RELEASE NOTES

Ruckus ZoneDirector 10.0.1 Refresh 2 Release Notes

Supporting ZoneDirector 10.0.1

Part Number: 800-71722-001 Rev C
Publication Date: January 2018

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 10.0.1, including new features, enhancements, known issues, caveats, workarounds, upgrade details and interoperability information for version 10.0.1.

> NOTE
> By downloading this software and subsequently upgrading the ZoneDirector and/or the AP to version 10.0.1, 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 10.0.1.0.44 supports the following ZoneDirector models:

- ZoneDirector 1200
- ZoneDirector 3000
- ZoneDirector 5000

Access Points

ZoneDirector version 10.0.1.0.44 supports the following Access Point models:

- C110
- H320
- H500
- H510
- R300
- R310
- R500
- R510
- R600
- R610
- R700
- R710

- R720
- T300
- T300e
- T301n
- T301s
- T610
- T610s
- T710
- T710s
- ZF7055
- ZF7352
- ZF7372
- ZF7372-E
- 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 Upgrade Paths

The following ZoneDirector builds can be directly upgraded to this ZoneDirector this 10.0.1 MR1 Refresh release:

- 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 MR2)
- 9.12.2.0.204 (9.12 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)
- 9.12.3.0.49 (9.12 MR3 Refresh 2)
- 9.12.3.0.61 (9.12 MR3 Refresh 3)
- 9.12.3.0.75 (9.12 MR3 Refresh 4)
- 9.12.3.0.83 (9.12 MR3 Refresh 5)
- 9.13.0.0.232 (9.13 GA)
- 9.13.1.0.11 (9.13 MR1)

- 9.13.1.0.26 (9.13 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 MR3 Refresh)
- 9.13.3.0.106 (9.13 MR3 Refresh 2)
- 9.13.3.0.121 (9.13 MR3 Refresh 3)
- 9.13.3.0.133 (9.13 MR3 Refresh 4)
- 9.13.3.0.145 (9.13 MR3 Refresh 5)
- 10.0.0.0.1424 (10.0 GA)
- 10.0.0.0.1449 (10.0 Patch 1)
- 10.0.1.0.17 (10.0 MR1)
- 10.0.1.0.35 (10.0 MR1 Refresh)

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 any customer-reported issues from previous releases that have been resolved in this release.

New Access Points

- New Access Point: H320

  The H320 is an 802.11a/b/g/n/ac Wave 2 dual band access point with integrated 3-port Ethernet, in a form factor designed for mounting to electrical outlet boxes. The H320 is targeted for hospitality and MDU applications where it will be installed one per room for a typical hotel room. The switch ports can be used for in-room wired applications like IPTV and/or to provide a wired alternative for guest internet access.

  The H320 has one 10/100/1000 Mbps Ethernet port and two 10/100 Mbps Ethernet ports. The Gigabit port on the rear of the unit supports 802.3af PoE input. The PD will identify as a Class 3 device with a max draw of 12.95W.

  NOTE
  The H320 does not support mesh.

- New Access Point: R720

  The R720 is a new dual-band concurrent 4x4:4 802.11ac Wave 2 access point capable of 160 MHz and 80+80 MHz channelization, designed for high density indoor applications. The R720 features one 10/100/1000 Ethernet port, and one 100/1000/2500 Ethernet port that supports 802.3af and 802.3at Power Over Ethernet (PoE), and a USB port for IoT applications.

  See the *Known Issues* section for more information on R720 limitations/power supply considerations.

Enhancements

- Increased ZoneDirector 1200 Capacity Limits

  The maximum AP and client limits that ZoneDirector 1200 supports have been increased. The max number of APs has been increased from 75 to 150, and the max clients/DPSKs/guest passes has been increased from 2,000 to 4,000. The max number of temporary licenses remains 75.

- New User Interface

  This release includes an updated and redesigned web user interface. The new UI provides an updated layout, updated network health dashboard overview, reorganized menu structure, and a new map view interface based on Google Maps.

- New AP Model Support

  This feature allows administrators to import a new AP model patch file to ZoneDirector to add new AP models without requiring a full upgrade of the ZoneDirector firmware. In this way, new APs can be introduced without the need to wait for the next ZD firmware release.

- Bonjour Fencing

  Bonjour Fencing provides a mechanism to limit the scope of Bonjour (mDNS) service discovery in the physical/spatial domain. While Bonjour Fencing is related to Bonjour Gateway, they are two separate features designed for different purposes. Bonjour Gateway bridges mDNS services across VLANs, and is useful because Bonjour is designed as a same-VLAN protocol.

  Bonjour Fencing limits the range of Bonjour service discovery within physical space, which is useful because logical network boundaries (VLANs) do not always correlate well to physical boundaries within a building/floor.

- RADIUS CoA Message Support

  Added support for RADIUS Change of Authorization (CoA) messages. CoA enables the dynamic reconfiguration of sessions from external authentication, authorization, and accounting (AAA) servers. The following CoA attributes are supported in this release:

  - Idle timeout
  - Session Timeout
  - Accounting interval
  - Uplink rate limit
  - Downlink rate limit
  - Filter ID (ACL ID)

- Role Based and Named ACL

  The Role Based ACL feature allows administrators to apply different access controls to different groups of users based on role. This enhancement complements the existing per-WLAN ACL functionality by providing another way to enforce access control rules without the need to create separate WLANs for different user groups.

- 160 MHz and 80+80 MHz Channelization for R720 and T610
- BSS Min Rate, OFDM Only and Mgmt Tx Rate

  Added the ability to set BSS Min Rate, OFDM Only and Mgmt Tx Rate in WLAN configuration forms. These options can be configured to improve overall throughput capacity and prevent older 802.11b clients from joining in high density environments.

- Per-SSID Rate Limiting

  Added the option to configure rate limiting on a per-WLAN basis (in addition to the existing per-user rate limiting). If per-SSID rate limiting is enabled, per-user rate limiting is disabled.

- Application Recognition and Control Enhancements

  This release adds the ability to import new application signature packages to ZoneDirector to update the list of system-defined applications and the ability to define QoS traffic shaping and rate limiting on a per-application basis.

- 802.11w Protected Management Frames

  Added the ability to enable management frame protection for any WPA2-AES (either 802.1X or PSK) encrypted WLANs. The Protected Management Frame (PMF), also known as Management Frame Protection (MFP), is defined in 802.11w to protect 802.11 Robust Management frames, including Disassociation, Deauthentication, and Robust Action frames.
- Spectrum Analysis

  Spectrum Analysis is now supported on all 802.11ac Wave 1 and Wave 2 APs.
- 802.1X WLAN Performance Enhancement

  Improved 802.1X handling procedures to prevent overloading in high density 802.1X environments.
- Captive Portal WLAN Performance Enhancement

  This enhancement improves handling of captive portal service by offloading the process to the AP, reducing the impact on ZoneDirector’s resources. Additionally, several enhancements have been made to ZoneDirector to improve handling of HTTP/HTTPS requests and authentication rate.
- Guest Access Enhancements

  Guest access options have been redesigned to allow greater flexibility and convenience for both admin-generated guest passes and self-service guest passes. The guest pass generation workflow has been updated, and guest passes can now be generated and managed from the Monitor page as well as the configuration page.
- The Self-Service Guest Pass sponsor email now contains ZoneDirector’s IP address.
- Added the ability to manually approve AP join requests via CLI command.

Resolved Issues in Build 10.0.1.0.44

- Resolved an issue where the SNMP ID of the WLAN interface would change after an AP reboot or failover. [ER-5718]
- Resolved a security issue related to DNSMASQ (CVE-2017-14491, CVE-2015-3294). For information on security incidents and responses, see https://www.ruckuswireless.com/security. [AP-6652]
- Resolved an issue where an AP couldn't forward wireless client multicast packets to the network. [ER-5100]
- Resolved an issue where the station MAC address is wrongly carried as the user name in the radius accounting messages. [ER-5623]
- Resolved multiple unexpected reboot issues on C110 AP. [ER-5851]
- Resolved an issue where ZoneDirector would incorrectly approve unsupported AP join requests when the AP model value carried in the join request packet was empty. [ER-5763]
- Resolved an issue where per-station rate limit settings could not be configured via web UI when the interface language selected was a European language other than English. [ER-5744]
- Added "Ruckus-Location" attribute in RADIUS request packets for 802.1x WLAN authentication. [ER-5880]
- Resolved an issue where multicast and broadcast IPs could not be configured as destination in L3 ACL rules via ZD CLI. [ER-5894]
- Resolved an issue where LLDP settings would be overwritten after upgrading. 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 several display issues on Guest Pass printout pages. [ER-5901/ER-5975]
- Resolved an issue where an additional blank page would appear in the Guest Pass printout page.[ER-5966]

Resolved Issues in Build 10.0.1.0.35

- 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 guest pass email and SMS messages where the validity period would be displayed incorrectly, including the following typo: "MOE_ days." [ER-5716]

Resolved Issues in Build 10.0.1.0.17

- Resolved an issue that R710/R610/T710/T610 APs' Ethernet link could not come up with certain multipleG supported switches. [ER-5466]
- Resolved an issue where rate limiting did not work properly for WLANs with the "drop multicast packets from associated clients" option enabled. [ER-5319]
- Resolved an issue where Domain Name System (DNS) in the AP crashed randomly when it attempts to resolve a Domain Name [ER-5398]
- Updated the “Generating and Delivering a Single Guest Pass” chapter in the online help to remove a few unnecessary steps. [ER-5597]
- Resolved several guest pass issues: [ER-5612]

  1. The validation date of an existing guest pass did not show correctly in the printed instructions, if the user logged off and then logged back on.
  2. The "Guest Pass Generated" page displayed duplicated guest passes.
  3. 'Generated PSK/certificate' under Monitor tab was shown as 'Generierte' instead of 'Generierte PSK/Zertifikate'
  4. "Day" in Guest Pass printout was shown as "Tage" when German was selected as the system language.

- Resolved an issue where a newly created AP group failed to inherit Tx power setting from the default AP group as "Full." [ER-5586]

- Resolved an issue where DVLAN for 802.1x EAP+MAC authentication could not be enabled using the ZoneDirector CLI. [ER-5584]
- Resolved an issue where the Microsoft VSA value for the RADIUS server was incorrectly applied as the station's rate limit. [ER-5461]
- Resolved an issue where the LLDP settings were overwritten after ZoneDirector was upgraded. With the fix, ZoneDirector now retains the AP's LLDP settings ("Keep AP setting"). [ER-5106]
- Resolved an issue where SNMP OIDs related to APLAN statistics showed incorrect values. [ER-5560]
- Guest pass printout instructions should no longer display incorrect values for guest pass validity. [ER-5499]

Resolved Issues in Build 10.0.0.0.1449

- Resolved an issue with Facebook WiFi WLANs where mobile device redirection stopped working after upgrading to 10.0. [ER-5481]
- The C110 Cable Modem APs can now be configured with both Ethernet ports as Access Ports. [ER-5244]
- Optimized the severity levels of several syslog messages to prevent flooding syslog servers with excessive log messages. [ER-5400, ER-5410]
- Resolved a “Terms of Use” display issue on Android devices using the default browser. [ER-5422]
- Resolved an issue where Guest Passes generated via the admin console would display as "Invalid Guest Pass" when the WLAN name contained special characters. [ER-5439, ZF-17090]
- Resolved an issue where clients could be assigned incorrect VLAN IDs if the client switches between 802.1x and portal based WLANs with different VLAN settings. [ER-5362]
- Resolved an AP kernel panic reboot issue caused by receiving malformed BTM response frames from some types of clients. [ER-5386]

Resolved Issues in Build 10.0.0.0.1424

- Upgraded Dropbear version to 2016.74 to address security vulnerabilities. [ER- 5033]
- Resolved an issue that could cause AP heartbeats to be lost and APs to move from one controller to another, and added syslog messages to indicate when ARP usage and UIF queue thresholds are exceeded. [ER-5117]
- Lowered the severity level of an incorrectly categorized error message that could cause customer syslogs to fill up with “ieee80211_vlan_clr_filter” errors. [ER- 5065]
- Resolved an issue that could prevent Ubuntu clients from being properly identified as Linux OS. [ER-5121]
- Resolved a false radar detection issue for 7982 and R500 APs. [ER-4632]
- Resolved a security issue related to the x-frame options. See https://www.ruckuswireless.com/security for security incidents and responses. [ER-4966]
- Double colons “::” can now be used in IPv6 addresses when creating IPv6 ACLs from the web interface. [ER-5182]
- Upgraded OpenSSL version from 1.0.1q (1.0.1m) to 1.0.2i to address security vulnerabilities. [ZF-15764]
- 802.11r Fast BSS Transition can no longer be enabled when WLAN type is Autonomous. [ER-5135]

Caveats, Limitations, and Known Issues

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

Known Issues

General

- When Ekahau tag detection is enabled, the AP encapsulates tag frames in TZSP and UDP, but the TZSP header is incorrectly encapsulated with the protocol byte set to the wrong value and device type bytes missing in the 802.11 data field. [ZF-15992]
- MAC Authentication Bypass on ZF 7055 wired ports does not work when a Management IP address is enabled. [ZF-15335, ER-3789]

  Workaround: Disable the “Default gateway is connected with this interface” option.
- Some web pages are not completely translated into all languages supported by the new web user interface. [ZF-17158]
- QoS Null Data frames cannot be captured by Ruckus AP’s packet capture using Wireshark with its default settings. [ZF-16840]
- With Ruckus AP R720 when in sniffer mode, the Phy type, bandwidth and data rate elements are decoded incorrectly. [ZF-16839]
- Zero-IT provisioning file is not properly downloading for some Android clients running older versions of Chrome browser. [ZF-16771]
- 160 MHz and 80+80 MHz channelization options are not available in AP group settings. [ZF-16584]

  Workaround: Configure 160 / 80+80 MHz channelization for specific APs from the AP settings.

R720

- 160 MHz channelization is only available in 2x2:2 mode.
- On APs that support 160/80+80 MHz channelization (R610 and R720), Smart Mesh is currently unsupported if the AP is configured with either 160 or 80+80 MHz channelization. Mesh is supported for all other channelization modes. [AP- 4425]
- LACP bonding of Eth1 and Eth0 is not supported in the initial R720 GA release. [SCG-64854]
- Configuring static link speed on the R720’s 2.5G Ethernet port using Ruckus AP CLI command is not supported. The port will auto-negotiate to 2.5Gbps/1000Mbps/100Mbps rates. [SCG-63519]
- When an AP running the solo image configured to use 80+80 MHz channelization attempts to join a ZoneDirector, it will reboot repeatedly. [ZF-17061]

  Workaround: Set channelization to 80 MHz, or factory reset the AP before migrating it to ZoneDirector.
- 160/80+80 MHz requires two chains for Tx and Rx. In 802.3af mode, there is only sufficient power to enable one Tx chain on 2.4 GHz and 5 GHz on R720. Due to this constraint, the AP will effectively operate in 80 MHz channelization mode even if it is configured to operate in 160/80+80 MHz mode. [ZF-16890]
- 802.1x operation of the Eth1 (PoE) interface may not operate in supplicant or authenticator mode. [SCG-67078, SCG-67079]
- In 80+80 channelization mode, Channel 138 is unable to detect radar so this channel has been removed from the supported AP channels. However, channels 132-144 might still be visible on the SmartZone web interface. [SCG-66704]
- Sensitive 2.4GHz clients might get disconnected from the AP. This issue occurs because of baseband timeouts, which cause clients to reconnect or roam. Enabling the OFDM-only option reduces these client reconnects or roams. [SCG- 66325]
- SpeedFlex uplink test results are lower than actual. The performance deviation can be as high as 30%. [SCG-64611]
- TCPDUMP via AP Shell on Eth1 fails to capture LLDP packets. To capture LLDP frames, Ruckus Wireless recommends performing port mirroring on the AP interconnect switch port. [SCG-64323]
- The PoE switch port must run link layer discovery protocol (LLDP) power over Ethernet/MDI (PoE+) in order for the R720 to operate in AT-power mode (802.3at). This may require enabling both LLDP and Power via MDI (dot3) on the switch, if available. When operating with an 802.3af-only capable switch, the AP radios will operate in suboptimal (1x4) mode.

The following table lists the R720's power modes and the corresponding feature set under the different power modes.

PoE Mode	Power Level	5GHz Radio	2.4GHz Radio	2.5G Eth Port	1G Eth Port	USB	160/ 80+80
DC	Full Power	4 x 4	4 x 4	2500M/ 1000M/ 100M	10M/100M/ 1000M	0.5 W	Yes 2 x 2
802.3af	15.4 W	1 x 4	1 x 4	2500M/ 1000M/ 100M	X	X	No
802.3at	25.54 W	4 x 4	4 x 4	2500M/ 1000M/ 100M	X	X	Yes 2 x 2

Bonjour Fencing

- Background scanning and rogue AP detection take some time when performing neighbor AP updates. The amount time varies depending on the scanning frequency, the physical environment and other factors. As a result, Bonjour services provided by a neighbor AP may not be discoverable by wireless users immediately.
- For wired fencing, only one wired rule can be configured per Bonjour service in each Bonjour fencing policy. [ZF-16911]
- Services coming from Bonjour fencing-disabled APs cannot be fenced.
- Bonjour fencing of Chromecast services is not supported in this release.
- Bonjour fencing is not supported on Mesh APs in this release.
- Bonjour fencing is not supported for tunneled WLANs in this release.

RUCKUS™
an ARRIS company

350 West Java Dr. Sunnyvale, CA 94089. USA
www.ruckuswireless.com