

Ruckus Wireless ZoneFlex 8.1.1 (ZoneDirector and ZoneFlex Access Point) Release Notes

Feb 5, 2010



Contents

1	Introduction	3
2	What's New in This Release	3
3	Supported Platforms	3
4	Resolved Issues in This Maintenance Release	4
4.1	ZoneDirector	5
4.2	ZoneFlex Access Points	6
4.3	Smart Mesh Networking	6
5	Caveats, Limitations and Known Issues	6
5.1	ZoneDirector	7
	General	7
	Web Interface.....	9
	Smart Mesh Networking.....	9
	WISPr (Hotspot Service).....	11
5.2	ZoneFlex Access Point.....	11
	General	11
	802.11n Operation	12
	ZoneFlex 7962 /7762 Access Point	12
	Interoperability with PoE Switches.....	13
6	Upgrading to This Version	13
6.1	ZoneDirector.....	13
7	Interoperability Information	15

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 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 FlexMaster, ZoneDirector, supported ZoneFlex platforms, known issues, caveats, workarounds, upgrades, and interoperability information for version 8.1.1.

2 What's New in This Release

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

<http://support.ruckuswireless.com/documents>

3 Supported Platforms

Release 8.1.1 supports the following platforms:

- ZoneDirector 1000 version 8.1.1.0.12
- ZoneDirector 3000 version 8.1.1.0.12
- ZoneFlex 2925 802.11g Access Point main image version 8.1.1.0.12 and backup image version 8.1.0.0.5
- ZoneFlex 2942 802.11g Access Point version 8.1.1.0.12
- ZoneFlex 7942 802.11n Access Point version 8.1.1.0.12
- ZoneFlex 7962 Dual-band 802.11n Access Point version 8.1.1.0.12
- ZoneFlex 2741 802.11g Outdoor Access Point version 8.1.1.0.12
- ZoneFlex 7762 Dual-band 802.11n Outdoor Access Point version 8.1.1.0.12

4 Resolved Issues in This Maintenance Release

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

4.1 ZoneDirector

- 4.1.1 Changed the system-wide max client description from per AP basis to per radio (ID 10097).
- 4.1.2 Added ZeroIT support for clients running MS Windows 7.
- 4.1.3 Fixed an issue with SNMP OID ruckusDeviceName when AP Device Name is 64 characters long (ID 10067).
- 4.1.4 Improved issue of ZD Web engine causing high CPU utilization at certain times and with certain browsers, such as when loading debuginfo using Safari or IE7 (ID 10681).
- 4.1.5 Resolved issue with ZoneDirector sending stop and start notifications to RADIUS accounting server when client roams between APs (ID 9870).
- 4.1.6 Resolved ZoneDirector 1000 crash issue when there are more APs on the same LAN than a ZoneDirector 1000 can manage (total number larger than 75).
- 4.1.7 Replaced special characters with '?' characters to avoid empty events and display errors on ZoneDirector (ID 10125).
- 4.1.8 Resolved issue with AP's not using ZD manually configured channels when background scanning is disabled (ID 11176).
- 4.1.9 Added client IP address in Framed-IP attribute in accounting reporting packets for WISPr and 802.1x clients.
- 4.1.10 Resolved ZoneDirector lock up when RADIUS server application stops working but the server system is still responding (ID 8960).
- 4.1.11 Fixed channel description for certain non-English language on WebUIs incorrectly displaying 11b/g rather than 11n (bug 10068).
- 4.1.12 Fixed ZoneDirector dashboard widget drag and drop issue when Firefox 3.5.1 is used as the browser.
- 4.1.13 Fixed guest access issue while using Internet Explorer on WinMobile based hand-held devices (ID 10755).
- 4.1.14 Fixed an issue with ZoneDirector authenticating 802.1x based clients after a RADIUS server interruption when the computer the server application is running on still responds (ID 11810).
- 4.1.15 Fixed guest access issue when running Internet Explorer on Windows Mobile-based hand-held devices (ID 10755).

- 4.1.16 Extended Key exchange response timeout value to avoid slow clients to be timed out during key exchange in association process (ID 12087)

4.2 ZoneFlex Access Points

- 4.2.1 Enabled restarting TR069 client after changing remote-management method from SNMP to auto (ID 11113).
- 4.2.2 Enabled configurable PHY error reporting via AP CLI, using the following syntax:

set phyrrpt wifi0 enable/disable

get phyrrpt wifi0
- 4.2.3 Fixed a problem with ZoneFlex 7762 APs not being able to directly connect and provide power to a ZoneFlex 7731 Wireless Bridge (ID 11548).

4.3 Smart Mesh Networking

- 4.3.1 Fixed an issue with mesh link disruption during mesh link encryption key updates every two hours.
- 4.3.2 Fixed mesh recovery mechanism for 2 and more hop APs (ID 9504).
- 4.3.3 Allowed channel change on mesh APs with dual radio (ZF 7962 and ZF 7762) on their non-mesh interfaces (ID 10400 and ID 10822).

5 Caveats, Limitations and Known Issues

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

5.1 ZoneDirector

General

5.1.1 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.

5.1.2 Windows Vista clients should be upgraded to Vista Service Pack 1 (ID 5847)

Windows Vista Service Pack 1 includes important fixes for 802.1x EAP-WPA-TKIP encryption and PEAP authentication that will significantly improve client behavior.

5.1.3 Configuration changes after reboot (ID 5507)

In some cases, if ZoneDirector is rebooted after configuration changes are made, the changes may 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.

5.1.4 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, ZoneFlex 2925 LMG (Lite Mesh Gateway) or MediaFlex 7111/2111 adapters, do not work when the ZoneDirector WLAN is in tunnel mode.

5.1.5 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.

5.1.6 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.

5.1.7 10/100Mbps half-duplex mode with no auto-negotiation is not supported on the ZoneDirector 1000 (ID 8495)

The ZoneDirector 1000 cannot be connected to a 10/100Mbps half-duplex switch when auto-negotiation is disabled.

- 5.1.8 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).
- 5.1.9 Accounting service option is not available for clients of a Guest WLAN (ID 8825)
Workaround: If accounting for clients is required, configure normal WLAN.
- 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 7942/7962/7762 (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 server 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 If an AP has an SSL certificate loaded in the system, Zero-IT configuration can support 24 WLANs (ID 8087).
- 5.1.14 The customized guest pass printout page supports standard ASCII characters only
Extended ASCII characters (see http://www.webopedia.com/TERM/E/extended_ASCII.html) are unsupported on the guest-pass printout page.
- 5.1.15 Maximum number of guest passes
ZoneDirector 3000/1000 supports a combined maximum number of users on the local database and guest passes (5000 for ZoneDirector 3000 and 1250 for ZoneDirector 1000).
Example: If the administrator has already created 1000 users on ZoneDirector 1000 (which supports 1250 users and guest passes), he can only create 250 guest passes.

Web Interface

5.1.16 If there is no WLAN configured, changing the AP's radio channel will not take effect.

Workaround: Configure at least one WLAN before changing the AP's radio channel.

5.1.17 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.

5.1.18 Map View requires latest Java version (ID 7410)

The ZoneDirector Map View does not appear on the Web interface if the Java software version is 6 Update 5 or earlier.

Workaround: Update the Web browser's Java software to the latest version.

5.1.19 If using Mozilla Firefox 3.5, widgets on the ZoneDirector Dashboard cannot be dragged-and-dropped (ID 10104)

Workaround: Temporarily use a different browser for widget arrangement on the ZoneDirector Dashboard page.

Smart Mesh Networking

5.1.20 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.

5.1.21 Smart Mesh Networking is only supported for APs with the same radio type

Smart Mesh Networking is only supported for ZoneFlex APs with the same radio type (802.11g or 802.11n). For example, a ZoneFlex 7942 802.11n AP cannot form a mesh with a ZoneFlex 2925/2942 802.11g AP.

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

5.1.23 Smart Mesh Networking is only supported for APs on the same subnet (ID 5559, 5930, 6279)

Smart Mesh Networking cannot be formed by APs that belong to different network subnets. For example, a ZoneFlex 7942 Mesh AP with the IP address 192.168.10.1/24 will be unable to form a mesh with a ZoneFlex 7942 Root AP with the IP address 192.168.20.1/24. When connecting a MAP on a different subnet, the result may be unpredictable.

5.1.24 Smart Mesh Networking hops

While the maximum number of mesh hops is eight, it is strongly recommended that administrators design the mesh network in a way that minimizes the hop count. Each additional hop reduces overall network performance.

5.1.25 Smart Mesh Networking configuration process

Configuring Smart Mesh Networking requires all APs to be connected via Ethernet until Smart Mesh Networking is fully provisioned. After provisioning is completed, they will appear as Root APs on the **Monitor > Access Points** page. At that point, they will automatically reboot. Refer to the Quick Start Guide for details.

If APs appear as *Connected* on the **Monitor > Access Points** page, they do not have Smart Mesh Networking activated yet. If the problem persists for more than 15 minutes, reboot the APs.

5.1.26 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.

5.1.27 Smart Mesh Networking and maximum number of WLANs (ID 8571)

If mesh networking is enabled on ZoneDirector, the number of WLANs that is supported on all ZoneFlex APs is reduced from eight to six (per radio).

5.1.28 APs in one mesh tree can join different ZoneDirectors

When both Primary ZoneDirector and Secondary ZoneDirector are configured on APs, APs in one mesh tree can join different ZoneDirectors. Users should not notice any difference in functionality.

WISPr (Hotspot Service)

5.1.29 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.

5.1.30 WISPr Walled Garden and external links issue (ID 7999)

The walled garden feature is IP-based (not hostname-based). If a Web site on an allowed IP address contains links to sites on another IP address, users will be unable to access these other sites when they click on the links.

For example, if the administrator adds the IP address of domain.com to the Walled Garden, users will be able to access the main Web site at www.domain.com. But if a subdomain (for example, sub.domain.com) is hosted on a different IP address, users will be unable to access the page.

5.1.31 WISPr Walled Garden and URLs with multiple IP addresses issue (ID 7999)

Configuring WISPr walled garden to URLs that could resolve to multiple IP addresses redirects users to a login page.

If a URL that can be translated to more than four IP addresses is used as the WISPr walled garden, users will be redirected to the ZoneDirector login page for authentication.

Workaround: Avoid using URLs like www.yahoo.com as the walled garden URL.

5.2 ZoneFlex Access Point

General

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

If an AP is being managed by ZoneDirector, administrators 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.

5.2.3 When both AP and ZoneDirector are configured with VLAN management enabled, on AP WebUI display, its WAN IP address could be shown as 0.0.0.0 (ID 11962)

802.11n Operation

5.2.4 ZoneFlex 7942, 7962 and 7762 operate at 802.11g or 802.11a rates when using WPA-PSK-TKIP or WEP encryption (ID 3633)

In compliance with the 802.11n Draft 2.0 requirements, ZoneFlex APs use 802.11g rates (up to 54Mbps) when using WPA-PSK-TKIP or WEP encryption.

5.2.5 Some 802.11n clients (such as the ones with Intel 5100 NIC, when it is in “dynamic power saving” mode) may choose to use a lower transmit rate (such as 65Mbps) to connect to ZoneFlex APs

Workaround: If high transmit rate is desired, make sure that there are no clients that stay in dynamic power saving mode.

ZoneFlex 7962 /7762 Access Point

5.2.6 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.

5.2.7 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.

5.2.8 Video streaming and background scanning issue (ID 8571)

If there is a ZoneFlex 7962/7762 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.

5.2.9 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 803.3at-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.

5.2.10 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

5.2.11 If a 10/100Mbps PoE injector is used to power ZoneFlex 7942/7962/7762 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.

6 Upgrading to This Version

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

6.1 ZoneDirector

- Only ZoneDirector 1000 and ZoneDirector 3000 with firmware versions 7.1, 8.0 and 8.1.0 can be upgraded to this release. Upgrading from any other firmware versions might result in loss of configuration settings. ZoneDirector 1000 devices using firmware version 3.0 must be upgraded to 6.0 before they can be upgraded to 7.1.
- After upgrading to ZoneDirector version 8.1.1, administrators 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 8.1.1.

*Ruckus Wireless ZoneFlex 8.1.1
(ZoneDirector and ZoneFlex Access Point)
Release Notes*

- When upgrading ZoneDirector 1000 to 8.1.1, 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.

7 Interoperability Information

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

A list describing the specific platforms that were tested by Ruckus Wireless for interoperability is available at:

<http://support.ruckuswireless.com/documents/118-zonedirector-client-interoperability-list>