Ruckus Wireless™ ZoneDirector™ 10.0 GA (Supporting the H320 AP)

Release Notes

Part Number 800-71689-001 Rev C
Published August 2017

www.ruckuswireless.com

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. 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, ZoneFlex, FlexMaster, ZoneDirector, SmartMesh, ChannelFly, SmartCell, Dynamic PSK, and Simply Better Wireless 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

Copyright Notice and Proprietary Information

1 About This Release

Introduction 4

2 Supported Platforms and Upgrade Information

Supported Platforms 5

Access Points 5

Upgrading to This Version 7

Officially Supported Upgrade Paths 7

3 Adding a New AP Model in Release 10.0

4 Enhancements and Resolved Issues

New Access Points 10

Enhancements 10

Resolved Issues 13

5 Caveats, Limitations, and Known Issues

Known Issues 14

H320 14

General 14

R720 15

Bonjour Fencing 16

6 Interoperability Information

Client Interoperability 18

PC OS: 18

Smart Phone/Tablet OS: 18

Officially Supported Browsers: 18

Zero-IT Compatibility with Client Devices 19

Client Interoperability Issues 20

About This Release

1

Introduction

This document provides release information on ZoneDirector release 10.0, including new features, enhancements, known issues, caveats, workarounds, upgrade details and interoperability information for version 10.0.

NOTE: By downloading this software and subsequently upgrading the ZoneDirector and/or the AP to version 10.0, 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

2

Supported Platforms

ZoneDirector version **10.0.0.0.1451** supports the following ZoneDirector models:

- ZoneDirector 1200
- ZoneDirector 3000
- ZoneDirector 5000

Access Points

ZoneDirector version **10.0.0.0.1451** 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 ZoneDirector build **10.0.0.0.1451**:

- 10.0.0.0.1424

Adding a New AP Model in Release 10.0

3

This ZoneDirector AP patch release (build 10.0.0.0.1451) supports the registration of new AP models that were not yet available when this ZoneDirector version was released.

NOTE: Before starting this procedure, verify that the controller is running release 10.0.

NOTE: To support this H320 Patch, ZoneDirector 10.0 GA build 10.0.0.0.1424 is recommended.

NOTE: Before uploading a new AP patch, Ruckus Wireless strongly recommends saving a configuration backup. If you need to restore the controller to the previous AP patch, you can use this backup file.

NOTE: Importing an AP patch will auto reboot the ZoneDirector to affect the patch, temporarily disconnecting APs (and any associated clients) from the network. To minimize network disruption, Ruckus Wireless recommends performing the upgrade procedure at an off-peak time.

NOTE: Upgrading ZoneDirector to a new release deletes all imported AP patches (although the new release will include native support for new AP models). Depending on whether the new release provides native support for your APs, you may need to install required AP firmware patches after upgrading ZoneDirector firmware.

When Ruckus introduces a new AP model, an AP firmware patch is made available for download from the Ruckus Support website. Simply download the patch file to a local computer, import it into ZoneDirector, and the new AP model is now supported. No other APs will be impacted by the patch.

Follow these steps to register a new AP model with the controller:

1. Download the AP patch file from the Ruckus Support site that will enable the controller to support the new AP model (for example, H320-10.0.0.0.1451-ap-arm-dakota.tar.bz2.encrypted).
2. Download the patch file, and the save or move the patch file to a location that you can access from the computer that you are using to access the controller's web interface.
3. Log on to the controller's web interface as Super Admin.
4. Go to **Administer > Upgrade**.
5. Under the *AP Patch Firmware* section, click **Browse**.
6. Browse to the location where you saved the upgrade package, and then click **Open**.
7. Click **Upgrade**. The controller adds H320 to AP release 10.0.0.0.1451. (H320 is added to the Administer > Upgrade page under Current Software).
8. After the controller completes upgrading, connect the new AP model to the network.The new AP model registers with the controller, and then the controller upgrades the AP firmware to release 10.0.0.0.1451.
9. Go to the **Monitor > Access Points** page, and then verify that the new AP model you added to the controller is listed in the **Currently Managed APs** table.
10. Under the **Status** column, verify that new AP model is not "Approval Pending." If it is Approval Pending, **Allow** it in the Action column.
11. You have completed adding a new AP model to the controller.

NOTE: The full network upgrade is successive in sequence. After ZoneDirector is upgraded, it will contact each active AP, upgrade it, and then restore it to service.

NOTE: The AP uses FTP to download firmware updates from ZoneDirector. If you have an access control list (ACL) or firewall between ZoneDirector and the AP, make sure that FTP traffic is allowed to ensure that the AP can successfully download the firmware.

Enhancements and Resolved Issues

4

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: 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 Known Issues 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 has 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 admins 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 reconfiguring 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 admins 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 R610
- 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

- Upgraded Dropbear version to 2016.74 to address security vulnerabilities. [ER-5033]
- 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 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 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

5

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

Known Issues

H320

- None.

General

- There is a known issue with build 10.0.0.0.1424 that could cause a ZoneDirector that is not offered an IPv4 address from a DHCP server or assigned a static IP address to incorrectly assign itself the address 192.168.0.1, rather than the default address 192.168.0.2 that it is supposed to use. [ZF-17268]

  Workaround: Either have a DHCP server assign an IP address or statically configure an IP address on the ZoneDirector.
- 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 UI languages in the new UI. [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 inter-connect 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.

Table 1. R720 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.

Interoperability Information 6

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 10.9.5
- Mac OS 10.10
- Mac OS 10.11.3
- Mac OS 10.12.2

Smart Phone/Tablet OS:

- iOS (6.1, 7.0, 7.1, 8.1, 8.4, 9.2, 9.3, 10.0, 10.2, 10.3)
- 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) - Zero-IT Not supported
- Chrome OS (47.0, 49.0) - Zero-IT Not Supported

Officially Supported Browsers:

- Internet Explorer 10, 11
- Firefox 34 and later
- Chrome 39 and later

Zero-IT Compatibility with Client Devices

Table 2. 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)
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 10.12.2	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

Table 2. Zero-IT Compatibility

	WPA2 WLAN			802.1x EAP (external Radius Server)		
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	Y	Y	Y	Y	Y
Android 7.0	Y	Y	Y	Y	Y	Y
Android 7.1	Y	Y	Y	Y	Y	Y
Android 8.0 (DV)	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]

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