



SmartZone 3.4.1

Release Notes

Part Number: 800-71382-001 Rev B
Published: 17 February 2017

www.ruckuswireless.com

Copyright Notice and Proprietary Information

Copyright 2016. Ruckus Wireless, Inc. All rights reserved.

No part of this documentation may be used, reproduced, transmitted, or translated, in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without prior written permission of Ruckus Wireless, Inc. ("Ruckus"), or as expressly provided by under license from Ruckus.

Destination Control Statement

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

Disclaimer

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

Limitation of Liability

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

Trademarks

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

Contents

Copyright Notice and Proprietary Information.....	2
---	---

1 Hardware/Software Compatibility and Supported AP Models

Hardware and Software Compatibility.....	5
Release Information.....	5
Supported and Unsupported Access Point Models.....	6

2 Caveats, Limitations, and Known Issues

3 Resolved Issues

4 Upgrading to This Release

Virtual SmartZone Recommended Resources.....	24
Using the "Extend Upload Precheck Timeout" Script.....	26
Performing Preupgrade Validation.....	27
Supported Upgrade Paths.....	28
Upgrading With Unsupported APs.....	29
Multiple AP Firmware Support in the SCG-200.....	33
EoL APs and APs Running Unsupported Firmware Behavior.....	33
Compatibility with 64MB APs.....	34

5 Interoperability Information

AP Interoperability.....	36
Redeploying ZoneFlex APs with SmartZone Controllers.....	37
Converting Standalone APs to SmartZone.....	37
ZoneDirector Controller and SmartZone Controller Compatibility.....	39
Client Interoperability.....	39

Hardware/Software Compatibility and Supported AP Models

1

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.

SCG200

- Controller version: 3.4.1.0.208
- Control plane software version: 3.4.1.0.38
- Data plane software version: 3.4.1.0.59
- AP firmware version: 3.4.1.0.329

SZ100

- Controller version: 3.4.1.0.208
- Control plane software version: 3.4.1.0.38
- Data plane software version: 3.4.1.0.20
- AP firmware version: 3.4.1.0.329

vSZ-H and vSZ-E

- Controller version: 3.4.1.0.208
- Control plane software version: 3.4.1.0.38
- AP firmware version: 3.4.1.0.329

vSZ-D

- vSZ-D software version: 3.4.1.0.208

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
- H510
- R300
- R310
- R500
- R500E
- R510
- 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.

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

Caveats, Limitations, and Known Issues²

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

H510 Access Point

- Under certain rare conditions, the H510/R510 AP in mesh mode may cease to pass traffic and cause the AP to reboot. If this occurs, the mesh will re-establish itself upon reboot with no manual intervention. [ZF-16040]
- 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]
- 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]
- The Ethernet port on the H510 AP does not auto negotiate the data transmission rate when the port speed is changed from 10Mbps to 100Mbps. [SCG-51790]
- The 802.1X Ethernet port (supplicant) on the H510 AP does not respond to EAP identity requests when the link is disconnected, and then reconnected. [SCG-51975]
- When the 802.1X Ethernet port on the H510 AP is configured for MAC-based authentication, it does not authenticate supplicants. [SCG-51986]

Access Points

- With Application Visibility enabled, the AP [R710] may crash under certain extraordinary circumstances. Please contact Ruckus Support (<https://support.ruckuswireless.com/contact-us>) for further instructions. [ER-4410]
- APs deployed in a SPoT deployment may fail to return to normal passive tracking mode after calibration is run.

WORKAROUND: Disable, and then re-enable the LBS service at the zone or AP group level. [ER-4587]

- Strange traffic flows with opposite flow directions but inconsistent uplink and downlink are displayed on the AVC page in release 3.4. [SCG-44169]
- Load rebalancing of APs across data planes works inconsistently. [SCG-50001]
- When the AP bundle is applied, there is no warning message to warn users that applying the bundle will upgrade and reboot **all APs**, resulting in a temporary service outage. [SCG-55178]
- 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]
- The R710 AP can be powered by an 802.3at-compliant (25.5W) Power over Ethernet (PoE) switch or PoE injector, or an 802.3af-compliant PoE switch or PoE injector.

The AP can operate off of 802.3af power, but the feature set is reduced, as follows:

- The USB port is disabled
- The non-PoE (eth1) Ethernet port is disabled
- The 2.4 GHz radio is reduced to two transmit streams (2x4 MIMO) with aggregate transmit power up to 22dBm (subject to country limits).
- If you are using a PoE switch to supply power to the T710 AP, the PoE switch must be capable of supporting a PoE+ (802.3at) powered device. It is recommended to reserve 30W for the T710 AP on the switch, to account for inefficiencies and losses. Failure to ensure a PoE+ (802.3at) supply to the access point may result in unpredictable operation of the access point. Additionally, if you are using a PoE switch, the T710's PoE OUT port cannot be used to power additional devices.
- The T710 AP does not support 802.3af PoE power. Power must be supplied using either the Ruckus supplied PoE injector, or an 802.3at PoE switch/injector, or AC power.
- If you are using the PoE OUT port on the T710 AP, it is mandatory to use the custom Ruckus supplied 60W PoE injector (part #902-0180-XX00), or to use AC power.
- 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 $200 * 100\text{kbps} = 20,000\text{kbps} = 20\text{ Mbps} > 10\text{Mbps}$.

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

- 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
 - ZF7762-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.

Caveats, Limitations, and Known Issues

- 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 interface 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]

Change-of-Authorization (CoA) and Disconnect Messages

- A call session is not deleted when the incorrect calling station ID is received from the AAA server (even when DM-ACK is sent). [SCG-56851]

CLI

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

Data Plane

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

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

Dual Stack APs

- Network tunnel statistics are not displayed for dual stack APs when queried with an IPv6 address. [SCG-57446]

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]

Historical Clients

- Querying the history of clients with IPv6 addresses is unsupported. [SCG-57445]

Public API

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

RADIUS Authentication and Accounting

- When the called station ID is configured to include the AP group name, the AP group name is not sent properly after an AP is moved from a configured AP group to the default AP group (and vice versa). [SCG-56398]
- When the primary authentication server is unavailable, wired clients do not use the secondary authentication server that has been configured. [SCG-52194]
- Ruckus Wireless strongly recommends avoiding using the at sign (@) when configuring the realm settings for administrator authentication. [SCG-52112]

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]

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

- Currently, vSZ-D and the SZ100 do not support differentiated services code point (DSCP). [SCG-58127, SCG-57638]
- Cluster formation fails if nodes that are up and running are not syncing time with the configured upstream NTP server. [SCG-49736]
- 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]

Caveats, Limitations, and Known Issues

- 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]

User Role Policy

- A UTP that is based on a user group ID from the AAA (that is configured as a secondary server) cannot be applied successfully. [SCG-56860]

User Traffic Profiles

- When rate limits are modified, the new limits are not applied to clients that are in the grace period. [SCG-51422]

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](#)). 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.

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]
- COANAK/DMNAK is received if COA/DM messages are sent to the node that does not have the corresponding WISPr/WebAuth session. [SCG-48959]

Caveats, Limitations, and Known Issues

- 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]

Resolved Issues

3

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

- Resolved a synchronization issue between the tunnel manager and the datacore in vSZ-D. [ER-4233]
- Resolved an issue where when a WISPr WLAN was configured for an AP zone when the SCG-200 was running version 3.1.1, and the SCG-200 was upgraded to 3.4 without upgrading the AP zone, WISPr users with spaces in their user names were no longer able to connect to the WISPr WLAN. [SCG-52319]
- Resolved an issue where if the external portal generated chunked data or large packets, the following hot fixes were required to support portal-based authentication:
 - SCG-200: SCG-52951_3_4_0_0_967-v1_0_SCG-200.ksp
 - SZ-100: SCG-52951_3_4_0_0_967-v1_0.ksp
 - vSZ: SCG-52951_3_4_0_0_967-v1_0.ksp [SCG-52951]
- Resolved an issue where, in a two-node cluster, the follower node lost historical data if the packet handling rate exceeded 55/s per node. [SCG-52310]
- Resolved an issue where before a solo R510 AP was converted to a controller-managed AP, Ruckus Wireless recommended disabling lwapp2scg on the controller to ensure that the AP could join the controller successfully. [SCG-52226]
- Resolved an issue where, in a flat and port-isolated network configuration, frequent unresponsive ARP broadcast due to AP to AP communication caused high CPU utilization.[SCG-53622]
- Resolved an issue where after the H510 AP joined the controller, it could not fetch the updated configuration from the controller while it was in the Staging Zone. [SCG-50087]
- Resolved an issue where the filter for events sent to an external syslog was only filtering events, which resulted in very high syslog file count every day. Added new configuration options in public API to filter application, administrator activity and other logs. [SCG-51953]
- Resolved an issue where users were still able to use unbound DPSKs that had already expired. [SCG-53675]
- Resolved an issue where the SZ100 upgrade could not be completed successfully because no DNS server was configured. [SCG-54771]
- Resolved an issue where the configuration of APs created using the public API could not be updated. [SCG-52531]
- Resolved an web interface cache issue where when a domain was selected on the Access Points page, and then the selected domain was deleted from the controller on another page, going back to the Access Points page results in an error. [SCG-50960]

- Resolved an issue where the access and core separation feature on the controller became disabled after switching from dynamic to static IP addresses without a control interface gateway. In this release, a control interface gateway is required for this operation. [SCG-49590]
- Resolved OpenSSL vulnerabilities. For more information, visit <https://support.ruckuswireless.com/security>, and then view security bulletin ID 071216. [SCG-53451]
- Resolved an issue where monitoring WLAN failed to report the client count to SPoT if all other WLANs were down. [ER-4201]
- Resolved an issue where clients could not connect to WLANs that use OAuth if the OAuth service name contained at least one space character. [ER-4190]
- Resolved an issue where the maximum length of the admin DNs was limited to 64 characters. Starting in this release, the admin Domain Name name is limited to 128 characters for AD and LDAP. Base Domain Name and Windows Domain Name are limited to 64 characters. [ER-4107]
- Improved mesh stability by enhancing the mesh keep-alive logic [ER-4096]
- Resolved an issue where a race condition issue occurred with upgrade failure/process start. In this release, the process start sequence has been modified to resolve this issue. [ER-4071]
- Resolved an issue where running either snmpget or snmpwalk on an AP showed all interfaces have a maximum throughput of only 10mbps. [ER-4057]
- Resolved a captive portal issue that prevented user traffic from getting redirected to the login page. [ER-4041]
- Resolved a gratuitous ARP issue on the SmartZone 100 data plane, which caused client traffic interruption. [ER-4018]
- Updated the maximum password length for SNMP queries to 128 characters to match the maximum password length for the web interface and command line interface. [ER-4005]
- Resolved an AP reboot issue that was caused by a hardware watchdog timeout when client isolation was enabled. [ER-3988]
- Resolved an issue where when the outbound firewall was set to enable, TACACS+ packets were dropped. [ER-3969]
- Resolved an issue where the web interface did not display any error message when the upgrade image file was corrupt and users were still able to trigger the upgrade process. [ER-3963]
- Resolved an issue where a customer could not take a snapshot of the controller successfully because the IPMI driver was broken. [ER-3947]
- Enhanced the error message that appears during system upgrade when the controller is managing AP models that are no longer supported. [ER-3714]
- Resolved a memory leak issue related to the mesh network process that could cause the APs to disconnect and be unable to reconnect. [ER-4265]
- Resolved a performance issue with the web interface. When displaying a high number of AP zones or domains on a monitor or configuration page, the page took significantly longer to load than normal. [ER-4250]

Resolved Issues

- Resolved an issue with R710 APs that could cause the AP to reboot due to watchdog timeout. [ER-4239]
- Resolved an issue where AP OID ruckusRadioNoiseFloor was not retrievable thru SNMP. [ER-4188]
- Resolved an issue where DFS channels on some APs were not be properly blocked whenever radar was detected on the channel. [ER-3922]
- Resolved multiple issues related to UE-to-UE traffic leak, large malformed packets causing the data plane to stop responding, and core dump facility binary. [ER-3888]
- Resolved an issue where event code 1909 was not triggered when no accounting service was configured. [ER-3493]
- Added an enhancement that enables users to select and export AP certificate requests per zone. [ER-4059]
- Enhanced the error message that appears when the vSZ cannot be upgraded because of insufficient hardware resources. [ER-4365]
- Resolved an issue where some clients encountered a “JSON not found” error after the UE was redirected to the hotspot portal page, resulting in login failure for a small number of clients. [ER-4299]
- Resolved an issue where configuration download to the RADIUS module could not be completed successfully because of a race condition. In this release, the RADIUS module start has been delayed to be in sync with other SmartZone modules. [ER-4276]
- Resolved an issue where the Unix datagram queue size was insufficient to handle network latency, causing the controller to be unable to respond to RADIUS messages. In this release, the Unix datagram queue size has been increased to cover the error cases. [ER-4155]
- Resolved an issue where the Radiusd process was being restarted while accessing unavailable memory. [ER-4218]
- Resolved an issue where identical logs were being generated in a short period of time. [ER-4279]
- Resolved an issue where when the new certificate replacement process failed, it could not be triggered again. [ER-4377]
- Resolved an issue where sometimes AP did not respond to TLS connection requests, preventing APs from creating new tunnels because all tunnel manager processes were blocked. [ER-4025, ER-4405]
- Resolved a crash issue that caused the AP to reboot when the wifi driver stopped responding. This issue occurred after the group key in a dynamic VLAN configuration was updated. [ER-4403]
- Resolved an issue where the vSZ-D was unable to recognize the same traffic flow coming from different VLANs. [ER-4205]
- Resolved an issue where the same event ID (914) was being shown for two separate disk-related events (disk present and disk removed). [ER-4364]
- Resolved an issue where the walled garden did not accept URL entries that contained the ".amsterdam" domain extension. [ER-4181]

- Resolved an issue where duplicate entries in the proxy ARP existed for the same MAC address, which led to network interruption for some clients in certain situations. [ER-3166, ER-4417]
- Resolved an issue where the database schema was not synchronized during upgrade process, which could potentially cause the upgrade process to fail. [ER-4370, SCG-55728]
- Resolved an issue where an LDAP account did not appear in the search results when tested. This issue occurred because the default LDAP search results in the AAA (LDAP) test function was limited to 1000 users. In organizations with a high number of LDAP users (for example, 1000 or more users), the test results did not show some of the LDAP accounts, even though they existed in the LDAP repository. Since the default LDAP account test function limits the results to 1000, results that are beyond the first 1000 (default limit) were not being displayed. This release removes the default limit of 1000 search results. [ER-3860]
- Added support for CLI session timeout. [ER-4065]
- Resolved an issue where the device name on the AP record did not get updated when configuration was updated. [ER-4363]
- Resolved an issue where inconsistent guest pass data prevented users from viewing the guest pass page. [ER-4236]
- Resolved an issue where the vSZ-D data plane kept restarting because the vSZ-D was missing its minimum MTU limit. [ER-4381, ER-4465]
- Resolved an issue where ZF7372 APs did not properly display results for SNMP queries. [ER-3677]
- Resolved an issue where UEs could not communicate with each other when on different VLANs but on the same SZ100 node. [ER-4496]
- Resolved an issue where the AP certificate request file could not be exported if the zone name contained special characters. [ER-4436]
- Improved the timing of accessing the new certificate when the AP boots up, added more debug messages to help troubleshoot related issues, and enhanced status updates to the controller to reflect more accurate AP certificate fresh states. [ER-3671]
- Resolved a kernel memory leak issue on APs, which eventually caused watchdog timeout reboots. [ER-3544]
- Resolved an issue where the Client Isolation Whitelist configured through the AP CLI was not persistent. In this release, a new command has been added for this feature to remain active even after an AP reboot. For more information, contact Ruckus Wireless Support (<https://support.ruckuswireless.com/contact-us>). [SCG-55139]
- Resolved an issue where a file descriptor memory leak occurred when a large number of APs were simultaneously connected and disconnected frequently from the controller. [ER-4367, SCG-53316]
- Resolved an issue where the radiusproxy process was restarted whenever the controller received more than 10,000 Accounting ON requests from Ruckus APs. [ER-4073]

Upgrading to This Release

4

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

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

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

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

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

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	Reserved 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	Reserved 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.

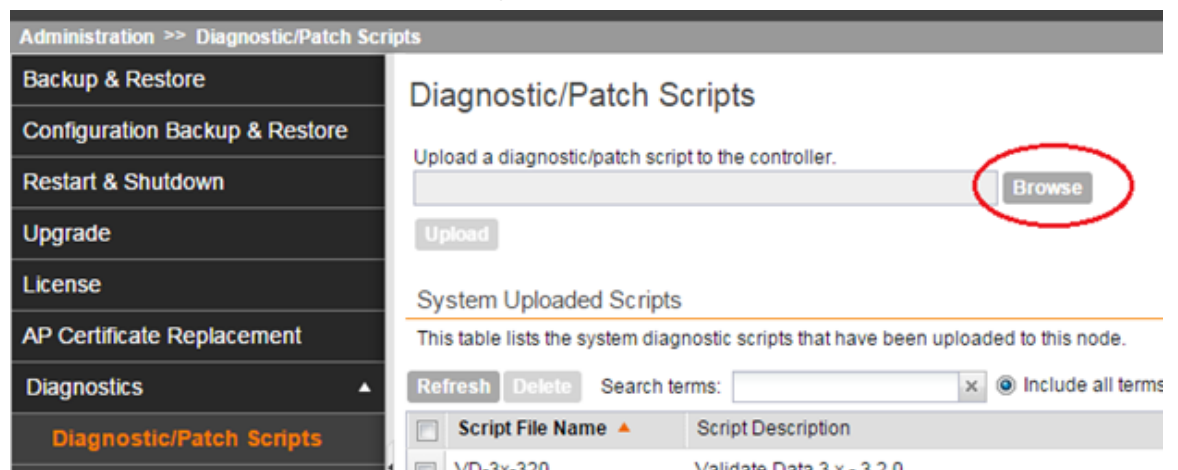
In release 3.2.1, Ruckus Wireless introduces a data migration precheck process that must be completed *before* the upgrade process can start. When you upload an upgrade image, the controller will first check the database for issues before it starts the upgrade process. This new pre-check increases the 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).

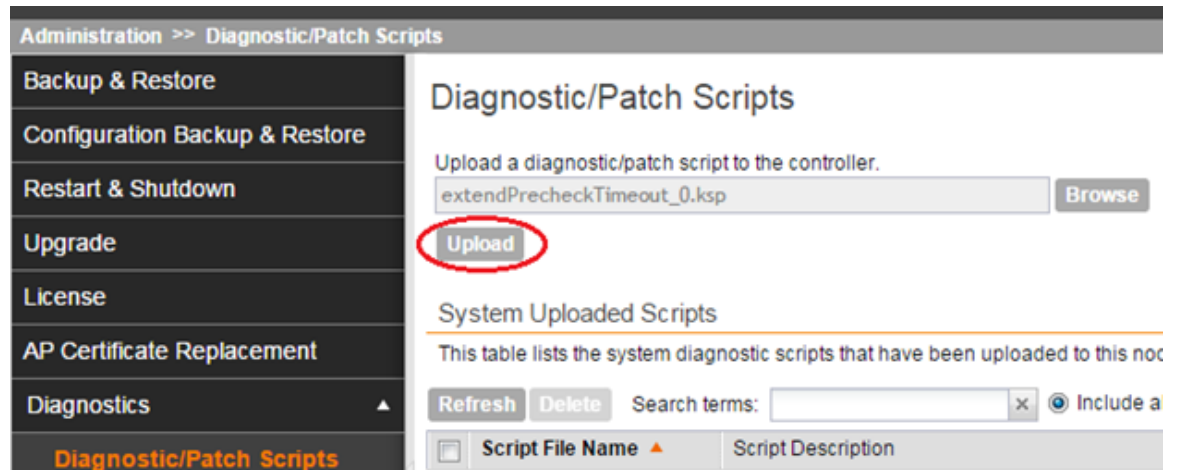
IMPORTANT Apply the KSP before you upload the upgrade image file.

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.

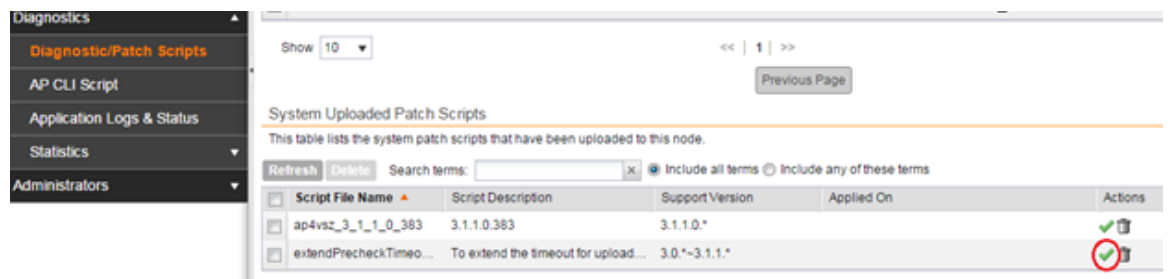
1. Download the KSP file from the Support website to your computer. The file name is `extendPrecheckTimeout_0.ksp`.
2. Log on to the controller, and then go to **Administration > Diagnostics > Diagnostic/Patch Scripts**.
3. Click **Browse**, and select the KSP file that you downloaded.



4. Click **Upload**.



- 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.

Upgrading to This Release

Supported Upgrade Paths

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**.

The screenshot shows the 'System Upgrade' section of a web interface. At the top, there's a 'Run Pre-Upgrade Validations' button highlighted with a red box. Below it, a text box says 'Upload the patch file (*.xmg) that you want to use to upgrade the controller.' with an 'Upload' button. A 'Cancel' button is also visible. Below this, a table titled 'Current System Information' shows the following data:

Current System Information		Patch for Pending Upgrade
Controller Version	3.2.1.0.46	Patch Version
Control Plane Software Version	3.2.1.0.39	
Data Plane Software Version	3.2.1.0.32	
AP Firmware Version	3.2.1.99.546	

Below the table is a 'System Upgrade History' section. It includes a 'Refresh' button, a search bar, and radio buttons for 'Include all terms' (selected) and 'Include any of these terms'. Below this is a table with the following data:

Start Time	System Version	Control Plane Software Version	Data Plane Software Version	AP Firmware Version	Path File Name	Upgrade Elapsed
2015/11/04 09:20:45	3.2.1.0.46	3.2.1.0.39	3.2.1.0.32	3.2.1.99.546	Fresh Installation	17m 46s

At the bottom, there's a 'Show' dropdown set to '20' and a pagination link '<< | 1 | >>'. A note at the bottom right says '1 total records'.

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	3.1.1.0.450
	3.1.1.0.474
	3.1.1.0.476
	3.1.2.0.95
	3.1.2.0.513
	3.1.2.0.520
	3.1.2.0.1015
	3.2.0.0.790
	3.2.1.0.134
	3.2.1.0.139
	3.2.1.0.163
	3.2.1.0.193
	3.2.1.0.217
	3.2.1.0.245
	3.4.0.0.659
	3.4.0.0.745
	3.4.0.0.976

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 <i>Staging Zone</i>. • 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 APs 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 64MB AP Support Zone	
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.

Upgrading to This Release

Compatibility with 64MB APs

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

The image shows the Ruckus Setup Wizard for SmartCell Gateway 200. The interface has a dark header with the Ruckus logo and the title "Setup Wizard - SmartCell Gateway 200". On the left is a blue sidebar with navigation links: "Language", "Management IP", "DataPlane IP", "Cluster Information" (highlighted in orange), "Administrator", "Confirmation", and "Finish". The main area is titled "Cluster Information" and contains several form fields: "Cluster Setting" (a dropdown menu set to "New Cluster"), "Cluster Name" (a text input), "Controller Name" (a text input), and "Controller Description" (a text input). Below these is the "NTP Server" field, which is set to "pool.ntp.org". Under the "AP Conversion" section, there is a checkbox labeled "Convert ZoneDirector APs in factory settings to SmartCell Gateway 200 APs automatically". Below the form fields, there is a prompt "Choose the cluster that you would like to join." followed by a "Scan" button. A "Cluster List" window is open below this, showing a table with columns "Cluster Name", "IP Address", and "Version". The table is currently empty. At the bottom of the interface, there is a dark footer bar containing the text "Version: 3.0.0.0.371", an "Upgrade" button, and navigation buttons "< Back" and "Next >".

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.



Copyright © 2016. Ruckus Wireless, Inc.
350 West Java Drive, Sunnyvale, CA

www.ruckuswireless.com