Ruckus Wireless™ ZoneDirector™ Version 9.13.2

Release Notes

Copyright Notice and Proprietary Information

Contents

About This Release

1

Introduction

This document provides release information on ZoneDirector release 9.13.2, including new features, enhancements, known issues, caveats, workarounds, upgrade details and interoperability information for version 9.13.2.

> **NOTE**: By downloading this software and subsequently upgrading the ZoneDirector and/or the AP to version 9.13.2, 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

2

Supported Platforms

ZoneDirector version **9.13.2.0.33** supports the following ZoneDirector models:

- ZoneDirector 1200
- ZoneDirector 3000
- ZoneDirector 5000

Access Points

ZoneDirector version **9.13.2.0.33** supports the following Access Point models:

- H500
- H510
- R300
- R310
- R500
- R510
- R600
- R610
- R700
- R710
- T300
- T300e
- T301n
- T301s
- T710
- T710s
- ZF7055
- ZF7352

- ZF7372
- ZF7372-E
- ZF7781CM
- ZF7782
- ZF7782-E
- ZF7782-N
- ZF7782-S
- ZF7982

EoS (End of Sale) APs

The following AP models have reached end-of-sale (EoS) status and, therefore, are no longer supported in this release. If your ZoneDirector is currently managing any of these models, a warning will appear when you attempt to upgrade.

If your ZoneDirector is currently managing any of these models, do NOT upgrade to this release. ZoneDirector will be unable to manage them.

- 7321
- 7321-U
- 7441
- 7761-CM
- 7762 series
- 7363
- 7343
- 7341
- sc8800-s
- sc8800-s-ac

Upgrading to This Version

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

Officially Supported 9.13.2 Upgrade Paths

The following ZoneDirector builds can be directly upgraded to ZoneDirector build 9.13.2.0.33:

- 9.10.0.0.218 (9.10 GA)
- 9.10.1.0.59 (9.10 MR1)
- 9.10.2.0.11 (9.10 MR2)
- 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)
- 9.13.0.0.232 (9.13 GA)
- 9.13.1.0.11 (9.13 MR1)
- 9.13.1.0.26 (9.13 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

3

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: R610

  The R610 is the first Ruckus three stream (3x3:3) Wave 2 802.11ac dual-band concurrent indoor Access Point. The R610 expands Ruckus' portfolio of 11ac Wave 2 APs, providing all of the benefits of Wave 2 along with an extensive list of features such as dual gigabit ports with Link Aggregation, USB port for IoT devices, and flexible power options including 12VDC, 802.3at and 802.3af PoE/ PoE+ support.

  Note that if 802.3af PoE is used to power the R610, the feature set is reduced, as follows:

  - 2.4 GHz radio chains reduced to 2x3 (2-chain transmit at 21dBm aggregate power, 3-chain receive)

  - USB port disabled

  - 2nd Ethernet port disabled

Enhancements

- Mesh Enhancements

  This release adds the ability to control mesh mode via AP Group, and an additional uplink max hop selection option to provide better control of how Mesh APs in an AP group choose an uplink AP.

- SNMP Trap Filter Support

  SNMP traps can now be configured to send only the traps that are specifically enabled, rather than all traps. Each trap switch can be enabled/disabled individually using the MIB node under the ruckusZDEventTrapSwitchCmd MIB tree.

Additionally, all trap switches can be enabled/disabled at once using the MIB node: ruckusZDEventALLEventTrapSwitchCmd (1.3.6.1.4.1.25053.2.2.3.200).

Resolved Issues

- The "HTTPS Guest Portal" behavior change introduced in 9.13, which changed the delivery of guest access captive portal pages from HTTP to HTTPS, has been reverted in this release. In 9.13.2, captive portal pages are delivered via HTTP by default. To improve security, users can change the behavior via Guest Access configuration using the following ZD CLI commands:

  - Enable force HTTPS redirection for Guest WLANs

    ```
    ruckus(config)# guest-access-force-https-redirection
    ```

  - Disable force HTTPS redirection for Guest WLANs

    ```
    ruckus(config)# no guest-access-force-https-redirec-
    tion
    ```

- Improved mesh stability by enhancing the mesh keep-alive logic [ER-4096]

- Resolved an issue where running either snmpget or snmpwalk on an AP showed all interfaces have a maximum throughput of only 10mbps. [ER-4057]

- Resolved an AP reboot issue that was caused by a hardware watchdog timeout when DHCP server responds with 5 or more DNS server entries and client isolation was enabled. [ER-3988]

- Resolved a memory leak issue related to the mesh network process that could cause the APs to disconnect and be unable to reconnect. [ER-4265]

- Resolved an issue where AP OID ruckusRadioNoiseFloor was not retrievable thru SNMP. [ER-4188]

- Resolved an issue where the wifi driver stopped responding after the group key in a dynamic VLAN configuration was updated. [ER-4403]

- Resolved an issue where ZF7372 APs did not properly display results for SNMP queries. [ER-3677]

- Improved the timing of accessing the new certificate when the AP boots up, added more debug messages to help troubleshoot related issues, and enhanced status updates to the controller to reflect more accurate AP certificate fresh states. [ER-3671]

- Resolved a kernel memory leak issue on APs, which eventually caused watchdog timeout reboots. [ER-3544]

- Resolved an issue where inactive clients displayed on the client monitoring page would be cleared after refreshing the page when 24 hour time span was selected. [ER-4443]

- Resolved a cross-site scripting (XSS) vulnerability discovered in ZD release 9.9.1. For more information, see https://www.ruckuswireless.com/security for security incidents and responses. [ER-4275]

- Resolved an issue that could cause ZoneDirector to reboot due to an "rhttpc" process hang. [ER-4585]

- Resolved an issue where guest pass validity periods would be displayed inconsistently in email and print when compared to the validity periods displayed on the guest pass monitoring page. [ER-4577]

- Resolved an issue that would prevent the creation of Social Media WLANs if the ZD had been upgraded from a release prior to 9.9. [ER-4535]

Caveats, Limitations, and Known Issues

4

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

Known Issues

General

- H510 APs deployed as eMesh APs may in some situations become disconnected from ZD due to an AP manager process failure. [ZF-15770]

- The 11ac radio on H510 APs is incorrectly displayed as 11an on ZoneDirector monitoring pages. [ZF-15814]

- 5GHz radio information for 11ac APs that were discovered by ZD on an earlier release as unsupported APs is incorrectly displayed as "11a/n" after upgrading to 9.13.2. [ZF-16034]

  Workaround: Delete the APs and allow them to rejoin after upgrading.

- Clients with Dell Wireless 1830 802.11ac wireless cards may fail to join Ruckus APs after upgrading ZD to 9.13.2. This is apparently an issue with the client device driver, and Ruckus has not yet identified a workaround. [ZF-15938]

- 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]

- With Hidden SSID enabled, Samsung devices that support 802.11r are not performing 802.11r association (i.e., FT using PSK or FT using 802.1x association). This is apparently a client limitation, and Ruckus has not yet identified a workaround. [ZF-15980]

- In mesh mode, if the Root AP is set to 80 MHz Channelization and the Mesh AP is set to 40/20 MHz, the Mesh AP fails to get an IP address. All other combinations should work properly. [SCG-57479]

- Guest pass self-registration will fail if special characters (such as "%") are included in the guest pass terms and conditions field. [ZF-15970]

- Under certain rare conditions, H510 and R510 APs in mesh mode may cease to pass traffic and cause the AP to reboot. If this occurs, the mesh will re-establish itself upon reboot with no manual intervention. [ZF-16040]