RUCKUS™
an ARRIS company

Ruckus ZoneDirector 10.2 Release Notes

Supporting ZoneDirector 10.2

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

Limitation of Liability

Trademarks

Contents

About This Release

This document provides release information on ZoneDirector release 10.2, including new features, enhancements, known issues, caveats, workarounds, upgrade details and interoperability information for version 10.2.

NOTE
By downloading this software and subsequently upgrading the ZoneDirector and/or the AP to version 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 version **10.2.0.0.189** supports the following ZoneDirector models:

- ZoneDirector 1200
- ZoneDirector 3000

ZoneDirector version **10.2.0.0.189** supports the following Ruckus Access Point models:

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

NOTE
The following APs have been discontinued as of this release, and cannot be upgraded to 10.2 or later. If you have any of these APs on your ZoneDirector-managed network, do *not* upgrade ZoneDirector to this release. ZoneDirector will be unable to manage them.

- 7055
- 7352
- 7372
- 7372-E
- 7982
- 7781-CM
- 7782
- 7782-E
- 7782-N
- 7782-S
- H500
- R300

Upgrading to This Version

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

Officially Supported 10.2 Upgrade Paths

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

- 10.0.0.0.1424 (10.0 GA)
- 10.0.0.0.1449 (10.0 Patch 1)
- 10.0.1.0.17 (10.0 MR1)
- 10.0.1.0.35 (10.0 MR1 Refresh)
- 10.0.1.0.44 (10.0 MR1 Refresh 2)
- 10.0.1.0.61 (10.0 MR1 Refresh 3)
- 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)

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.

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.

- Export Client Logging Info

  Provides a means of logging all client connection events and sending them to a syslog server for meeting regulatory requirements for public Wi-Fi systems in some countries.

- ARC Integration with SCI

  Allows collection of Application Recognition and Control data from access points to be delivered to Ruckus SmartCell Insight (SCI) for analysis.

- Zero Touch Mesh

  Zero Touch Mesh allows customers to skip the mesh configuration priming process, enabling Mesh APs already installed in their permanent locations to auto-discover, auto-provision and auto-form a mesh network without priming.

  > **NOTE**
  > Please refer to the *Ruckus Access Points Release 110.0 Release Notes* document for a list of AP models and firmware builds that support the Zero Touch Mesh feature. Note that APs not running a supported firmware version will be unable to join a ZoneDirector using Zero Touch Mesh.

- Captive Portal Customization

  Provides several new options for customizing the Captive Portal login page for Guest WLANs.

- Merging Social Media and Guest WLANs

  Social Media WLANs are now a subcategory of Guest WLAN, rather than a separate WLAN type as in previous releases.

- UI Enhancements

  Includes many enhancements to UI performance and functionality, including the Dashboard page, Bonjour fencing configuration, device access policy configuration, roles, admin-generated guest passes, client applications and self-service guest pass login page enhancements.

- CLI Setup Wizard

  Admins can now configure ZoneDirector with basic setup parameters using CLI commands, in addition to using the web-based setup wizard.

- Client Connection Diagnostics Enhancement

  Client connection troubleshooting can now be run on clients connected to Web Auth, Hotspot (WISPr), and Social Media Guest WLANs, in addition to standard usage WLANs.

- Support for 802.1X Authentication with Back-End Active Directory Server

- Multi-Language Support for Portal Page

  This feature is enabled by default for the Guest WLAN login portal page when the web interface language is not English.

- Bonjour Fencing Enhancements for Apple TV and Chromecast

This enhancement extends support for Bonjour Fencing to Chromecast service discovery, and allows creation of a custom "Service String" field for existing mDNS services.

- 2.4GHz Mesh on Dual-Band APs

The ZoneDirector Smart Mesh SSID can now be broadcast using the 2.4 GHz radio instead of the 5 GHz radio (default) on dual-band APs. Previously, only Ruckus single-band APs (7352, for example) could mesh using the 2.4 GHz radio. With this release, those APs are no longer supported and Ruckus no longer has a single-band AP available, so the option to enable Smart Mesh on the 2.4GHz radios of dual-band APs has become more significant.

> **NOTE**
> Zero Touch Mesh is not supported when the mesh radio setting is set to 2.4 GHz.

Resolved Issues

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

- Removed "Generated Dynamic Certs" from the web interface and replaced "Generated Certs/PSKs" with "Generated PSKs." [ER-6526]
- Resolved an issue where ZoneDirector would fail to update GPS info received from an AP and would display the AP's map location incorrectly. [ER-6439]
- Resolved an issue where the first packet of a UE session was tagged with the VAP VLAN ID instead of ID of the UE. Packets of a UE with different VLAN tags could cost more resources at the switch. [ER-6586]
- Resolved an issue with Z2 county code that could allow users to change to another country code via AP CLI command. [ER-6262]
- Resolved an issue that could cause AP reboots due to a target fail detected error. [ER-5965]
- Resolved an issue that could cause APs to report an incorrect number of visitors detected to SPoT location service when MAC address hashing was enabled. [ER-5971]
- Resolved an issue that could cause performance degradation in single client throughput testing with 10 TCP streams on T811-CM APs. [ER-6230]
- The CLI command "mcast-airtime" is now also available on 11ac Wave 1 APs, in addition to 11ac Wave 2 APs. [ER-6606]
- Resolved an issue with PDA connectivity on hidden SSIDs. [ER-5457]

Caveats, Limitations and Known Issues

- Macbook clients may fail to be redirected to the captive portal page due to an issue with the Apple Captive Network Assistant (CNA) feature. [ZF-19195]

    Workaround: Close the CNA success window, and then reconnect to the WLAN.
- Huawei Honor 8 phones may fail to authenticate to an AAA server via Web Auth when using Chrome browser due to a compatibility issue with Chrome version 65+ and HTTPS redirection. [ZF-19339]

    Workaround: Disable the "Force HTTPS" feature for the web portal from the ZoneDirector web interface.
- Windows 10 clients may fail to be properly redirected when using Chrome version 65+ and HTTPS redirection. [ZF-19359]

    Workaround: Use HTTP redirection rather than HTTPS in web portal WLAN settings.

- Apple iOS and Mac clients fail to authenticate to an 802.1X WLAN when 802.11w MFP is enabled and set to Required. [ZF-19239]
- When a user clicks "Use Wi-Fi Code" on the Facebook login portal, the client may fail to be redirected properly due to an Apple CNA issue. [ZF-19156]

  Workaround: Enable Bypass Apple CNA Feature for the Guest WLAN.
- Apple clients running iOS version 11.4.1 fail to download the Zero-IT profile when selecting "Register Device" from the onboarding portal. [ZF-19663]

  Workaround: Upgrade devices to iOS 12+ or enable the "Bypass Apple CNA Feature" in WLAN settings.
- iOS clients running iOS version 11.4 are unable to redirect properly to a WeChat WLAN due to the Apple CNA feature. [ZF-19361]

  Workaround: Upgrade clients to iOS 12+ or enable the "Bypass Apple CNA Feature" in WLAN settings.
- Sony Z5 clients fail to roam properly when 802.11r Fast Roaming is enabled, due to a client limitation. [ZF-19502]
- The Apple Captive Network Assistant may prevent iOS clients from being properly redirected if captive.apple.com is unreachable, displaying an error message and forcing the user to reconnect to the WLAN. [ZF-19363]

  Workaround: Enable "Bypass Apple CNA Feature" in WLAN settings.
- iOS clients are unable to access WeChat WLANs due to the Apple CNA feature. [ZF-19362]

  Workaround: Enable "Bypass Apple CNA Feature" in WLAN settings.
- Android clients fail to be redirected when accessing a Google guest WLAN using the default Android browser or other embedded browsers. [ZF-19352]
- Due to a limitation in the Intel Wi-Fi management software (Intel PROSet Wi-Fi Connection Utility) in Windows 7, Zero-IT profiles are not saved properly when there is more than one Zero-IT profile. [ZF-19299]

  Workaround: Select "Use Windows to Manage Wi-Fi" in the Intel PROSet settings to retain all saved Zero-IT profiles.
- Android devices fail to redirect to to the Zero-IT activation login portal when using Chrome v67. [ZF-19360]

  Workaround: Import a trusted SSL certificate to ZoneDirector.
- Guest users are redirected back to the login page after authenticating to a Microsoft guest WLAN using Chrome browser. [ZF-19267]

  Workaround: Import a trusted SSL certificate to ZoneDirector.
- Client Fingerprinting fails to properly identify the OS type for clients including Bose wireless speakers and Nest cameras. [ZF-19481]
- Apple Macbook clients fail to download the Zero-IT profile due to an Apple CNA issue. [ZF-19504]
- Host name is not properly displayed in client fingerprinting for Nokia Android 8.1 devices. [ZF-19471]
- User can not download Zero-IT profile for some Android clients via automatic browser redirection using the Onboarding Portal. [ZF-19664]

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)

TABLE 1 Zero-IT Compatibility (continued)

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
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]