

Ruckus Wireless™ ZoneDirector™ Release Notes 9.13.3

Supporting ZoneDirector 9.13.3 Refresh 4

Copyright Notice and Proprietary Information

Copyright 2017. Ruckus Wireless, Inc. All rights reserved.

No part of this documentation may be used, reproduced, transmitted, or translated, in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without prior written permission of Ruckus Wireless, Inc. ("Ruckus"), or as expressly provided by under license from Ruckus.

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. RUCKUS AND ITS 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. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL 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, Simply Better Wireless, SmartCell, SmartMesh, SmartZone, Unleashed, ZoneDirector and ZoneFlex are trademarks of Ruckus Wireless, Inc. in the United States and other countries. All other product or company names may be trademarks of their respective owners.

Contents

- About This Release..... 4**
 - Introduction.....4
- Supported Platforms and Upgrade Information.....4**
 - Supported Platforms.....4
 - Upgrading to This Version..... 5
- Enhancements and Resolved Issues..... 6**
 - New Access Points.....6
 - Resolved Issues..... 7
- Caveats, Limitations, and Known Issues..... 9**
 - Known Issues..... 9

About This Release

Introduction

This document provides release information on ZoneDirector release 9.13.3, including new features, enhancements, known issues, caveats, workarounds, upgrade details and interoperability information for version 9.13.3.

NOTE

By downloading this software and subsequently upgrading the ZoneDirector and/or the AP to version 9.13.3, 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 **9.13.3.0.133** supports the following ZoneDirector models:

- ZoneDirector 1200
- ZoneDirector 3000
- ZoneDirector 5000

Access Points

ZoneDirector version **9.13.3.0.133** supports the following Access Point models:

- C110
- H500
- H510
- R300
- R310
- R500
- R510
- R600
- R610
- R700

- R710
- T300
- T300e
- T301n
- T301s
- T610
- T610s
- T710
- T710s
- ZF7055
- ZF7352
- ZF7372
- ZF7372-E
- ZF7781CM
- ZF7782
- ZF7782-E
- ZF7782-N
- ZF7782-S
- ZF7982

EoS (End of Sale) APs

The following AP models have reached end-of-sale (EoS) status and, therefore, are no longer supported in this release. If your ZoneDirector is currently managing any of these models, a warning will appear when you attempt to upgrade.

If your ZoneDirector is currently managing any of these models, do NOT upgrade to this release. ZoneDirector will be unable to manage them.

- 7321
- 7321-U
- 7441
- 7761-CM
- 7762 series
- 7363
- 7343
- 7341
- sc8800-s
- sc8800-s-ac

Upgrading to This Version

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

Officially Supported 9.13.3 Upgrade Paths

The following ZoneDirector builds can be directly upgraded to ZoneDirector build **9.13.3.0.133**:

- 9.10.0.0.218 (9.10 GA)
- 9.10.1.0.59 (9.10 MR1)
- 9.10.2.0.11 (9.10 MR2)
- 9.10.2.0.29 (9.10 MR2 Refresh)
- 9.12.0.0.336 (9.12 GA)
- 9.12.1.0.140 (9.12 MR1)
- 9.12.1.0.148 (9.12 MR1-Refresh)
- 9.12.2.0.101 (9.12.2 MR2)
- 9.12.2.0.204 (9.12.2 MR2 Patch)
- 9.12.2.0.219 (9.12 MR2 Refresh)
- 9.12.3.0.28 (9.12 MR3)
- 9.12.3.0.34 (9.12 MR3 Refresh)
- 9.13.0.0.232 (9.13 GA)
- 9.13.1.0.11 (9.13.1 MR1)
- 9.13.1.0.26 (9.13.1 MR1 Refresh)
- 9.13.2.0.33 (9.13 MR2)
- 9.13.3.0.22 (9.13 MR3)
- 9.13.3.0.41 (9.13.3 MR3 Refresh 1)
- 9.13.3.0.106 (9.13.3 MR3 Refresh 2)
- 9.13.3.0.121 (9.13.3 MR3 Refresh 3)

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

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

New Access Points

- New Access Point: C110

The C110 is a new 802.11ac dual-band concurrent wall plate cable modem AP. Designed to be installed in an outlet box with a coaxial cable termination, the C110 features a DOCSIS/EuroDOCSIS 3.0 cable modem for backhaul, a USB port for uses such as a BLE dongle or other IoT applications, and two RJ-45 LAN ports for in-room wired Ethernet access.

- New Access Point: T610 and T610s

The T610 is a carrier-grade 802.11ac Wave 2 outdoor AP designed for enterprise and service provider outdoor WLAN applications. The T610 includes dual radios with 4x4:4 spatial streams, two 10/100/1000 Ethernet ports (one port supports PoE

input), and 802.1ax Ethernet port aggregation. The T610 also includes a USB port for BLE Smart Beacon, Zigbee or other IoT devices.

The T610s is the sector antenna version of the T610. It includes all of the same features as the T610.

Resolved Issues

Resolved Issues in Build 133

- 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 with Aeroscout tags not functioning properly on R510 APs. [ER-5191]
- Resolved an issue where Dynamic VLAN could not be enabled via CLI for 802.1x EAP+MAC authentication. [ER-5584]
- Resolved an issue where a newly created AP group would fail to inherit Tx power settings from the system default AP group as "Full". [ER-5586]
- Resolved an issue with online help "Generating and Delivering a Single Guest Pass" chapter where unnecessary steps were removed. [ER-5597]

Resolved Issues in Build 121

- Resolved an issue with R510 APs that could cause the AP to reboot due to an incorrect sleep function call being invoked in an interrupt context, causing unexpected behavior. [ER-5213]
- Resolved an AP kernel panic reboot issue caused by receiving malformed BTM response frames from certain clients. [ER-5386]

Enhancements and Resolved Issues

Resolved Issues

- Resolved an issue where rate limiting would not work properly for WLANs with the "drop multicast packets from associated clients" option enabled. [ER-5319]
- Guest pass printout instructions should no longer display incorrect values for guest pass validity. [ER-499]
- Resolved a memory leak issue which was causing R510 APs to target assert. [ER-5383]
- Resolved an issue that potentially blocked users from configuring the AP port setting through ZD CLI. [ER-5587]

Resolved Issues in Build 106

- Fixed an AP reboot issue caused by corruption of beacon buffer. [ER-4212]
- 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 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 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 with an 'X-Frame Options Header Not Set' configuration error reported by Nessus. [ER-4966]
- Resolved an issue that could cause incorrect user name data to be sent in RADIUS accounting packets under specific circumstances. [ER-5315]
- Resolved an issue where both Ethernet ports on the C110 Cable Modem AP could not be configured as Access Ports with wired 802.1x authentication enabled. [ER-5244]
- Double colons "::" can now properly be used in IPv6 addresses when creating IPv6 ACLs from the web interface. [ER-5182]
- Resolved an LLDP MAC address issue. [ER-5228]
- Resolved a device fingerprinting issue where Ubuntu clients would fail to be categorized as Linux OS clients. [ER-5121]
- Resolved an issue where, if Force DHCP was enabled, clients would be deauthenticated after roaming to another AP if the VLAN after roaming was the same as the previous VLAN. [ER-4992]
- Resolved an issue with excessive "ieee80211_vlan_clr_filter" error messages sent to syslog. [ER-5065]
- Resolved an issue where an AP could fail to stay on a statically configured channel. [ER-5074]
- Resolved an R700 Target Assert failure issue occurring on multiple APs. [ER-4971]
- Resolved an issue with excessive AP-to-AP ARP traffic causing network congestion in high-density settings where port isolation rather than fast roaming is used. [ER-5138]

Resolved Issues in Build 41

- Resolved an issue that could cause the ZoneDirector web interface to become unresponsive and new clients unable to connect when very large numbers of 802.1X clients attempted to authenticate at the same time. [ZF-16335, ER-4712]
- Resolved an issue that could cause ZoneDirector 5000 web process failure, resulting in failover to the standby ZoneDirector. [ER-4123, ER-5003]
- Resolved an issue where R710 Root APs would be incorrectly categorized as Mesh APs when Link Aggregation was enabled and in Auto mode. [ER-4616]
- Improved handling of LWAPP packets to reduce errors due to ZoneDirector unexpectedly receiving certain kinds of LWAPP packets. [ER-4793]
- Added language translations for Self-Service Guest Pass UI pages. New languages include Dutch, German, Japanese, Swedish, Arabic, Czech, Turkish, and Brazilian Portuguese.[ER-4956]
- Resolved a "Terms of Use" display issue. [ER-4975]

- Resolved an issue where, in dense environments, sometimes the AP sent an incorrect number of associated client events to the controller. [ER-4844]
- Resolved an issue that could cause clients configured with static IP addresses to be incorrectly displayed as automatically assigned DHCP addresses. [ER-5027]
- Resolved an ARP table leak issue that could prevent clients from completing hotspot authentication after ZoneDirector had been running for a long time. [ER-5041]
- Resolved an R710 “target fail detected” issue. [ER-4982]
- Upgraded Dropbear version to 2016.74 to address security vulnerabilities.[ER-5033]

Resolved Issues in Build 22

- Resolved a security issue related to Redhat CVE-2016-5195. For information on security incidents and responses, see <https://www.ruckuswireless.com/security>. [ER-4687]
- Resolved several Ruckus Cloud security issues. For information on security incidents and responses, see <https://www.ruckuswireless.com/security>. [ER-4697], [ER-4555], [ER-4560]
- Resolved a kernel memory leak issue on APs, which eventually caused watchdog timeout reboots. [ER-3544]
- Guest Pass keys are no longer incorrectly displayed on the screen when the Notification Method is set to “Mobile” and not “Show on Screen.” [ER-3188]
- Resolved an issue that could cause ZD-controlled ZF 7372 APs to reboot due to watchdog timeout. [ER-1922]
- Resolved an issue where IPTV connected to AP may experience pixelation due to packet loss on eth0 interface. [ER-4038]
- 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 an issue with cloning L3/L4/IP address ACLs that would prevent the user from replicating an existing ACL successfully. [ER-4792]
- Resolved an Ethernet port stuck issue on R510 APs that could cause the APs to reboot and disconnect from the controller. [ER-4685]
- Resolved an issue that could cause ZF7781-CM APs to reboot continuously with the message “reset to factory defaults.” This fix enables the AP to detect the condition and reboot to recover when this condition occurs. [ER-4689]

Caveats, Limitations, and Known Issues

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

Known Issues

- C110 stops sending packets in testing when using an Ethernet port as the uplink and pushing 60-80Mbps tunneled traffic to ZoneDirector. This issue should have no customer impact since the C110 typically uses its coaxial cable port as its uplink. [ZF-16212]
- C110 Cable Modem IP address is displayed incorrectly on ZoneDirector monitoring pages when the CM is assigned an IPv6 address. [ZF-16183]
- T610 USB Port status is displayed incorrectly on ZoneDirector monitoring pages when the AP is in 802.3af PoE mode. [ZF-16278]
- The Zero-IT prov file might fail to download/install via the auto pop-up mini browser on Macbook/Android devices. [ZF-16510]

Caveats, Limitations, and Known Issues

Known Issues

Workaround: Manually open any of the normal web browsers (Safari, Chrome, IE or Firefox) to re-download and install the zero-IT prov file.