710
- T300
- T300E
- T301N
- T301S
- T504
- T710
- T710S
- 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.

- SC 8800-S
- SC 8800-S-AC
- 7321
- 7321-U
- 7441
- 7761-CM
- 7762
- 7762-AC
- 7762-T
- 7762-S
- 7762-S-AC
- 7363
- 7343
- 7341
- 7363-U

- 7343-U
- 7025
- 7351
- 7351-U
- 2942
- 2741
- 2741-EXT
- 7962

Caveats, Limitations, and Known Issues 3

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

Access Points

- Short Guard Interval support on 160 MHz is displayed as enabled in beacons (in VHT capabilities info) on R610 AP even though the AP does not support 160MHz operation. [SCG-52531]
- If the user changes the Channelization setting for the 5 GHz radio, the Channel settings for the 2.4 GHz radio will be displayed as "Auto." (Note that the actual channel settings are unaffected, this is only a display bug).

  WORKAROUND: Reconfigure the 2.4 GHz radio settings after changing the 5 GHz radio settings, and the 2.4 GHz settings will remain in place. [SCG-52152]

- 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-512529]

- 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]
- BEACON-MISS may be observed on the wlan63 interface of mesh APs if the channel on the root AP changes continuously. [SCG-49635]
- A high number of tx timeouts may occur in the presence of multi AC traffic streams. [SCG-49373]
- The R710/T710 AP does not honor the idle timeout setting as received in the RADIUS access accept message. [SCG-48133]
- 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]
- Client frame IP addresses are sometimes sent as 0.0.0.0 in AP-initiated accounting messages. [SCG-47164]
- When 11w is set to capable, the throughput goes down to less than 1Mbps after the channel is changed. [SCG-47051]
- When the controller is behind a NAT server, APs are assigned both public and private IP addresses. [SCG-46949]

- 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]
- 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]

- Some access points may use channel 0 on the 5GHz radio, which prevents wireless clients from associating successfully with them. [ER-3791]
- 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 will not 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 R710 and R510 APs do not support the RTS packet size threshold when operating in 11ac 20 Mhz mode. [SCG-45294]
- When configuring rate limiting, the total rate will be higher than the SSID rate limit because the rate limit on each STA cannot be lower than 100kbps. Based on the current implementation, the minimum rate limit per station is 100kbps. As a result, the total rate (station number * 100kbps) will be more than the SSID rate limit -- this is design intent. For example, if the rate limit for downlink is 10Mbps for one SSID, when an AP has 200 STAs associated with that SSID, the total rate will be 200 * 100kbps = 20,000kbps = 20 Mbps > 10Mbps.

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

- Before you convert a solo R510 AP to a controller-managed AP, make sure you disable lwapp2scg on the controller. Otherwise, the AP may be unable to join the controller successfully. [SCG-52226]
- Solo APs running release 100.x may be unable to obtain firmware from the controller's control IP address if the control IP address is behind NAT.

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

Application Recognition for Visibility and Policy Control

- 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 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

- 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 user-defined app and app port mapping, instead of only user-defined app name. [SCG-44724]
- When setting the denial policy in AVC, take note of the following limitations:

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

- When blocking Hotmail or Outlook.com traffic, set the denial policy to "live" or "live.com". If you block "hotmail" or "outlook.com", user will still be able to access Outlook.com. [SCG-44384]

- The 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 cannot identify Vindictus traffic accurately. [SCG-43487]
- AVC cannot identify BT traffic accurately. [SCG-43336]
- 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]

Authentication and Accounting

- 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 `Idle-Timeout` RADIUS attribute does not override the WLAN-configured inactivity timeout on 11ac APs. [SCG-45783, SCG-48133]

Backup and Restore

- If an administrator performs a configuration restore via CLI after an upgrade failure on the SZ-100, in some situations, the nodes will remain in service but the image upgrade failure state cannot be reset. [SCG-52344]

  WORKAROUND:

  1. Wait for 1~2 hrs for the cluster to return to service, and then use the web GUI to restore backup.
  2. Use restore local by CLI command if disconnecting the network is possible.

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

CLI

- CLI configuration logic differs between configuring individual APs and configuring model-specific settings from the AP Group context. [SCG-52077]

IPv6

- 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]
- Wireless clients may sometimes be unable to access the IPv6 web server. [SCG-50797]
- The IPv6 syslog does not work when the AP is in a dual IP mode AP zone. Take note of the following:

  - The AP supports only one syslog IP configuration -- either IPv4 or IPv6. It cannot support both at the same time.

    Having both the IPv4 and IPv6 as required fields on the web interface is a known issue. Ruckus Wireless recommends against performing syslog override at the AP level.

    To configure syslog with IPv6, you must create an IPv6-only zone, and then configure syslog at zone level only. [SCG-51272]

Session Manager

- The session manager process does not send a UE update context response if the UE is using an IPv6 address or connected to a WLAN-enabled tunnel. [SCG-52361]
- The session manager process does not handle the session timeout of WISPr clients after a UE roams from one AP to another. [SCG-52369]
- Tunnel Termination Gateway (TTG) and PMIP are supported only when the controller is in standalone mode (not in cluster mode). [SCG-38585]

System

- In a two-node cluster, the follower node may lose historical data if the packet handling rate exceeds 55/s per node. [SCG-52310]
- 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]
- vSZ logs may display an "update failed" error message when updating configuration for R710 APs the first time.

  WORKAROUND: Wait five minutes and the issue will resolve itself. [SCG-51436]

- 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: Subsequent calls will work fine. [SCG-50826]

- 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]
- Forwarding service is unsupported on the SZ-100 so 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 be still configured in the WLAN settings, but the settings are not applied. [SCG-45440]
- When an AP switches to another cluster, authorized hotspot (WISPr) clients are unable to log off from the original portal page. [SCG-41756]
- 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]
- The controller may be unable to renew its DHCP server-assigned IP address, which may cause all controller services to go down.

WORKAROUND: Assign static IP addresses to the controller's interfaces. [SCG-40383]

- 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]
- After the controller is restored from release 3.2 to 2.6, mesh network on the R700 cannot be 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]

- 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]
- 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 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]
- 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]
- The controller's management interface IP address may not be changed from DHCP to static IP address mode. [SCG-35281]

- Packet operation causes memory corruption and the SZ100 data plane to stop responding. [SCG-44904, ER-4115]
- The controller does not support multiple LDAP AAA server profiles that use the same IP address and port number. [ER-3948]
- 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]
- 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 one of the following:

  - Do not shut down the Azure hypervisor, or;
  - Set a static IP address for the controller on the Azure hypervisor. [SCG-42367]

- 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]

- 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]
- 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]

Web Interface

- 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]
- The SZ-100 Setup Wizard does not validate the IPv6 address if the IPv6 prefix is not configured. [SCG-40257]
- 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]

- Some of the options for the Certificate Store page may not show up on the Safari web browser. [SCG-34971]
- Administrators who do not have the privilege to manage alarms may be able to clear or acknowledge alarms in bulk. [SCG-34126]
- Internet Explorer 11 cannot be used to access the vSZ web interface after the controller is upgraded from release 3.2. [SCG-48747]

Wireless Clients

- Wireless clients based on Intel Dual Band Wireless AC-7256 and Intel Centrino N 6300 AGN, and Samsung S5 mobile device fail to perform OKC (Opportunistic Key Caching) roam, and will go through full 802.1x authentication. [SCG-48792]
- Clients may be unable to receive well-known multicast traffic when associated to a WLAN with DVLAN enabled. [SCG-52654]
- 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]

WISPr

- WISPr client session statistics are not properly moved to historical data after logout. [SCG-52507]
- If a WISPr WLAN is configured for an AP Zone when SZ is running version 3.1.1, and SZ is upgraded to 3.4 without upgrading the AP Zone, users with spaces in their user names will be unable to connect. [SCG-52319]
- If the external portal generates chunked data or large packets, the following hot fix must be applied to support portal-based authentication:

    - SCG-200: SCG-52951-3_4_0_0_967-v1_0_SCG-200.ksp
    - SZ-100, vSCG: SCG-52951_3_4_0_0_967-v1_0.ksp

    The hot fix must be applied on all nodes in the cluster. [SCG-52951]
- COANAK/DMNAK is received if COA/DM messsages are sent to the node that does not have the corresponding WISPr/WebAuth session. [SCG-48959]
- In a third party AP WISPr call (L2oGRE as access), the UE MAC becomes that user name in the Accounting Stop message after the user signs out and disconnects. [SCG-50975]
- TTG Session Summary will not be shown as part of associated clients for TTG sessions established using TTG+WISPr profile. [SCG-32706]

Upgrade

- The minimum VM Memory size for vSZ-H with 2 CPU cores has been changed to 13G in this release (see Virtual SmartZone Recommended Resources on page 32). If you are upgrading vSZ-H from release 3.2 to release 3.4, you must increase the VM memory size to 13G before the upgrade.

> **NOTE** The minimum memory size requirement for the vSZ has been updated for both vSZ-H and vSZ-E in this release.

Resolved Issues 4

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

Legacy Issues

- Resolved an issue where events 226 and 227 were not displayed on the web interface. [SCG-49617]
- Resolved an issue where the 5470 - 5725 MHz band were unavailable when the country code was set to Singapore. [SCG-49412]
- Resolved an issue where -Z2 (Zone 2) AP SKUs could not join the controller and the controller, when set to "Zone 2," did not allow -IL locked AP SKUs to join it. This issue prevented customers in Israel from being able to have a mix of -IL and -Z2 SKUs on the same network. [SCG-49328]
- Resolved an issue where the SmartZone CLI and web interface did not support remote FTP directory names that contain special characters (for example, question mark [?], exclamation mark [!], etc.). [SCG-49248, SCG-48914]
- Resolved an issue where when an AP was restarted, the AP properties page on the SmartZone web interface did not update the uptime value. For example, the uptime value showed "three days" a few minutes after the AP was restarted. [SCG-48559]
- Resolved an issue where after an AP was moved to an IPV6 zone, it could no longer build a GRE tunnel to the data plane. [SCG-48053, SCG-44620]
- Enhanced rate limiting to support mesh APs. In previous releases, rate limiting did not work on mesh WLANs on the P300 AP model. [SCG-44294, SCG-38152]
- Enhanced the MVNO account privileges to allow MVNO administrators to update AP certificates. [SCG-43684]
- Resolved an issue where AP zones could not be created from the SmartZone CLI. [SCG-43320]
- Resolved an issue where RADIUS accounting on messages were not being sent when a standalone AP in proxy mode came up. [SCG-40491, SCG-46019]
- Updated the IP table rules to resolve an issue where APs could not connect to the vSZ when the management ACL was enabled. [SCG-44029]
- Resolved an issue where the cluster restore process on the SCG-200 could not be completed if the cluster backup file that was being restored has issues. [SCG-49877]

Access Points

- Resolved an issue where a static IP address could not be assigned to the R700 AP. This issue occurred because GRE connection was enabled by default in SCG release 3.2.1. Starting in this release, GRE connection is disabled by default. [SCG-48023]
- For the T710 AP, in addition to ChannelFly, support for using background scanning for auto channel selection has been added. [SCG-47732]

- Resolved an issue where large size packets were dropped by the AP when the "Gateway Path MTU" value is set to less than or equal to 1383. [SCG-44872]
- Resolved an issue where when an AP roams from one controller to another, the Accounting On message was not being sent. [SCG-45745]
- Resolved an issue where the R710 AP always requested 25W through LLDP to run in full power mode. [SCG-50538]
- Resolved an issue where, in Jumbo-enabled network, ping between wired and wireless clients with MTU size larger than 1578 failed. [SCG-49884]
- Resolved an issue where after an AP was preprovisioned to a dual stack AP zone, the IPv6 settings of the AP were not configured. [SCG-47686]
- Disabled the 11w (Protected Management Frames) feature, which is enabled by default in earlier releases, to resolve performance issues on older iOS (8.1.1) and Samsung devices. [SCG-46184]
- Resolved an issue where traffic degradation (and, in some cases, extreme slow down between mesh APs) occurred when the RTS threshold was enabled on 11ac mesh APs. [SCG-42607]
- Resolved an issue where the R710 AP could not be assigned as a Root AP in an IPv6 zone. [SCG-44886]

Data Plane

- Enhanced the data plane implementation by preventing the same NAT IP address to be configured for multiple data planes. [SCG-45578, SCG-44756]
- Resolved an issue where after a static route was configured for the SZ100, the updated configuration was not propapagated to the data plane. [SCG-46896]

Documentation

- Enhanced the *SNMP Reference Guide* to document the MIB changes from release 3.1.1 to 3.4 and from release 3.2 to 3.4.

Hotspot 2.0

- Resolved an issue where local DB authentication for 802.1x and Hotspot 2.0 did not support manually created local DB user credentials. [SCG-32304]

IPv6

- Resolved an issue where large size packets were dropped by the AP when the Gateway Path MTU value was set to less than or equal to 1383 for IPV6 SoftGRE. [SCG-45743]
- Resolved an issued where the accounting proxy stopped working when a WLAN was changed from WISPr + TTG to standard open WLAN. [SCG-44783]
- Resolved an issue where the SZ-D could not obtain an IPv6 address from the DHCP server. [SCG-44652]

Public API

- Enhanced the public API by adding support for creating a new web authentication of a zone. [SCG-45819]
- Resolved an issue where an external FTP server could not be deleted from the web interface when controller data was auto exported to the server once and then auto export was disabled. [SCG-43493]
- Resolved an issue where APs could not be added to AP groups using the public API. [SCG-43378]
- Resolved an issue where the AD enum definition was missing, which prevented the public API from creating an authentication profile. [SCG-37869]
- Resolved an issue where user traffic profiles could not be updated using the public API. [SCG-37610]

Session Manager

- Changed the default session timeout to 48 hours (12 hours in earlier releases).

  - WLAN: For open authentication (other than WISPR, Guest Access, Web Auth), the default session timeout for clients authenticated via DPSK is now 48 hours.
  - DPSK: The default session timeout for clients authenticated via DPSK is now 48 hours . [SCG-50668, SCG-50654]

Setup Wizard

- Resolved an issue where the setup wizard for vSZ GCE always redirected users to the controller's internal IP address, even when an external NAT IP address was configured. [SCG-44311]
- Resolved an issue where when the vSZ was installed on the GCE platform, after setup was completed, the setup wizard redirected the administrator to internal IP address (instead of the external address) of the controller. [SCG-43713]

SmartZone-specific Issues

- Resolved an issue where the web session could not be terminated if the timeout value was set to less than five (5) minutes. [SCG-47202]
- Resolved an issue where after SZ100 was upgraded from release 3.1.1 to 3.2.1, the ZeroIT file for HS 2.0 could not be downloaded to Apple devices. In this release, ZeroIT is no longer supported. [SCG-46480]
- Resolved an issue where when access-core separation was enabled on the vSZ web interface, multiple default IPv6 routes were present in the system, which caused AP tunnel establishment to fail. [SCG-50421, SCG-49408]
- Resolved an issue where vSZ-D did not mark the DSCP bit in southbound traffic towards APs. [SCG-45129]

SNMP

- Resolved an issue where the controller was fetching SNMP traps with missing attributes. [SCG-45098]

System

- Resolved an issue where log snapshots did not include all log files because the snapshot process timed out before it was completed. [ER-3115]
- Resolved an issue with the correct time offset for Moscow. [SCG-44278]
- Resolved an issue where the SZ100 and vSZ-E allowed the creation of reports even when the filters were configured incorrectly. [SCG-43524, SCG-41407]
- Resolved an issue where the **Disable** option for client isolation was grayed out on the web interface. [SCG-38878]
- Resolved an issue where no error message was displayed when the SCG-200 cluster backup file could not generated successfully. Consequently, when the problematic cluster backup file was used to restore the cluster, the cluster restore process failed. [SCG-47417]
- Resolved an issue where port 6721 was missing from the list of allowed ports for the outbound firewall feature. This issue caused PMIP calls to fail in some scenarios. [SCG-46218]
- Resolved an issue where the virtual controller was installed on either Google Compute Engine (GCE) or Microsoft Azure, configuring the control NAT IP address on the Setup Wizard was not mandatory. This prevented some APs from communicating with the virtual controller. [SCG-39323, SCG-44306]
- Resolved an issue where wireless users could connect to a WLAN profile that was not part of the group to which they were assigned. [SCG-44191, SCG-42934]
- Resolved an issue where the control NAT IP configuration was not required and IP mode could be set to Static IP on the Setup Wizard when a vSZ instance was installed on GCE and Azure cloud. [SCG-43902]

UTP

- Enhanced the UTP configuration options by supporting adding and deleting the default wildcard (*) from authentication service profiles. [SCG-46332]

Web Interface

- Resolved an issue where web interface sessions were not terminated when the session timeout value was set to less than five (5) minutes. [SCG-44016]

Wireless Clients

- Resolved a client fingerprinting OS error for Windows 10 Mobile. [SCG-43275]

WISPr-TTG

- Resolved an issue where WISPr location information was not included in accounting message in case of WISPr+TTG call after MWSG restart. [SCG-42858]

ZeroIT

- Added support for ZeroIT for Android 5.0 via CloudPath. [SCG-35097]

Resolved Customer Reported Issues 5

This section lists the customer reported issues that have been resolved in this release.

- Resolved a memory leak issue that caused the data plane to reboot. [ER-3464]
- Resolved a memory leak issue. [ER-3461]
- Resolved an issue where memory consumption in nodes increased continuously. [ER-3388]
- Resolved an issue that caused incorrect search results when a user entered a non-Latin character in the search box. [ER-3307]
- Resolved an issue where after the controller was upgraded to release 3.2.1.0.193, the "Access Points Configuration" public API could no longer retrieve the UE count and connection state of managed APs. [ER-3913]
- Resolved an issue where an error occurred when an AP was moved from an AP group to the default AP group and then back to the AP group. [ER-3435]
- Resolved an issue where an invalid packet received on a certain port caused the eAut and CIP processes to restart. [ER-3241]
- Resolved an issue where C500 APs could not receive updates from the SCG-200 when the country code was set to Argentina. [ER-3574]
- Resolved an issue where no alarm was being generated when the fan was physically removed. [ER-3631]
- Resolved an issue where packets from an outer R-GRE tunnel VLAN with an ID of 400 or higher caused the data plane to stop responding. [ER-3405]
- Resolved an issue where Remote Capture with Filter was unsupported on the AP. [ER-3504]
- Resolved an issue where repeated authorization requests from the SZ-100 caused the RADIUS server to become unresponsive. In addition, a MAC auth + WISPr loop issue was addressed with additional MAC authorization RADIUS enhancements. [ER-3172, ER-3579]
- Resolved an issue where the "From Display Name" field was missing from SMTP settings page of the web interface. [ER-3929]
- Resolved an issue where the configured download rate limit was not being applied. [ER-3621]
- Resolved an issue where the controller was not processing any new authentication/accounting packets from APs for WLANs in proxy mode in high load scenarios after the AAA server slowed down their replies. [ER-3601]
- Resolved an issue where the encryption settings of WLANs were changed from TKIP to auto after the AP was rebooted. [ER-3440]
- Resolved an issue where the gkeeper daemon was not monitoring the data plane for recovery. [ER-3301]
- Resolved an issue where the internal IP address of the data plane could be used to log on to the management interface. [ER-3780]

- Resolved an issue where the Java KeyStore (JKS) file could not be generated in follower nodes (because of a missing .p12 certificate), which caused attempts to upgrade the controller to release 3.1.1 to fail. [ER-3345]
- Resolved an issue where the R710 Status LEDs were incorrect during AP reboot. [ER-3030]
- Resolved an issue where the VSA Ruckus-BSSID was not recognized by the AAA server because it was not included in the dictionary file. [ER-3043]
- Resolved an issue where the vSZ host name in the network configuration file contained the double quote (") character. This caused migration issues from release 3.0 to 3.1. [ER-3177, ER-3658]
- Resolved an issue where the web proxy feature of the captive portal used up too much system memory, which prevented the captive portal from processing new connection requests. [ER-3798]
- Resolved an issue where the WLAN scheduler caused tunnel SSIDs to be broadcast at the same time as recovery SSIDs. [ER-3556]
- Resolved an issue where the ZoneDirector and standalone APs could not join the SCG-200. [ER-3495]
- Resolved an issue where unauthenticated hotspot users could not be redirected when the redirect URL that was configured contained the question mark (?) character. [ER-3315]
- Resolved an issue where vSZ could not retrieve system statistics because a number of MIBs were missing from the system. [ER-3485]
- Resolved an issue where when the remote FTP folder name contained either a period (.) or hypen (-) character, the FTP server settings could not be saved. [ER-3467]
- Resolved an issue where when the security certificate for the Communicator/Core process was replaced, and the key and cert were placed in the same file, the Communicator/Core process was unable to load the certificate. This caused the Communicator/Core process to go out of service. [ER-3641]
- Resolved an issue where wireless clients could not be deleted from the web interface when the SSID with which these clients were associated contained Traditional Chinese characters. [ER-3848]
- Resolved an issue with mesh uplink selection that could cause mesh APs to sporadically disconnect from their uplink APs. [ER-3471]
- Resolved an issue with the user interface that prevented users from seeing the drop-down menu from which WLAN groups could be selected. [ER-3627]
- Resolved an R710 PoE issue that occurred when the AP was connected to a switch that only supported 802.3af PoE mode. [ER-3225, SCG-47346]
- Resolved an issue where zero session time was shown in accounting stop records. [ER-4019]
- Resolved a race condition that caused the RADIUS proxy to stop responding and stop processing any new authentication requests when the AAA rate limiting feature was enabled. [ER-3617]
- Enhanced the Ruckus Wireless RADIUS dictionary for the SCG by updating it with the correct VSA (Ruckus-WSG-User) information. [ER-3302].

- Resolved an issue where when the LAN port settings were updated in the AP Model Specific Configuration page of the web interface, some APs could not update their statuses or obtain updated configuration from the controller. This issue occurred because the controller's database was taking too long to respond to the requests, eventually resulting in connection timeout. [ER-3932]
- Resolved an issue where APs were getting disconnected from Virtual Data Plane bcause of "[fail to authenticate] error." [ER-3522]
- Resolved an issue where after the vSCG was upgraded to a newer version, APs on which hotspots were configured started redirecting wireless clients to random redirect URLs that contained the "zoneName" value. [ER-3494]
- Resolved an issue where packet capture was disabled automatically when executed twice on an AP. [ER-3521]
- Resolved an issue where a customer could not take a snapshot of the controller successfully because the IPMI driver was broken. [ER-3947]
- Resolved an issue where device policy settings were not being applied to Windows clients. [ER-3885]
- Resolved an issue where the web interface displayed two instances of the Enable RFC 5580 Location Delivery Support check box. [ER-3823]
- Resolved an issue where the AAA server log and RADIUS debug file displayed incorrect values for acct-session-time and multi-session-id. [ER-3740]
- Resolved an issue where the web inteface did not support the hyphen (-) character in the value for APN name. [ER-3736]
- Resolved an issue where APs could not be deleted from vSCG. [ER-3710]
- Resolved an issue where the controller could not test the configured SMTP server settings because the SMTP host name value that was being sent was enclosed in double quotation marks. [ER3658]
- Resolved an issue where after controllers in a cluster were upgraded, all access points went down. This issue occurred because follower nodes did not the receive the database schema update request during the upgrade process and could not recognize the new table columns that the new controller software was using. [ER-3554]
- Resolved a man-in-the-middle vulnerability in the control interface of earlier SmartZone releases. [ER-3547]
- Resolved an issue where random clients could not connect to the Internet. [ER-3458]
- Resolved an issue where when a large number of RPC requests was sent from one Communicator process to notify the Greyhound process about AP failover, these requests jammed the the configurer and blade channels, which resulted in cluster state inconsistency (for example, a cluster may have two two leader nodes, node states were inconsistent, etc.) [ER-3452, ER-3050]
- Resolved an issue where SNMP traps contained attributes that were missing values. [ER-3432]
- Resolved an issue where a customer's automated provisioning system stopped working because the AP registration flow in release 3.x and later was changed. [ER-3426]

- Resolved an issue where some wireless clients could not associate with controller-managed APs when MAC address authentication was enabled. [ER-3413]
- Resolved an issue where in-memory entries for accounting on/off messages were not cleared, which resulted in high memory usage and caused the node to restart. [ER-3399]
- Resolved an issue where during periods of high traffic, dropped management frames caused the R600 AP to stop responding. [ER-3348]

Upgrading to This Release 6

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.

WARNING!   If you are upgrading from release 2.6 to this release, please contact Ruckus Wireless Support before performing the upgrade.

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: vSZ High Scale recommended resources

APs	Clients	Max Nodes per Cluster	Disk Volume Size	vCPU (Core)	RAM
100	2,000	2	100GB	2	13GB
500	10,000	2	100GB	4	14GB
1000	20,000	2	100GB	4	15GB
2500	50,000	2	300GB	6	19GB
10,000	10,0000	4	600GB	24	48GB

Table 2: vSZ Essentials recommended resources

APs	Clients	Max Nodes per Cluster	Disk Volume Size	vCPU (Core)	RAM
100	2,000	2	100GB	2	15GB
1024	25,000	4	250GB	8	23GB

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.
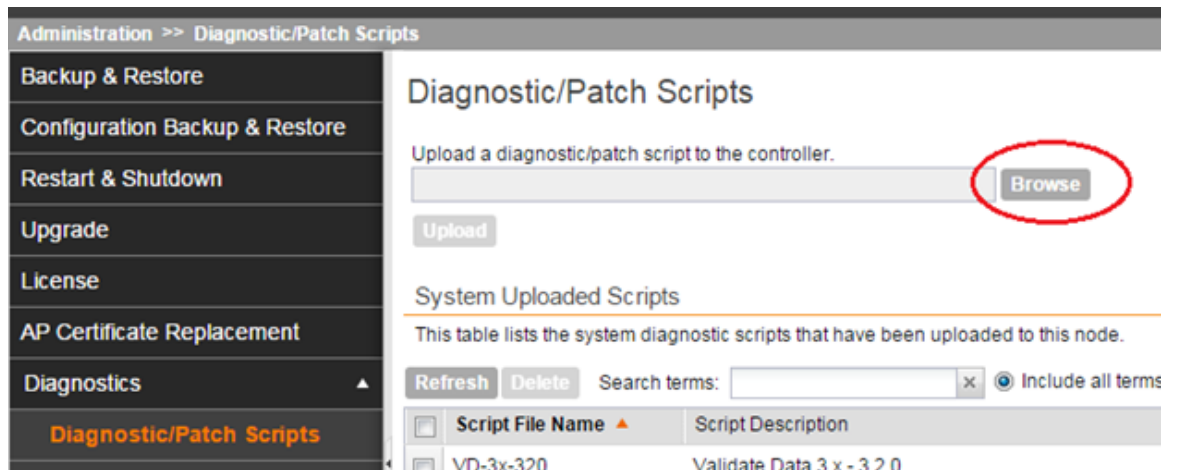
4. Click **Upload**.
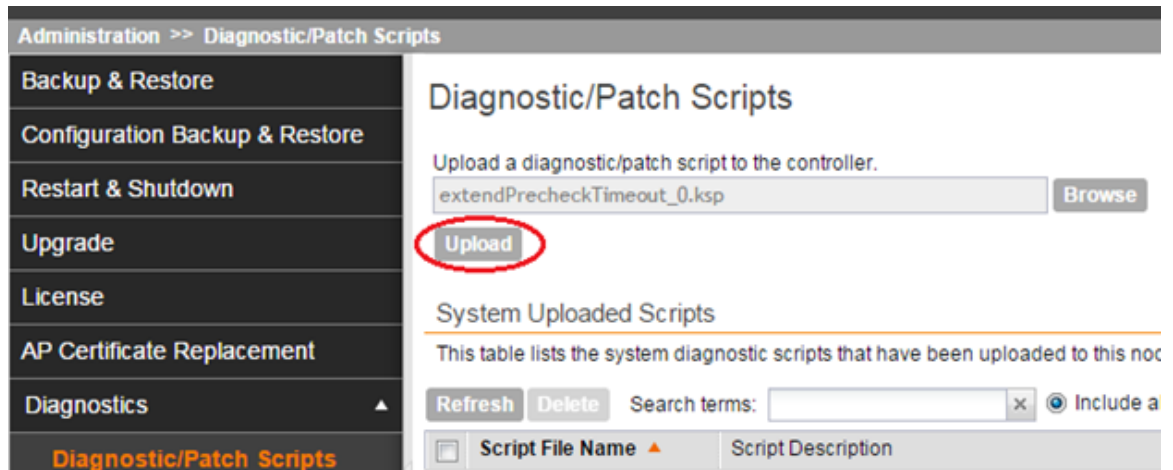
5. When the KSP file appears on the list of available scripts, click the green check mark under the **Actions** column.
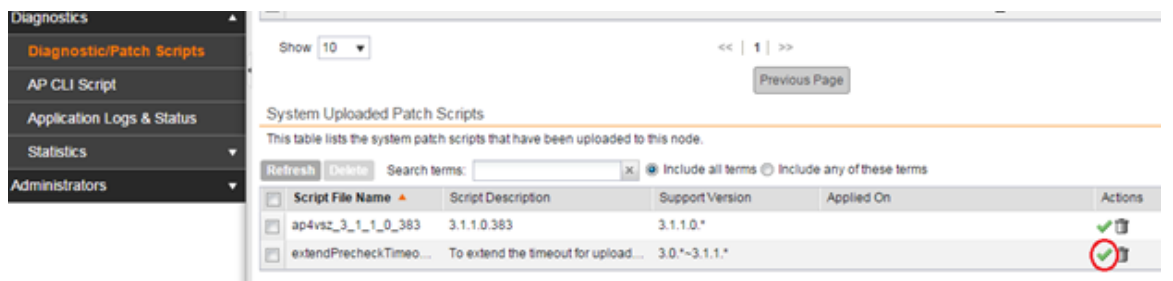
After the KSP script is applied, upload the upgrade image file, and then upgrade the controller to this release.

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. The logs of the validation process are available at: `/opt/ruckuswireless/wsg/log/datamanager/datamanager.log`
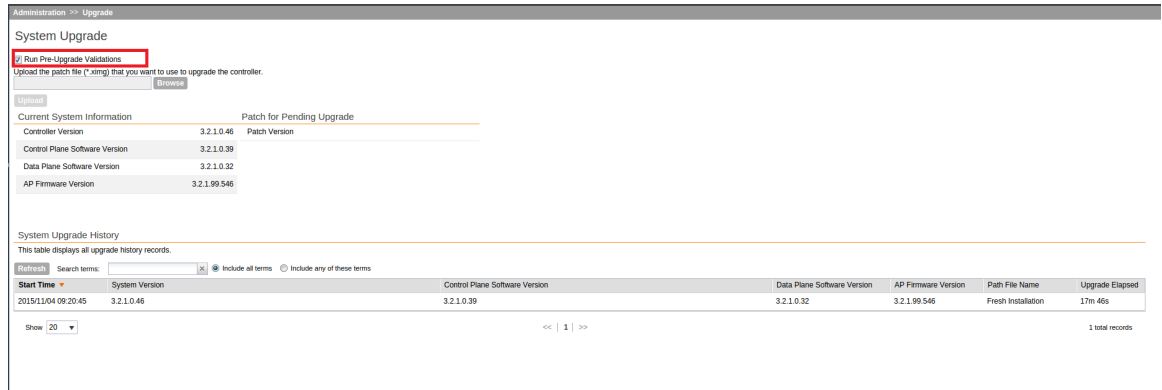
Figure 1: Pre-upgrade validation

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 previous releases that can be upgraded to this release.

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

Platform	Release Build
SCG-200	3.1.0.0.236
SZ-100	3.1.0.0.249
vSZ (vSCG)	3.1.1.0.442
vSZ-D	3.1.1.0.474
	3.1.1.0.476
	3.1.1.0.450
	3.1.2.0.95
	3.1.2.0.1015
	3.1.2.0.513
	3.1.2.0.520
	3.2.0.0.790
	3.2.1.0.134
	3.2.1.0.163
	3.2.1.0.193
	3.2.1.0.139
	3.2.1.0.217
	3.2.1.0.245
	3.4.0.0.659
	3.4.0.0.745

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 SCG-200 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 SCG-200

In the SCG-200, 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 SCG-200 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 SZ-100 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 SCG-200 will retain depend on the SCG-200 release version from which you are upgrading.

- If you are upgrading the SCG-200 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 SCG-200 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 SCG-200 will be deleted automatically.

EoL APs and APs Running Unsupported Firmware Behavior

Understanding how the SCG-200 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 SCG-200 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 SCG-200 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 SCG-200 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

7

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.