RELEASE NOTES

Ruckus ZoneDirector Release Notes For E510

Supporting ZoneDirector 10.1

Part Number: 800-71845-001 Rev A
Publication Date: March 2018

Copyright, Trademark and Proprietary Rights Information

© 2018 ARRIS Enterprises LLC. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from ARRIS International plc and/or its affiliates ("ARRIS"). ARRIS reserves the right to revise or change this content from time to time without obligation on the part of ARRIS to provide notification of such revision or change.

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, ARRIS 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. ARRIS 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. ARRIS 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 ARRIS 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 ARRIS, ARRIS 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 ARRIS 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, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, ZoneFlex are trademarks of ARRIS International plc and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access (WPA), the Wi-Fi Protected Setup logo, and WMM are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are 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 10.1, including new features, enhancements, known issues, caveats, workarounds, upgrade details and interoperability information for version 10.1.

NOTE
By downloading this software and subsequently upgrading the ZoneDirector and/or the AP to version 10.1, 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 10.1.0.0.1515 supports the following ZoneDirector models:

- ZoneDirector 1200
- ZoneDirector 3000

NOTE
ZoneDirector 5000 is discontinued as of this release, and cannot be upgraded to version 10.1 or later.

Access Points

ZoneDirector AP Patch version 10.1.0.0.1527 supports the following Access Point models:

- E510*
- T310c
- T310d
- T310n
- T310s

NOTE
*This patch release adds support for new AP: E510.

Upgrading to This Version

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

AP Bundle Upgrade Paths

This AP Bundle can be applied to the following ZoneDirector release build(s):

- 10.1.0.0.1515 (10.1 GA) or above

If you are running an earlier version, you must upgrade ZoneDirector to the 10.1 GA release build (build 1515 or above) before installing this AP bundle (build 1527).

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

Adding a New AP Model

ZoneDirector 10.1 release supports the registration of new AP models that were not yet available when this ZoneDirector version was released.

Before starting this procedure, verify that the controller is running release 10.1 (GA) or later.

> NOTE
> This procedure will restart ZoneDirector services. During the upgrade process, service outage will occur as the ZoneDirector will restart automatically to complete the upgrade.

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

1. Download the AP bundle patch file that will enable the controller to support the new AP model (*10.1.0.0.1527-E510T310.encrypted.patch*) from the Ruckus Support website.
2. Save the file to a location that you can access from the computer that you are using to access the controller's web interface.
3. Log in to the controller's web interface as Super Admin.
4. Go to the **Administer** > **Upgrade** page, and then click **Choose File** under **AP Patch Firmware**. Select the AP bundle patch file to upload.
5. Click **Upgrade** .

   The controller adds the E510 (and T310 series) to AP release 10.1.0.0.1527. (New AP models are added into *Administer > Upgrade* page under *Current Software*.)
6. 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 10.1.0.0.1527.
7. Go to the *Access Points* page, and then verify that the new AP model you added to the controller is listed under *Currently Managed APs*.
8. Under the **Status** column, verify that new AP model isn’t Approval Pending. **Allow** it from the **Action** column if it is Approval Pending.

You have completed adding a new AP model to the controller.

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: E510

  The E510 is a modular outdoor AP designed for installation in scenarios where the Wi-Fi intelligence and the antenna modules must be physically separated, such as light poles, light fixtures, street furniture, railway carriages and track side installations.

Enhancements and New Features

This section lists the new features and enhancements in this release.

- New UI – Phase 2

  This release introduces the second stage of the new redesigned web interface, which highlights network health and traffic statistics visibility, and includes several enhancements to the overall UI organization and user-friendliness.

- Adaptive Band Balancing

  This feature enhances the existing Band Balancing feature by allowing client redistribution dynamically after association, rather than only once during the initial association.

- Additional SMS Service Provider Support

  Customers can now configure a custom SMS service provider for delivering alarms and guest passes, in addition to the existing Twilio and Clickatell SMS provider options.

- Client Connection Troubleshooting

  This feature is designed to help customers diagnose wireless client connection issues to determine why a client fails to connect to the wireless network.

- Multiple Social Media Logins on the Same WLAN

  Existing Social Media login methods (Facebook, Google, LinkedIn and Microsoft) can now be used simultaneously on the same WLAN.

- WeChat Support

  A new social media WLAN type – WeChat – is now available.

- Social Media Login Scale Enhancement

  Enhanced the scaling capabilities of Social Media WLANs.

- Role-Based Application Recognition and Control

  Application Recognition and Control (ARC) features can now be applied to users based on user role, in addition to the existing per-WLAN configuration. Role-based application policies take precedence when both role-based and WLAN-based policies exist.

- Source IP/Port-Based Access Control Lists

  Customers can now configure ACLs to allow or deny access to wireless clients from an external source IP address or port.

- LWAPP Tunnel Performance Enhancement

  This enhancement improves the performance of tunneled WLAN traffic by reducing some time-consuming operations in the Ruckus GRE tunnel module.

- Ability to Export DPSK Records

  The Dynamic PSK Batch Generation page now provides an additional option to download generated DPSK records.

- Recovery SSID Enhancement

  Enhanced the AP configure and recovery SSIDs to allow remote wireless configuration of newly installed APs and recovery of isolated mesh APs.

- Client Flow Data Logging

  This feature allows ZoneDirector to transmit client session data to a syslog server for use in legal obligation compliance for Hotspot service providers in certain countries, or for emerging Wi-Fi monetization projects, where the ability to export session data could be useful for marketing or for use by a third-party platform.

- DTIM, Directed Multicast, and RTS-CTS Configuration Options

  The following new configuration options are available for configuring advanced wireless settings: DTIM, Directed Multicast/ Broadcast Threshold, and Protection Mode.

- New SNMP OID Support

  Several new SNMP OIDs have been introduced for configuring 802.11d and BSS Minrate settings.

- Bonjour Fencing Enhancement

  This release enhances the functionality of the Bonjour Fencing feature by allowing fencing policies to be deployed on multiple wired devices.

- End of Support for ZoneDirector 5000

  ZoneDirector 5000 is discontinued as of this release, and cannot be upgraded to version 10.1 or later.

- Disabled TLSv1.0

  TLSv1.0 has been disabled in this release due to security concerns, and ZoneDirector now supports only TLSv1.1 and v1.2. For information on security incidents and responses, see https://www.ruckuswireless.com/security.

Resolved Issues

- 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 the max clients limit was not enforced on Autonomous WLANs when an AP was disconnected from ZoneDirector. [ER-3887]

Caveats, Limitations and Known Issues

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

E510 AP

- When a Ruckus Beamflex antenna (Part Number: 902-2101-0000) is connected, users must *disable* the "external" antenna setting in the AP/AP group configuration. When a non-Beamflex antenna (for example, Part Number: 911-0505-DP01, or third-party antenna) is used, users must *enable* the external antenna check boxes and configure gain values according to calculated cable loss, etc.
- An AP reboot is required when enabling and disabling the non-Beamflex antenna (Part Number: 911-0505-DP01). [SCG-81588]
- AP Tx power is not reverting to default values after applying non-Beamflex antenna (Part Number: 911-0505-DP01) gain and switching back to a Beamflex antenna (Part Number: 902-2101-0000).

  Workaround : Set 3 dBi for 2.4 GHz and 5 dBi for 5 GHz, apply the configuration and disable the non-Beamflex antenna (Part Number: 911-0505-DP01). Another option is to factory reset the AP. [SCG-81705]

General

- Some new or modified UI pages have not been fully translated into all available UI languages. [ZF-17158, ZF-18280, ZF-18230]
- Apple iOS 11.x clients are unable to connect to an 802.1x WLAN using Zero-IT in some situations due to changes in the way iOS 11 handles TLS connections. [ZF-18254]
- When running the R720 AP in sniffer mode, the Phy type, bandwidth and data rate elements are decoded incorrectly. [ZF-16839]
- R720 APs are unable to properly fence Bonjour services when Bonjour Fencing is enabled on the AP. [ZF-18314]
- BSS Fast Transition roaming is not working properly for Google Pixel and Sony Z5 clients. [ZF-18319]
- Client Fingerprinting does not properly display the Host Name for some clients, including some Android 8.0 and Chrome OS clients. [ZF-18143]
- For APs that were upgraded to 10.1 from a previous release, the uniform recovery SSID passphrase will continue to use the previous format until after a factory reset (e.g., "ruckus-<admin password>"), instead of the new passphrase format ("<admin-password>"). [ZF-18625]
- Northbound Portal interface may be incompatible with some versions of curl or python. [ZF-18649]
- Mac OS clients may fail to be redirected to the intended URL after authentication to a Facebook WLAN. [ZF-18607]
- Spectrum Analysis on the 5 GHz radio may fail to run on some outdoor APs in certain situations due to an error that prevents the AP from changing to certain channels correctly. [ZF-18573]
- Nexus 5X clients will not connect to dot1x Zero-IT profiles using the Android Zero-IT app. [ZF-18252]