RUCKUS ZoneDirector 10.2.1 Refresh 11 Release Notes

Supporting ZoneDirector 10.2.1

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, COMMSCOPE 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. CommScope 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. CommScope 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 CommScope 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 COMMSCOPE, COMMSCOPE 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 COMMSCOPE 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

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see https://www.commscope.com/trademarks. All product names, trademarks, and registered trademarks are the property of their respective owners.

Patent Marking Notice

For applicable patents, see www.cs-pat.com.

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 **10.2.1.0.236** supports the following ZoneDirector models:

- ZoneDirector 1200
- ZoneDirector 3000

ZoneDirector version **10.2.1.0.236** supports the following RUCKUS Access Point models:

Indoor AP	Outdoor AP
C110	T300
E510	T300e
H320	T301n
H510	T301s
R310	T310c
R320	T310d
R500	T310n
R510	T310s
R600	T610
R610	T610s
R700	T710
R710	T710s
R720	

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 10.2.1 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 1)
- 10.0.1.0.44 (10.0 MR1 Refresh 2)
- 10.0.1.0.61 (10.0 MR1 Refresh 3)
- 10.0.1.0.83 (10.0 MR1 Refresh 4)
- 10.0.1.0.88 (10.0 MR1 Refresh 5)
- 10.0.1.0.90 (10.0 MR1 Refresh 6)
- 10.0.1.0.93 (10.0 MR1 Refresh 7)
- 10.0.1.0.123 (10.0 MR1 Refresh 8)
- 10.0.1.0.133 (10.0 MR1 Refresh 9)
- 10.0.1.0.136 (10.0 MR1 Refresh 10)
- 10.0.1.0.146 (10.0 MR1 Refresh 11)
- 10.0.1.0.151 (10.0 MR1 Refresh 12)
- 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)
- 10.1.1.0.62 (10.1 MR1 Refresh 4)
- 10.1.1.0.79 (10.1 MR1 Refresh 5)
- 10.1.2.0.120 (10.1 MR2)
- 10.1.2.0.210 (10.1 MR2 Refresh 1)
- 10.1.2.0.251 (10.1 MR2 Refresh 2)
- 10.1.2.0.270 (10.1 MR2 Refresh 3)
- 10.1.2.0.275 (10.1 MR2 Refresh 4)
- 10.1.2.0.277 (10.1 MR2 Refresh 5)
- 10.1.2.0.306 (10.1 MR2 Refresh 6)
- 10.1.2.0.318 (10.1 MR2 Refresh 7)
- 10.2.0.0.189 (10.2 GA)
- 10.2.1.0.75 (10.2 MR1)
- 10.2.1.0.79 (10.2 MR1 Patch1)
- 10.2.1.0.129 (10.2 MR1 Refresh 1)
- 10.2.1.0.135 (10.2 MR1 Refresh 2)
- 10.2.1.0.147 (10.2 MR1 Refresh 3)
- 10.2.1.0.159 (10.2 MR1 Refresh 4)
- 10.2.1.0.183 (10.2 MR1 Refresh 5)
- 10.2.1.0.187 (10.2 MR1 Patch)
- 10.2.1.0.192 (10.2 MR1 Refresh 6)
- 10.2.1.0.200 (10.2 MR1 Refresh 7)
- 10.2.1.0.212 (10.2 MR1 Refresh 8)
- 10.2.1.0.218 (10.2 MR1 Refresh 9)
- 10.2.1.0.232 (10.2 MR1 Refresh 10)

NOTE
R730 is not supported in this release and cannot be upgraded to 10.2.1. If you have R730 APs connected to ZoneDirector, upgrading to this release will cause these APs to stop functioning.

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.

- New AP Support: R320

  The R320 is an entry-level 2x2:2 802.11ac Wave 2 indoor AP designed for medium-density enterprise deployments. It features one GbE port, dual 2.4/5 GHz radios, BeamFlex support, 802.3af/at PoE support and a small form factor for flexible installation.

- LACP Support on R720

  Link Aggregation can be used to bond multiple Gigabit Ethernet links into a single, high capacity logical link. The R720 supports LACP (Link Aggregation Control Protocol) as defined in the 802.1ax (formerly 802.3ad) standard, allowing the bonding of its two Gigabit Ethernet ports to form a single 2Gbps link.

Resolved Issues in Build 232

- Resolved an issue where imported certificate does not work properly for FTP service. [ER-12291, ZF-22139]
- Resolved an issue where Twilio SMS feature does not work properly, caused by API change. [ER-12575]

Resolved Issues in Build 218

- Resolved an issue where connected clients lost network connection randomly. [ER-10797]
- Resolved an issue that caused R750 AP to reboot due to kernel panic. [ER-10795]
- Enhanced the SMS notification feature to support JSON format in POST data. [ER-11148]
- Resolved a fingerprints-related issue. [ER-10981]
- Resolved a performance issue on AP with 3X3 MIMO devices. [ER-10474]
- Resolved an issue where packet loss issue during background scanning on some particular APs. [ER-10181]
- Resolved an issue that caused AP kernel panic due to buffer overflow. [ER-10918]
- Enhanced the DNS Spoofing on Access Point to resolve the domain name of ZoneDirector for clients associated with WISPr, Gues,t and Web authentication WLANs. [ER-7915]
- Added support for Twilio's new API. [UN-6659]

Resolved Issues in Build 212

- Resolved an issue where ZoneDirector system would become unresponsive under certain conditions. [ER-10223]
- Resolved an issue where AP would unexpectedly reboot when download AVP setting failure after serval retries. [ER-10050]
- Resolved an issue where the "mcast-airtime" setting would not persist on 11ac APs. [ER-10202]
- Resolved an issue where MacBook client would be intermittently disconnected. [ER-9831]

Resolved Issues in Build 200

- Resolved an issue related to FragAttacks. For more details, refer to https://www.commscope.com/fragattacks-commscope-ruckus-resource-center/.
- Resolved an issue where AP would unexpectedly reboot when download AVP setting failure after serval retries. [ER-10050]
- Resolved an issue where memory leakage would happen under certain conditions on controller with location service enabled. [ER-9496]
- Resolved an issue where message "read lock not preceded by unlock" of AP was not categorized with the correct priority level. [ER-9939]

- Resolved an issue where AP would unexpectedly reboot under certain conditions. [ER-9170, UN-4818]

- Resolved an issue related to ZoneDirector web interface. For information on security incidents and responses, refer to https://www.ruckuswireless.com/security. [ZF-21768, ER-9802]

- Resolved an issue where the "Management Access Control" would not work properly under certain conditions. [ER-9940]

Resolved Issues in Build 192

- Resolved an issue where the AP was unable to connect to ZoneDirector [ER-4327].

- Resolved an issue where the number of configured MAC addresses exceeded the maximum allowed of 128, but the GUI was not displaying a pop-up error message. [ER-8781]

- Resolved an issue where traffic flooding occurs sometimes. [ER-8625]

- Hide unnecessary information in syslog. [ER-8875]

- Removed "no ftp" CLI command and "force ftp enable" on ZoneDirector. [ZF-21701]

- Resolved an issue where the EMFD daemon on ZoneDirector crashed due to corrupted statistics data reported from the Access Point. [ER-9021]

- Resolved an issue where clients sometimes encountered roaming failures between MAC-authorized WLANs. [ER-8945]

- Resolved an issue where the ethernet interface of the R610 failed to pass traffic through the 2.5G port on an ICX switch. [ER-8328]

- Resolved an issue where "Join another Controller" was not working properly when migrating a ZoneDirector AP to SmartZone or Clould AP. [ER-7730/ER-8683]

- Resolved an issue where client got randomly kicked off by the Access Point under certain conditions. [ER-8440]

- Resolved an issue where the AP would unexpectedly reboot under certain conditions. [ER-8862]

- Resolved a security issue related to LLDP vulnerability. For security incidents and responses, see https://www.ruckuswireless.com/security. [AP-13802]

- Added CLI commands to configure the supported TLS version on the Access Point. [ER-9044]

- Resolved an issue where the syslog got truncated on the AP. [ER-9189]

- Resolved an issue where the user who has correct SNMP RW community is able to use SNMP command to shutdown ZD Ethernet interface. [ER-9075]

Resolved Issues in Build 183

- Resolved several security issues related to UI vulnerabilities. For security incidents and responses, see *www.ruckuswireless.com/security*.

- Resolved an issue with throughput performance in WPA/WAP2 WLANs. [ER-7956]

- Resolve an issue where "Join another Controller" would not work properly for migrating a ZoneDirector AP to SmartZone/Clould AP. [ER-7730]

- Resolved an issue where accessing the ZoneDirector GUI would intermittently fail. [ER-8267/ER-8217/ER-8056]

- Resolved an issue where the configured gateway for the management interface would not work properly on ZoneDirector. [ER-8053]

- Resolved an issue where the "Directed-Multicast" setting would not persist on the WLAN and Ethernet interfaces on APs. [ER-7600]

- Resolved an issue where the reported MAC address and other content was inaccurate in packets sent from the AP to the Aeroscout server. [ER-7937/ER-8161]

Resolved Issues in Build 159

- The SmartCell Insight management password is no longer visible on the ZoneDirector web interface. [ZF-21179]

- Resolved an issue where the guest pass generation page would not allow entry of Chinese characters in the "Full Name" field. [ER-7958]
- Resolved an issue that could cause failure to configure an AP via the web interface. [ER-7834]
- Resolved an ARP drop issue on Access Points. [ER-6748]
- Resolved two security issues related to UI vulnerabilities. For security incidents and responses, see *www.ruckuswireless.com/security*.
- Resolved an issue where the connection between the ZoneDirector/Access Points and the LBS location server would become disconnected under certain conditions.

Resolved Issues in Build 147

- Resolved an issue where ZoneDirector would not report session data by default when "management by SmartCell Insight" was enabled. [ER-7762]
- Resolved a ZoneDirector memory leak issue. [ER-7475]
- Resolved an issue that could cause failure to configure an AP via the web interface. [ER-7834]
- Resolved an issue that could cause failure to configure an NTP server when the server name contains dashes. [ER-7843]
- Resolved an issue where CLI commands would not work properly for configuring auto channel selection algorithms. [ER-7846]

Resolved Issues in Build 135

- Resolved an issue that could cause APs to unexpectedly reboot with reason "reset button". [ER-7419]
- Added an AP CLI command to permanently save the debug level of APMGR on AP. [ZF-20919]
- Enhanced the debug log for the background scanning based auto channel selection algorithm and changed the default age-out value of Neighbor APs. [ZF-20924]
- Enhanced the debug log output for the backgrounding scanning based auto channel selection algorithm and made it configurable to save in ZoneDirector locally, remote syslog server, or both. [ZF-20925],

Resolved Issues in Build 129

- Resolved an issue where the AP CLI command "get scanresults" did not work properly. [ER-7630]
- Enhanced the Background scanning auto channel selection algorithm. [ER-7327, ZF-20709]
- Resolved an issue related to TCP SACK Panic - Kernel Vulnerability CVE-2019-11477, CVE-2019-11478 and CVE-2019-11479. [AP-11589]

  For information on security incidents and responses, see https:// www.ruckuswireless.com/security.
- Resolved an issue where channels 100-140 were unavailable in India country code. [ER-7515]
- Resolved an issue where UNII-3 channels were unavailable for R310/R510/R710 in UK country code. [ER-7563]
- Resolved an issue where guest pass generation did not work properly for newly created WLANs. [ER-7487]
- Resolved an issue where UNII-3 channels were unavailable for outdoor APs in Russia country code. [ER-7223]
- Resolved an issue where the start/end time of DST Daylight Saving Time was incorrect for GMT0 time zone. [ER-7446]
- Resolved an issue where the authentication portal page would continue to be displayed for MacOS clients even after guest authentication was complete. [ER-7392]
- Resolved an issue where BSS minrate and management rate settings would not be applie when the UI language was set to Dutch. [ER-7411]
- Resolved an issue where APs might fail to receive WLAN settings from ZoneDirector after failover in high density environments. [ER-7307]
- Removed unnecessary space character in the wireless client roam out event messages. [ER-7332]

- Resolved an issue where the "Remarks" column did not display correctly in the "Generated Guest Pass" web page. [ER-7257]
- Resolved an AP issue with Singapore country code where DFS channels were not listed in the supported channel list for certain AP models. [ER-7247]
- Resolved a kernel panic issue on APs located in high density environments when associated wireless clients were frequently roaming in and out of range. [ER-6689]
- Resolved an issue where rogue device reporting would not work properly when the SSID name was configured as a non-English name. [ER-6248]
- Resolved an issue on 11ac Wave 1 APs where unsupported data rates were used to send the first data packet to a wireless client over the 5 GHz radio. [ER-7018]
- Resolved an issue where the incorrect redirection URL was sent for guest authentication by ZoneDirector if the "domain" field was not set in the uploaded certificate. [ER-7156]
- Resolved an issue where the R700 APs rebooted on detection of target failure. [ER-7073]
- Resolved an issue where stations could not reach the redirect portal page for guest WLANs with tunnel mode enabled. [ER-7093]
- Resolved an issue on R310 APs where the 5G radio would not function properly in 20 MHz channelization mode. [ER-6969]
- Resolved an issue where Force DHCP feature did not work properly after client roaming or reconnect. [ER-7579]
- Resolved an issue where multicast traffic unexpectedly dropped for wireless clients associated with Open/None WLANs with tunnel mode enabled. [ER-7291]
- Resolved an issue on R720 APs where wireless clients could experience low uplink throughput if they had previously associated to a WLAN with rate limiting enabled on the same R720 AP. [ER-6567, ER-6576, ER-6830]
- Unified the CLI/web UI configuration settings for directed threshold. [ER-7600]

Resolved Issues in Build 75

- Resolved an issue with incorrect IP addresses being displayed on the "Wireless Client" page for connected clients. [ER-6968]
- Resolved an issue where customizing the "Terms of Use" field with non-ASCII characters would fail for Guest Access. [ER-7006]
- Resolved an issue where SNMP walk results on node "ruckusZDWLANStaSignalStrength" were inaccurate and renamed the node name from the previous name "ruckusZDWLANStaAvgRSSI" to "ruckusZDWLANStaAvgSNR". [ER-6943]
- 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 an issue on R720 APs where wireless clients could experience low uplink throughput if they had previously associated to a WLAN with rate limiting enabled on the same R720 AP. [ER-6567, ER-6576, ER-6830]
- Added an AP CLI command to allow configurable Multicast Airtime in percentage where the default value is 25%. [ER-6606]
- Resolved an issue where the following special characters would be disallowed when used in WPA2-PSK passphrases: "`",";", "%", "$", "&&", "||"). [ER-6875]
- Added an AP CLI command to allow configurable mcast-q-limit where the default value is 4. [ER-6517]

Caveats, Limitations and Known Issues

- When creating a new AP group, model-specific settings are inherited from the system default group, but they are not shown properly on the web interface. [ZF-20775]
- Until now, ZD supports only RSA Encryption Certificate. [ER-10829]

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

TABLE 1 Zero-IT Compatibility (continued)

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)
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]

- Due to the limitation of the App WiFiAutoConf_Zero-IT on Android version 10+, user cannot click the button "on" to connect to the SSID directly. [ZF-21703]

  Workaround: In the Android WLAN setting, connect the SSID manually.