RELEASE NOTES

Ruckus ZoneDirector 10.3 Release Notes

Supporting ZoneDirector 10.3

Part Number: 800-72158-001 Rev A
Publication Date: July 2019

Copyright, Trademark and Proprietary Rights Information

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, CommScope, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, and ZoneFlex are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

About This Release

This document provides release information on ZoneDirector release 10.3, including new features, enhancements, known issues, caveats, workarounds, upgrade details and interoperability information for version 10.3.

NOTE
By downloading this software and subsequently upgrading the ZoneDirector and/or the AP to version 10.3, 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 **10.3.0.0.362** supports the following ZoneDirector models:

- ZoneDirector 1200

NOTE
ZoneDirector 3000 is discontinued as of this release and cannot be upgraded to version 10.3 or any later release.

ZoneDirector version **10.3.0.0.362** supports the following Ruckus Access Point models:

Indoor AP	Outdoor AP
C110	T300
E510	T300e
H320	T301n
H510	T301s
R310	T310c
R320	T310d
R500	T310n
R510	T310s
R600	T610
R610	T610s
R700	T710
R710	T710s
R720	
R730	

Upgrading to This Version

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

Officially Supported 10.3 Upgrade Paths

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

- 10.1.0.0.1515 (10.1 GA)
- 10.1.1.0.26 (10.1 MR1)
- 10.1.1.0.35 (10.1 MR1 Refresh 1)
- 10.1.1.0.42 (10.1 MR1 Refresh 2)
- 10.1.1.0.55 (10.1 MR1 Refresh 3)
- 10.1.1.0.79 (10.1 MR1 Refresh 4)
- 10.1.2.0.120 (10.1 MR2)
- 10.1.2.0.210 (10.1 MR2 Refresh 1)
- 10.1.2.0.251 (10.1 MR2 Refresh 2)
- 10.2.0.0.189 (10.2 GA)
- 10.2.1.0.75 (10.2 MR1)

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

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

> **NOTE**
> For information and detailed instructions (including video tutorials) on upgrading ZoneDirector, visit the Ruckus Support How-To Hub at https://support.ruckuswireless.com/how-to-hub.

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.

Enhancements

This section lists the enhancements and new features that have been added in this release.

- R730 Enhancements

  5 GHz mesh support
- URL Filtering

  URL filtering allows administrators to manage internet usage by preventing access to inappropriate websites using a customizable combination of blacklists and whitelists.
- WPA3 Support

WPA3 is the latest secure Wi-Fi encryption standard that provides several security enhancements over WPA2. The WPA3 standard was announced by the Wi-Fi Alliance in 2018, and is not yet widely supported on client devices. As more devices appear on the market, WPA3 is expected to gradually replace WPA2, just as WPA2 replaced WPA.

- Shared DPSK

  This feature allows a single DPSK to be shared among multiple devices. By default, a single DPSK is bound to a single MAC address. This feature allows admins to override this rule and allow a single DPSK to be used by multiple client devices.

- ARC Engine Enhancement

  The Application Recognition engine has been upgraded to a new system with improved application detection.

- Removed ZoneDirector 3000 Support

  ZonDirector 3000 is discontinued as of this release and cannot be upgraded to release 10.3 or later. As of this release, ZoneDirector 1200 is the only model supported.

- LACP Control

  The ZoneDirector web interface now provides controls for configuring Link Aggregation Control Protocol (LACP) on AP models that support Ethernet port link aggregation.

  This feature is only supported on R610, R710, and R720 APs.

- New Upgrade Mechanism

  Enhanced the upgrade process to allow upgrading from any release to the current release, rather than limiting upgrades to N-2 releases. The N-2 limitation remains for upgrading to version 10.3, but beginning with release 10.3, future upgrades can be performed directly (for example, upgrading directly from 10. 3 to 10.6 or 10.7 will be supported).

- UI Enhancements:
  - Client Performance Chart update
  - VLAN Pooling and other Tabs in WLAN Global Selection
  - SMS Gateway Customization

    Additional country code options can now be configured for custom SMS servers.
  - WLAN Profile Edit Option
  - Display Debug Logs Download Progress

    A progress indicator now indicates the download progress when downloading debug logs to a local computer.
  - Display Upload Progress on Upgrade Page

    A progress indicator now indicates the upload progress when uploading a new firmware image file to ZoneDirector on the Upgrade page.
  - Hotspot UI enhancement

- GDPR: Right to Know and Right to Delete

  Enables compliance with the EU's General Data Protection Regulation "right to know" and "right to delete" rules for protection of client data.

- Separate Client Flow Data Logging to Syslog Server

  A new option is available for syslog delivery: "Client Flow Data Only," which allows admins to separate client flow data from other syslog messages and send those messages only.

- Security Enhancements:
  - New CLI Command to disable TLS 1.1
  - Disabled HTTP Options/Delete method on ZoneDirector

  - Upgraded sftpd to latest version to address “CVE-2011-0762”and “CVE-2015-1419”
  - Upgraded Dropbear to 0.76
  - Enhanced shell access algorithm to prevent brute force attacks

    NOTE
    For information on security incidents and responses, see *https://www.ruckuswireless.com/security*.

- Load Balancing Threshold Enhancement

  Optimized the default client count thresholds for load balancing across 2.4 and 5 GHz radios.
- Transient Client Management

  Reduces the impact of clients quickly passing by in high traffic environments. Enable this option to allow the AP to delay client association to a wireless LAN for a brief time to prevent passers-by from unintentionally joining the network.
- Min Client RSSI

  Network administrators can manually set a minimum client RSSI threshold below which client association requests will be refused.
- 5.8 GHz C-band channel support for R310, R510, R710 and R320 in United Kingdom (GB)

Resolved Issues

This section lists the customer-reported issues that have been resolved in this release.

- Resolved an issue with Support Entitlement license display errors. [ER-4848]
- Resolved an issue where certain VOIP clients were unable to connect to a WPA2 WLAN on R610/R710 APs. [ER-7151]
- Resolved an issue where BSS Minrate was not configurable when the UI language was set to Dutch. [ER-7411]
- Resolved an issue with Mesh APs having difficulty connecting to a Root AP when ChannelFly was enabled and automatic mesh uplink selection was enabled. [ER-7204]
- Resolved an issue with R300/R500 APs that were not properly implementing the DHCP backoff algorithm per RFC-2131. [ER-7259]
- Resolved an AP kernel panic issue on R720 APs that could cause the AP to reboot sporadically. [ER-7252]
- Resolved an R500 AP issue where the AP would randomly disconnect and require a factory reset before being able to reconnect. [ER-7225]
- Resolved an AP issue with "Singapore" country code where DFS channels were not listed in the supported channel list for certain AP models. [ER-7247]
- Resolved a kernel panic issue on APs located in high density environments when associated wireless clients were frequently roaming in and out of range. [ER-6689]
- Resolved an issue on 11ac Wave 1 APs where unsupported data rates were used to send the first data packet to a wireless client over the 5 GHz radio. [ER-7018]
- Resolved an issue where the switch reports two MAC addresses of AP R720. [ER-6901]
- Resolved an issue where the password was displayed in clear text when using openSSH followed by any command to login to the AP CLI. [ER-7078]

Caveats, Limitations and Known Issues

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

Issue	ZF-20077
Description	When both URL filtering and application recognition are enabled for a WLAN, application recognition statistics may be incorrect because traffic that is categorized by the URL filtering feature is not counted by the application recognition engine.

Issue	ZF-20205
Description	Secure FTP upload of GDPR reports is not supported.

Issue	ZF-20186
Description	GDPR commands do not support all MAC address formats. Supported MAC address formats: • aa-bb-cc-dd-ee-ff • aa:bb:cc:dd:ee:ff • AA-BB-CC-DD-EE-FF • AA:BB:CC:DD:EE:FF Unsupported MAC address formats: • aabbccddeeff • AABBCCDDEEFF

Issue	ZF-19481
Description	User may not be able to apply Device Access Policy rules for Amazon Kindle OS devices, as the relevant option is not available.

Issue	ZF-19369
Description	Some clients, including Google Pixel and Nexus 6P phones, do not provide the client host name information in DHCP requests and are therefore not properly identified by the client fingerprinting feature.

Issue	ZF-20631
Description	R730 Mesh APs will reboot after two minutes if they are unable to find an uplink AP, which prevents the AP from broadcasting the recovery SSID.

Issue	ZF-20472
Description	Client fingerprinting does not properly identify Ubuntu wireless clients as Linux OS/ Type when the WLAN encryption method is WPA3.

Issue	ZF-20401
Description	R730 APs may exhibit false radar detection on DFS channels when the country code is GB or DE, resulting in DFS channels not being able to be used. Work around: If this issue is observed in the customer environment, the DFS channels can be disabled to avoid the use of those channels.

R730 Feature Limitations

The following features are unsupported in this release:

- MU-MIMO
- ATF/BSSP
- OFDMA
- 160Mhz and 80+80 Mhz BW on 5G radio
- 2.4G MESH
- LACP
- Onboard BLE/Zigbee is not supported
- TxBF
- Spectrum Analysis
- Zero-touch mesh

R730 Power Modes

The R730 can be powered by 48V DC power, or 802.3at or 802.3at+ PoE (Power over Ethernet) switch or PoE injector. 802.3af PoE is *NOT* supported. Refer to the following table for power modes supported, and AP limitations when powered with sub-maximum power supply.

NOTE
The 5 Gbps PoE In port supports auto-negotiation with support for the following speeds: 100/1000/2500/5000 Mbps.

NOTE
The PoE switch port must run link layer discovery protocol (LLDP) power over Ethernet/MDI (PoE+) in order for the R730 to operate in full-power mode. This may require enabling both LLDP and Power via MDI (dot3) on the switch, if available.

Power Mode	2.4 GHz Radio		5 GHz Radio		5 Gbps Eth Port	1 Gbps Eth Port	USB Port	Comments
	Tx/Rx chains	Tx/Rx streams	Tx/Rx chains	Tx/Rx streams				
DC	4/4	4/4	8/8	8/8	Enabled	Enabled	Enabled (3W limit)	Requires 35W power
802.3af PoE **(not supported)**	N/A	N/A	N/A	N/A	N/A	N/A	N/A	**Not Supported**
802.3at PoE switch	4/4	4/4	4/8	4/4	Enabled	**Enabled**	Enabled (0.5W limit)	
802.3at+ PoE switch	4/4	4/4	8/8	8/8	Enabled	Enabled	Enabled (3W limit)	Requires 35W power
PoE injector Model GRT-480125A (In GUI select POE operation mode = AT+)	4/4	4/4	8/8	8/8	Enabled (1 Gbps speed)	Enabled	Enabled (3W limit)	Injector model GRT-480125A is rated only for 1Gbps speed. If POE operating mode = Auto, POE injector will power AP

Power Mode	2.4 GHz Radio		5 GHz Radio		5 Gbps Eth Port	1 Gbps Eth Port	USB Port	Comments
								in AT mode only.

Client Interoperability

ZoneDirector and Ruckus APs use standard protocols to interoperate with third-party Wi-Fi devices. Ruckus 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 10.9.5
- Mac OS 10.10
- Mac OS 10.11
- Mac OS 10.12
- Mac OS 10.13

Smartphone/Tablet OS

- iOS (6.1, 7.0, 7.1, 8.1, 8.4, 9.2, 9.3,10.0,10.2,10.3,11.1/2/3/4,12.0)
- Android (4.1.2, 4.2.2, 4.3, 4.4.2, 4.4.4, 5.0.1, 5.0.2, 5.1, 6.0, 7.0, 7.1.1, 8.0)
- Windows Phone (7, 8, 8.1, 10)
- BlackBerry OS (10, 10.3.2) not supported with Zero-IT
- Chrome OS (47.0, 49.0) not Supported with Zero-IT

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

	WPA2 WLAN			802.1x EAP (external Radius Server)		
OS	**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)
iOS 10 .0	Y	Y	N (ZF-2888)	Y	Y	N (ZF-2888)
iOS 10 .2	Y	Y	N (ZF-2888)	Y	Y	N (ZF-2888)
iOS 10 .3	Y	Y	N (ZF-2888)	Y	Y	N (ZF-2888)
iOS 11.x	Y (ZF-19663)	Y (ZF-19663)	N (ZF-2888)	Y (ZF-19663)	Y (ZF-19663)	N (ZF-2888)
iOS 12.0	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)
Mac OS 10.12	Y	Y	Y	Y	Y	N (ZF-4699)
Mac OS 10.13	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
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
Android 6.0	Y (ZF-19664)	Y	Y	Y (ZF-19664)	Y	Y
Android 7.0	Y (ZF-19664)	Y	Y	Y (ZF-19664)	Y	Y
Android 7.1.1	Y (ZF-19664)	Y	Y	Y (ZF-19664)	Y	Y

TABLE 1 Zero-IT Compatibility (continued)

Android 8.0	Y (ZF-19664)	Y	Y	Y (ZF-19664)	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 Known 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]