RELEASE NOTES

ZoneDirector Version 9.10.2 Refresh 5 Release Notes

Supporting ZoneDirector Release 9.10.2 Refresh 5

Part Number: 800-72118-001 Rev A
Publication Date: December 2018

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, 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 9.10.2, including new features, enhancements, known issues, caveats, workarounds, upgrade details and interoperability information for version 9.10.2.

By downloading this software and subsequently upgrading the ZoneDirector and/or the AP to version 9.10.2, 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

ZoneDirector version **9.10.2.0.73** supports the following ZoneDirector models:

- ZoneDirector 1100
- ZoneDirector 1200
- ZoneDirector 3000
- ZoneDirector 5000

Access Points

ZoneDirector version **9.10.2.0.73** supports the following Access Point models:

- H500 ***(ZoneDirector 1200, 3000, 5000 only. Not supported on ZD 1100)*
- R300
- R500
- R600
- R700
- SC8800-S
- SC8800-S-AC
- T300
- T300e
- T301n

- T301s
- ZF7055
- ZF7321
- ZF7321-u
- ZF7341
- ZF7343
- ZF7352
- ZF7363
- ZF7372
- ZF7372-E
- ZF7441
- ZF7761-CM
- ZF7762
- ZF7762-AC
- ZF7762-S
- ZF7762-S-AC
- ZF7762-T
- ZF7781CM
- ZF7782
- ZF7782-E
- ZF7782-N
- ZF7782-S
- ZF7982

NOTE
ZoneFlex 7025 APs are no longer supported as of 9.10, and cannot be upgraded to ZoneFlex version 9.10, 9.10.1 or 9.10.2.

NOTE
H500 is not supported on ZoneDirector 1100.

Upgrading to This Version

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

Officially Supported 9.10.2 Upgrade Paths

The following ZoneDirector builds can be directly upgraded to this ZoneDirector 9.10.2 Refresh release:

- 9.9.0.0.205 (9.9 GA release)
- 9.9.0.0.212 (9.9 GA refresh)
- 9.9.0.0.216 (9.9 GA refresh 2)
- 9.9.1.0.31 (9.9 MR 1 release)
- 9.9.1.0.40 (9.9 MR 1 refresh)

- 9.10.0.0.218 (9.10 GA release)
- 9.10.1.0.59 (9.10 MR 1 release)
- 9.10.2.0.11 (9.10 MR 2 release)
- 9.10.2.0.29 (9.10 MR 2 refresh)
- 9.10.2.0.41 (9.10 MR 2 refresh 2)
- 9.10.2.0.53 (9.10 MR 2 refresh 3)
- 9.10.2.0.63 (9.10 MR 2 refresh 4)

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

> **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.

Due to the enforcement of the Support Entitlement feature in ZoneDirector 9.10, Ruckus recommends upgrading to 9.10.2 from one of the above builds only.

You can also upgrade directly to 9.10.2 from one of the following 9.8 builds. However, you will be prompted to reset to factory defaults before the upgrade can continue. (This is not required when upgrading from 9.9 to 9.10.2)

9.8 builds that can be directly upgraded to 9.10.2 (requires factory default):

- 9.8.0.0.379 (9.8 GA)
- 9.8.1.0.101 (9.8 Maintenance Release 1)
- 9.8.2.0.15 (9.8 Maintenance Release 2)

Enhancements and Resolved Issues

This section lists the new features and enhancements in this release, and any customer-reported issues from previous releases that have been resolved in this release.

Enhancements

- Zero-IT support for Android 5.0 and 5.1.
- Client Fingerprinting for Android 6, iOS 9, Windows 10 and Windows 10 Mobile.
- Upgraded OpenSSL from version 1.0.1m 1.0.1q.
- Updated new FlexMaster SSL certificate into ZoneDirector. (Note: See for limitations related to new FM SSL certificate.)

Resolved Issues

Resolved Issues in Build 73

- Enhanced 802.1X authentication scalability and performance on ZoneDirector. [ER-6754]
- Resolved an AP kernel memory leak issue that could eventually lead to watchdog timeout reboots. [ER-3544/ER-6666]
- Added CLI command to disable/enable TLS1.0. [ER-6623]

- Resolved an issue where the following special characters would be disallowed when used in WPA2-PSK passphrases: "`","';", "%", "$", "&&", "||"). [ER-6875]
- Redefined the account-terminate-cause in accounting stop packets. [ER-6758]
- Resolved an issue where users attempting to authenticate to a Hotspot WLAN 10 times within 5 minutes would be unexpectedly blocked by ZoneDirector. [ER-6978]

Resolved Issues in Build 63

- 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 client fingerprinting would fail to properly identify certain recent Android devices. [ER-5644]
- Resolved an issue where a ZoneDirector-managed network could be compromised if a rogue client associated to tunneled WLAN was used to spoof the gateway's MAC address. [ER-6471]
- Resolved an issue where newly created AP groups would fail to inherit Tx power settings from the System Default AP group. [ER-5586]
- Resolved an issue where no Groups would be associated when running Test Authentication using Mac OS X LDAP open directory server for web authentication. [ER-3063]
- Added "Ruckus-Location" attribute in RADIUS request packets for 802.1x WLAN authentication. [ER-5880]
- Resolved an issue where RADIUS authentication with TLS encryption enabled would fail due to ZoneDirector's use of the default certificate instead of the newly imported certificate. [ER-6316]
- Resolved an issue where LDAP authentication would fail if extended ASCII characters were included in the account user name. [ER-6372]
- Resolved an issue where client fingerprint would not properly identify clients running Windows 10 version 1803. [ER-6414]
- Resolved an issue where client fingerprinting would not properly identify clients running Ubuntu version 17. [ER-6325]

Resolved Issues in Build 53

- 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 unauthorized clients connected to a guest WLAN could access the internet by encapsulating data traffic as DNS packets using a certain tool. [ER-5434]

Resolved Issues in Build 41

- Resolved an issue where ZoneDirector would send incorrect input/output octets in RADIUS Accounting packets. [ER-5354]
- 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 Issues in Build 38

- Resolved a roaming issue where some mobile clients would fail to roam smoothly between APs when connected to an 802.1X WLAN with a single client only RADIUS policy enabled. [ER-3340]

Resolved Issues in Build 34

- 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 issue that could cause ZoneDirector 5000 web process failure, resulting in failover to the standby ZoneDirector. [ER-4123, ER-5003]
- Upgraded Dropbear SSH server version to address a security vulnerability in earlier releases. [ER-4782]

Resolved Issues in Build 29

- 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 issue that could cause ZoneDirector 5000 web process failure, resulting in failover to the standby ZoneDirector. [ER-4123, ER-5003]
- Upgraded Dropbear SSH server version to address a security vulnerability in earlier releases. [ER-4782]

Resolved Issues in Build 22

- Resolved an issue that could cause APs to fail to reconnect to ZoneDirector for a long time after a Smart Redundancy failover. [ER-3890]
- Resolved an issue related to client isolation where devices connected to the 5GHz radio could not access the Internet. [ER-3489]
- Resolved an issue with RADIUS message "Acct-Output-Gigawords" values causing issues with billing systems. [ER-3893]
- Resolved an issue where ZF 7372 APs would not properly display results for SNMP queries. [ER-3677]
- Resolved a ZoneDirector 3000 issue that could cause the emfd process to hang when calling "fprintf()" in "get_QueueEvent" function. [ER-3926, ER-4375]

- Resolved an issue with Smart Redundancy ZoneDirectors that could cause flapping between active and standby modes during installation of new APs in rare conditions. [ER-1941]
- Resolved an issue that could potentially cause ARP entry leaks, which could eventually lead to ZoneDirector reboots. [ZF-15476]

Resolved Issues in Build 16

- Resolved an issue with the station manager process on ZoneDirector 3000 and 5000 consistently increasing memory usage, eventually leading to reboot. [ER-3275]
- Resolved an issue that could cause repeated HTTP redirect failures due to an invalid HTTP header without HTTP version string. [ER-3822]
- Resolved an issue where clients would be unable to pass traffic after roaming when Force DHCP is enabled on the WLAN. [ER-2900]
- Resolved an issue that could cause ZoneDirector to hang and require a reboot when the max clients limit was reached in extremely high density environments. [ER-2847]
- Resolved an issue that could result in GUI and SSH access unresponsiveness on ZoneDirector 5000 when 11,000 clients were connected. [ER-2807]
- Fixed the corner case causing the station manager process to hang as it runs out of request handlers by optimizing the timers to quickly release the request handlers. [ER-2974]
- Resolved an issue where when WLAN 102 is deleted from the AP, then WLAN 100 would fail to report location data to SPoT. [ER-4201]

Resolved Issues in Build 11

- Removed country codes Korea2 and Korea3. [ER-2451]
- Resolved a security issue related to Logjam attack. Please see www.ruckuswireless.com/security for security incidents and responses. [ER-2647]
- Resolved an issue with incorrect values for some SNMP MIBs. [ER-2838]
- Resolved an issue where, when using 802.1x with VLAN Pooling and moving between APs, the device loses its dynamically assigned VLAN and defaults to the WLAN's Access VLAN. [ER-2784]
- Resolved an issue where EAPSIM clients were unable to connect. [ER-823]
- IPv6 addresses are now properly displayed on the client monitoring page. [ER-2963]
- Resolved an issue with printing customized Guest Passes when using Firefox and Chrome browsers. [ER-3000]
- Resolved an issue where iOS devices could be unable to access the network access when Force DHCP is enabled. [ER-2933]
- Multiple SPoT venues can now be configured with the same FQDN. [ZF-14033]
- Resolved an issue where the SNMP MIB "ruckusZDWLANAPRadioStatsResourceUtil" would return incorrect values. [ER-3047]
- Resolved an issue where the SNMP MIB "ruckusZDSystemStatsWLANTotalRxErrFrm" would return incorrect values. [ER-2649]
- Resolved an issue with VLAN pool address assignment after roaming. [ER-3025]
- The SNMP value for maximum number of stations on ZoneDirector 3000 now properly returns 10,000. [ER-3074]
- Resolved a DST error with GMT+1 (Brussels Time) time zone that could cause the time displayed to be off by an hour. [ER-3194]

- Resolved an issue with Zero-IT support for Android 5.0 clients. [ZF-14649]
- Resolved a Hotspot redirect issue in high retransmission environments where clients could intermittently fail to be redirected to the Hotspot login page. [ER-2913]
- Resolved an issue where the packet capture feature on solo APs was disabled. [ER-2802]
- Resolved an issue where the AP was intercepting the wrong client IP address from malformed IP packets from the client. [ER-2290]
- Resolved an issue with incorrect values for some SNMP MIBs. [ER-2838]
- Resolved an issue that could cause the web interface and CLI interface to become unresponsive due to a support entitlement activation error. [ER-2896]
- The "Framed-IP-Address" value is now included in Acct-Start packets in 802.1x WLANs on standalone APs. [FR-1626]
- Values for Airtime stats are now retrievable from standalone AP as well as ZoneDirector SNMP queries. [ER-2845]
- Client Fingerprinting now properly recognizes iOS 9 clients. [ZF-14502]
- Resolved an issue where APs could become unreachable due to an IP address conflict when a 192.168.50.0 subnet was used. [ER-2338]
- Device Access Policy now properly identifies Mac OS X "EI Capitan" clients. [ZF-14586]
- Removed an erroneous error message "Cannot notify kernel for Delete AP" from syslog messages. [ER-3141]
- Resolved an issue where executing the "fw check image" command resulted in "bad header magic" error messages. [ER-3270]
- Client Fingerprinting now properly identifies Windows 10 Mobile clients. [ZF-14656, ZF-14403]
- Client Fingerprinting now properly recognizes Android 6 clients [ZF-14717]
- Resolved an issue where when there were no packets in the queue for UAPSD clients, the client sent a trigger to the AP and the AP went into a loop in transmitting QoS NULL frames. [ZF-14907]
- Resolved an issue that could cause R500, R600 or T300 AP Ethernet ports to get stuck, thus causing the APs to remain disconnected from the network and to recover only after a reboot. [ER-2983]
- Resolved an issue that could cause Bonjour Gateway rules to fail to be applied in certain situations. [ER-3018]
- Resolved an issue where duplicate entries in the proxy ARP existed for the same MAC address, which led to network interruption for some clients in certain situations. [ER-3166]
- Resolved an issue with ZoneDirector XML data records sent to FlexMaster and SCI causing data dropouts. [ER-3290]
- Resolved an issue that could cause ZoneDirector 5000's system clock to drift from NTP time by about 5 seconds a day. [ER-2190]
- Resolved an issue that could result in APs rebooting when Open Auth with Dynamic VLAN was enabled. [ER-3122]
- Resolved an issue with the AP proxy ARP feature where IPv6 neighbor advertisement messages from the AP were incorrectly formatted. [ER-3113]
- Resolved an issue with loop detection on ZF 7025, 7055 and H500 APs. [ER-3098]
- Resolved an issue with H500 APs that would prevent the AP from using DFS channels with US country code. With this release H500 now supports all DFS channels in the 5 GHz band. [ER-2839]
- Resolved an issue that could prevent wireless printers from connecting to H500 APs when WPA/WPA2/WPA-Mixed encryption was enabled. [ER-3009]
- Resolved an issue where iOS 9-based Apple devices could not associate with hidden SSIDs when L2 MAC ACL was enabled. [ER-3186]
- Resolved an issue that could cause ZD 3000 to reboot due to an sqlitedTac.socket error. [ER-3295]
- Resolved an issue that could cause the AP to reboot as a result of kernel panic. [ER-2927]

- Resolved an issue in which very rarely clients associated with the 5GHz band on the R700 AP could not pass traffic. [ER-3161]
- Resolved an issue that could cause ZoneDirector to become unresponsive or reboot when autonomous WLANs were deployed and the connection between the AP and ZoneDirector was unstable or the AP or ZD was under heavy load. [ER-3157]
- Resolved an issue that could cause the ZoneDirector web interface to become slow or unresponsive in high query scenarios, such as when sending data to SCI, and concurrently handling many guest association/disassociation requests. [ER-3090]
- Resolved an issue where UEs associated with the 5GHz radio on the R710 AP were stuck in a paused state permanently. This issue was caused by the unavailability of TX descriptors. [ER-3175, ER-3318]

Caveats, Limitations and Known Issues

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

Ethernet Port Settings

ZoneFlex AP Ethernet ports can become disabled if half-duplex is forced on any port. [ID ER-1208, ER-1229]

This problem affects the following:

- ZoneDirector 1100
- ZoneFlex 7341
- ZoneFlex 7343
- ZoneFlex 7363
- ZoneFlex 7761
- ZoneFlex 7762

Workaround: Uplink switch ports must be set to 100Mbps auto-negotiation or 1000Mbps auto-negotiation.

Web Interface

ZoneDirector release 9.10.2 supports the following Web browsers:

- Firefox 31 and later
- Internet Explorer, 10, 11
- Chrome 36 and later

Chrome browser may fail to redirect to the authentication page for WISPr and Guest Access profiles when a user attempts to browse to a page that uses HTTP Strict Transport Security (HSTS).

Workaround: browse to a website that does not use HSTS, complete the authentication, then browse to any site. (ZF-10401)

- Google Chrome version 66 or later fails to redirect to the login page after a ZoneDirector upgrade or soft restart. [ZF-19441]

  Workaround: Manually enter the ZoneDirector IP address in the browser address bar and press enter to access the ZoneDirector web interface.

VLAN Pooling

When VLAN pooling (option 2 or 3) is enabled on an Open/None or 802.1X EAP WLAN, clients may fail to retain the same IP address and may be assigned to a different VLAN after roaming. [ZF-15063]

R500, R600, R700 and T300 Series APs

The following features are not included in this release:

- Airtime Fairness on 5 GHz radio
- Spectrum Analysis on 5 GHz radio
- WLAN Prioritization on 5 GHz radio

FlexMaster SSL Certificate

As a result of the new FlexMaster SSL certificate into ZoneDirector, ZoneDirector 9.10.2.0 will NOT work with FlexMaster 9.10.1 and prior versions. Customers who use FlexMaster to manage ZoneDirector will need to upgrade FlexMaster to 9.10.2 to continue to be able to communicate with ZoneDirector 9.10.2.

Ruckus Wireless, Inc., a wholly owned subsidiary of ARRIS International plc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com