

# *Ruckus Wireless ZoneFlex 8.2.2 (ZoneDirector and ZoneFlex Access Points) Release Notes*

September 27, 2010



# Contents

1	Introduction .....	3
2	What's New in This Release.....	3
3	Supported Platforms.....	3
4	Enhancements and Resolved Issues in This Maintenance Release .....	4
4.1	ZoneDirector .....	4
4.2	ZoneFlex Access Points.....	4
5	Caveats, Limitations and Known Issues .....	5
5.1	ZoneDirector .....	5
	General .....	5
	VLAN, Dynamic VLAN, and Tunnel Mode .....	7
	AP Upgrade .....	8
	Web Interface.....	8
	SNMP .....	8
	AeroScout .....	8
	Batch Generation of Dynamic PSKs.....	9
	Batch Generation of Guest Passes .....	9
	Dynamic PSK for Mac Clients .....	9
	Band Steering .....	9
	Email Alarm.....	9
	Dual Band APs and Mesh Networking in Indonesia.....	10
	Event Format.....	10
	Smart Mesh Networking .....	10
	WISPr (Hotspot Service) .....	11
	Alarm Notification .....	11
	Voice .....	11
	ZeroIT .....	11
5.2	ZoneFlex Access Points.....	12
	General .....	12
	ZoneFlex Access Points.....	12
	Interoperability with PoE Switches.....	13
6	Upgrading to This Version .....	13
	Changed Behavior.....	13
	ZoneDirector.....	14
7	Interoperability Information .....	14

## 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 hotspot operators. ZoneDirector 3000, on the other hand, supports up to 250 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, on a global scale.

This document provides release information on ZoneDirector, supported ZoneFlex platforms, known issues, caveats, workarounds, upgrades, and interoperability information for version 8.2.2.

## 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 8.2.2 supports the following platforms:

- ZoneDirector 1000 version 8.2.2.0.7
- ZoneDirector 3000 version 8.2.2.0.7
- ZoneFlex 2741 802.11g Outdoor Access Point build 8.2.2.0.7 (both main and backup)
- ZoneFlex 2942 802.11g Access Point build 8.2.2.0.7 (both main and backup)
- ZoneFlex 7343 2.4GHz 802.11n Smart Wi-Fi Access Point build 8.2.2.0.7 (both main and backup)
- ZoneFlex 7363 Dual Band 802.11n Smart Wi-Fi Access Point build 8.2.2.0.7 (both main and backup)
- ZoneFlex 7762 Dual-band 802.11n Outdoor Access Point build 8.2.2.0.7 (both main and backup)
- ZoneFlex 7942 802.11n Access Point build 8.2.2.0.7 (both main and backup)
- ZoneFlex 7962 Dual-band 802.11n Access Point build 8.2.2.0.7 (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 8.2.2.0.7. 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 5.1.26.

## **4 Enhancements and Resolved Issues in This Maintenance Release**

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

### **4.1 ZoneDirector**

- 4.1.1 RADIUS Accounting can now be enabled on WLANs that use Open, Shared, or MAC Addresses for authentication (ID 8825, 14019).
- 4.1.2 The RADIUS Accounting attribute Acct-Multi-Session-ID is now used in accounting messages. This attribute links together multiple sessions for a single end user. It identifies accounting records as belonging to a single end user when the client roams from one AP to another (ID 12767).
- 4.1.3 Resolved that RADIUS Accounting messages did not use the same NAS Identifier as used for the authentication, causing accounting messages to be rejected by the RADIUS server with an error of "invalid account detail" (ID 12530).
- 4.1.4 Resolved that user roles returned by an external RADIUS server after the user successfully authenticated using 802.1x were not enforced. Users can only associate to SSIDs permitted by use policies (ID 12665).
- 4.1.5 Several fixes were made to increase the stability of ZoneDirector, improving user connectivity issues (ID 13749, 13763, 14523, 14846).
- 4.1.6 Resolved that ZoneDirector rebooted when the APs it was managing encountered and reported frequent radar activity, as in radar-dense environments such as near airports or harbors (ID 15730).
- 4.1.7 Resolved some broadcast packets, such as ARP request, from a Mesh AP to ZoneDirector got dropped, causing ping failures (ID 15519).
- 4.1.8 Resolved that messages weren't being sent to the syslog server when it's IP address fully contained ZoneDirector's IP address string (ID 15326).
- 4.1.9 Resolved that ZoneDirector displayed an incorrect "Disconnect Time" in the Monitor > Access Points > [AP MAC Address] > Mesh-related Information > Uplink History table (ID 15448).
- 4.1.10 Corrected a display error in certain Dashboard widgets that resulted in misaligned buttons (ID 13559).

### **4.2 ZoneFlex Access Points**

- 4.2.1 Multiple administrators can now be logged into the AP WebUI at the same time from different consoles (ID 12042).
- 4.2.2 Improved the resiliency of APs to low-memory conditions, which could cause an AP to crash and reboot (ID 14159).

- 4.2.3 Improved the APs ability to handle certain conditions that could prevent the AP from allowing client connections or that lead the AP to cease broadcasting SSIDs. These errors were noted in syslog as “user.warn kernel: Failed to alloc mq node” or “MLME-REPLAYFAILURE” (ID 13043, 13771, 13885, 14895).
- 4.2.4 Resolved that Mesh APs were unreachable through a Ping test, even though the APs were still connected to the mesh, when the connection to a device on their Ethernet port (such as a camera) was disrupted or flapped (ID 12719).
- 4.2.5 Access points will no longer send out a gratuitous ARP messages incorrectly using 255.255.255.255 as the source IP address. This happened when a WLAN is configured with a VLAN. (ID 14979)
- 4.2.6 When an AP has not received an IP Address (either through an external DHCP server or self-assigned), we no longer send gratuitous ARP messages incorrectly using 255.255.255.255 as the source IP address (ID 14979).
- 4.2.7 Enhanced the mesh uplink selection algorithm to increase the stability of the mesh (ID 15582).
- 4.2.8 Resolved that that 2<sup>nd</sup>, 3<sup>rd</sup> (and etc) Mesh APs could not connect to a 1<sup>st</sup> hop MAP when a DFS channel was used for the backhaul (ID 15439).

## 5 Caveats, Limitations and Known Issues

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

### 5.1 ZoneDirector

#### General

- 5.1.1 The RADIUS Accounting attribute Acct-Multi-Session-ID provides inconsistent values across RADIUS messages on Open or Shared WLANs that were enabled with Captive Portal/Web Authentication after the WLAN was initially created (ID 15868).  
  
Work around: Delete the WLAN configuration and recreate it with all the desired options before saving it.
- 5.1.2 Importing a certificate for a WLAN using Captive Portal or Guest Access does not prevent the user from seeing a security risk notice (ID 15328).
- 5.1.3 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.
- 5.1.4 Configuration changes after reboot (ID 5507)  
  
In some cases, if ZoneDirector is rebooted 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.

- 5.1.5 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.
- 5.1.6 Rate Limiting is not supported in tunnel mode  
When tunnel mode is enabled on a WLAN, enabling, configuring, or disabling Rate Limiting does not have any effect on that WLAN.
- 5.1.7 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.
- 5.1.8 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.
- 5.1.9 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).
- 5.1.10 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).
- 5.1.11 ZoneDirector does not support hierarchical LDAP servers topology (ID 9559)  
If an LDAP server is configured to be the authentication server for Web Portal based WLAN authentication, ZoneDirector does not support hierarchical LDAP topology.  
Workaround: Avoid using hierarchical LDAP servers, or use a RADIUS server as the front end to ZoneDirector.
- 5.1.12 For Active Directory, if a group is set as a “Primary Group”, ZoneDirector will be unable to determine whether a client is a member of that group or not (ID 9137).  
If an Active Directory server is configured as the authentication server for Web Portal based WLAN authentication and a client belongs to an AD group that is marked as a “Primary Group”, ZoneDirector will not be able to detect whether the client is a member of that group.  
Workaround: Avoid setting the AD group as the “Primary Group”.
- 5.1.13 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 (ID 11091).
- 5.1.14 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).
- 5.1.15 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).

- 5.1.16 Batch generated guest passes can be sorted in different orders depending on the number of guest passes entered (ID 11495).
- 5.1.17 Guest pass names can use special characters (ID 11515)  

ZoneDirector does not currently check the character composition of guest pass names. For example, a user can type “!@#%#^@#^@&\*^” as the guest pass name and ZoneDirector will allow it.
- 5.1.18 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).
- 5.1.19 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.
- 5.1.20 Map View cannot be displayed on Opera browser because Opera uses its own java plug-in  

Work around: Use Internet Explorer, Firefox, Chrome, Safari to access ZoneDirector’s WebUI.
- 5.1.21 MIB browsers display the speed of all interfaces on the AP as 10Mbps (ID 12548).

## **VLAN, Dynamic VLAN, and Tunnel Mode**

- 5.1.22 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
- 5.1.23 Per-user VLAN segmentation depends on the user credentials configured on the RADIUS server.
- 5.1.24 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.
- 5.1.25 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.

## AP Upgrade

5.1.26 The ZoneFlex 2925 Access Point is unsupported in this release. If you upgrade ZoneDirector to this release via the Web interface and you have a 2925 AP on the network, an alert message appears and cautions you that upgrading to this release will cause 2925 APs to stop functioning. You will have the option to continue or cancel the upgrade process. If you decide 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, you can do one of the following:

- Cancel the upgrade to release 8.2 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 you have a significant number of 2925 APs on the network, you can provision a ZoneDirector device to manage only these 2925 APs. 2925 APs can be managed by ZoneDirector releases up to 8.1.
- If you have FlexMaster on the network, you can use any version of FlexMaster to manage 2925 APs (running on release 8.1 or earlier) directly.

## Web Interface

5.1.27 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.

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

Workaround: reboot ZoneDirector.

## SNMP

5.1.29 A value is not returned for .iso.org.dod.internet.mgmt.mib-2.interfaces when queried (ID 15727).

5.1.30 The wrong OID is returned when .SysObjectID (.1.3.6.1.2.1.1.2) is queried (ID 15731).

## AeroScout

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

## Batch Generation of Dynamic PSKs

- 5.1.32 Up to 100 Dynamic PSKs can be generated simultaneously.
- 5.1.33 ZoneDirector 1000 supports up to 1000 PSKs, which include batch-generated keys and normal keys from Zero-IT Activation.
- 5.1.34 ZoneDirector 3000 supports up to 5000 PSKs, which include batch-generated keys and normal keys from Zero-IT Activation.
- 5.1.35 If the maximum number of PSKs that ZoneDirector supports has been reached, you may not be able to access the ZoneDirector Web interface 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. (ID 10454)
- 5.1.36 When the maximum number of PSKs that ZoneDirector supports has been reached, the Web interface may be slower in responding to requests.

## Batch Generation of Guest Passes

- 5.1.37 Each guest pass key is unique and is distributed on all guest WLANs, so you cannot create the same guest pass on different WLANs.  
  
Workaround: Use unique guest pass keys.

## Dynamic PSK for Mac Clients

- 5.1.38 Release 8.2 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.app (the Ruckus Wireless application that is used to generate the dynamic PSK). Moreover, any user who attempts to run prov.app will be prompted for his password, even if he is an administrator.

## Band Steering

- 5.1.39 When mesh is enabled, band steering is disabled unless the AP's *Mesh Mode* setting is disabled on the **Configure > Access Points** page.

## Email Alarm


- 5.1.40 If you are sending alarm email notifications via a Yahoo! Mail server, you need to disable STARTTLS to be able to send email notifications.
- 5.1.41 Popular SMTP ports for encrypted sessions include ports 587 and 465.
- 5.1.42 If you use the standard SMTP port 25 (for non-encrypted sessions), you must disable both TLS and STARTTLS to be able to send email notifications.
- 5.1.43 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.
- 5.1.44 If you click the **Test** button, 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.

- 5.1.45 After you upgrade ZoneDirector to software version 8.2, you should reconfigure the alarm email notification settings and include the mail server IP address and port number. This will help ensure that you continue receiving email notifications for ZoneDirector alarms.
- 5.1.46 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.

## Dual Band APs and Mesh Networking in Indonesia

- 5.1.47 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.
- 5.1.48 Mesh-enabled dual band APs that are using Indonesia as the country code are unable to join ZoneDirector because of missing radio information. Dual band APs can only use the 5GHz radio for mesh networking, but use of the 5GHz radio is restricted in Indonesia. Because of this restriction, these mesh-enabled APs are unable to send their radio information to ZoneDirector. To resolve this issue, disable mesh networking on dual band APs that are using Indonesia as the country code. (ID 10508)

Workaround:

1. Log in to the ZoneDirector Web interface, and then go to the **Monitor** page.
2. In the *Currently Managed APs* section, look for the AP on which you want to disable mesh networking, and then click the  (Allow) button to allow the AP to join ZoneDirector. The AP joins ZoneDirector successfully.
3. Go to the **Configure > Access Points** page, and then look for the AP that you just approved.
4. Click the **Edit** link that is on the same row as the AP's MAC address. A form appears where you can edit the AP's settings.
5. Scroll down to the *Mesh Mode* section, and then click the **Disable** option.
6. Click **OK**.

You have completed disabling mesh networking on the AP.

## Event Format

- 5.1.49 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`.

## Smart Mesh Networking

- 5.1.50 This release supports meshing ZoneFlex 7363, ZoneFlex 7962 and ZoneFlex 7762 APs together.
- 5.1.51 This release supports meshing ZoneFlex 7343 and ZoneFlex 7942 APs together.

5.1.52 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.

5.1.53 For dual-radio APs (ZoneFlex 7363/7762/7962), Smart Mesh Networking is only supported on the 802.11a/n (5GHz) radio.

5.1.54 Connecting APs via a separate wired network segment to a mesh AP is unsupported

Connecting an AP via a separate wired network segment (for example, in an adjacent building) to a mesh AP will result in that AP advertising itself as a Root AP. This is because the AP will discover ZoneDirector via its Ethernet port. This might cause the Mesh AP (that connects the segment to ZoneDirector) to try to connect to the new Root AP and lose its connection to ZoneDirector, resulting in an isolated mesh network.

Workaround: Connect APs in the isolated network segment via mesh.

5.1.55 Channel width of the AP on the Monitor > Access Point page may be incorrect (ID11803).

## **WISPr (Hotspot Service)**

5.1.56 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.

## **Alarm Notification**

5.1.57 Alarm email notification for rogue access points does not include channel information, although it is shown on the Monitor page (ID 10740).

## **Voice**

5.1.58 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

## **ZeroIT**

5.1.59 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.

Workaround: the end user must manually disconnect from the SSID used to provision the DPSK, and connect to their secured SSID (ID 14960).

## 5.2 ZoneFlex Access Points

### General

- 5.2.1 If an AP is being managed by ZoneDirector, you should not log in to the AP's Web interface or command line interface.

If an AP is being managed by ZoneDirector, you 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.

- 5.2.2 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.

### ZoneFlex Access Points

- 5.2.3 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.

- 5.2.4 DFS channels support

In this release, Dynamic Frequency Selection (DFS) channels are unavailable (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.

- 5.2.5 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.

- 5.2.6 The internal heater in ZoneFlex 7762 AP (which helps ensure that the AP remains operational in a low temperature environment) is available only if an 802.3at-compliant power source or a Ruckus Wireless custom-made PoE injector is used as the power source. The heater must be enabled from the ZoneDirector Web interface or the AP's Web interface or command line interface.

- 5.2.7 The PoE Out port is disabled on ZoneFlex 7762 by default

By default, the "PoE Out" port on ZoneFlex 7762 is disabled. If a Ruckus Wireless custom-made power injector is used as the power source for ZoneFlex 7762, then the PoE out port can be enabled manually from the ZoneDirector Web interface or the AP's Web interface or command line interface. The PoE OUT port can be used for networking and to provide power to other 802.3af compliant devices.

## Interoperability with PoE Switches

- 5.2.8 If a 10/100Mbps PoE injector is used to power 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.

- 5.2.9 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
- DLink DES-1228P
- TrendNet TPE-S88

## 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.

## Changed Behavior

(Applies to all Roles except the Default Role) If a Role is allowed to create guest passes (by selecting the Configure > Role > Allow guest pass generation check box), the administrator must also allow that Role to access at least one guest WLANs (under the Allow All WLANs section). Otherwise, Users that are assigned this Role will be unable to generate guest passes. (ID 12607)

## **ZoneDirector**

- ZoneFlex 2925 APs cannot be upgraded to this release and, therefore, cannot be managed by ZoneDirector running on release 8.2. To continue using the 2925 APs on the network, you can do one of the following:
  - Cancel the upgrade to release 8.2 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. Standalone 2925 APs are supported up to release 8.1.
  - If a significant number of 2925 APs are deployed on the network, you can provision a ZoneDirector device to manage only these 2925 APs. 2925 APs can be managed by ZoneDirector releases up to 8.1.
  - If a FlexMaster server is deployed on the network, you can use any version of FlexMaster to manage 2925 APs (running on release 8.1 or earlier) directly.
- Only ZoneDirector 1000 and ZoneDirector 3000 with firmware versions 7.1, 8.0, 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 could be upgrade to 7.1.
- After upgrading to ZoneDirector version 8.2.1, you should clear the Web browser cache. This will ensure that the ZoneDirector Web interface shows all the changes and enhancements that were implemented in version 8.2.1.
- When upgrading ZoneDirector 1000 to 8.2.1, you 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.

## **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.