RELEASE NOTES

Ruckus ZoneDirector Release Notes, 9.12.3 Refresh 5

Supporting ZoneDirector 9.12.3 Refresh 5

Part Number: 800-71820-001 Rev A
Publication Date: December 2017

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

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN ("MATERIAL") IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. ARRIS and RUCKUS WIRELESS, INC. AND THEIR LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. ARRIS and RUCKUS RESERVE THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL ARRIS or RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless, Ruckus, the bark logo, BeamFlex, ChannelFly, Dynamic PSK, FlexMaster, ICX, Simply Better Wireless, SmartCell, SmartMesh, SmartZone, Unleashed, ZoneDirector and ZoneFlex are trademarks of Ruckus Wireless, Inc. in the United States and in other countries. Other trademarks may belong to third parties.

Contents

About This Release

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 Platforms and Upgrade Information

Supported Platforms

ZoneDirector version **9.12.3.0.83** supports the following ZoneDirector models:

- ZoneDirector 1200
- ZoneDirector 3000
- ZoneDirector 5000

ZoneDirector version **9.12.3.0.83** 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 Upgrade Paths

The following ZoneDirector builds can be directly upgraded to this ZoneDirector 9.12.3 Refresh release:

- 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)
- 9.10.2.0.41 (9.10.2 MR 2 refresh 2)
- 9.10.2.0.53 (9.10.2 MR 2 refresh 3)
- 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 MR 3)
- 9.12.3.0.34 (9.12 MR 3 refresh 1)
- 9.12.3.0.49 (9.12 MR 3 refresh 2)
- 9.12.3.0.61 (9.12 MR 3 refresh 3)
- 9.12.3.0.75 (9.12 MR 3 refresh 4)

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

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.

Enhancements and Resolved Issues

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

Resolved Issues

Resolved Issues in Build 83

- Resolved an issue that could cause the connection between an AP and the SPoT Location Services server to randomly disconnect. [ER-5821]
- Resolved an issue that could cause AP heartbeats lost and APs to move from one controller to another, and added syslog messages to indicate when ARP usage and UIF queue thresholds have been exceeded. [ER-5117]
- Resolved a security issue related to DNSMASQ (CVE-2017-14491, CVE-2015-3294). [AP-6652] For information on security incidents and responses, see https://www.ruckuswireless.com/security.
- Resolved an AP kernel panic issue that occurred when a back-end switch has enabled DHCP option 82. [ER-5735]
- Added "Ruckus-Location" attribute in RADIUS request packets for 802.1x WLAN authentication. [ER-5880]

Resolved Issued in Build 75

- Resolved an issue related to the WPA KRACK vulnerability. For information on security incidents and responses, see https://www.ruckuswireless.com/security. [AP-6463]

  This release fixes multiple vulnerabilities (also known as KRACK vulnerabilities) discovered in the four-way handshake stage of the WPA protocol. The Common Vulnerabilities and Exposures (CVE) IDs that this release addresses include:

  – CVE-2017-13077
  – CVE-2017-13078
  – CVE-2017-13079
  – CVE-2017-13080
  – CVE-2017-13081

– CVE-2017-13082

Client devices that have not yet been patched are vulnerable to KRACK attacks. To help protect unpatched client devices from KRACK attacks, Ruckus strongly recommends running the CLI commands below:

```
ruckus# config
ruckus(config)# system
ruckus(config-sys)# eapol-no-retry
```

Use the following command to disable:

```
ruckus(config-sys)# no eapol-no-retry
```

Enabling the eapol-no-retry feature (disabled by default) prevents the AP from retrying packets in the key exchange process that have been found to be vulnerable to KRACK attacks. Note that enabling this feature may introduce client connectivity delay in high client density environments.

For more information about KRACK vulnerabilities, visit the Ruckus Support Resource Center at https://support.ruckuswireless.com/krack-ruckus-wireless-support-resource-center.

- Resolved an issue where new APs locked to country code Z2 would fail to join a ZoneDirector configured with country code Egypt. [ER-5308]
- Resolved an AP kernel panic reboot issue caused by receiving malformed BTM response frames from certain clients. [ER-5386]
- Resolved an issue where input/output traffic in RADIUS accounting messages was incorrect after station roaming when "roaming-acct-interim-update" setting was disabled. [ER-4961, UN-1100]
- Resolved an issue where newly created AP groups would fail to inherit Tx power settings from the system default AP group as "Full". [ER-5586]
- Resolved an issue where Client Fingerprinting would fail to recognize certain recent Android client devices. [ER-5644]

Resolved Issued in Build 61

- Resolved an issue where the following erroneous error message would recur every hour: “Radius server [ ] has not responded to multiple requests. [This server may be down or unreachable.].” [ER-5122]
- Resolved an issue where LLDP settings would be overwritten after upgrading from 9.8.1. With this fix, ZoneDirector will now by default configure APs’ LLDP settings as “Keep AP setting” to prevent overwriting the existing settings. [ER-5106]
- Resolved an issue that could cause ZoneDirector 5000 web process failure, resulting in failover to the standby ZoneDirector. [ER-5003]
- Resolved a ZoneDirector 5000 issue that could cause the web UI to become unstable in high density environments. [ER-2037]
- Upgraded Dropbear SSH server version to address a security vulnerability in earlier releases. [ER-4782]
- Resolved an issue that could cause clients to be unable to access a Hotspot redirect page due to an ARP table full error. [ER-5041]
- Resolved an issue where the Management Interface would become unreachable after a Smart Redundancy failover. [ER-4903, ZF-16471]
- Resolved a security issue listed in the following advisory Linux Kernel Local Privilege Escalation "Dirty Cow" - CVE-2016-5195. [ER-4687]
- 802.11r Fast BSS Transition can no longer be enabled when WLAN type is Autonomous. [ER-5135]
- Resolved an issue where the max clients limit was not enforced on Autonomous WLANs when an AP was disconnected from ZoneDirector. [ER-3887]

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_KEEPALIVE_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]

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 GHz 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 28

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]

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

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 776

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.