Ruckus Wireless ZoneFlex 9.3.2 (FlexMaster, ZoneDirector and ZoneFlex Access Points) Release Notes

May 23, 2012

Contents

1 Introduction

Ruckus Wireless ZoneDirector is a WLAN access point controller that is capable of operating at both Layer 2 and Layer 3. ZoneDirector 1000/1100 supports up to 50 ZoneFlex access points (APs) and is developed specifically for small-to-medium enterprises (SMEs) and hotzone operators. ZoneDirector 3000, on the other hand, supports up to 500 ZoneFlex APs and is intended for larger enterprise environments.

ZoneDirector 5000 is a highly scalable controller platform designed for carrier-class and large enterprise deployments. It supports up to 1,000 ZoneFlex APs and up to 20,000 concurrent client connections.

FlexMaster is a centralized management system that can manage ZoneDirector devices, as well as standalone ZoneFlex APs and Bridges, on a global scale.

This document provides release information on FlexMaster, ZoneDirector, supported ZoneFlex platforms, known issues, caveats, workarounds, upgrades, and interoperability information for version 9.3.

2 What’s New in This Release

For a list of features that have been added in this release, visit:

http:/support.ruckuswireless.com/documents

Please refer to Release Notes for prior releases for information on previously documented caveats, limitations, enhancements and resolved issues. Previous Release Notes can also be found at:

http:/support.ruckuswireless.com/documents

3 Supported Platforms

Release 9.3 supports the following platforms:

- FlexMaster 9.3.0.0.18 supports the ZoneDirector and ZoneFlex AP models listed below. FlexMaster also supports the MediaFlex product line (not included in Release 9.3).
- ZoneDirector 1000 version 9.3.2.0.3
- ZoneDirector 1100 version 9.3.2.0.3
- ZoneDirector 3000 version 9.3.2.0.3
- ZoneDirector 5000 version 9.3.2.0.3
- ZoneFlex 2741 802.11g Outdoor Access Point build 9.3.2.0.3 (both main and backup)
- ZoneFlex 2942 802.11g Access Point build 9.3.2.0.3 (both main and backup)
- ZoneFlex 7025 802.11n Wired/Wireless Wall Switch build 9.3.2.0.3 (both main and backup)
- ZoneFlex 7341 2.4GHz 802.11n Smart Wi-Fi Access Point build 9.3.2.0.3 (both main and backup)
- ZoneFlex 7343 2.4GHz 802.11n Smart Wi-Fi Access Point build 9.3.2.0.3 (both main and backup)
- ZoneFlex 7363 Dual Band 802.11n Smart Wi-Fi Access Point build 9.3.2.0.3 (both main and backup)
- ZoneFlex 7761-CM Dual Band 802.11n Outdoor Access Point with integrated Cable Modem build 9.3.2.0.3 (both main and backup)
- ZoneFlex 7762 Dual-band 802.11n Outdoor Access Point build 9.3.2.0.3 (both main and backup)
- ZoneFlex 7762-S Dual-band 802.11n Outdoor Access Point with Sector Antenna build 9.3.2.0.3 (both main and backup)
- ZoneFlex 7762-T Dual-band 802.11n Outdoor Access Point with Omni Antenna build 9.3.2.0.3 (both main and backup)
- ZoneFlex 7762-AC Dual-band 802.11n Outdoor Access Point build 9.3.2.0.3 (both main and backup)
- ZoneFlex 7762-S-AC Dual-band 802.11n Outdoor Access Point with Sector Antenna build 9.3.2.0.3 (both main and backup)
- ZoneFlex 7942 802.11n Access Point build 9.3.2.0.3 (both main and backup)
- ZoneFlex 7962 Dual-band 802.11n Access Point build 9.3.2.0.3 (both main and backup)

4 Enhancements and Resolved Issues in This Release

This section lists enhancements that have been added and issues from previous releases that have been resolved in this release.

4.1 FlexMaster

Enhancements

4.1.1 Support for new product models: ZoneDirector 5000, ZoneFlex 7762-S, 7762-T, 7762-AC, 7762-S-AC and 7761-CM.

4.1.2 New Features

- IPv6 support
- Scheduled ZoneDirector configuration backup
- Dashboard widget to show most recent events
- New Reports: Rogue AP, AP Trends for specific AP
- Version control for database backup/restore
- Disable AP LEDs
- Logo customization (replace the Ruckus Wireless logo with customer logo)
- DHCP Option 82 configuration
- Northbound SNMP trap support
- FlexMaster ZoneDirector template support
- ZoneDirector performance monitoring
- Association time (session time) for each client (based on MAC address) can now be collected

4.1.3 Enhancements

- Dashboard widget export to PDF
- Report column editing
- Updated Standalone view
- Client Association Activity count changes
- Easy to use report date/time picker
- Change Tx Power configuration
- Allow the use of 5.8 GHz channels in the UK
- AP status management
- ZoneDirector now reports Restart and Shutdown events to FM before ZD reboots
- Add to audit logs login attempts to the FlexMaster Web interface that fail for three consecutive times
- Longitude/Latitude in Reports > Device view > APs/Connected APs/Disconnected APs 3 tiers
- Full log download
- Report AP statistic/traffic per SSID

- Display external IP and port of APs behind NAT
- Send SNMP trap to northbound when APC failure occurs

Resolved Issues from Previous Releases

4.1.4 GPS coordinates are automatically calculated from Location Field information.

4.1.5 The Clients column on the ZD Device View widget now properly updates the number of clients displayed more quickly. (ID 20319)

4.1.6 The AP Uptime TopN graph and Histogram graphs now report consistent information on the Dashboard. (ID 18468)

4.1.7 FlexMaster now sends out email notifications via SMTP host rather than localhost when SMTP user and password are not configured. (ID 20298)

4.1.8 FlexMaster no longer displays inconsistent client statistics from those sent from ZoneDirector after client roaming. (ID 24280)

4.2 ZoneDirector

Enhancements

4.2.1 ZoneDirector 5000

A new ZoneDirector model, ZoneDirector 5000 is now available. The ZoneDirector 5000 is a 2RU rack mountable controller platform that supports up to 1,000 APs and 20,000 concurrent client connections.

http://www.ruckuswireless.com/products/controllers

4.2.2 New AP model support

Release 9.3 supports the ZoneFlex 7762-S, 7762-T, 7762-AC and 7762-S-AC Outdoor Access Points and the ZoneFlex 7761-CM Dual Band 802.11n Outdoor Access Point with integrated Cable Modem.

http://www.ruckuswireless.com/products/zoneflex-outdoor

4.2.3 Backup configuration

ZoneDirector 3000 and ZoneDirector 5000 backup files are compatible. Therefore if you are upgrading from a ZoneDirector 3000 to a ZoneDirector 5000, you can back up your current configuration and import it into the new ZoneDirector 5000.

4.2.4 Ethernet port configuration

ZoneDirector provides new tools for configuring AP Ethernet ports, allowing administrators to set ports as access ports, trunk ports or general ports, to assign VLANs to ports, or to disable ports entirely from the ZoneDirector Web interface.

All Ethernet ports on APs other than the ZoneFlex 7025 are VLAN Trunk Ports by default, and the 7025’s four configurable ports are Access Ports by default.

- Access Port behavior: Untagged ingress packets and tagged packets with VLAN ID equal to the default PVID will be forwarded. All other ingress packets will be dropped. Egress packets are sent untagged.
- VLAN Trunk Port behavior: Untagged and tagged ingress packets will be forwarded. Egress packets will be tagged with non-default PVID. Administrators can configure one untagged VLAN ID on a Trunk Port, or assign no untag VLAN ID to force the port to drop all untagged packets.

- General Port behavior: Administrators can configure an Ethernet port to support multiple tagged VLANs and either none or one untagged VLAN.

4.2.5 Ethernet port security (802.1X port-based authentication)

In addition to standalone APs, ZoneDirector-controlled APs can be configured to use 802.1X authentication on each Ethernet port. One or more ports can be configured with an Authenticator role. At most one port on each AP can be configured with a Supplicant role.

- Authenticator: Administrators can require devices connecting to the Ethernet ports of ZoneFlex Access Points to authenticate using 802.1X authentication. This secures against unauthorized network access through APs installed in public areas.
- Supplicant: ZoneFlex APs can be deployed in networks with 802.1X wired port security. Equipped with an EAP-MD5 supplicant, the AP can provide authentication credentials to a requesting upstream switch.

4.2.6 Secure tunneling between AP and ZoneDirector

With this release, tunneled traffic over the Ethernet interface between ZoneFlex Access Points and ZoneDirector can be encrypted. This AES encryption provides an additional layer of security for traffic transmitted over the wire, such as in some architectures designed to be PCI compliant.

Tunneling is only recommended for light traffic loads such as POS (point of sale). It is not recommended for heavy traffic.

4.2.7 IPv6

ZoneDirector now supports IPv6 only and dual IPv6/IPv4 settings.

- Note that some features are not supported when in IPv6 mode. Specifically, internal DHCP server, LAN rogue AP detection, DHCPv6 vendor specific options, Aeroscout RFID tag detection, SSL certificate generation, UPnP and remote access to ZD, and for standalone APs, L2TP and WISPr are not supported when in IPv6 mode.

4.2.8 More WLANs and WLAN groups

The maximum number of WLANs and WLAN groups that can be created on each ZoneDirector device has been increased for some ZoneDirector models. ZoneDirector 1100 now supports creation of up to 128 WLANs and 128 WLAN groups, ZoneDirector 3000 now supports up to 1024 WLANs and WLAN groups, and ZoneDirector 5000 supports up to 2048 WLANs and WLAN groups. The maximum number of WLANs and WLAN groups that ZoneDirector 1000 supports remains 32.

4.2.9 Access Point groups

With this release, administrators can configure access points by grouping them in related sets. Administrators can define up to 8, 32, 256 or 512 groups in ZoneDirector 1000, 1100, 3000 or 5000, respectively. For each group, administrators create a configuration profile that defines the access points' channels, power level, ports and other configurable fields. An AP that is assigned to that group will use the configuration profile. Settings defined in the group can also be overridden for the individual parameters for individual APs.

In previous releases, Global Configuration settings were applied to all APs. These settings have been moved to Access Point Groups and any previous configurations will be retained in the System Default AP Group after upgrade.

4.2.10 Auto-Proxy

The new Auto-Proxy configuration feature allows the administrator to upload a `wpad.dat` file either to ZoneDirector directly, or to point to the location of the wpad.dat file on an external server. Using this feature, clients connecting to a WLAN with a Web proxy server can be automatically configured to retrieve the proxy configuration file on connection.

4.2.11 Packet Sniffer

The Packet Capture feature allows administrators to capture packets from an AP to a local file or stream them to a packet analyzer such as Wireshark.

4.2.12 Global Client Isolation

Global Client Isolation limits all client broadcast/multicast communication to upstream devices only.

4.2.13 Beacon interval and Mgmt PHY rate on service WLANs and Mesh link

New ZoneDirector CLI commands are available for setting management PHY rate and beacon intervals.

4.2.14 Mesh packet forwarding filter

The Mesh Packet Forwarding Filter can help increase downstream performance by reducing the occurrence of traffic looping.

4.2.15 Multicast Traffic Filter

By enabling the Multicast Traffic Filter, the administrator can force the access points to drop all multicast packets from clients associated to the WLAN.

4.2.16 ARP Broadcast Filter

The ARP Broadcast Filter (ABF) is designed to reduce ARP broadcasts over the air. This feature is disabled by default and the allowed range of rate limiting is 1 ~ 1000 packets per second.

4.2.17 Three/Four Channel Selection

Administrators can now choose which set of non-overlapping 2.4GHz channels to operate on (1, 6, 11 or 1, 5, 9, 13) if the ZoneDirector’s country code is set to a regulatory domain that allows the use of channel 13.

4.2.18 Flexible LWAPP message MTU size

Administrators can now set the maximum transmission unit size of LWAPP messages between ZoneDirector and access points.

4.2.19 Telnet server support

ZoneDirector now supports Telnet connections to the CLI in addition to SSH. The Telnet server is disabled by default.

4.2.20 AP sync timing from ZD every 24 hours

Access points will now synchronize their internal clocks with ZoneDirector’s every 24 hours after joining ZoneDirector. This is an internal enhancement and no Web interface or CLI commands are exposed for configuration.

4.2.21 ZoneDirector behind NAT

ZoneDirector can now be placed behind a NAT (Network Address Translation) device and still be reachable through the NAT, as long as the following ports are configured to ZoneDirector’s private IP address on the NAT device’s port mapping table: ports 21, 22, 80, 443, 12222, 12223.

Several restrictions apply:

- Both ZoneDirectors may not be behind the same NAT when Smart Redundancy is enabled (APs will not be able to determine which ZoneDirector to communicate with).
- Unable to upgrade standby ZoneDirector when active ZoneDirector is behind NAT.

- SpeedFlex will not work when ZoneDirector is behind NAT.

4.2.22 Mesh Recovery SSID

The Mesh Recovery SSID assists in recovering isolated Mesh APs in the event that they lose connection to their uplink AP (and are unable to locate another uplink AP to mesh with). When a Mesh AP becomes isolated, it begins broadcasting a recovery SSID named "`island-<last 6 digits of AP's MAC address>`". Users can connect to this WLAN using WPA and the passphrase "`ruckus-<admin password>`". Thereafter, most stations will autoconfigure their IP addresses to 169.254.x.x after DHCP failure, and the AP's Web interface can be accessed by entering the AP's recovery IP address `"169.254.1.1"` in the browser.

4.2.23 Grace Period configuration

The "Idle Timeout" setting for Hotspot services in previous releases is now called "Grace Period" in version 9.3. This setting can be configured to allow disconnected users a grace period after disconnection, during which clients will not need to re-authenticate. The grace period is disabled by default unless upgrading from a previous version with "Idle Timeout" configured, in which case it will inherit the original setting.

Guest Access and Web Authentication WLANs can now also be configured with a grace period. It is disabled by default unless upgrading from a previous version, in which case it will be enabled with a setting of 30 minutes.

4.2.24 Inactivity Timeout

Idle user sessions can now be set to time out after a specified period of inactivity (1 ~ 500 minutes). Inactivity timeout affects connected clients while grace period affects disconnected clients on WLANs that require authentication.

4.2.25 Increased Max Clients per AP to 256

All 802.11n ZoneFlex APs other than ZF 7025 now support up to 256 clients per radio, per AP, when using WLANs without encryption. Each radio is individually able to support up to 256 clients, but is subject to the limit of the AP of 256 total clients.

- When an AP is servicing WLANs with encryption enabled, the total number of clients supported is 100 per radio, up to 200 per AP.
- 11g APs (ZoneFlex 2741, 2942) support max 100 clients per AP. ZoneFlex 7025 also supports max 100 clients per AP.

4.2.26 Allow use of indoor channels on outdoor APs

In certain countries where some channels are restricted for indoor-only use, Outdoor ZoneFlex APs (ZF 7762, 7762-S, 7762-T, 7762-AC, 7762-S-AC, 7761-CM) now avoid, by default, those channels when automatically selecting a channel and do not offer those channels to the admin when manually selecting a channel. Inclusion of those channels in automatic channel selection or made available for manual setting can be enabled.

4.2.27 The Rate Limiting feature now provides more granular limits (increments of 250Kbps).

4.2.28 New auto channel selection algorithm: ChannelFly™

ChannelFly introduces an adaptive channel selection feature that maintains optimum Wi-Fi throughput based on real, observed Mbps capacity potential. By default, standalone APs select channels using the ChannelFly auto channel selection algorithm. ZoneDirector-managed APs automatically select channels using background scanning unless ChannelFly is enabled.

4.2.29 Mesh enhancement

With this release, Ruckus Smart Mesh Networking is enhanced for large-scale mesh networks. A series of timers have been optimized to provide faster self-healing and mesh stability during link failures and uplink re-building. To improve network throughput, uplink decisions now favor an eMAP vs. a MAP and enhancements were made to reduce the effect of hidden node interference.

4.2.30 WISPr Smart Client support

With this release, ZoneDirector supports automatic authentication for devices with a WISPr Smart Client. Operators who have a WISPr Smart Client available for their subscribers' devices can configure ZoneDirector Hotspot Services to automatically authenticate a device when it attempts to join the network. The WISPr Smart Client automatically extracts XML data from the welcome or login pages, and responds with their authentication credentials. Users do not need to launch their browser to manually login.

4.2.31 Dynamic per-user rate limiting

With this release, administrators can control the upstream and downstream bandwidth rates for Hotspot WLANs on a user by user basis. When a user authenticates to a Hotspot network, if individual rate limits are defined in RADIUS, ZoneFlex APs will apply those limits to the specific user to control their upstream and downstream bandwidth. Along with per-WLAN rate limiting, dynamic, per-user rate limiting provides the network operator with more options to control network usage.

4.2.32 Dynamic VLAN for Open WLAN clients

In previous versions, ZoneDirector supported Dynamic VLAN only on WLANs configured with 802.1X EAP, MAC Address, or 802.1X EAP + MAC Address authentication. With this release, Dynamic VLAN support is extended to be usable on WLANs configured with Open authentication and WPA/WPA2 and Zero-IT/Dynamic PSK encryption methods.

In short, any type of WLAN that uses a RADIUS server for user authentication can now be configured to receive Dynamic VLAN settings from the RADIUS server, and clients can be dynamically segmented into different VLANs based on RADIUS attributes.

4.2.33 New AP Transmit Power configuration

Available transmit power options now provide more granularity when manually configured. Previous versions allowed only five settings: "Full, Half, 1/4, 1/8 and Min".

ZoneDirector now allows configuration of Tx power in 12 settings. The new settings are: Full, -1dB, -2dB, -3dB, -4dB, -5dB, -6dB, -7dB, -8dB, -9dB, -10dB, Min.

4.2.34 EU C-Band channels for United Kingdom country code

ZoneDirector now allows the use of 5.8 GHz channels (channels 149-165) for license holders when the country code is set to "United Kingdom" for the 5 GHz radio on 7762, 7762-S, 7762-T, 7762-AC, 7762-S-AC and 7761-CM outdoor APs. This can be configured globally or per-AP (on affected APs only). The C-band channels are disabled by default and should only be enabled by customers with a valid license to operate on these restricted channels.

4.2.35 DHCP Option 82 support

The "DHCP Relay Agent Information Option" (Option 82) allows a DHCP Relay Agent to insert specific identification information into a request that is being forwarded to a DHCP server. When this option is enabled on an SSID, the interface type (WLAN or Ethernet), AP Base MAC Address, AP Name, Model Name, Interface ID, and ESSID will be inserted into DHCP request packet's Agent Circuit sub-option, and the Station's MAC Address and VLAN ID will be inserted as the Agent Remote ID sub-option.

When this option is enabled for an Ethernet port, the AP's base MAC address and device name will be inserted as the Agent Remote ID sub-option for DHCP request packets.

4.2.36 ZoneDirector FQDN provisioning on APs

APs can now utilize the Fully Qualified Domain Name (FQDN) to discover ZoneDirector (rather than using ZoneDirector's IP address), if the FQDN is registered on the DNS server.

The maximum length of domain names has been reduced to 63 characters from 127 to comply with limits imposed by many popular DNS servers.

4.2.37 Selectable email alarm notifications

Administrators can now select which email alarms to receive from ZoneDirector when an alarm-level event occurs.

4.2.38 Additional SNMP trap servers

ZoneDirector now allows configuration of multiple SNMP trap receivers (up to 4 each for SNMPv2 and SNMPv3). Each trap receiver can operate in SNMPv2 or v3 mode, not both.

4.2.39 Configurable admin auto-logout

By default, administrators logged into either the ZoneDirector Web interface or the CLI are automatically logged out after 30 minutes of inactivity. This timeout can now be configured with a value between 1 and 1440 minutes for both Web interface and CLI.

4.2.40 Radius CHAP for Web-based authentication

With this release, ZoneDirector allows configuration of a RADIUS server entry with Challenge-Handshake Authentication Protocol (CHAP) authentication, in addition to PAP (default).

If your RADIUS server is configured to use CHAP, you can now set ZoneDirector to authenticate users with CHAP instead of PAP for features including Web Auth and Hotspot WLANs, guest pass generation, Zero-IT and administrator authentication.

4.2.41 Show external IP and port numbers for APs behind NAT

The ZoneDirector Web interface now displays the AP's external IP address and port number on the AP detailed view screen for APs connected via Layer 3 behind a NAT device.

4.2.42 Walled Garden rules increased to 35

The number of configurable Walled Garden rules for Hotspot WLANs has been increased from 5 to 35.

4.2.43 User names and passwords limited to ASCII range

User names and passwords are allowed to contain any characters in the ASCII range. If any character outside this range is detected, ZoneDirector will reject the client directly without forwarding the credentials to RADIUS.

4.2.44 Suppress broadcast traffic in tunneled WLANs

When a WLAN is set to tunnel mode and full wireless client isolation is enabled, ZoneDirector now prevents clients' broadcast traffic from being sent back through the AP's tunnels.

4.2.45 Disable tunnel-enabled WLANs when AP is disconnected from ZD

When an AP loses its connection to ZoneDirector, it now automatically disables tunnel mode service WLANs so that clients will not remain connected when service is down. Mesh and locally bridged service WLANs are not affected.

4.2.46 Import AP list

Rather than completely restoring ZoneDirector to a previously backed up configuration, administrators can now choose to import only the AP list from a backup file, while maintaining the current ZoneDirector configuration settings.

4.2.47 Prefer primary ZoneDirector

A new configuration setting allows users to set the primary ZoneDirector as the preferred device by APs when Limited ZD Discovery is enabled. This feature is not compatible with Smart Redundancy.

4.2.48 Manual Mesh provisioning via AP CLI

APs in factory default state can now be manually configured with settings to allow them to mesh with an existing Smart Mesh network without having to physically connect them to ZoneDirector.

4.2.49 The SSL certificate CSR country code drop-down list now includes more countries (including Barbados), and a “Country Not Listed” option is now available to allow users to manually enter a country if it is not listed. (ID 23920).

4.2.50 Tunneled broadcast/multicast filter

Two new options are available to filter broadcast and multicast traffic in tunneled WLANs to prevent excessive chatter between APs and clients when all APs are ZoneDirector-controlled. The first option allows ZoneDirector to block all tunneled multicast traffic. The second option blocks tunneled broadcast traffic other than ARP packets.

Resolved Issues from Previous Releases

4.2.51 eMAP information is now properly displayed when using the `show mesh topology` command. (ID 16245)

4.2.52 Resolved an issue with sending multiple types of data streams upstream that led to occasional AP crashes. (ID 22327)

4.2.53 ZoneDirector 1100 time zone changes are now properly reflected in syslog server event timestamps. (ID 18647)

4.2.54 Zero-IT application now properly works on OS X version 10.6.8 and higher. (ID 20599)

4.2.55 The DPSK passphrase can no longer be corrupted by using the “%” character on a WPA-PSK WLAN. (ID 21177)

4.2.56 Upgrading factory default ZoneFlex APs to this version (via ZoneDirector) will no longer result in Ethernet ports being blocked due to existing VLAN configuration on access ports not migrating properly to the new port-type mechanism. Additionally, if L2TP is enabled on an AP running pre-9.2 firmware, the bcp7 interface will now properly migrate to port type “Trunk Port” with VLAN membership 1-4094 upon upgrading to 9.3. (ID 24612)

4.2.57 Resolved an issue with ZoneDirector failing to clean ARP tables properly when WLANs in tunnel mode are deployed, resulting in ZoneDirector instability and frequent failover. (ID 24437)

4.2.58 Added called-station-id-type information for Web Auth WLANs to prepare RADIUS authentication request messages. (ID 24501)

4.2.59 Improved Zero-IT for Android phones; resolved a compatibility issue with the prov.apk provisioning file on some versions of Android OS. (ID 24524)

4.2.60 The number of alarm events recorded in the alarm-list.xml file is now limited to 1,250 (half of max events in event list) to improve stability under extremely high utilization. (ID 24388)

4.2.61 Improved ZD1000 upgrade file management process to address storage limitations and ensure that enough space is available for the new image when the ZD 1000 is filled with other data (such as configurations, dump files, etc.). (ID 24320)

4.2.62 Added a fix in the “check connection state” debug process to allow for trace generation when ZD loses network connectivity. (ID 23482)

4.2.63 Increased maximum physical memory allocation threshold for webs server processes to prevent safety mechanisms from impacting performance. (ID 23884)

4.2.64 Resolved an issue with Real Time Monitoring feature on ZD1000 that occasionally resulted in Web interface becoming slow or unresponsive. (ID 24350)

4.2.65 PoE out ports will now remain enabled for ZF 7762 and 7761-CM APs after upgrade from version 9.1 to 9.3.2, if the global AP policy for PoE out ports was set to enabled prior to upgrade. (ID 24210)

4.2.66 Resolved an issue with APs failing to update tunnel QoS settings from ZoneDirector after rejoining. (23488)

4.2.67 Resolved an issue with AP mesh configuration becoming out of sync with ZoneDirector after upgrade to 9.3. (ID 24461)

4.2.68 Resolved a discrepancy between reported SSID traffic statistics and client traffic statistics after client roaming between two APs or between two radios on the same AP. (ID 24221, 24550, 24195)

4.2.69 Resolved an issue with frequent WLAN configuration changes causing instability due to nodes leaving/disassociating before being fully associated. (ID 24175)

4.2.70 Resolved a Smart Redundancy issue which caused intermittent Web interface freezes after failover. (ID 25594, 25510)

4.2.71 Upgrading from 9.2 to 9.3 with tunnel encryption enabled no longer requires APs to be rebooted before clients can connect. (ID 24641)

4.2.72 Upgrading from 9.1.2 to 9.3 with a WISPr WLAN configured and IPv6 addressing no longer allows existing authorized clients to bypass authentication after upgrade. (ID 24511)

4.2.73 Denial of Service protection now excludes MAC authentication attempts on Hotspot WLANs when MAC auth bypass is enabled. (ID 25929)

4.2.74 Smart Redundancy failover stability during debug file generation has been improved. (ID 26185, 25229, 24829, ER-49, ER-77, ER-80)

4.2.75 Resolved an issue with clients not associating on the 2.4GHz radio, and corrected watchdog timeouts. (ID ER-76, ER-39, 24369)

4.2.76 Resolved an issue with tunneled traffic causing ZoneDirector crash due to tunnel packet fragmentation, when the fragment contains only the IP header and the first four bytes of the TCP header. (ID ER-64, ER-79, 26126)

4.2.77 Auto Tx power adjustment now works properly after upgrading from a pre-9.3 version to 9.3.2. This issue was causing frequent failovers between Smart Redundancy ZoneDirectors due to Tx power settings mismatch. (ID 26335)

4.2.78 Improved handling of client roaming between 2.4 GHz and 5 GHz radios on the same AP. Clients will no longer encounter “disassociated from WLAN [ssid_name] due to timeout waiting for AP to add station” errors. (ID 26365)

4.2.79 Improved compatibility with Android smartphones. Specifically, resolved an issue with previous 9.3 firmware that caused certain Motorola Droid phones running Android OS version 2.3.4 to reboot after associating to a WPA2-PSK/AES encryption WLAN. (ID 26462)

4.2.80 Web UI now properly displays Swedish text when Swedish is chosen as the Web interface language. (ID 26296)

4.2.81 Resolved an issue that could cause the Web interface to become unresponsive after running the “Save Debug Info” operation. (ID 26340)

4.2.82 Improved PMK caching for client sessions that quickly leave and return, which was allowing clients to reconnect without re-authentication. (ID 26320)

4.2.83 Channel selection list no longer includes channel 14 for Japan country code due to Japan’s restriction of channel 14 for use with 802.11b only. (ID 23807)

4.3 **ZoneFlex Access Points**

Enhancements

4.3.1 With this release, the ZoneFlex AP Web interface includes a LAN Ports configuration page, which allows configuration of each Ethernet port as either an Access Port, Trunk Port or General Port.

- Access port behavior: Untagged ingress packets and ingress packets tagged with the VLAN ID equal to the default PVID will be forwarded. Other ingress packets will be dropped. Egress packets are sent untagged.
- Trunk port behavior: All ingress packets (tagged and untagged) will be forwarded. Egress packets will be tagged with a non-default PVID. Untagged VLAN can be configured with a PVID other than 1.
- General Port behavior: Administrators can configure an Ethernet port to support multiple tagged VLANs and one untagged VLAN.

4.3.2 The ZoneFlex 7025 supports four priority queues (voice, video, data and background) on both the wired and wireless interfaces, allowing traffic prioritization based on VLAN ID.

VLAN QoS (802.1p prioritization) can be performed from the ZoneDirector CLI.

- ZoneDirector CLI command: (from the directory path /ruckus/config/ap-policy):
  `vlan-qos <vlanid> <traffic class> <Interface Name>`

4.3.3 802.1X

Ethernet ports on standalone ZoneFlex APs can also be configured for 802.1X authentication. Ports can be individually defined as either Authenticator or Supplicant ports. Default is 802.1X disabled.

4.3.4 PPPoE on standalone APs

Standalone ZoneFlex APs can now be configured to use PPPoE instead of DHCP or static IP addressing methods.

4.3.5 IPv6

Standalone APs can also be configured to use IPv6 addressing. Default is dual stack IPv4/IPv6.

4.3.6 AP Hotspot Configuration (WISPr)

Standalone APs can now be configured to provide Hotspot service using the WISPr standard.

4.3.7 L2TP

Layer 2 Tunneling Protocol can now be enabled on 802.11n ZoneFlex APs, in addition to the existing functionality on 11g APs.

4.3.8 Enhanced channel selection

With this release a new, more aggressive auto channel selection algorithm has been introduced. This is on by default when the access point is in auto channel mode. The new algorithm introduces an adaptive channel selection feature that maintains optimum Wi-Fi throughput based on real, observed Mbps capacity potential. After an initial evaluation process the access point will settle on the channel with the best throughput based on the surrounding network conditions.

4.3.9 Router mode support

Standalone APs can now be configured as NAT gateway devices with the ability to manage their own subnets and support DHCP server and DNS cache functions. Client stations connected to the AP via wired or wireless can be assigned private IP addresses in different subnets with different VLANs. Up to four subnets can be configured for each AP.

4.3.10 More granular transmit power configuration

When AP transmit power is manually configured, the available power options now provide more granularity. Previous versions allowed only five settings: “Full, Half, 1/4, 1/8 and Min”.

Standalone APs now allow configuration of Tx power in 12 settings. The new settings are: Full, -1dB, -2dB, -3dB, -4dB, -5dB, -6dB, -7dB, -8dB, -9dB, -10dB, Min.

4.3.11 ChannelFly statistics are now included in AP support.txt log files.

Resolved Issues from Previous Releases

4.3.12 Resolved a voice quality issue with Microsoft Lync clients (Intel client interoperability issue). (ID 23503)

4.3.13 Dynamic VLAN can now be enabled on MAC Auth WLANs. (ID 24485)

4.3.14 ZF 7761-CM Web interface (and ZoneDirector, if under ZoneDirector control) now properly displays the correct MAC address for the cable modem. (ID 25593)

4.3.15 Updated Australia channel list to properly allow use of DFS channels when Australia country code is selected. (ID 26341)

5 Caveats, Limitations and Known Issues

This section lists the caveats, limitations, and known issues for FlexMaster, ZoneDirector and ZoneFlex Access Points in this version.

5.1 FlexMaster

Installation, Backup and Restore

5.1.1 Ruckus Wireless recommends installing FlexMaster on a Red Hat Enterprise 5.x 64-bit server (required).

5.1.2 Minimum hardware requirements: Core 2 Duo CPU, 8GB RAM.

Managed Population	Min RAM	Min CPU
ZoneDirector-managed APs:		
Up to 1,000 ZD managed APs	8G	2.0G Quad core Intel (Xeon E5606 equivalent or above)
Up to 5,000 ZD managed APs	16G	2.5G Six core (Intel Xeon X5670 equivalent or above)
Up to 10,000 ZD managed APs	32G	2* 2.5G Six core (Intel Xeon X5670 equivalent or above)
Standalone APs: (http/https)		
Less than 1,000 standalone APs	8G	2.5G Six core (Intel Xeon X5670 equivalent or above)
Up to 2,000 standalone APs	32G	2* 2.5G Six core (Intel Xeon X5670 equivalent or above)

5.1.3 Scalability testing has been completed for up to 5,000 APs and 20,000 clients.

5.1.4 If you use the Web interface to back up the FlexMaster database, and then you use the CLI to restore it to a fresh FlexMaster installation, FlexMaster is unable to start up successfully (ID 21329).

Web Interface

5.1.5 FlexMaster release 9.3 supports the following Web browsers:

- Firefox 3.0 and later
- Internet Explorer 7 and later
- Chrome 5.0 and later

FlexMaster does not support Internet Explorer 6.0. Some Web interface elements may not display correctly in this browser.

5.1.6 The maximum number of entries that FlexMaster drop-down menus support is 1000. If there are more than 1000 entries, there will be multiple pages on the drop-down menu, and the user can use the pagination arrows to switch between pages.

5.1.7 The Dashboard displays the most recent events and it refreshes automatically every 15 seconds. To pause the auto refresh function, click either the **10 more records** button or the **show all** button.

5.1.8 If a large number of events occur within a short period of time, the *Most Recent Events* widget on the Dashboard may show fewer events compared to the **Monitor** > **Events** page (ID 20998).

5.1.9 If an AP is reassigned from one ZoneDirector device to another, it may temporarily fail to show up in the search results when you run a device search using the AP’s MAC address (ID 20992).

5.1.10 When the number of currently managed devices exceeds the number of available licenses, the warning on the Device Registration page sometimes does not appear (ID 21551).

Provisioning

5.1.11 When creating a configuration template to provision 802.1X settings to a standalone AP, the user must configure both **VLAN & Port Setting** and **802.1X Settings**.

5.1.12 When a configuration template includes Management Server Configuration Settings, the template name becomes very long. This is because the model names of all supported products are included in the template name (ID 22925).

AP-Related Issues

5.1.13 The value for Transmit RSSI is inaccurate for ZF2741 (ID 20048, 22231).

5.1.14 ZF7761CM cannot be reset successfully from either the AP Device View or using SNMP (ID 20177).

Workaround: Reset ZF7761CM from the AP's Web interface.

5.1.15 FlexMaster currently ignores WISPr configuration errors from managed devices; this is to ensure that WISPr configuration tasks provisioned from FlexMaster will always be successful.

5.1.16 The LAN5 port on the ZoneFlex 7025 can only be configured as a Trunk Port.

5.1.17 The Ping Test feature on the AP is disabled by default.

Reports

5.1.18 The **Association** > **Connected Clients** report does not show the association and disassociation time for each client.

5.1.19 The maximum number of rows that reports exported to XLS can contain is 65,536. If a report contains more than 65,536 rows, the excess rows will be deleted automatically from the report.

5.1.20 Exporting multiple reports to XLS format simultaneously may fail.

5.1.21 FlexMaster generates the Capacity, SLA, and Troubleshooting reports on the hour (for example, at exactly 12:00PM). While FlexMaster is in the process of generating these reports, the graphs and reports on the FlexMaster Web interface may appear blank. Report generation time depends on the number of managed APs and the number of clients that report to them. When FlexMaster completes generating these reports, the graph and report pages are populated with the latest data.

5.1.22 The Client Association report sometimes does not display the client model (ID 21357).

5.1.23 Clicking the ➔ (Navigate) icon on the Client Association Activity widget on the Dashboard shows the Client Association Activity report for the previous hour, instead of the current hour (ID 21929, 24016).

5.1.24 The Client Associated Time report shows an uptime of 100% even for clients that were only connected for half an hour (ID 22953).

5.1.25 When an AP is disconnected multiple times within an hour, its uptime and downtime information may appear incorrect on the **SLA** > **AP** page of the FlexMaster Web interface (ID 23356).

5.1.26 Client Association Activity data cannot be exported to PDF (ID 23511).

5.1.27 ZoneDirector devices on which mesh networking is disabled are still included in the Mesh Report for All ZoneDirectors (ID 17999, 21437).

5.1.28 The event type details are incomplete on the **Dashboard** > **Most Recent Events** widget on the FlexMaster Web interface.

5.1.29 When you generate an AP with No User Connectivity report and you set the period to 1 Hour, the report shows no entries for the first 15 minutes of the hour (ID 22865).

5.1.30 Deleted ZoneDirector devices still generate duplicate records in AP statistics, hotzone association, and other tables (ID 22651).

5.1.31 Alert emails for reset and heartbeat lost events are sometimes not sent. This typically happens when the FlexMaster server is busy (ID 21549).

5.1.32 If a client is disconnected multiple times, FlexMaster only records the client traffic information from its last connection. Traffic information from previous connections is not recorded (ID 22991).

5.1.33 Some messages in the Audit Log are incomplete (ID 21526).

5.1.34 Client count in reports exported to PDF is shown in decimal numbers, instead of whole numbers (ID 21556).

5.1.35 Dashboard AP graph and Connectivity graph may show incorrect report data for a brief period after shutdown and restart. (ID 24150, 24131)

SpeedFlex

5.1.36 The **Monitor** > **SpeedFlex** page only shows up to five (5) wireless clients per AP, even when there are more than five clients associated with the AP (ID 21263).

5.1.37 Downlink multi-hop mesh test fails if performed in an L3 environment (ID 22105).

5.1.38 Values are sometimes missing from the SpeedFlex test results (ID 21554).

Other Caveats

5.1.39 The default number of days for triggering the purge policies (on **Administer > System Settings** page) is missing.

5.1.40 FlexMaster generates an audit log whenever a scheduled report is not sent out successfully (ID 21419).

5.2 **ZoneDirector**

General

5.2.1 If a manually selected channel should no longer be allowed for a certain country code (due to changes in regulatory rules on allowable channels), the fixed channel configuration will be changed to "auto" after upgrade. (ID 17925)

5.2.2 Available 11an channels differ between AP and ZoneDirector when country code is set to Colombia (APs display more channels available than ZoneDirector). (ID 21255)

5.2.3 ZoneDirector-controlled ZoneFlex 7300 series Ethernet ports may fail to prioritize voice/video packets correctly when the port is connected to a switch port set to 100m full duplex mode and the port is congested. (ID 19644, 20846)

5.2.4 ZoneFlex 7025 may experience slight maximum downlink performance degradation between 9.1.1 and later versions when rate limiting is enabled. (ID 20900).

5.2.5 If ZoneDirector is set to obtain a dynamic IP address from DHCP, it may send the incorrect IP address to APs after the DHCP lease has expired. (ID 23351)

5.2.6 When setting the primary and secondary ZoneDirector IP addresses from AP CLI, the CLI displays an error message if the FQDN of one is invalid (over 64 bytes). However, the CLI still prompts the user to reboot the AP for changes to take effect. (ID 23495)

5.2.7 Secondary ZoneDirector address information is lost after the AP joins with the “Keep AP’s Primary ZD and secondary ZD settings” enabled. (ID 22058)

5.2.8 ZoneDirector 5000-controlled APs may fail to redirect users to their intended destination URL after successful authentication on a Web Auth WLAN. Other ZoneDirector models do not encounter this issue. (ID 23790)

ZoneDirector 1000

> Release 9.3 will be the last release that supports ZoneDirector 1000. ZD1000 will be discontinued as of release 9.4. For more information, refer to the ZD1000 End of Life Notification available from http://support.ruckuswireless.com/products/32-end-of-life.

5.2.9 ZoneFlex 7025 is not supported by ZoneDirector 1000

The ZoneFlex 7025 Wired/Wireless Wall Switch is not supported by ZoneDirector 1000 (including 1006, 1012, 1025 and 1050). If you have a ZoneFlex 7025, you can manage the device with ZoneDirector 1100, ZoneDirector 3000 or ZoneDirector 5000 Series, as a Standalone AP, or with FlexMaster.

5.2.10 ZoneDirector 1000 does not support IPv6.

5.2.11 An AP set to IPv4 only mode that joins a ZoneDirector 1000 will be set to dual IPv4/IPv6 mode after joining, despite the fact that ZoneDirector 1000 does not support IPv6. (ID 21710)

Workaround: If you want the AP to use IPv4 only mode, first allow it to join ZoneDirector and then manually change the IP addressing method to IPv4 only.

5.2.12 ZoneDirector 1000 does not support local packet capture. ZoneDirector 1000 only supports streaming mode.

Web Interface

5.2.13 ZoneDirector release 9.3 supports the following Web browsers:

- Firefox 3.0 and later
- Internet Explorer 7 and 8
- Chrome 5.0 and later

> **Note**: Internet Explorer 9 is currently not supported in version 9.3 (ID 23688). The workaround is to run IE 9 in “Compatibility Mode” by enabling **Tools > Compatibility View** in the browser.

5.2.14 RSSI information for the same Access Point is inconsistent between the Downlinks and Neighbor APs sections on the **Monitor** > **Access Points > [AP MAC Address]** page. (ID 11527)

5.2.15 Web UI displays some text in English when another UI language is selected. Some new or modified text strings have not yet been translated into all languages. This will be updated in a future release. (ID 18839, 20160, 21705)

5.2.16 ASCII code used in DHCP option 60 may be displayed incorrectly in ZoneDirector Web interface because ZoneDirector does not support unprintable characters. (ID 19667)

5.2.17 The Currently Active Clients list now displays the client’s authentication method along with other client information. When a client is connected with WPA or WPA2 encryption, the authorization method displays “EAP” (Extensible Authentication Protocol). When the client is connected using WEP-64, WEP-128 or “none” encryption, the authentication method displays “DWEP”. (ID 21682)

5.2.18 The failover restore feature description neglects to mention that management VLAN settings will not be restored during a “restore everything, except system name and IP address settings” restore. (ID 20310)

5.2.19 The number of guest restricted access rules is inconsistent between Web interface and CLI. (ID 20161)

256 Clients per AP

5.2.20 ZoneFlex APs support up to a maximum of 256 clients per AP, including dual radio APs. When configuring this feature, ZoneDirector interface only provides a global setting, which is applied to each radio. To avoid overloading the AP, this number should be configured to a maximum of 128 on dual radio APs to ensure that no more than 256 clients join the AP. (ID 18661, 20419, 20924, 21265, 21106, 21071, 21022)

5.2.21 When max clients per AP is set to 256 and the number of clients attempting to connect to an AP exceeds that number, ZoneDirector incorrectly displays the total of associated and non-associated clients (exceeding the maximum) rather than only those allowed to associate. (ID 22664)

CLI

5.2.22 The `show-currently-active-clients all` command may consume excessive CPU resources on the ZoneDirector 1000 when many clients are connected, debug log is enabled and other processes are running (such as Real-Time Monitoring), resulting in ZoneDirector disconnecting APs and stations (ID 16617)

Workaround: Disable debug or Real-Time Monitoring to improve performance.

5.2.23 Entering an AP group name in the CLI with a space character in the name requires enclosing the name in quotes, e.g., “APGROUP 1”. (ID 18623)

5.2.24 Several CLI commands have been redesigned in versions 9.2 and 9.3, and some previous commands no longer work. For example, the `vlan` and `mgmt-vlan` commands have been replaced with arguments for the `interface` command. (ID 19063, 19153, 19087)

5.2.25 ZoneDirector CLI allows setting an AP’s IP address to manual without entering a valid IP address when ZoneDirector is in dual stack IPv4/IPv6 mode. (ID 20527)

IPv6

5.2.26 When IPv6 is enabled but ZoneDirector is assigned a static IPv4 address, 802.11 data frames are forwarded to stamgr, with the “station MAC” address being our AP. (ID 17391)

5.2.27 IPv6 only APs can mesh with other IPv6 only APs in different subnets. (ID 19854)

5.2.28 IPv6 multicast video streams are allowed to traverse the WLAN tunnel. (ID 20531)

5.2.29 ZoneDirector 1000 sends IPv6 information to external syslog server despite the fact that ZoneDirector 1000 does not support IPv6. (ID 20961)

5.2.30 APs retain the IPv4 address of a ZoneDirector that has been switched to IPv6 only mode. (ID 21010)

5.2.31 APs may erroneously be allowed to join a ZoneDirector’s Management Interface rather than the original IP address when an IPv6 Management Interface is enabled and the control IPv6 address is not the same as the primary ZoneDirector’s IP address. (ID 20818, 20831)

5.2.32 The Mesh Recovery SSID is only supported with IPv4 addressing.

5.2.33 ZoneDirector Web interface does not display client IP address when IPv6 only mode is set from the client. (ID 23188)

5.2.34 APs are unable to dynamically discover ZoneDirector via Layer 3 in an IPv6 only network, as there is no DHCP option 43 with which to inform the APs of ZoneDirector's IPv6 address.

Workaround: Configure a static address if using IPv6 only.

PPPoE

5.2.35 When an AP WAN port is configured in PPPoE mode, ZoneDirector admins will be unable to run SpeedFlex or launch the System Info, RF Info or Network Connectivity tools from the ZoneDirector Web interface. (ID 17224)

5.2.36 PPPoE Server on Linux establishes a PPP connection and assigns an IP address and DNS Server IP address, but does not assign search domain (DNS suffix), therefore APs are unable to locate ZoneDirector via DNS lookups. (ID 19331)

5.2.37 ZoneDirector fails to add Layer 2 PPPoE pass through rules for IPv4 policies when a WISPr WLAN is created on an earlier version prior to upgrading to 9.2 or 9.3. (ID 21563)

Workaround: Remove all WISPr WLANs before upgrading to 9.2 or 9.3 from an earlier version. Restore ZoneDirector to factory defaults after upgrading, then recreate WISPr WLANs.

5.2.38 ZoneDirector is unable to display a connected client's IP address if the client obtains its IP address from a PPPoE server that passes address information through the AP. (ID 22290)

AAA Servers

5.2.39 RADIUS Accounting interim-update packets may be delivered in incorrect sequence when roaming occurs. (ID 19527)

5.2.40 ZoneDirector does not support Idle-Timeout values in RADIUS CoA messages. (ID 20686)

VLAN, Dynamic VLAN, and Tunnel Mode

5.2.41 If the VLAN, Dynamic VLAN, and Tunnel Mode features are all enabled and they have conflicting rules, ZoneDirector prioritizes and applies these three features in the following order:

1. Dynamic VLAN (top priority)
2. VLAN
3. Tunnel Mode

Ethernet Ports and Port-based VLAN

5.2.42 ZoneFlex 7300 Series AP Ethernet ports can become disabled if half-duplex is forced on any port. (ID 15916)

Workarounds: Do not force half-duplex on any port; use gigabit port for uplink connection.

5.2.43 The Active Wired Clients page displays incorrect authorization status ("unauthorized") when port-based 802.1X clients are connected and authorized without username/password. (ID 17904)

5.2.44 When configuring an AAA server object in the ZoneDirector Web interface, it is possible to lose configuration changes by changing the AAA server type (from RADIUS to Active Directory, for example), after you have modified 802.1X settings when the server object was set to RADIUS. (ID 23354)

Smart Redundancy

5.2.45 When two ZoneDirectors in a Smart Redundancy configuration are set to use static IPv6 addresses, the “Additional Management Interface” may become inaccessible after failover or reboot. (ID 21709, 21713)

Workaround: Ensure that all the settings (IP address, VLAN, etc.) are exactly the same on both the active and standby ZoneDirectors before performing a failover or reboot.

5.2.46 When two ZoneDirectors are deployed in a Smart Redundancy configuration and the active ZoneDirector is behind NAT, upgrade to standby ZoneDirector fails. (ID 20528)

5.2.47 Changing the admin login session timeout with Smart Redundancy enabled does not take effect until the next session (after closing and restarting the browser). (ID 22470)

5.2.48 Synchronization from active to standby device may take a long time to complete when very large configurations need to by synchronized (>3,000 users). (ID 21818)

Smart Mesh Networking

5.2.49 Smart Mesh networking is not supported on ZoneFlex 7025 Wired/Wireless Wall Switch.

5.2.50 Meshing between indoor and outdoor dual radio ZoneFlex APs in US country code

Indoor dual band ZoneFlex APs (ZF 7962 and 7363) support DFS channels in the US country code, while the outdoor dual band APs (ZF 7762/7762-S/7762-T/7762-AC/7762-S-AC/7761-CM) do not. If meshing between these APs with the 7962/7363 as the Root AP, the APs need to be on a channel usable by all APs. If the 7962 or 7363 is set to one of the DFS channels, the outdoor AP will not be able to connect to it.

Workaround: Under **Configure** > **System** > **Country Code**, set the Channel Optimization to either *Optimize for Compatibility* or *Optimize for Interoperability*, or set the 7962/7363 Root AP to a non-DFS channel (e.g. channels 149-165).

5.2.51 Mesh AP temporarily loses mesh connection when beacon-interval for mesh interface is manually changed. (ID 20324)

5.2.52 Mesh AP scanning timer sends out probe requests at longer intervals than the interval configured. For example, when interval is set to 10 seconds, the actual interval is approximately 14 seconds; when interval is set to 40 seconds, the actual interval is 54 seconds. (ID 20420)

5.2.53 When Mesh is enabled, ZoneFlex 11g APs (ZF 2942 or 2741) can support a maximum of 4 WLANs with Rate Limiting enabled. (ID 20429, ID 20612)

5.2.54 Mesh APs will be unable to mesh successfully with Root APs after upgrade or downgrade due to SSID or Mesh passphrase mismatch if either value was changed during the process. (ID 21159, 20877)

Workaround: Do not change the Mesh SSID or passphrase during upgrade or downgrade.

5.2.55 When a Root AP’s channel is reverted from a fixed channel to Auto, it begins a scan of all available channels and the Mesh AP may lose heartbeats. (ID 19929)

5.2.56 ZoneDirector-controlled APs in a Layer 2 topology may enable the Mesh Recovery SSID while still connected to ZoneDirector if they are unable to contact the gateway, or the default gateway is not defined. (ID 23497, 24216, 24214)

WLAN Service Schedule

5.2.57 Service Schedules, which are used to define the day and time that a WLAN is enabled, are based on the ZoneDirector’s System Time (UTC). WLANs are enabled and disabled based on the ZoneDirector’s time, regardless of where the AP is located.

5.2.58 If accessing the ZoneDirector Web interface from a time zone other than the one where ZoneDirector is located, the configured WLAN service schedule will use the time zone as configured on the accessing PC rather than the time zone where ZoneDirector is located. (ID 21784).

Band Steering

5.2.59 Band steering is disabled on mesh-enabled APs.

Zero-IT and Dynamic PSKs

5.2.60 The maximum number of PSKs that is supported is

- 1,250 on ZoneDirector 1000 and ZoneDirector 1100
- 5,000 on ZoneDirector 3000 licensed up to 250 APs
- 10,000 on ZoneDirector 3000 licensed up to 500 APs
- 20,000 on ZoneDirector 5000 licensed up to 1,000 APs

5.2.61 Users are not disconnected when a DPSK expires. (ID 16784)

Current behavior is to allow authorized clients to remain connected even after the DPSK has expired. Once the user disconnects from the network, he will be unable to log in again with an expired DPSK.

5.2.62 Running the Zero-IT application to automatically configure a Win 7 or Vista client with wireless settings requires the user to manually deselect “Validate server certificate” and “Automatically use my Windows logon name and password” when attempting to connect to an 802.1X WLAN with an external RADIUS server. (ID 21517)

5.2.63 Zero-IT on some Android devices may encounter errors when trying to install. Specifically, Zero-IT can be downloaded and installed properly on Android versions 2.2 and 2.3.3, but with version 2.2.2 or 2.2.4, the Zero-IT application downloads but fails to execute properly on some HTC smartphones. (ID 22721, 22477)

SpeedFlex

5.2.64 SpeedFlex is not supported on 11g access points (ZoneFlex 2942/2741). (ID 20058)

5.2.65 SpeedFlex is unable to accurately measure performance of clients connected to a WLAN with rate limiting enabled. (ID 22591)

Access Point Groups

5.2.66 When Smart Mesh is enabled, 802.1X settings are unavailable from the AP Groups configuration page. (ID 21707)

Workaround: If you need to set 802.1X settings for a non-meshing AP that is being managed by ZoneDirector with Smart Mesh enabled, you cannot do this using AP Groups. You must configure these ports for each AP individually.

Packet Capture

5.2.67 ZoneDirector 1000 supports packet capture to streaming mode only; local file packet capture is supported on ZoneDirector 1100, 3000 and 5000 only.

5.2.68 Streaming mode is unsupported when AP addressing is IPv6 only.

5.2.69 The packet capture feature may continue capturing packets on some AP interfaces even after streaming mode has stopped. (ID 21505)

Workaround: Reboot the AP.

Auto-Proxy Configuration

5.2.70 Auto-Proxy configuration using DNS requires that the `wpad.dat` file is stored in the root directory of the Web server that will be queried (multiple wpad.dat files in different directories does not work). Therefore, to send clients to different proxy servers by subnet, the admin should place one wpad.dat file in the root directory of ZD or external web server and write all the proxy logic in one wpad.dat file. Additionally, note that some browsers (Firefox, Chrome, Safari) do not support DNS lookup. (ID 17157)

5.2.71 ZoneDirector's internal DHCP server does not support DHCP option 252. (ID 17158)

5.2.72 Some smart phones (such as iPhone 4, Android 2.3) are not supported by the new Auto Proxy feature due to lack of support for DHCP Option 252 (Safari browser) or the WPAD protocol (Android). (ID 21228)

APs Behind NAT

5.2.73 When an AP behind NAT is serving a non-tunneled Hotspot WLAN, authenticated users are unable to log out via the logout URL. (ID 21848)

Per-Client Rate Limiting

5.2.74 Per-client rate limiting via RADIUS attributes is currently only supported for WISPr WLANs. Per-client rate limiting on 802.1X WLANs is currently not supported. (ID 22396)

DHCP Option 82

5.2.75 When DHCP option 82 is enabled on a Hotspot WLAN in tunnel mode, the option 82 information is correctly added to DHCP request packets from joining clients, but the information is not properly removed from unicast DHCP packets sent back to the station (offer/ack messages). When those packets are broadcast however, Option 82 works as intended. (ID 22038, 23371)

Remote Troubleshooting

5.2.76 The Remote Troubleshooting process continues running after SSH connection timeout. (ID 21560)

Hotspot and WISPr Smart Client Support

5.2.77 Some Smart Clients that do not redirect may be incompatible with the ZoneDirector WISPr Smart Client support feature. (ID 23285)

5.2.78 Creating a Hotspot or Walled Garden rule with an invalid URL may cause the Web interface to become unresponsive for up to one minute, as ZoneDirector tries to resolve the invalid URL to an IP address and fails. (ID 20925, 22129)

5.2.79 When the maximum number of Hotspot WLANs and the maximum number of Hotspot Walled Garden rules are created, the AP may fail to complete its configuration and may become unable to re-join ZoneDirector after reboot. (ID 22922, 23153)

Workaround: The increase to max 35 walled garden rules is for specific scenarios where more rules are needed for one or two Hotspot services per AP. Use only as many walled garden rules and Hotspot services as needed. Do not attempt to deploy 16 Hotspot WLANs (on a dual radio AP) with 35 Walled Garden rules each.

5.3 **ZoneFlex Access Points**

General

5.3.1 DFS channels support

In this release, Dynamic Frequency Selection (DFS) channels are unavailable for all APs other than ZoneFlex 7962 and ZoneFlex 7363 (restricted by ZoneDirector/AP) when the country code is set to US.

5.3.2 AP intermittently reports incorrect PHY errors which adversely affects channel blacklisting. (ID 17684, 17169, 20186)

5.3.3 AP beacons and probe responses allow RIFS bits and 11n greenfield mode with no protection. Although most clients do not use RIFS or greenfield mode, this could create a problem for any clients that do. (ID 19002)

5.3.4 AP watchdog timer may be triggered after about eight hours of stress testing when transmitting L2 tunneled Tx traffic. (ID 19634)

5.3.5 In some conditions, the ZoneFlex 7761-CM access point fails to complete noise floor calculations and sends a syslog error message: *kernel: >>>>>> ar5416GetNf: Failed to read CCA reg*. (ID 18294)

5.3.6 ZoneDirector 1100 encounters a memory leak issue when generating large numbers of rogue AP alarms during testing. (ID 19991)

5.3.7 When a large number of clients is connected to a single AP (~255 clients), the “Connected Devices” displays SSID information incorrectly. (ID 20974)

5.3.8 APs are unable to mesh again automatically when the IP type is changed from PPPoE to DHCP/Static, until the AP is rebooted again. (ID 19044, 20282)

Workaround: Reboot the AP once after changing from PPPoE to DHCP or Static, let it join ZoneDirector, then reboot the AP again to ensure mesh is re-enabled.

5.3.9 When more than 255 clients connect to a standalone ZoneFlex 7363, the new clients are allowed to connect and previous clients are kicked off. (ID 21000)

5.3.10 When 255 clients are connected to an AP and clients are attempting to exchange ARP messages with all 8 WLANs enabled on a radio, the AP Web interface may become unresponsive. (ID 21394)

5.3.11 When a Hotspot Walled Garden rule is created to allow unauthenticated clients to access certain websites, parts of those websites may not display correctly if they are dynamic pages displaying content from other (non-walled garden) websites. (ID 22718)

5.3.12 When the Access VLAN for an AP is set via FlexMaster, the value displayed in Device View is inconsistent with the AP Web interface display. (ID 22202)

5.3.13 Hotspot service does not work if the AP’s management VLAN and the Hotspot VLAN are in different subnets. (ID 23619)

Router Mode

5.3.14 Packets from local network are NAT’ed to the AP’s management VLAN. (ID 22278)

5.3.15 Clients behind the NAT fail to receive multicast packets after router mode is enabled. (ID 21958)

Workaround: If multicast support is required, use the AP in bridge mode.

802.1X and Ethernet Port Configuration

5.3.16 On standalone ZoneFlex 7363 APs with 802.1X ports configured, the supplicant port continues sending EAPOL start frames periodically after authentication failure and EAPOL-failure frame has been received from the authenticator port. (ID 18662)

5.3.17 Invalid IP addresses for RADIUS/RADIUS Accounting servers can be entered and saved in the 802.1X Authenticator fields on standalone APs. (ID 18719)

5.3.18 Downstream multicast and broadcast streams can pass through an AP even when the AP is not authorized. (ID 19195)

5.3.19 Changing the PVID of the uplink Trunk port on an AP from 1 to another number may cause the AP to disconnect and be unable to reconnect to ZoneDirector. APs do not automatically send a DHCP renew/restart request whenever an Ethernet port configuration change is made. Therefore, if the PVID of the (uplink) Trunk port is changed from 1, the AP will lose connection to ZoneDirector until the AP reboots. If mesh is enabled, the AP will continuously attempt to connect as a Mesh AP when it is intended to be a Root AP. (ID 19612, ID 19838)

Interoperability with PoE Switches

5.3.20 ZoneFlex APs support standard Power-over-Ethernet (802.3af). The following PoE switches were tested with ZoneFlex 2942, 2741, 7343, 7363, 7942, and 7962 APs:

- Ruckus ZoneSwitch 4124 and 4224
- Linksys 2008MP
- Linksys SRW 224P
- NetGear FS726TP
- SMC | SMCGS8P-SMART 8P+1SFP
- HP ProCurve-24 2610
- HP ProCurve 2520-8-PoE
- BayStack 470
- D-Link DES-1228P
- TrendNet TPE-S88

6 Upgrading to This Version

This section lists important notes on upgrading ZoneDirector and ZoneFlex to this version.

6.1 ZoneDirector

6.1.1 Official 9.3 upgrade path:

9.1.2.0.8 and later to 9.3.2.0.3

9.2.0.0.138 and later to 9.3.2.0.3

9.3.0.0.87 and later to 9.3.2.0.3

6.1.2 Additionally, the following 9.1.0 builds can be upgraded directly to 9.3:

9.1.0.3.95 to 9.3.2.0.3

9.1.0.3.124 to 9.3.2.0.3

These builds may require a special procedure to ensure that all previous settings are retained after upgrade. (ID 24210, 24013)

Recommended upgrade procedure from 9.1.0.3 to 9.3

==

Assuming that ZD1 is Active running 9.1.0.3 and ZD2 is Standby running 9.1.0.3. (If only one Zone Director is involved and no Smart Redundancy is used, only step 1 is necessary before upgrading to 9.3)

1. From the Active ZD1’s Web UI, go to the Configure > Access Points page, Global Configuration section. If PoE OUT port is enabled and is expected to be enabled after upgrade, disable it, wait for 10 seconds, and re-enable it. Note this step may cause connected APs’ PoE OUT ports to lose power during this period of time.
2. From the Active ZD1’s Web UI, go to the Configure > Access Points page, Access Point Policies section, and make sure that ZD1’s IP address is configured as the primary ZoneDirector IP and standby ZD2’s IP address is configured as the secondary ZoneDirector IP.
3. From the Active ZD1’s Administer > Backup page, back up the current 9.1.0.3 configuration.
4. Disconnect ZD2 from the live network.
5. From the Standby ZD2’s Administer > Backup page, restore ZD2 to factory defaults. Then go through the Setup Wizard to configure basic settings. (Do not enable Smart Redundancy at this point.)
6. From the Standby ZD2’s Administer > Back up page, restore the backup configuration from the file saved from ZD1, using the “Restore everything” option.
7. Re-configure the System Name, IP address, VLAN and Smart Redundancy settings on ZD2.
8. Reconnect ZD2 to the network and it will sync up with ZD1 to become the Standby ZD.
9. Perform upgrade to 9.3 on the Active ZD1.

6.1.3 Only ZoneDirector 1000 and ZoneDirector 3000 with firmware versions 9.1.1 or later can be upgraded to this release. Upgrading from any other firmware versions might result in loss of configuration settings. ZoneDirectors that are using a firmware version earlier than 9.1.1 (including 9.1.0) must first be upgraded to version 9.1.1 or later before they can be upgraded to 9.3. (Aside from two minor exceptions, see 6.1.2).

ZoneDirector 1100 does not support any firmware version earlier than 9.1, and ZoneDirector 5000 does not support any firmware version earlier than 9.2.

6.1.4 After upgrading to ZoneDirector version 9.3, clear the Web browser cache. This will ensure that the ZoneDirector Web interface shows all the changes and enhancements that were implemented in version 9.3.

6.1.5 When upgrading ZoneDirector 1000 to version 9.3, the administrator may be prompted to reboot ZoneDirector manually to delete temporary files and clear the system memory. This happens when there is insufficient memory to perform the upgrade process.

Downgrading from version 9.3 to previous versions

6.1.6 ZoneDirector 1000 downgrading from 9.3 to 9.2 or 9.1.1

Because of memory limitations in ZoneDirector 1000, downgrading from version 9.3 to 9.2 or 9.1.1 requires a special procedure. If ZoneDirector 1000 is running 9.3.2.0.3, please follow these steps to downgrade to 9.2 or 9.1.1:

1. Disconnect all of the APs connected to the ZoneDirector 1000.
2. Reboot the ZoneDirector 1000 to clean up memory.
3. Downgrade ZoneDirector 1000.
4. After the downgrade is complete, reconnect the APs to ZoneDirector.

6.1.7 When downgrading from 9.3 to 9.1.1, ZoneDirector 1000 will factory reset and will not restore the original 9.1.1 configuration settings. Therefore it is very important that you backup your existing configuration prior to upgrading to 9.3.

6.1.8 ZoneDirector 1100 running firmware version 9.3 only supports downgrade to version 9.1.1.0.58 or later.

6.1.9 ZoneDirector 5000 running firmware version 9.3 only supports downgrade to version 9.2.0.0.138 or later.

6.2 **ZoneFlex Access Points**

6.2.1 Standalone ZoneFlex 2741, 2942, 7025, 7341, 7343, 7363, 7762, 7762-S, 7762-T, 7942, and 7962 units running on version 9.1.1, 9.1.2 and 9.2 can be upgraded to this version.

6.2.2 ZoneFlex 7761-CM, 7762-AC and 7762-S-AC are not compatible with versions earlier than 9.2.

6.2.3 Downgrading APs from version 9.3 to 9.2 or 9.1.1

If APs running version 9.3 are downgraded to version 9.2 or 9.1.1, APs will resume operation based on the last saved 9.2 or 9.1.1 configuration, or be reset to factory default state if no prior configuration is found. For example, an AP running a non-9.3 image upgrades to 9.3 and is factory-reset while running 9.3, a downgrade to a non-9.3 image will cause the AP to be reset to factory default state. However, if you upgrade from 9.1.1 or 9.2 to 9.3 and then downgrade back without factory resetting the AP, the AP will preserve its last saved 9.2 or 9.1.1 configuration state.

6.3 **Changed Behavior**

6.3.1 In previous releases, Global Configuration settings were applied to all APs. These settings have been moved to Access Point Groups and any previous configurations will be retained in the System Default AP Group after upgrade.

6.3.2 Upgrading to releases 9.1.2-and-later:

Some countries restrict certain 5 GHz channels to indoor use only. For instance, Germany restricts channels in the 5.15 GHz to 5.25 GHz band to indoor use. When ZoneFlex Outdoor APs and Bridges with 5 GHz radios (ZoneFlex 7762, 7762-S, 7762-T, 7762-AC, 7762-S-AC and 7761-CM) are set to a country code where these restrictions apply, the AP or Bridge can no longer be set to an indoor-only channel and will no longer select from amongst a channel set that includes these indoor-only channels when SmartSelect or Auto Channel selection is used, unless the administrator configures the AP to allow use of these channels.

For instance, if the AP is installed in a challenging indoor environment such as a warehouse, the administrator may want to allow the AP to use an indoor-only channel. These channels can be enabled for use through the AP CLI or ZoneDirector Web interface by configuring Configure > System > Country Code > Channel Mode and checking “Allow indoor channels (allows ZoneFlex Outdoor APs to use channels regulated as indoor use-only)”.

If you have a dual-band ZoneFlex Indoor AP functioning as a RAP with dual-band ZoneFlex Outdoor APs functioning as MAPs, the mesh backhaul link must initially use a channel that is not restricted to indoor-only use. Your ZoneFlex Outdoor MAPs may fail to join if the mesh backhaul link is using a restricted indoor-only channel.

7 Interoperability Information

ZoneDirector and ZoneFlex APs use standard protocols to interoperate with third-party Wi-Fi devices. Ruckus Wireless qualifies its functionality on the most common clients.