

*Ruckus Wireless ZoneFlex 9.0
(FlexMaster, ZoneDirector and ZoneFlex
Access Points and Bridges)
Release Notes*

January 28, 2010



Contents

1	Introduction	4
2	What's New in This Release	4
3	Supported Platforms.....	4
4	Enhancements and Resolved Issues in This Release	5
4.1	FlexMaster	5
4.2	ZoneDirector	5
4.3	ZoneFlex Access Points.....	6
4.4	ZoneFlex Wireless Bridge	6
5	Caveats, Limitations and Known Issues	7
5.1	FlexMaster	7
	System Requirements	7
	Installation.....	7
	Licenses.....	7
	Network Environment/Firewall	7
	TR069 Limitations.....	8
	Web Interface	8
	Device View	9
	Provisioning	9
	User Security	11
	FlexMaster Server Time	11
	AP-related Issues	11
	Reports	12
	SpeedFlex.....	12
	VLANs.....	12
	Other Caveats	13
5.2	ZoneDirector	13
	General	13
	AP Upgrade	15
	Web Interface	15
	CLI	16
	SNMP.....	16
	VLAN, Dynamic VLAN, and Tunnel Mode	16
	Smart Redundancy.....	17
	Smart Mesh Networking	18

*Ruckus Wireless ZoneFlex 9.0
(FlexMaster, ZoneDirector and ZoneFlex Access Points and Bridges)
Release Notes*

WLAN Service Schedule	18
Band Steering	18
Dynamic PSKs.....	18
Guest Access	19
Captive Portal	20
WISPr (Hotspot Service)	20
Voice	20
Real-Time Monitoring	20
Email Alarm	20
Dual Band APs and Mesh Networking in Indonesia.....	21
AeroScout.....	21
Bradford Network Access Control (NAC) Server	21
5.3 ZoneFlex Access Points.....	21
Interoperability with PoE Switches.....	22
5.4 ZoneFlex Wireless Bridges	23
General	23
Dynamic Channel Selection and Channel Optimizer.....	24
6 Upgrading to This Version.....	26
6.1 Changed Behavior.....	26
6.2 ZoneDirector	26
6.3 ZoneFlex Access Points.....	27
6.4 ZoneFlex Bridge	27
Upgrading an Existing PtP Network to a PtMP Network	27
7 Interoperability Information.....	27

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 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 deployment in larger enterprise environments. 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 9.0.

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>

3 Supported Platforms

Release 9.0 supports the following platforms:

- FlexMaster 9.0.0.0.157 supports the ZoneDirector and ZoneFlex AP models listed below. FlexMaster 9.0 also supports the Ruckus Wireless MediaFlex product line (not included in Release 9.0).
- ZoneDirector 1000 version 9.0.0.0.80
- ZoneDirector 3000 version 9.0.0.0.80
- ZoneFlex 2741 802.11g Outdoor Access Point build 9.0.0.0.80 (both main and backup)
- ZoneFlex 2942 802.11g Access Point build 9.0.0.0.80 (both main and backup)
- ZoneFlex 7343 2.4GHz 802.11n Smart Wi-Fi Access Point build 9.0.0.0.80 (both main and backup)
- ZoneFlex 7363 Dual Band 802.11n Smart Wi-Fi Access Point build 9.0.0.0.80 (both main and backup)
- ZoneFlex 7762 Dual-band 802.11n Outdoor Access Point build 9.0.0.0.80 (both main and backup)
- ZoneFlex 7942 802.11n Access Point build 9.0.0.0.80 (both main and backup)
- ZoneFlex 7962 Dual-band 802.11n Access Point build 9.0.0.0.80 (both main and backup)
- ZoneFlex 7731 802.11n Wireless Bridge build 9.0.1.0.7 (both main and backup)

Starting from ZoneDirector Release 8.2, ZoneDirector does not support the ZoneFlex 2925 Access Point. Therefore, the 2925 cannot be upgraded to Release 9.0. Moreover, upgrading a ZoneDirector device (that is managing a 2925 AP) to this release will result in the 2925 AP becoming unmanaged and unable to rejoin ZoneDirector. For information on possible workarounds, refer to 5.2.14.

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

- 4.1.1 AP device tags now appear on the **Inventory > Device Registration** page. (ID 11148)
- 4.1.2 Incorrect display order of AP or ZoneDirector views when sorted on Dashboard has been resolved. (ID 11603)
- 4.1.3 If a certain device view is used to create an autoconfiguration task, the administrator is now able to delete that device view and the autoconfiguration task that was created. (ID 9730)
- 4.1.4 When the FlexMaster database is backed up, the timestamp on the backup file is now synchronized with the time that appears on the upper-right corner of FlexMaster Web interface. (ID 11453)

4.2 ZoneDirector

- 4.2.1 The NAS-IDs that ZoneDirector sends out in RADIUS authorization and accounting packets are now the same (ID 12530).
- 4.2.2 Rate Limiting is now supported in tunnel mode.
- 4.2.3 ZoneDirector now supports hierarchical LDAP server topology. (ID 9559)
- 4.2.4 Resolved that for Active Directory, if a group is set as a "Primary Group", ZoneDirector is now able to determine whether a client is a member of that group or not. (ID 9137)
- 4.2.5 Connecting APs via a separate wired network segment to a mesh AP is now supported.
This feature is referred to as *Hybrid Mesh*. See the *ZoneDirector User Guide* for information on this feature.
- 4.2.6 ZoneFlex 7962 APs now support DFS channels for US country code.
Because not all clients and dual-band APs use all DFS channels, interoperability for clients or for meshing between different AP models may be reduced if the AP is set to one of the DFS channels. When ZoneDirector is set to the US Country Code, ZoneDirector provides different options for the network to automatically select channels from among different sets of channels, depending on whether certain clients or meshing between different AP models is necessary. See the User Guide, Configuring System Settings chapter, Channel Optimization section for more information on the different options. The default setting is Optimize for Compatibility.
- 4.2.7 Resolved an issue with Smart Redundancy causing numerous "lost connection to peer" events to occur in the Events/Activities log (ID 15955).
- 4.2.8 Resolved an issue with APs behind a NAT router occasionally failing to connect to ZoneDirector (ID 16147).

- 4.2.9 Resolved an issue with RADIUS accounting inaccuracies when counting station statistics over 4GB (ID 16284 and 16299).
- 4.2.10 Resolved an issue where ZoneDirector incorrectly displayed the old IP address rather than the new one when a management IP address was enabled (ID 15247).
- 4.2.11 Resolved an Active Directory issue that occurred when a user name begins with "0" (zero). Note that ZoneDirector still does not support user names beginning with 0 when using the internal database (ID 16445).
- 4.2.12 RADIUS NAS-IP now correctly uses the ZoneDirector's IP address instead of a broadcast IP address for authentication (ID 16098).
- 4.2.13 Improved resiliency of ZoneDirector's handling of frequent Mesh topology changes (ID 16739).
- 4.2.14 Resolved an issue where Mesh APs were not downloading configuration from ZoneDirector correctly (ID 16762).
- 4.2.15 Resolved an issue with importing CSV files in Mac format for use in Guest Pass and Dynamic PSK batch generation (ID 16770).
- 4.2.16 Resolved an issue with frequent "heartbeat lost" messages after failover to standby ZoneDirector (ID 16776)
- 4.2.17 Improved association process for Apple iPad clients (ID 16199).
- 4.2.18 Added visibility into client TX rates in ZoneDirector CLI and Web interface (ID 15962) .

In the Web interface, the TX value is located under **Monitor > Currently Active Clients > [client detail view]**
- 4.2.19 If the Setup Wizard is used to set the Country Code, the APs now properly allow use of DFS channels. This bug did not apply to US country code (ID 15806 and 16179).

4.3 ZoneFlex Access Points

- 4.3.1 Access points no longer need to be rebooted after changing WLAN priority. Resolved issue where APs continuously reported "Assertion failed" and disconnected after changing WLAN priority (ID 16204).
- 4.3.2 Resolved an issue with standalone access points failing to auto-upgrade and autoconfigure with customized firmware through TFTP (ID 16319 and 16367).

4.4 ZoneFlex Wireless Bridge

- 4.4.1 Resolved an issue with the CLI command to clear the channel blacklist (`set blacklist wifi0 clear`) failing to complete when many channels were included in the blacklist (ID 15248).
- 4.4.2 Added support for querying external antenna for 5GHz and setting external antenna gain. Default is 5dBi external antenna gain (ID 16039).
- 4.4.3 Improved handling of noise floor values (ID 16085).

5 Caveats, Limitations and Known Issues

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

5.1 FlexMaster

System Requirements

- 5.1.1 RedHat Linux 5 required by memory optimization feature

Ruckus Wireless recommends installing FlexMaster on Red Hat Enterprise Linux 5, especially if the administrator intends to enable the memory optimization feature in FlexMaster. Earlier versions of Linux do not support the memory optimization feature.

Installation

- 5.1.2 To enable a device to be managed by FlexMaster, its firmware image must support TR069.
- 5.1.3 Ruckus Wireless recommends installing FlexMaster on a Red Hat Enterprise 5 server, although it supports both versions 4 and 5.

Licenses

- 5.1.4 A FlexMaster installation provides 100 license seats by default. This means that the FlexMaster server can support up to 100 APs without requiring additional licenses.
- 5.1.5 If the maximum number of devices that the FlexMaster license supports has been reached, an alert message appears on the Dashboard and on the **Administer > License** page.
- 5.1.6 If FlexMaster is also used to manage ZoneDirector, note that the number of license seats that ZoneDirector will consume depends on the maximum number of APs that it can support. ZoneDirector 3500 (which supports up to 500 APs), for example, will consume 500 license seats.

Network Environment/Firewall

- 5.1.7 If a device is behind a NAT server, FlexMaster will be unable to communicate with it using TCP or UDP.
- 5.1.8 FlexMaster is unable to open the Web User Interface for devices that are behind a NAT server. To enable FlexMaster to open a Web User Interface for a device behind a NAT server, the administrator must edit the device details and configure the device's *Device Web Port Number Mapping* settings.
- 5.1.9 FlexMaster will only be able to communicate with the device behind a NAT server at inform intervals, at which time the device will send an inform packet to FlexMaster via HTTP and HTTPS.
- 5.1.10 The shortest allowed periodic inform interval is one minute, the longest is four weeks.


- 5.1.11 If the ZoneDirector or Access Point is behind a NAT server, port forwarding must be configured on FlexMaster and the NAT server to enable FlexMaster to communicate with the device behind the NAT server.
- 5.1.12 SpeedFlex does not work if the target device is behind a NAT server.

TR069 Limitations

- 5.1.13 FlexMaster tasks are not implemented in real time. For example, if the managed device is behind a NAT server, the administrator may need to wait for the device to communicate successfully with FlexMaster before the task can be executed.
- 5.1.14 If a device loses communication with FlexMaster while it is being provisioned with a task, FlexMaster will mark the task as expired if the device does not re-establish communication within three inform intervals (see exception below).
- 5.1.15 If the task is 'Firmware Upgrade' or 'Reboot', FlexMaster will mark the task as expired if the AP reboots and does not re-establish communication within 60 minutes.

Web Interface

- 5.1.16 FlexMaster release 9.0 and later support the following Web browsers:
 - Firefox 3.0, 3.5, and 3.6
 - Internet Explorer 7 and 8
 - Safari 5.0
 - Chrome 5.0 and 6.0

FlexMaster does not support Internet Explorer 6.0. Some Web interface elements may not display correctly in this browser.
- 5.1.17 To show the most up-to-date information from the managed device or FlexMaster database on the Web interface, click the  (refresh) button.
- 5.1.18 If DHCP Option 43 is configured with a FlexMaster server URL that is different from the FM configuration template, the managed device will use the FlexMaster server URL that has been set in DHCP Option 43.
- 5.1.19 The Client Association and Connectivity charts may show zero clients on the hour (for example, at exactly 4:00 PM). This is an indicator that FlexMaster is in the process of retrieving data from its database. This issue is typically resolved after a few minutes (at the next refresh interval). (ID 11552)
- 5.1.20 Group administrators may see an incorrect number of ZoneDirector backup configuration files. For example, a group administrator may see only five backup files when "Number of files" shows "6" on the *Backup ZD Configurations* page. This is because group administrators can only see backup files that they created, but "Number of files" on the Backup ZD Configuration page shows the *total number of backup files*, including those that have been created by the Administrator. (ID 11631)
- 5.1.21 If the administrator types a single English character in the search box on the Event page, all serial numbers will be highlighted, in addition to all events that contain that English character. (ID 11659)

- 5.1.22 Certificate error prevents administrator from accessing the AP Web interface (after connecting to the FlexMaster Web interface via HTTPS) (ID 8074)

If the administrator uses Firefox 3.0.5 (or later) to connect to the FlexMaster Web interface via HTTPS, and then connects to a standalone AP's Web interface, a certificate error occurs and prevents access.

Workaround: Go to **Tools > Options > Advanced**. Click **View Certificates**. Under *Certificate Name*, look for and delete all certificates named "Ruckus Wireless Inc".

- 5.1.23 When setting the time to run a task using the date/time picker, the administrator must set the hour, minute, and AM/PM settings separately. This applies to all pages that have report filtering options. (ID 8148)
- 5.1.24 The location of the date on the Association State graph is inconsistent with other graphs. (ID 14238)
- 5.1.25 Loading the **Monitor > Events** page shows "First TR-069 client registration" events, even though no filters have been configured in the Event Search Criteria section. (ID 14704)
- 5.1.26 The *AP Traffic - TX* and *AP Traffic - RX* widgets on the Dashboard may show incorrect information if failover (from Active ZD to Standby ZD) occurs on the ZoneDirector device to which APs are reporting. See *Smart Redundancy* in the ZoneDirector section of this document. (ID 15289)

Device View

- 5.1.27 The information displayed in the ZoneDirector Device View of the Dashboard is retrieved from connected ZoneDirector devices every five minutes; it may not be real-time information.
- 5.1.28 If any setting is changed from the AP Web interface, this change will not be reflected on the FlexMaster Web interface in real-time. The administrator may need to click the refresh button on the FlexMaster Web interface to see this change.
- 5.1.29 Configuring the Country Code and Channel settings must be done separately. If the administrator configures them at the same time, only the Country Code settings will be applied.

Workaround: Set the Country Code first, and then save the settings. Then, set the Channel settings, and then save the settings again.

Provisioning

- 5.1.30 A ZoneDirector backup file that has been used to create a ZoneDirector configuration task cannot be deleted. (ID 11411)
- 5.1.31 Upgrading a ZoneDirector device that is managing at least one ZoneFlex 2925 Access Point will fail. This is because 2925 is only supported in software version 8.1 or earlier. FlexMaster 9.0 can continue managing 2925 APs directly if the APs are running on release 8.1 or earlier. (ID 10878)

To upgrade the ZoneDirector device, do one of the following:

- Log into ZoneDirector Web interface, and upgrade the software from there.
- Reset ZoneDirector to factory default settings, and then disable auto approval. Then, upgrade ZoneDirector from the FlexMaster Web interface. After ZoneDirector is upgraded successfully, enable auto approval.

- 5.1.32 Provisioning a template that can temporarily turn off all remote management access (HTTP, HTTPS, SSH, and Telnet) will return the failure message “setAccess returned error:9001name=SSHAccess”. (ID 8544)

The AP will ensure that at least one remote management option is enabled. Because FlexMaster executes remote management enable/disable in the order of HTTP, HTTPS, SSH, and Telnet, this error message indicates that AP may be temporarily locked out of remote management.

Workaround: Provision two separate configuration templates. Configure the first template to enable all of the remote management options, and the second template to disable those remote management options that are not needed.

- 5.1.33 FlexMaster is unable to distinguish between far-end and near-end 7731 bridges if the bridge topology is modified after a task is provisioned. (ID 12889)

FlexMaster applies provisioning tasks to the 7731 bridges in the following order of priority:

1. Far-end non-root bridge
2. Far-end root bridge
3. Near-end non-root bridge
4. Near-end root bridge

Provisioning tasks to far-end bridges (those with the least number of connections within the topology) first minimizes the chances of a downtime in case errors occur during the provisioning process. However, if the topology is modified (for example, if a far-end bridge becomes a near-end bridge) after a task is provisioned, FlexMaster may be unable to detect the topology change right away and may apply the task first to the now near-end bridge.

Consider the following bridge topology:

```
FM Server -- Ethernet -- BR1 (Non-Root) -- Wireless -- BR2 (Root)
                                         -- Wireless -- BR3 (Non-Root)
```

If the administrator unplugs the Ethernet cable from Bridge 1 (BR1), and then plugs it into Bridge 3 (BR3), the bridge topology will change automatically to:

```
FM Server -- Ethernet -- BR3 (Non-Root) -- Wireless -- BR2 (Root)
                                         -- Wireless -- BR1 (Non-Root)
```

FlexMaster will not detect this topology change and will provision the task to BR3 first. If an error occurs during provisioning to BR3 and BR3 crashes, FlexMaster will no longer be able to provision to BR1 and BR2, since BR3 connects FlexMaster to these far-end bridges.

Workaround: If the bridge topology is modified after a task is provisioned, Ruckus Wireless recommends that all 7731 bridges that are part of the topology be rebooted to update FlexMaster about the new bridge topology.

- 5.1.34 MediaFlex 2825 AP does not support the “Clear persistent file” settings in FlexMaster. If MediaFlex 2825 AP is provisioned with a configuration upgrade task that includes “Clear persistent file” settings, the task will be successful, but the persistent file will not be cleared. (ID 8370)
- 5.1.35 MediaFlex 2825 templates can be provisioned to APs with different customer profiles, even if these profiles contain different settings.
- 5.1.36 FlexMaster currently allows duplicate Auto Configuration rule names. Ruckus Wireless strongly recommends assigning unique and descriptive rule names. (ID 13071)
- 5.1.37 If an administrator creates a template and then uses that template to provision a task, changing the template settings later on will not affect tasks that have already been provisioned. The new template settings will only be applied to new tasks.

User Security

- 5.1.38 FlexMaster allows multiple instances of the same user account to be logged in simultaneously.
- 5.1.39 Some pages of the FlexMaster Web interface that use AJAX query the status from the FlexMaster server periodically. If a user navigates to a page that uses AJAX and stays there, the HTTP session will not time out.

FlexMaster Server Time

- 5.1.40 If the FlexMaster server time is not synchronized with the local time, scheduled tasks may not execute when expected. To ensure that scheduled tasks run exactly when scheduled, synchronize the time on the FlexMaster server with the local time. The administrator can do this by installing an NTP client on the FlexMaster server. (ID 11550)

AP-related Issues

- 5.1.41 If a wireless client roams between managed APs, the traffic information that FlexMaster receives for that client may be inaccurate.
- 5.1.42 Provisioning a template that contains both the country code and channel width settings to a ZoneFlex 7731 Bridge will fail. The country code and channel settings must be configured separately because wireless channels are dependent on the country code settings. (ID 14550)
- 5.1.43 Although ZoneFlex 2925 APs cannot be upgraded to this release, FlexMaster 9.0 can continue managing 2925 APs directly if they are running on release 8.1 or earlier.
- 5.1.44 After importing a VeriSign certificate into FlexMaster, the FlexMaster server must be restarted.
- 5.1.45 MediaFlex 2825 and MediaFlex 7811 do not support SpeedFlex.
- 5.1.46 MediaFlex 2825 backup image can only support bare image version 4.2.0.0.6 or later.
- 5.1.47 L2TP tunneling is not supported on ZoneFlex 7343/7363/7762/7942/7962 Access Point and ZoneFlex 7731 Wireless Bridge.
- 5.1.48 A 2942 VLAN template cannot be provisioned to APs that are running software version 5.1.

- 5.1.49 Clearing persistent configuration using a factory reset template is supported only on APs that are running software version 8.0 and later (except MediaFlex 2825 and 7811)
- 5.1.50 If a template is provisioned to a ZoneDirector device or an Access Point and the template is edited after it was provisioned, the change will not be applied to the task that was provisioned previously.
- 5.1.51 If an automatic monthly report is created and the date that was set is invalid (for example, FlexMaster was configured to send the report every 31st and the current month only has 30 days), then report will be sent out on the last day of the month.
- 5.1.52 Provisioning a restricted wireless channel to an AP (using a configuration template) changes the AP's wireless mode to SmartSelect automatically (ID 8358).

For example, if the AP's country code is set to US and the administrator creates a configuration template that changes the wireless channel to 13 (a restricted channel in the US), the AP's wireless mode will change to SmartSelect when it is provisioned.
- 5.1.53 MediaFlex 7811 does not support SNMP management.
- 5.1.54 Enabling rate limiting on all eight WLANs of ZoneFlex 2925 generates high CPU usage on the AP and causes it to stop functioning.
- 5.1.55 In a two-tier environment, the AP's downtime information may be incorrect if Periodic Inform Interval is set to 1 Hour or longer.

Reports

- 5.1.56 The filter function may not work correctly when applied to client association or disassociation event reports. (ID 13603)
- 5.1.57 Automatic reports are sometimes received 30 minutes later than scheduled. This can occur if temporary network or mail server issues prevent FlexMaster from sending the report as scheduled. If such issues occur, FlexMaster will attempt to resend the report after 30 minutes. (ID 15241)

SpeedFlex

- 5.1.58 SpeedFlex tests cannot be completed successfully if the source or target device (or both) is behind a NAT server.
- 5.1.59 SpeedFlex tests cannot be performed on wireless clients that are associated with standalone APs.
- 5.1.60 SpeedFlex tests cannot be run on MediaFlex 2825 (VF2825) and MediaFlex 7811 (VF7811) APs.

VLANs

- 5.1.61 When creating a VLAN configuration template, note that only the management VLAN is active by default. All other VLANs are inactive, even though they each have a unique VLAN ID by default. To activate one of these VLANs, either assign a wireless interface to it or configure the VLAN tagging of at least one Ethernet port.

- 5.1.62 The VLAN configuration pages on the FlexMaster Web interface and the AP Web interface are inconsistent with each other. On the FlexMaster Web interface, VLAN configuration templates can be saved and provisioned successfully even if no wireless interfaces are bound to any VLAN. On the AP Web interface, on the other hand, VLAN settings cannot be saved successfully unless at least one wireless interface is bound to a VLAN.

Other Caveats

- 5.1.63 LT2P is not supported on the ZoneFlex 7942, 7343, 7363, 7731, 7762, and 7962.
- 5.1.64 This FlexMaster release does not support provisioning a VLAN template that contains 8 VLANs to APs running Release 5.x and earlier.
- 5.1.65 Post factory persistent configuration can be cleared by a factory reset task only in Release 8.0 and later.
- 5.1.66 VF2825 and VF7811 do not support clearing persistent configuration via a factory reset task.
- 5.1.67 FlexMaster currently supports only one SMTP server, but can send email alerts to multiple email recipients.

5.2 ZoneDirector

General

5.2.1 AP License

A new AP license upgrade type is supported with release 9.0. The license increases the number of allowed APs by a particular amount (for example, by 50 APs). The previous type increased the AP license from a specific value to a specific value (for example, from 100 APs to 150 APs).

To upgrade the AP license to this new type of license, the administrator must upgrade ZoneDirector to 9.0 first, and then apply the new AP license. License types supported by 9.0 follow the format `zd_ordernumber_serialnumber_incr450ap3k.lic`.

If an AP license for 8.2 (or earlier version) has not been installed, the administrator must upgrade the AP license on ZoneDirector first, and then upgrade ZoneDirector to release 9.0. License types supported by 8.2 or earlier versions follow the format `zd_ordernumber_serialnumber_12ap.lic`.

Release 9.0 is required to increase the AP license above 250 APs. For instance, release 9.0 is needed if the ZoneDirector is to be upgraded to support from 300 to 500 APs.

- 5.2.2 RADIUS Accounting is only available on WLANs that use 802.1x Authentication. It is not available for WLANs using Open, Shared, or MAC Addresses authentication. If you enabled RADIUS Accounting with Open, Shared or MAC Address authentication WLANs using release 8.2.2, do not upgrade to this release. This feature will be added to a future release.

- 5.2.3 If an additional management IP interface is used for Web UI management, the actual IP address must still be used when configuring ZoneDirector as a client for a backend RADIUS server, FlexMaster server or in any SNMP systems. If two ZoneDirectors are deployed in a Smart Redundancy configuration, both of the actual IP addresses must be used rather than the management IP. (ID 15259)
- 5.2.4 After the AP blacklisting feature is enabled, APs that are under ZoneDirector control may not change channels from a blacklisted channel for up to 10 minutes (ID 14879).
- 5.2.5 SNMP trap is not sent when a client authentication fails or is blocked (ID 14998).
- 5.2.6 MIB browsers display the speed of all interfaces on the AP as 10Mbps (ID 12548).
- 5.2.7 Configuration changes after reboot (ID 5507)
- In some cases, if ZoneDirector is unplugged or manually rebooted immediately after configuration changes are made, the changes do not take effect after the reboot.
- Workaround: Use the *Shutdown* or *Reboot* option on the ZoneDirector Web interface to reboot ZoneDirector gracefully. This will help ensure that the configuration changes are saved even after the reboot.
- 5.2.8 10/100Mbps half-duplex mode with no auto-negotiation is unsupported on the ZoneDirector 1000 (ID 8495)
- ZoneDirector 1000 cannot be connected to a 10/100Mbps half-duplex switch when auto-negotiation is disabled.
- 5.2.9 SpeedFlex for mesh links is supported on 802.11n APs only (ID 8314)
- SpeedFlex between ZoneDirector and AP (for mesh link performance measurement) is only available for ZoneFlex 7343/7363/7762/7942/7962 (802.11n) APs.
- SpeedFlex to clients is supported through all ZoneFlex APs (802.11g and 802.11n).
- 5.2.10 SpeedFlex is unable to measure the throughput between two devices if those two devices are not on the same VLAN or the same subnet. (ID 11282)
- 5.2.11 AP may not forward multicast stream from the wireless interface to the Ethernet interface if it is connected to a switch on which IGMP snooping is enabled because the switch can filter out IGMP network packets between the AP and hosts (ID 11091)
- 5.2.12 Clients that are automatically blocked because they failed authentication too many times do not appear in the list of blocked clients. As a result, there is no way to unblock these blocked clients manually and immediately. When the configured block time period has elapsed, clients will be unblocked and they can re-attempt to connect to the wireless network. (ID 11405)
- Workaround: Go to **Configure > Services**, and locate the Intrusion Prevention section. Reduce the number of seconds in the field next to the text "Temporarily block wireless clients with repeated authentication failures for ___ second."
- 5.2.13 Acct-Interim-Interval RADIUS attribute not being honored on 802.1X WLANs (ID 13342)
- This RADIUS attribute has been tested to work correctly with Web Auth and Hotspot WLANs, but currently still assumes ZoneDirector's WLAN setting rather than the RADIUS server setting when using 802.1X WLANs.

AP Upgrade

- 5.2.14 The ZoneFlex 2925 Access Point is unsupported in this release. If ZoneDirector is upgraded to this release via the Web interface and a 2925 AP exists on the network, an alert message appears and cautions the administrator that upgrading to this release will cause 2925 APs to stop functioning. The administrator will have the option to continue or cancel the upgrade process. If the administrator decides to continue, ZoneDirector will no longer be able to manage the 2925 AP, nor will the 2925 AP be able to rejoin ZoneDirector after the upgrade.

To continue using the 2925 APs on the network, do one of the following:

- Cancel the upgrade to release 9.0 and continue using the current ZoneDirector version. 2925 APs can be managed by ZoneDirector releases up to 8.1.
- Convert the 2925 AP from a ZoneDirector-managed AP to a standalone AP. Do this by resetting the AP to factory default settings. Standalone 2925 APs are supported up to release 8.1.
- If there is a significant number of 2925 APs on the network, the administrator can provision a ZoneDirector device to manage only these 2925 APs. 2925 APs can be managed by ZoneDirector releases up to 8.1.
- If FlexMaster exists on the network, any version of FlexMaster can be used to manage 2925 APs (running on release 8.1 or earlier) directly.

Web Interface

- 5.2.15 ZoneDirector release 9.0 and later support the following Web browsers:

- Firefox 3.0, 3.5, and 3.6
- Internet Explorer 7 and 8
- Safari 5.0
- Chrome 5.0 and 6.0

- 5.2.16 Map View cannot be displayed on Opera browser because Opera uses its own java plugin.

Workaround: Use Internet Explorer, Firefox, Chrome, or Safari to access the ZoneDirector Web interface.

- 5.2.17 The semicolon character (;) is unsupported in passphrases for WPA or WPA2-PSK (ID 15741)

If WPA or WPA2-PSK is selected as the encryption method for a WLAN and the administrator sets a passphrase that contains a semicolon, users will be unable to join the WLAN successfully despite using the passphrase (with a semicolon).

Workaround: do not use a semicolon when establishing the passphrase value.

- 5.2.18 ZoneDirector incorrectly displays the value for PHY Errors and % Air Time (total/busy/RX/TX) on the **Monitor > Access Points > [AP MAC Address] > Access Point Information** as zero (ID 15716).

- 5.2.19 Dashboard Usage summary may show incorrect number of rogues (ID 15483).

Workaround: reboot ZoneDirector.

- 5.2.20 AP Noise Floor value is incorrect (ID 14337)

In **Monitor > Access Points > AP MAC Address**, the noise floor value displayed is incorrect.

- 5.2.21 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)
- 5.2.22 Channel width of the AP on the **Monitor > Access Point** page may be incorrect (ID 11803).
- 5.2.23 ZoneDirector Web interface shows ZoneFlex 7962 as using radio channel 0 (ID 8611)
On rare occasions, the **Monitor > Access Point** page shows ZoneFlex 7962 as using radio channel 0 (zero).
Workaround: Delete the AP, and then allow it to rejoin. After it rejoins, the correct channel information will appear.
- 5.2.24 If the AP event includes a description of the event, the event format is AP[description@AP's MAC address] reason, ("description" can contain up to 17 characters). If the AP event does not include a description, the event format is AP[AP's MAC Address] reason.

CLI

- 5.2.25 The RF statistics may show incorrect values after the AP reboots (ID 13340).
- 5.2.26 The CLI command `show ap all` shows all approved and unapproved APs, though no information will be provided for unapproved APs (ID 13861).

SNMP

- 5.2.27 A value is not returned for `.iso.org.dod.internet.mgmt.mib-2.interfaces` when queried (ID 15727).
- 5.2.28 The wrong OID is returned when `.SysObjectID (.1.3.6.1.2.1.1.2)` is queried (ID 15731).

VLAN, Dynamic VLAN, and Tunnel Mode

- 5.2.29 When configuring or updating the management VLAN settings, make sure that the same VLAN settings are applied on the **Configure > Access Points > Access Point Policies > Management VLAN** page, if APs exist on the same VLAN as ZoneDirector. (ID 11724)
- 5.2.30 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
- 5.2.31 Per-user VLAN segmentation depends on the user credentials configured on the RADIUS server.
- 5.2.32 If Dynamic VLAN and Tunnel Mode are both enabled and the Dynamic VLAN attributes have not been configured on the RADIUS server, the Tunnel Mode rule will override the Dynamic VLAN rule.

- 5.2.33 If Dynamic VLAN and VLAN are both enabled and the Dynamic VLAN attributes have not been configured on the RADIUS server, the VLAN rule will override the Dynamic VLAN rule.
- 5.2.34 WDS clients do not work on a ZoneDirector WLAN in tunnel mode (ID 6127)
Wireless distribution system (WDS) clients (using 4-address mode), for example, MediaFlex 7111/2111 adapters, do not work when the ZoneDirector WLAN is in tunnel mode.
- 5.2.35 Multicast video packets on tunneled WLAN
When tunnel mode is enabled on a WLAN, multicast *video* packets are blocked on that WLAN. Multicast *voice* packets, however, are allowed.

Smart Redundancy

- 5.2.36 Smart Redundancy versus Limited ZD Discovery
Smart Redundancy supports Active/Standby redundant controller deployments. Configuration and client runtime information is automatically synchronized between controllers so that in the event the Active controller becomes unavailable, the Standby controller can seamlessly take over managing the WLAN.
Limited ZD Discovery configures connected APs with the IP addresses of a Primary and Secondary ZoneDirector that the AP should connect to when reachable. Limited ZD Discovery does not provide configuration or run-time synchronization, and APs need to reboot when joining the Secondary controller to obtain the current configuration.
Ruckus recommends deploying Smart Redundancy instead of Limited ZD Discovery. If Limited ZD Discovery was enabled previously (as with using a release earlier than 9.0), Ruckus recommends disabling it under **Configure > Access Points > Access Point Policies** prior to configuring Smart Redundancy. Limited ZD Discovery can be used concurrently with Smart Redundancy. However, in that case, the Primary and Secondary ZoneDirector IP Address must be configured with the IP Addresses of both ZoneDirectors.
- 5.2.37 Certificates needed on both ZoneDirectors
If you install a certificate on ZoneDirector to eliminate the browser Security warning, you should install certificates on both ZoneDirectors to avoid seeing this warning when the system fails over to the Standby ZoneDirector. Using the Management IP address will not eliminate this requirement.
- 5.2.38 Manually initiating failover
On the Dashboard Smart Redundancy widget, when attempting to force a failover from the Active ZoneDirector to the Standby ZoneDirector by clicking on the "Failover" button in the Active ZoneDirector Web interface, do not click on the browser's "Refresh" button. Clicking on "Refresh" may cancel the task. After the failover is complete, the browser will eventually refresh itself and display that the ZoneDirector is now the Standby. Alternatively, the Dashboard on the original Standby ZoneDirector can be refreshed and the now Active status will be presented.
- 5.2.39 Dashboard layout is not synchronized across ZoneDirectors
ZoneDirector Dashboard layout – for instance, which widgets are opened, where they are positioned on the Dashboard – is not synchronized between ZoneDirector Smart Redundancy peers. If you want the Dashboard to look the same on both ZoneDirectors, manually replicate the layout on both ZoneDirectors individually.

Smart Mesh Networking

5.2.40 This release supports meshing ZoneFlex 7363, ZoneFlex 7962 and ZoneFlex 7762 APs together. (Dual-band 802.11n APs may mesh with one another.) (ID 15147).

5.2.41 Meshing between ZoneFlex 7962 and 7363/7762 APs in US country code

The ZoneFlex 7962 supports DFS channels in the US country code, while the 7363 and 7762 do not. If meshing between these APs, with the 7962 as the Root AP, the APs need to be on a channel usable by all APs. If the 7962 is set to one of the DFS channels, the 7363 and 7762 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 Root AP to a non-DFS channel (e.g. channels 149-165).

5.2.42 This release supports meshing ZoneFlex 7343 and ZoneFlex 7942 APs together. (Single-band 2.4 GHz 802.11n APs may mesh with one another.) (ID 15147).

5.2.43 If an eMesh AP is 8 hops away from the RootAP, it will join the mesh, but the information displayed may not be correct (ID 13935).

5.2.44 Smart Mesh Networking cannot be disabled.

Once Smart Mesh Networking is enabled (either via the Setup Wizard or via the Web interface) it cannot be disabled. To prevent Mesh APs from becoming orphaned, Ruckus Wireless has removed the ability to change Smart Mesh Networking on the fly.

Workaround: Restore ZoneDirector and APs to factory default settings. Alternatively, disable the smart mesh functionality on a per-AP basis.

WLAN Service Schedule

5.2.45 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.

5.2.46 If ZoneDirector is managing APs in different time zones that need the same local-time Service Schedule, create different WLANs with different Service Schedules (based on the ZoneDirector's UTC time) and apply them to different APs based on time zone. For instance, if the ZoneDirector is in Pacific Time, create WLANPT with Service Schedule M-F, 9 am – 5pm for APs located in the Pacific time zone, and create WLANET with Service Schedule M-F, 6 am – 2 pm for APs located in the Eastern time zone.

When configuring the Service Schedule, your browser will interpret the ZoneDirector's UTC time to your PC's time. For instance, if the ZoneDirector is set to the Pacific time zone, if your PC clock is set to the local Pacific Time, you will see WLANPT configured for M-F, 9 am – 5 pm. If your PC is changed to the local Eastern Time (while ZoneDirector remains on Pacific time zone; for instance, when you travel to New York), you will see WLANPT configured for M-F, 12 pm – 8 pm.

Band Steering

5.2.47 Band steering is disabled on mesh-enabled APs.

Dynamic PSKs

5.2.48 When using an Apple iPhone to connect to the ZoneDirector activation page, the Safari

browser crashes if AutoFill is enabled. This is a bug in Apple's latest Safari release for iPhone.

Workaround: Disable AutoFill in the iPhone's Safari browser settings (**Settings > Safari > AutoFill**).

- 5.2.49 When provisioning a Zero-IT/Dynamic Pre-Shared Key on Windows 7 clients over a wireless connection, users are not automatically reconnected to the secured SSID (ID 14960).

Workaround: the end user must manually disconnect from the SSID used to provision the DPSK, and connect to their secured SSID.

- 5.2.50 ZoneDirector supports dynamic PSK generation on clients running Mac 10.5 (Leopard) and 10.6 (Snow Leopard). However, only users who have the privilege to change the Mac client's wireless settings can run prov.exe (the Ruckus Wireless application that is used to generate the dynamic PSK). Moreover, any user who attempts to run prov.exe will be prompted for his password, even if he is an administrator.

- 5.2.51 If the maximum number of PSKs that ZoneDirector supports has been reached, the ZoneDirector Web interface may not be accessible after bootup, even if the Status LED shows green. This may be because one or more STAMGR sockets failed to initialize. Typically, this automatically resolves itself after five or so minutes.

The maximum number of PSKs that is supported is

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

- 5.2.52 When the maximum number of PSKs that ZoneDirector supports has been reached, the Web interface may be slower in responding to requests.

Guest Access

- 5.2.53 Accounting service option is not available for clients of Guest WLAN (ID 8825)

Workaround: If accounting for clients is required, configure normal WLAN.

- 5.2.54 ZoneDirector doesn't redirect client to a long URL (ID 13896)

If the URL that the user originally visited before being prompt to login with their guest pass is long, they may not be redirected there after successfully logging in.

Workaround: On the **Configure > Guest Access** page, set Redirection to *Redirect to the following URL* rather than *Redirect to the URL that the user intends to visit*.

- 5.2.55 Batch generated guest passes can be sorted in different orders depending on the number of guest passes entered. (ID 11495)

- 5.2.56 When the maximum number of guest passes or Dynamic PSKs (or a combination of both) has been reached on ZoneDirector 1000, ZoneDirector takes longer to boot up. (ID 10454)

- 5.2.57 In batch generation, each guest pass key is unique and is distributed on all guest WLANs, so the administrator cannot create the same guest pass on different WLANs.

Workaround: Use unique guest pass keys.

Captive Portal

5.2.58 Guest captive portal does not work when accessed via HTTPS (ID 3816)

If the guest captive portal is accessed via HTTPS before authentication, the guest user is not redirected to the authentication server.

Workaround: Try browsing to an HTTP page.

5.2.59 Web portal based authentication does not redirect the client to the Web login page if the ZoneDirector and the AP/Client are on the same subnet, but using different VLANs. (ID 11904)

Workaround: If ZoneDirector and APs need to use different VLANs, they should also be placed on different subnets.

WISPr (Hotspot Service)

5.2.60 Cross-subnet clients connection issue with WISPr

In some cases, clients that associate with an AP that is on a different IP subnet than ZoneDirector may need to connect more than once before they can reach the WISPr captive portal. This is because ZoneDirector needs to learn the client addresses first before it can redirect them to the captive portal.

Voice

5.2.61 Multicast traffic on Vocera communication badges and Vocera App on smartphones may be delayed when a receiver roams (ID 14379).

5.2.62 ZoneFlex APs may occasionally be delayed in sending Broadcast or Multicast traffic from when their DTIM interval is scheduled. Devices operating in power save mode may not receive the Broadcast or Multicast traffic, as they may no longer be awake when the traffic is finally sent (ID 14383).

5.2.63 Some soft phones (Nortel X-lite) on a client with an Intel 5300 adapter do not work on 802.11n APs (ID 14127).

Workaround: Use 11g AP or different soft phone client

Real-Time Monitoring

5.2.64 Real-Time Monitoring loads the ZoneDirector CPU and may impact performance. Ruckus recommends that you run Real-Time Monitoring for only as long as necessary to provide analytical information, and disable it otherwise.

Email Alarm

5.2.65 If the administrator is sending alarm email notifications via a Yahoo! Mail server, STARTTLS must be disabled to be able to send email notifications.

5.2.66 Popular SMTP ports for encrypted sessions include ports 587 and 465.

5.2.67 If the standard SMTP port 25 (for non-encrypted sessions) is used, both TLS and STARTTLS must be disabled to be able to send email notifications.

5.2.68 When the alarm email is first enabled, the alarm recipient may receive a flood of alarm notifications. This may cause the mail server to treat the email notifications as spam and

to temporarily block the account.

- 5.2.69 If the *Test* button is clicked, ZoneDirector will attempt to connect to the mail server for 10 seconds. If it is unable to connect to the mail server, it will stop trying and quit.
- 5.2.70 After ZoneDirector is upgraded to software version 9.0, the alarm email notification settings must be reconfigured to include the mail server IP address and port number. This will help ensure that ZoneDirector alarm recipients will continue to receive email notifications.
- 5.2.71 ZoneDirector sends email notifications for a particular alert only once, unless (1) it is a new alert of the same type but for a different device, or (2) existing alert logs are cleared.
- 5.2.72 Alarm email notification for rogue access points does not include channel information, although it is shown on the Monitor page. (ID 10740)
- 5.2.73 ZoneDirector is unable to send out email alarms when the `auth_user` is empty or in an invalid email format (ID 16633)

Dual Band APs and Mesh Networking in Indonesia

- 5.2.74 Dual band APs, such as ZoneFlex 7962, ZoneFlex 7762 and ZoneFlex 7363, can only use the 5GHz radio for mesh networking. Therefore, in countries where the 5GHz band is restricted (such as Indonesia), mesh networking on these dual band APs cannot be enabled.

AeroScout

- 5.2.75 Tag locations are not accurate if the 2.4GHz band is noisy or if the AP setup is not optimal (according to AeroScout documents).

Bradford Network Access Control (NAC) Server

- 5.2.76 Release 9.0 is not compatible with the Bradford NAC Server software version 4.1.1.192.P7. Instead, release 9.0 works with Bradford software version 4.1.1.P12. If you are upgrading ZoneDirector to release 9.0, you will also need to upgrade your Bradford NAC Server to 4.1.1.P12. Please contact Bradford for the software update.

5.3 ZoneFlex Access Points

- 5.3.1 If an AP is being managed by ZoneDirector, the administrator should not log in to the AP's Web interface or command line interface (CLI). When an AP is being managed by ZoneDirector, its Web interface is in *read-only* mode. Additionally, making configuration changes via the CLI might result in unexpected and inconsistent behavior.
- 5.3.2 Configuration of physical ports on a ZoneDirector-controlled AP
 - If VLAN tagging is configured for one or more non-tunneled WLANs on ZoneDirector, the VLAN tag will propagate to all physical ports on the access point.
 - If VLAN tagging is configured on one or more WLANs (either tunneled or non-tunneled) on ZoneDirector, the VLAN tag will propagate to the physical port on ZoneDirector.
- 5.3.3 Channels 100 to 140 unsupported by some 802.11a and 802.11a/n clients

Some 802.11a and 802.11a/n clients (such as US-based Atheros, Broadcom, and Centrino NICs) do not support radio channels 100 to 140.

5.3.4 DFS channels support

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

This will be fixed upon FCC approval in a later software release this year.

5.3.5 Video streaming and background scanning issue (ID 8571)

If there is a ZoneFlex 7363/7762/7962 AP on the network and it is being used to stream video traffic (UDP traffic), Ruckus Wireless recommends that background scanning be disabled (on the **Configure > Services** page) to improve video performance.

Similarly, if a particular WLAN will be used primarily for voice traffic and VoIP clients are expected to roam frequently between APs, disabling background scanning can improve performance (reduce latency) when roaming occurs. In this case, Ruckus recommends disabling background scanning for this specific WLAN only (from the **Configure > WLANs** page).

5.3.6 Enabling or disabling *HTTP Access* or *HTTPS Access* on the **Administration > Management** page of the AP Web interface causes the Web interface to be inaccessible for about one (1) minute. This is because the Web service is restarted immediately after a change in HTTP or HTTPS management access is applied (ID 15753).

Interoperability with PoE Switches

5.3.7 If a 10/100Mbps PoE injector is used to power a ZoneFlex 7343/7363/7942/7762/7962 AP and the injector is connected to a switch port that supports 10/100/1000Mbps, the Ethernet connection of the AP may not work. (ID 7634)

This incompatibility is caused by the link speed negotiation between the AP and the Gigabit-Ethernet port. The AP and the Gigabit-Ethernet port can support 1000Mbps connection, but the PoE injector cannot.

Workaround: Use a Gigabit-Ethernet compliant PoE injector or a 10/100/1000Mbps PoE switch instead. Alternatively, connect the 10/100Mbps PoE injector to a 10/100Mbps switch port, or configure the Gigabit-Ethernet port of the switch to use full duplex at 100Mbps.

5.3.8 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:

- 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

5.4 ZoneFlex Wireless Bridges

General

- 5.4.1 Provisioning a pair of 7731 Bridges with different SSIDs or encryption settings will undo the pairing and disconnect the Bridges from each other (ID13123).
- 5.4.2 If the country code is changed to another country, the ZoneFlex 7731 Wireless Bridge will set the channelization to 20 MHz, and will set the channel to SmartSelect. This may be different than the settings that the Bridge had under the previous country code setting.
- 5.4.3 Channels 52 to 140 are unavailable for the US country code at this time. These channels will be made available in a later release.
- 5.4.4 ZoneFlex 7731 units use "US" as the default country code, including those units that are purchased outside of the United States. If deploying the Bridges outside the United States, the correct country code must be set prior to mounting to ensure compliance with local and national regulatory requirements. Both the Root Bridge and Non-Root Bridge must be configured with the same country code; otherwise, they might not be able to communicate with each other.
- 5.4.5 When one 7731 device is set to 20MHz and its peer is set to 40MHz, the channel width used is 20MHz. However, the Web interface on both devices does not display the effective channel width; it displays the channel width with which the devices were configured (ID 13047).
- 5.4.6 When the root bridge is set to 20MHz and the non-root bridge is set to 40MHz, the non-root bridge will use the 20MHz mode. If both devices are later set to use 40MHz, the effective channel width mode will remain 20MHz. This results in significant throughput degradation, compared to devices that are correctly configured to use the 40MHz channel width mode (ID 13050).
- Workaround: To resolve this issue, simply reboot the non-root bridge. Alternatively, set the non-root bridge to 20MHz, and then change it to 40MHz.
- 5.4.7 When high traffic is being sent from the root bridge to the non-root bridge and the channel in use is manually changed from **SmartSelect** to the same channel that SmartSelect (automatically) previously selected, the connection between the root bridge and non-root bridge may be dropped. When this happens, the root bridge will flash its WLAN LED and report that the non-root bridge has been disconnected. The non-root bridge, on the other hand, will show that it is still connected to the root bridge.
- Workaround: To resolve this issue, change the channel to another one, and then change it back to the intended channel.
- 5.4.8 When running SpeedFlex from the non-root bridge side, the results page sometimes displays error or warning messages even when the SpeedFlex test has completed successfully (ID 13077).
- 5.4.9 Dot1p packets go to the wrong queue (ID 15229)
- Dot1p packets classified into the background queue are not displayed in the command `get mqstats wlanx all` while they are updated properly in the proc file `"/proc/media/ifs/eth0/qos"`
- Workaround: none
- 5.4.10 Non-root bridge Web UI fails to display IP address of root bridge after reboot (ID 15249)

After both the root and non-root bridges are rebooted, the NRB occasionally fails to display the proper IP address of the root bridge until SpeedFlex is run from the RB.

Workaround: run Speed Flex from the peer's Web UI.

- 5.4.11 Changing QoS values (ToS and Dot1p values) in one action does not work. (ID 15162)
The Web UI does not allow users to exchange values between the queues in one action.

Workaround: remove the values from the lower queues, apply the action (press Submit), then set the values to the top queue, and apply the action again.

- 5.4.12 Packets classified by heuristics are not updated on the QoS Status page. (ID 15227)

While the packets classified by heuristic algorithm are displayed using the command `get mqstats wlanx`, they are not updated in the proc file `"/proc/media/ifs/eth0/qos"`.

Workaround: none

- 5.4.13 CLI: `rkscli` quits unexpectedly when deleting a line from beginning of the line. (ID 15265)

The SSH session is terminated unexpectedly when removing a line using the DEL key from the beginning of the line.

Workaround: none

Dynamic Channel Selection and Channel Optimizer

- 5.4.14 Dynamic Channel Selection does not work properly on India 10MHz (ID 15801)

When the devices are set to country code India and 10MHz channel width, after their Channel Optimizer databases have been built, the RFM logic sometimes does not work properly due to incorrectly mapped channel indices.

Workaround: none

- 5.4.15 Country code Argentina doesn't support 40Mhz but it can be set to 40MHz in the provisioning wizard (13287)

Workaround: select 20MHz channel width when setting to Argentina in the provisioning wizard, or set to 20MHz after the device is provisioned and boots up.

- 5.4.16 After the external antenna is enabled (using the command: `set extant wifi0 enable`), users can set its gain by using the command `set extantgain` from the command line interface. (ID 15794)

- Syntax: `set extantgain <wifi_device> <gain_in_dBi>` (`wifi_device` is `wifi0` for ZF7731).
- The granularity of the gain is from 0 to 90 dBi.
- The default value is 14 dBi. It should be 22dBi.
- Once the gain of the external antenna is set, the device will adjust the transmit power at the IR to comply with the current regulatory domain.
- However, if the gain of the external antenna exceeds the allowed limit and this value is configured in the device, it always adjusts to 1 dBm no matter how high the gain is.

- 5.4.17 The Dynamic Channel Selection feature relies on the channel list created by the Channel Optimizer Process, which is automatically launched right after the Aiming process is run

on the root bridge the first time after resetting to factory defaults.

- 5.4.18 Since the Channel Optimizer database is crucial to the operation of the Dynamic Channel Selection process, the Channel Optimizer process must be run at least once immediately after upgrading the devices' firmware from 8.2 to 9.0.
- 5.4.19 If the Channel Optimizer performance data is not present or corrupted, the Dynamic Channel Selection process cannot move to a new channel when the current channel experiences performance issues.
- 5.4.20 If the Channel Optimizer database is not present on the root bridge, a warning message is displayed next to the link reminding users to activate it.
- 5.4.21 Ensure that the IP addresses of all the ZF7731 devices in a system are assigned properly. If for any reason one device cannot detect the IP address of its peer(s), Channel Optimizer will not run successfully.
- 5.4.22 Ruckus recommends re-running the Channel Optimizer process any time that the country code or channelization of the root bridge is changed. Otherwise, the available channel list may not match the information available to the Channel Optimizer, and therefore Dynamic Channel Selection may not function properly. (ID 15242)
- Workaround: rerun Channel Optimizer after the country code or channel width are changed.
- 5.4.23 Web UI fails to update display of current channel after running Channel Optimizer (ID 15822)
- The Web interface sometimes fails to display the channel chosen by Channel Optimizer as the channel currently in use.
- Workaround: refresh Web page until the display is updated.
- 5.4.24 Running Channel Optimizer many times in succession may cause process to hang (ID 15887)
- Workaround: reboot the root bridge if you encounter this issue.
- 5.4.25 Channel Optimizer errors not reported in Web UI (ID 14225)
- When Channel Optimizer fails to initiate for any reason, the error is not reported in the Web UI, though messages will appear in logs.
- Workaround: none
- 5.4.26 Dynamic channel selection does not work well with DFS (ID 15416)
- The original issue happened when RFM selects a channel that is blocked by DFS. It has been fixed but a minor issue still exists. When the DFS is idling a channel, a short moment after that RFM detects interference on it and changes to a non-DFS channel. However, DFS is still idling the new channel.
- Workaround: none.

6 Upgrading to This Version

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

The ZoneFlex 2925 AP is not supported in this release and, therefore, cannot be upgraded.

6.1 Changed Behavior

Between releases prior-to-8.2 and releases 8.2-and-later: (Applies to all Roles except the Default Role) If a Role is allowed to create guest passes (by selecting the *Allow guest pass generation* check box in **Configure > Roles**), the administrator must also allow that Role to access at least one guest WLAN (under the Allow All WLANs section). Otherwise, users that are assigned this role will be unable to generate guest passes. (ID 12607)

Between release 8.2.2 and release 9.0: RADIUS Accounting is not available for WLANs using Open, Shared, or MAC Addresses authentication. If you enabled RADIUS Accounting with Open, Shared or MAC Address authentication WLANs using release 8.2.2, do not upgrade to release 9.0. This feature has been added to release 9.1.

Between releases 9.0.0.0.69 and 9.0.0.0.80: In Australia, channels 120, 124 and 128 are restricted weather band channels and are no longer used by access points when the country code is set to Australia.

6.2 ZoneDirector

- ZoneFlex 2925 APs cannot be upgraded to this release and, therefore, cannot be managed by ZoneDirector running on release 9.0. To continue using the 2925 APs on the network, do one of the following:
 - Cancel the upgrade to release 9.0 and continue using the current ZoneDirector version. 2925 APs can be managed by ZoneDirector releases up to 8.1.
 - Convert the 2925 AP from a ZoneDirector-managed AP to a standalone AP. Do this by resetting the AP to factory default settings. Standalone 2925 APs are supported up to release 8.1.
 - If there is a significant number of 2925 APs on the network, the administrator can provision a ZoneDirector device to manage only these 2925 APs. 2925 APs can be managed by ZoneDirector releases up to 8.1.
 - If FlexMaster exists on the network, any version of FlexMaster can be used to manage 2925 APs (running on release 8.1 or earlier) directly.
- Only ZoneDirector 1000 and ZoneDirector 3000 with firmware versions 8.1 and 8.2 can be upgraded to this release. Upgrading from any other firmware versions might result in loss of configuration settings. ZoneDirector 1000 devices that are using firmware version 3.0 must be upgraded to 6.0 before they can be upgraded to 7.1.
- After upgrading to ZoneDirector version 9.0, clear the Web browser cache. This will ensure that the ZoneDirector Web interface shows all the changes and enhancements that were implemented in version 9.0.
- When upgrading ZoneDirector 1000 to 9.0, 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.

6.3 ZoneFlex Access Points

- ZoneFlex 2942, 7942, 7762, 7962 units running on version 8.1 and 8.2 can be upgraded to this version
- ZoneFlex 7343 and 7363 Access Points running on version 8.2 can be upgraded to this version.

6.4 ZoneFlex Bridge

- ZoneFlex 7731 units running on version 8.2 can be upgraded to this version.

Upgrading an Existing PtP Network to a PtMP Network

Perform the following procedure to upgrade an existing point-to-point network to a point-to-multipoint network:

- Provision an additional non-root bridge device:
 - If the device does not have the 9.0 FCS build, follow the instructions in the User Guide to upgrade the firmware to the latest 9.0 FCS build.
 - Reset the device to factory defaults.
 - Use the instructions in the User Guide to provision the device either by using a local data file exported from the root bridge or running the provisioning wizard.
- Mount the new non-root bridge to its location.
- Run aiming from the new device. Adjust its orientation to get the best performance while leaving the existing devices fixed.
- Repeat the above steps for any additional non-root bridges.
- Make sure all the non-root bridge devices are within a 30 degree viewing angle from the root bridge for best performance.

7 Interoperability Information

ZoneDirector 1000/3000 and ZoneFlex APs use standard protocols to interoperate with third-party Wi-Fi devices. Ruckus Wireless qualifies its functionality on the most common clients.