Ruckus Wireless™ ZoneDirector™ Version 9.12.3 MR 3 Refresh 2

Release Notes

Copyright Notice and Proprietary Information

Destination Control Statement

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

Disclaimer

Limitation of Liability

Trademarks

Contents

About This Release

<div style="text-align: right; font-size: large;">1</div>

Introduction

This document provides release information on ZoneDirector release 9.12.3, including new features, enhancements, known issues, caveats, workarounds, upgrade details and interoperability information for version 9.12.3.

> **NOTE**: By downloading this software and subsequently upgrading the ZoneDirector and/or the AP to version 9.12.3, please be advised that:
>
> - The ZoneDirector will periodically connect to Ruckus and Ruckus will collect the ZoneDirector serial number, software version and build number. Ruckus will transmit a file back to the ZoneDirector and this will be used to display the current status of the ZoneDirector Support Contract.
> - The AP may send a query to Ruckus containing the AP's serial number. The purpose is to enable your AP to autonomously connect with a wireless LAN controller operated by your choice of cloud service provider. Ruckus may transmit back to the AP, the Fully Qualified Domain Name (FQDN) or IP address of the controller that the AP will subsequently attempt to join.
>
> Please be advised that this information may be transferred and stored outside of your country of residence where data protection standards may be different.

Supported Country Codes

Refer to the Ruckus Wireless Price List for available country certifications.

What's New in This Release

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

https://support.ruckuswireless.com/

Supported Platforms and Upgrade Information

2

Supported Platforms

ZoneDirector version **9.12.3.0.49** supports the following ZoneDirector models:

- ZoneDirector 1200
- ZoneDirector 3000
- ZoneDirector 5000

Access Points

ZoneDirector version **9.12.3.0.49** supports the following ZoneFlex Access Point models:

- H500
- R300
- R310
- R500
- R600
- R700
- R710
- SC8800-S
- SC8800-S-AC
- T300
- T300e
- T301n
- T301s
- ZF7055
- ZF7321
- ZF7231-u
- ZF7341

- ZF7343
- ZF7352
- ZF7363
- ZF7372
- ZF7372-E
- ZF7441
- ZF7761-CM
- ZF7762
- ZF7762-AC
- ZF7762-S
- ZF7762-S-AC
- ZF7762-T
- ZF7781CM
- ZF7782
- ZF7782-E
- ZF7782-N
- ZF7782-S
- ZF7982

Upgrading to This Version

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

Officially Supported 9.12.3 Refresh Upgrade Paths

The following ZoneDirector builds can be directly upgraded to ZoneDirector build 9.12.3.0.49:

- 9.9.0.0.205 (9.9 GA release)
- 9.9.0.0.216 (9.9 GA refresh)
- 9.9.1.0.31 (9.9 MR 1 release)
- 9.10.0.0.214 (9.10 GA release)
- 9.10.0.0.218 (9.10 GA refresh)
- 9.10.1.0.59 (9.10 MR 1 release)
- 9.10.2.0.11 (9.10 MR 2 release)
- 9.12.0.0.336 (9.12 GA release)
- 9.12.1.0.140 (9.12 MR 1 release)
- 9.12.1.0.148 (9.12 MR 1 refresh)
- 9.12.2.0.101 (9.12 MR 2 release)
- 9.12.2.0.204 (9.12.2 Patch 1 release)
- 9.12.2.0.219 (9.12 MR 2 refresh)
- 9.12.3.0.28 (9.12 MR3)
- 9.12.3.0.34 (9.12 MR3 refresh 1)

NOTE: If you do not have a valid Support Entitlement contract, you will be unable to upgrade ZoneDirector to this release. See *Administer > Support* page for information on Support Entitlement activation.

If you are running an earlier version, you must first upgrade to one of the above builds before upgrading to this release.

Enhancements and Resolved Issues

<div style="text-align: right">3</div>

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

Resolved Issues

ZoneDirector

- Resolved a ZoneDirector CLI logic issue that would prevent the user from configuring static IP addresses for APs ending in 255 or 0. [ER-3647]

- Updated the error message "internal error, authsvr not found!" to be an informational level debug message rather than an error level message. [ER-3475]

- Resolved an issue where Guest Pass printouts would fail to display the proper validity period. [ER-3383]

- Resolved an issue where ZoneDirector could include erroneous data in session statistics records sent to FlexMaster and SCI, resulting in data dropouts in SCI session reports. [ER-3290]

- Resolved an issue where Application Visibility would fail to identify traffic from clients connected to an 802.1X WLAN when dynamic VLAN was enabled. [ER-2837]

- Resolved an issue where radar pulses during the 802.11h countdown could result in rescanning the available channel list. [ER-3921, ZF-13769]

- Resolved an issue with mesh uplink selection that could cause Mesh APs to sporadically disconnect from their uplink APs. [ER-3471]

- Resolved an issue with lower than expected uplink throughput on 7781-CM, 7782, 7982, and the 2.4 GHz radio on R700 APs when traffic is tunneled to ZoneDirector. [ER-4030]

- Fixed an issue related to MU MIMO clients in a busy environment resulting in Target Assert on R710 APs. [ER-3877]

- Resolved issue with MAP losing uplink when LBS and Mesh are enabled. [ER-2420]

- Resolved an issue with iOS 9 clients authenticating to an Eduroam authentication server running Freeradius version 2.x. [ER-3158]

- Resolved an issue with invalid Data Usage reported under Most Active Client Devices. [ER-2791]

- Resolved an issue where the AP reboot reason displayed in ZD logs was incorrectly displayed as "Power Cycle" when the AP was rebooted by another failure. [ER-3879]

- Resolved an issue where Remote Capture with Filter was unsupported on the AP. [ER-3504]

Resolved Issues in Build 34

- Resolved an issue with R710 APs under ZoneDirector control running ZD version 9.12.2 that could cause the AP to reboot due to watchdog timeout. [ER-4239]

- Resolved a memory leak issue related to the mesh network process that could cause the APs to disconnect and be unable to reconnect. [ER-4265]

- Resolved an issue with 7982 APs running 9.8.3 firmware that could cause the APs to become unable to connect to ZoneDirector. [ER-4327]

- Resolved an issue with RADIUS message "Acct-Output-Gigawords" values causing issues with billing systems. [ER-3893]

- Resolved an issue related to client isolation where devices connected to the 5GHz radio could not access the Internet. [ER-3489]

- Resolved an issue with R500 APs where, when the Eth1 port was disabled via UI, traffic would still be able to pass after rebooting the AP. [ER-3689]

- Resolved an issue in 9.12.2 where the ruckusRadioNoiseFloor SNMP MIB was present but not supported. [ER-4188]

- Resolved an issue that could cause watchdog timeout on mesh-enabled APs. [SCG-41709]

- Resolved an issue where remote APs could be unable to rejoin after upgrading from 9.9.0.0.216 to 9.12.2.0.219. [ER-4304]

- Resolved an issue with Ascom VoIP phones that could prevent the phones from connecting properly after being idle for some time and then roaming to another AP. [AP-3319]

- Resolved an issue where ZF 7372 APs would not properly display results for SNMP queries. [ER-3677]

- Resolved an issue where the Performance graph would display incorrectly after the user adjusted the system time. [ER-4272]
- Resolved an issue where DPSK Expiration dates would not be properly applied when configured through API. [ER-4297]
- Resolved a cross-site scripting (XSS) vulnerability discovered in ZD release 9.9.1. For more information, see https://www.ruckuswireless.com/security for security incidents and responses. [ER-4275]
- Fixed an AP reboot issue caused by corruption of beacon buffer. [ER-4212]

Resolved Issues in Build 49

- Resolved an issue where inactive clients displayed on the client monitoring page would be cleared after refreshing the page when 24 hour time span was selected. [ER-4443]
- Resolved an issue that would prevent the creation of Social Media WLANs if the ZD had been upgraded from 9.8.3. [ER-4535]
- Resolved an issue that could cause ZoneDirector to reboot due to an "rhttpc" process hang. [ER-4585]
- Resolved an issue that could cause ZoneDirector 5000 web process failure, resulting in failover to the standby ZoneDirector. [ER-4123]
- Resolved a kernel memory leak issue on APs, which eventually caused watchdog timeout reboots. [ER-3544]
- Resolved an issue with beacon stuck being detected incorrectly on R710, causing the AP to reboot. [ER-4763]
- Resolved one WASP AP hardware watchdog timeout reboot issue. [ER-1922]
- Resolved an issue where the AP was intercepting the wrong client IP address from malformed IP packets from the client. [ER-2290]
- Improved handling of LWAPP packets to reduce errors due to ZoneDirector unexpectedly receiving certain kinds of LWAPP packets. [ER-4793]
- Enhanced ZD event logs related to DPSK entry deletion. [ER-4619]
- Resolved an issue that could cause ZoneDirector to become unresponsive due to kernel oops, possibly triggered by excessive failed SSH login attempts. [ER-4879]
- Resolved an issue that could cause client connection problems and AP logs filled with the following error message: "Kernel Warn VDEV_MGR_AP_KEEP-ALIVE_IDLE". [ER-4475]

- Resolved an issue with ZF 7781-CM APs that could result in the APs continuously rebooting with the error message "user.emerg kernel: *** Reset to factory defaults ***{}". [ER-4689]

- Resolved an issue with printing multiple Guest Passes at once, where the printout would incorrectly show "invalid date" for the expiration date. [ER-4724]

Access Points

- Resolved an issue that could lead to kernel panic on R710. [ER-3874]

- Resolved several issues that could lead to lower than expected performance on R710 compared to R700 due to incorrect handling of power save clients, target hang detection, DFS channel changes, and a beacon stuck issue due to VDEV channel mismatch. [ER-4060]

- Resolved an issue where DFS channels would not be properly blocked when radar was detected on the channel, for some APs. [ER-3922]

- Implemented several memory optimization changes for ZoneFlex 7762 APs, which could experience memory exhaustion leading to AP reboots when running recent ZD/SZ releases, due to limited memory on the AP. [ER-3487]

- Resolved a performance issue with ZF 7782 and 7372 APs in the event of not setting the correct noise floor value. [ER-3442]

- Resolved an issue with lower than expected throughput on R710 on non-DFS channels. [ER-4234]

Caveats, Limitations, and Known Issues

4

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

Ethernet Port Settings

ZoneFlex AP Ethernet ports can become disabled if half-duplex is forced on any port. [ID ER-1208, ER-1229]

This problem affects the following:

• APs: ZoneFlex 7341, 7343, 7363, 7761, and 7762

Workaround: Uplink switch ports must be set to 100Mbps auto-negotiation or 1000Mbps auto-negotiation.

R710 Known Issues

• No Syslog message is sent for 802.3af PoE mode change. [ZF-13160]

• R710 AP continues to request 25W power from the PoE switch even when the AP is configured to 802.3af mode. [ZF-14489]

   Workaround: Disable LLDP Power-Via-MDI TLV on the PoE switch (this is only necessary if you wish to force the AP into 802.3af PoE mode on an 802.3at PoE+ switch for power budgeting reasons). On some switches, you may need to reset the AP connected Ethernet port/s to force the switch to renegotiate the new power level.

• The R710 can be powered by an 802.3at-compliant (25.5W) Power over Ethernet (PoE) switch or PoE injector -- *or* -- an 802.3af-compliant PoE switch or PoE injector.

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

   • The USB port is disabled

   • The non-PoE (eth1) Ethernet port is disabled

   • The 2.4 GHz radio is reduced to two transmit streams (2x4 MIMO) with aggregate transmit power up to 22dBm (subject to country limits).

R710 Features Not Supported in This Release

Support for these features is planned for a future release.

- AirTime Fairness
- Smart Mesh
- Spectrum Analysis
- WLAN Prioritization

H500, R310, R500, R600, R700 and T300 Series APs

The following features are not included in this release:

- Airtime Fairness on 5 GHz radio
- Spectrum Analysis on 5 GHz radio
- WLAN Prioritization on 5 GHz radio

Ethernet Port Redundancy

- If both ZoneDirector ports are connected to the same switch, clients connected to a tunneled WLAN may become unable to access the Internet after eth0 goes down when the VLAN is not 1. This issue does not occur when the two ports are connected to separate switches. [ZF-13793]

SPoT Location Services

- When Location Services is enabled in an AP group, and the SPoT server configured in venue configuration is not reachable, other AP Groups may be unable to communicate with the SPoT server.

  Workaround: Disable SPoT location service on any AP groups that are configured with unreachable venues. [ZF-9747, ZF-9750]

FlexMaster SSL Certificate

- As a result of the new FlexMaster SSL certificate into ZoneDirector, ZoneDirector 9.12.3 will NOT work with FlexMaster 9.12.1 and prior versions. Customers who use FlexMaster to manage ZoneDirector will need to upgrade FlexMaster to 9.12.2 to continue to be able to communicate with ZoneDirector 9.12.3.

Interoperability Information

5

ZoneDirector Controller and SmartZone Controller Interoperability

To ensure reliable network operations, it is recommended that ZoneDirector controllers and SmartZone controllers (SmartCell gateway and SmartZone controllers) not be deployed on the same IP subnet or in such a way as the controllers share the same DHCP address scopes and domain name servers (DNS) as there may be limitations or restrictions in AP controller discovery capabilities. An effective network segmentation strategy should be developed when ZoneDirector and SmartZone controllers co-exist in the same network.

Redeploying ZoneFlex APs with SmartZone Controllers

Note that a supported ZoneFlex AP configured to operate with ZoneDirector will require an upgrade to a compatible SmartZone controller approved software release prior to interoperating with a SmartZone controller. Once the AP firmware is updated, the AP will no longer be able to communicate with its old ZoneDirector controller. The AP must be reset to factory-default setting before attempting to configure the AP from the SmartZone controller.

NOTE: There are established ZD to SZ controller migration tools and procedures. Contact support.ruckuswireless.com for the latest available procedures and utilities.

ZoneFlex Release 9.9 and AP Standalone Mode and FlexMaster Managed Mode Operation

Starting January 1, 2015 the default image that ships from the factory on Ruckus access points (APs) will change from ZoneFlex Release 9.8.x to ZoneFlex Base Image Release 100.0.x. Most customers will not notice any difference in AP operation. The APs will continue to support standalone mode and FlexMaster managed mode operations and will automatically discover and connect to ZoneDirector or SmartZone controllers.

Beginning in ZoneFlex Release 9.9 and higher, the AP has a new behavior: once an AP connects to a controller the AP will no longer support standalone mode and FlexMaster managed mode operation after the controller completes the necessary AP firmware update during initialization.

An AP removed from a controller managed network may be restored to operate in standalone mode and FlexMaster managed mode operation by updating the AP firmware back to ZoneFlex Base Image Release 100.0.x or to a ZoneFlex-AP Release 9.8.x or lower.

These software images are available on the Ruckus support site, see support.ruckuswireless.com for more information.

AP Interoperability

APs with ordering number prefix 901- (example 901-T300-WW81), may now be supplied with an AP base image release 100.0. or higher.

The AP base image is optimized for controller-discovery compatibility to support all Ruckus Wireless controller products including ZoneDirector, SCG, vSCG, SmartZone and SAMS.

Once the AP discovers and joins a controller (for example ZoneDirector), the AP is updated to the compatible controller-specific AP firmware version. The updated AP firmware version becomes the factory-default image. The updated AP firmware version (for example, ZoneFlex 9.9) will remain persistent on the AP after reset to factory defaults.

An AP configured with base image release 100.0 may be managed by the FlexMaster management tool or may be used in standalone controller-less operation if controller discovery is disabled on the AP web UI.

Client Interoperability

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

The following client operating systems and browsers have been tested for compatibility with this release (for specific OS and browser limitations, including compatibility with Zero-IT, see subsequent sections below).

PC OS:
- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Mac OS 10.8.5
- Mac OS 10.9.3
- Mac OS 10.9.4
- Mac OS 10.10
- Mac OS 10.11

Smart Phone/Tablet OS:
- iOS (6.x, 7.x, 8.0, 8.0.2, 8.1, 9.0)
- Android (4.0.4, 4.1.2, 4.4.2, 4.4.4, 5.0.1)
- Windows Phone (8, 8.1, 10)
- BlackBerry OS (10.1.0.4633, 10.3.0.1172)
- Kindle (7.4.9)
- Chrome OS

Officially Supported Browsers:
- Internet Explorer 10, 11
- Firefox 34 and later
- Chrome 39 and later

Not Officially Supported Browsers:

Safari, Dolphin, Opera Mini, Android Default, BlackBerry Default, etc.

Zero-IT Compatibility with Client Devices

Table 1.   Zero-IT Compatibility

OS	WPA2 WLAN			802.1x EAP (external Radius Server)		
	Step 1	Step 2	Step 3	Step 1	Step 2	Step 3
iOS 6.x	Y	Y	N(ZF-2888)	Y	Y	N(ZF-2888)
iOS 7.x	Y	Y	N(ZF-2888)	Y	Y	N(ZF-2888)
iOS 8.0	Y	Y	N(ZF-2888)	Y	Y	N(ZF-2888)
iOS 8.0.2	Y	Y	N(ZF-2888)	Y	Y	N(ZF-2888)
iOS 8.1	Y	Y	N(ZF-2888)	Y	Y	N(ZF-2888)
iOS 9.0	Y	Y	N(ZF-2888)	Y	Y	N(ZF-2888)
MAC OS 10.8.5	Y	Y	Y	Y	Y	N(ZF-4699)
Mac OS 10.9.3	Y	Y	Y	Y	Y	N(ZF-4699)
MAC OS 10.9.4	Y	Y	Y	Y	Y	N(ZF-4699)
Mac OS 10.9.5	Y	Y	Y	Y	Y	N(ZF-4699)
Mac OS 10.10	Y	Y	Y	Y	Y	N(ZF-4699)
Mac OS 10.11	Y	Y	Y	Y	Y	N (ZF-4699)
Windows 7	Y	Y	Y	Y	Y	Y
Windows 8	Y	Y	Y	Y	Y	Y
Windows 8.1	Y	Y	Y	Y	Y	Y
Windows 10	Y	Y	Y	Y	Y	Y
Windows Phone 8	N (ZF-3478)	N (ZF-3478)	N (ZF-3478)	N (ZF-3478)	N (ZF-3478)	N (ZF-3478)
Windows Phone 8.1	N (ZF-3478)	N (ZF-3478)	N (ZF-3478)	N (ZF-3478)	N (ZF-3478)	N (ZF-3478)
BlackBerry OS 10.1	N (ZF-6402)	N (ZF-6402)	N (ZF-6402)	N (ZF-6402)	N (ZF-6402)	N (ZF-6402)
BlackBerry OS 10.3	N (ZF-6402)	N (ZF-6402)	N (ZF-6402)	N (ZF-6402)	N (ZF-6402)	N (ZF-6402)
Kindle 7.4.9	Y	Y	Y	Y	Y	Y
Android 4.0.4	Y	Y	Y	Y	Y	Y

Table 1.   Zero-IT Compatibility

	WPA2 WLAN			802.1x EAP (external Radius Server)		
Android 4.1.2	Y	Y	Y	Y	Y	Y
Android 4.4.4	Y	Y	Y	Y	Y	Y
Android 5.0	Y	Y	Y	Y	Y	Y
Chrome OS	N (ZF-8076)	N (ZF-8076)	N (ZF-8076)	N (ZF-8076)	N (ZF-8076)	N (ZF-8076)

- Step 1: Download Zero-IT file
- Step 2: Install Zero-IT script
- Step 3: Automatically connect to the appropriate SSID

Client Interoperability Issues

- Zero-IT is not supported on Windows Phone 7/8/8.1 devices. [ZF-3478]
- Zero-IT is not supported on Blackberry OS devices. [ZF-6402]
- Zero-IT is not supported on Chrome OS devices. [ZF-8076]
- iOS clients cannot connect to the Zero-IT WLAN automatically. Users must reconnect to the target WLAN after installing the Zero-IT configuration file. [ZF-2888]
- Mac OS 10.7 and 10.8 cannot automatically connect to an 802.1x EAP WLAN after installing Zero-IT script. [ZF-4699]
- In some situations, Chromebook clients can take up to 10-50 seconds to resume sending traffic after a channel change. [ZF-14883]
- When a user connects to a WISPr WLAN using Internet Explorer 10, it is required that TLS1.1 and TLS1.2 are enabled in the browser. [ER-3608]