Ruckus Wireless™ ZoneDirector™ Version 9.13

Release Notes

Part Number 800-71225-001 Rev B
Published August 2016

www.ruckuswireless.com

Copyright Notice and Proprietary Information

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader’s responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN (“MATERIAL”) IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless, Ruckus, the bark logo, ZoneFlex, FlexMaster, ZoneDirector, SmartMesh, ChannelFly, SmartCell, Dynamic PSK, and Simply Better Wireless are trademarks of Ruckus Wireless, Inc. in the United States and other countries. All other product or company names may be trademarks of their respective owners.

Contents

About This Release

1

Introduction

This document provides release information on ZoneDirector release 9.13, including new features, enhancements, known issues, caveats, workarounds, upgrade details and interoperability information for version 9.13.

NOTE: By downloading this software and subsequently upgrading the ZoneDirector and/or the AP to version 9.13, 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 Country Codes

Refer to the Ruckus Wireless Price List for available country certifications.

What's New in This Release

For information on the new features that have been added in this release, see "Enhancements" on page 10. Please refer to the Release Notes for prior releases for information on previously documented caveats, limitations, enhancements and resolved issues. These Release Notes can be found at: https://support.ruckuswireless.com/

Supported Platforms and Upgrade Information

2

Supported Platforms

ZoneDirector version **9.13.0.0.232** supports the following ZoneDirector models:

- ZoneDirector 1200
- ZoneDirector 3000
- ZoneDirector 5000

Access Points

ZoneDirector version **9.13.0.0.232** supports the following Access Point models:

- H500
- R300
- R310
- R500
- R510
- R600
- R700
- R710
- T300
- T300e
- T301n
- T301s
- T710
- T710s
- ZF7055
- ZF7352
- ZF7372
- ZF7372-E

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

EoL (End of Life) APs

The following AP models have reached end-of-life (EoL) 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 Upgrade Paths

The following ZoneDirector builds can be directly upgraded to ZoneDirector build 9.13.0.0.232:

- 9.10.0.0.218 (9.10 GA release)
- 9.10.1.0.59 (9.10 MR1 release)
- 9.10.2.0.11 (9.10 MR2 release)
- 9.12.0.0.336 (9.12 GA release)
- 9.12.1.0.140 (9.12 MR 1 release)
- 9.12.1.0.148 (9.12 MR 1 refresh release)
- 9.12.2.0.101 (9.12 MR 2 release)
- 9.12.2.0.219 (9.12 MR2 refresh release)
- 9.13.0.0.103 (9.13 Beta release 1)
- 9.13.0.0.209 (9.13 Beta refresh 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.

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.

Enhancements

New Access Points

- New Access Point: R510

  The ZoneFlex R510 brings cutting edge 802.11ac Wave 2 to the mid-tier segment. It improves aggregate network throughput and benefits both Wave 2 & non-Wave 2 clients. It combines Ruckus patented technologies and best-in-class design with the next generation of 802.11ac features to deliver outstanding Wi-Fi performance and reliability. It future proofs the customer for emerging Internet of Things (IoT) technologies.

  With throughput capacities of 300 Mbps (2.4GHz) and 867 Mbps (5GHz), 802.11ac Multi-User MIMO (MU-MIMO) support allows the R510 to simultaneously transmit to multiple client devices, drastically improving airtime efficiency, overall throughput, and availability.

- New Access Point: T710

  The T710 is a carrier grade dual-band concurrent 802.11ac Wave 2 outdoor access point with 4x4: 4 antennas, dual GbE ports and an SFP fiber interface. The T710 supports PoE in, PoE out, Ethernet port aggregation, and hot-swappable SFP fiber optic module.

- New Access Point: T710s

  The T710s is the 120-degree sector antenna variant of the T710. It includes all of the same features as the T710.

General

- WLAN Configuration Flow Enhancement

Added several new buttons to the WLAN creation pages that allow users to configure service settings using a popup window rather than having to go to the service configuration page, and then return to WLAN creation once created. After selecting a WLAN Type (Hotspot WLAN, Guest Access WLAN, etc.), users can now directly click a button to begin configuring services that must be configured for the WLAN type (Hotspot service, Guest Access service, etc.).

New WLAN configuration popups:

- AAA server
- Accounting server
- Access Control > L2/MAC
- Access Control > L3/4/IP address
- Access Control > Client Isolation White List
- Access Control > Device Policy
- Access Control > Precedence Policy
- Access Control > Application Denial Policy
- Guest Access Service
- Hotspot Service
- Hotspot 2.0 Operator Profile
- Hotspot 2.0 Service Provider Profile
- GuestAccess > Authentication Server
- Hotspot > Authentication Server and Accounting Server

- Shared Username Control for Web Auth WLANs

  Allows users to authorize multiple clients using the same login credentials within the grace period, while also allowing the customer's authentication server to control whether the station is able to pass or not.

- Certificate Refresh

  This release refreshes all affected Ruckus APs with the new Ruckus Public Key Infrastructure (RPKI) certificate and key. By going to *Configure* > *Certificate* > *Advanced Options* > *Import Ruckus KPI Certificate Package*, customers can generate a Ruckus PKI certificate request. Once the Ruckus PKI certificate package is received, customers can import the certificates and ZoneDirector will distribute them to all connected APs. For more information, see https://support.ruckuswireless.com/certificate.

- HTTPS Guest Portal

To improve security prior to authentication, Guest Access captive portal pages are now delivered via HTTPS rather than HTTP.

- Disable Radios via AP Group

  Added a "WLAN Service" enable/disable option to the AP and AP Group configuration pages, allowing users to easily disable WLAN service on the 2.4 or 5 GHz radio for a single AP or an entire AP group with a single button.

- HTTPS Upgrade

  A new Security Upgrade section on the Upgrade page enables AP firmware upgrades over HTTPS rather than FTP. If the AP cannot support HTTPS upgrade, it will fall back to FTP.

- Application Visibility and Control Enhancements

  Enhanced the accuracy of the Application Visibility and Control features with the addition of a third-party DPI (Deep Packet Inspection) application identification engine.

- Upgraded OpenSSL version to address OpenSSL Security Advisory 3 Dec 2015. [ID 123015] Please see www.ruckuswireless.com/security for security incidents and responses. [ER-3364]

- SCI Enhancement

  A new "SmartCell Insight Management" section has been added to the Configure > System page, which allows ZoneDirector to communicate with SCI when the ZD is behind a firewall without having to open firewall ports for SCI-ZD communications.

- SPoT Enhancement

  This feature implements two new request/response message pairs between the SPoT Location Server and the ZoneDirector which allow the Location Server to query and synchronize AP system time.

- AP Diagnostic Information

  Provides an easy way to collect 11ac AP processor core dump information from ZoneDirector.

- AP Image Signing

  Improves security by requiring verification of AP firmware images to ensure the file has not been modified and that the source code executed by the system is authentic code provided by Ruckus Wireless.

- Zero-IT support for Android 6.0.

- Support for Chinese characters in SSID names.

- Migration to SmartZone/Cloud Controller

  This release adds a new button on AP lists that allows you to migrate a ZD-controlled AP to SmartZone or Cloud control more easily.

802.11ac Access Point Enhancements

This release adds support for the following features on 802.11ac APs:

- Air Time Fairness (ATF) for 11ac APs
- WLAN Prioritization for 11ac APs
- WAVE-2 11ac Mesh support

Resolved Issues

ZoneDirector

- Resolved an issue where clients were unable to pass traffic after roaming when Force DHCP was enabled on the WLAN. [ER-2900]
- Guest Pass pages are now fully translated into Spanish when the system language is set to Spanish. [ER-3403]
- If a Walled Garden is configured for WISPr or Guest WLANs, HTTPS redirection for client stations may fail, resulting in clients failing to reach the Login or Terms & Conditions pages. [ER-2581] [ER-3441]
- Updated the error message “internal error, authsvr not found!” to be an informational level debug message rather than an error level message. [ER-3475]
- Updated the max length of the “AP Description” SNMP OID from 64 to 128 characters. [ER-3633]
- Resolved an issue where the “Top 10 SSIDs by usage” widget would incorrectly display an SSID called “uif0” when no such SSID was configured. [ER-3730]
- Resolved an issue where ZoneDirector could include erroneous data in session statistics records sent to FlexMaster and SCI, resulting in data dropouts in SCI session reports. [ER-3290]
- Resolved an issue that could cause the web interface and CLI interface to become unresponsive due to a support entitlement activation error. [ER-2896, ER-3665]
- Resolved an issue that could result in Smart Redundancy failovers due to a “cluster connection_closure” error. [ER-3565]

- Resolved a Proxy ARP issue that could result in IP address conflicts. [ER-2954]
- Resolved an issue with the station manager process on ZoneDirector 3000 consistently increasing memory usage, eventually leading to reboot. [ER-3275]
- Resolved a ZoneDirector issue that could prevent clients from authenticating to a Web Auth WLAN if the username is longer than 31 characters. [ER-3926]
- Resolved an issue where ZoneDirector would send incorrect input/output attributes in RADIUS Accounting messages. [ER-3846, ZF-6646]
- Resolved a CLI command issue where setting the Tx power to "Auto" from the AP Group configuration would not become effective after saving changes. [ER-4009]
- Resolved an issue with invalid Data Usage reported under Most Active Client Devices. [ER-2791]
- Resolved an issue with Zero-IT activation where user passwords that include a backslash character would produce an error and login would would fail. [ER-3985]
- Resolved an issue where SNMP queries would return incorrect speed values for the br0 Ethernet interface; SNMP would display 10Mbps when the actual speed was 1000Mbps. [ER-3904]
- Resolved a ZoneDirector 1200 issue that could cause the emfd process to hang on the active ZoneDirector in a Smart Redundancy pair. [ER-3880]
- 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]
- 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 with Self Service Guest Pass validity periods. [ER-3749]
- Resolved an issue with excessive "IPv6 address invalid" messages in logs. [ER-2995]
- Resolved an issue where zero session time was shown in accounting stop records. [ER-4019]
- Resolved an issue with Mesh APs losing uplinks when both SPoT Location services and Mesh were enabled. [ER-2420]

Access Points

- Resolved an issue that could cause DNS spoofing to be incorrectly applied to all WLANs after a Social Media WLAN was created, which could prevent clients from connecting to web pages carried by ZoneDirector. [ER-3599]
- Resolved an issue where Remote Capture with Filter was unsupported on the AP. [ER-3504]
- Updated access point copyright messages from 2014-2015 to 2016. [ER-3898]
- Resolved an issue where T300 APs running standalone AP firmware build 100.1 would fail to detect radar signal during the first 60sec scan. [ER-3052]
- Resolved an issue with Physical Link status of Ethernet Link when Logical Link is down. This fix sets Physical Link to down when Logical Link is down. [ER-3700]
- Implemented several memory optimization changes for ZoneFlex 7762 APs, which could experience memory exhaustion leading to AP reboots when running recent ZD/SZ releases, due to limited memory on the AP. [ER-3487]
- Resolved an issue with lower than expected uplink throughput on 7781-CM, 7782, 7982, and the 2.4 GHz radio on R700 APs when traffic is tunneled to ZoneDirector. [ER-4030]

Caveats, Limitations, and Known Issues

4

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

Known Issues

General

- iPhone 6 clients running iOS 9.3 fail to associate to an Open SSID on channels 100-136 when the country code is set to Uruguay. [ZF-15377]
- In some situations, ZoneDirector may drop the “last statistic” for roaming clients when roaming from an older AP to a newer one. This can cause data inaccuracy in SCI AP and session statistics reports. [ER-1958, ZF-12414]
- HTTPS redirection may fail for clients connecting to a Hotspot WLAN if the user enters a URL like 'https://www.facebook.com' using Chrome browser. [ZF-15399]
- In some cases, an AP may reboot due to power cycle but report as "unknown reason." [SCG-50193]
- If a backslash is used in the user password for RADIUS admin authentication, the user will be unable to access or log into the ZoneDirector web interface. [ZF-15563]
- If a backslash is used in the user password for Hotspot WLAN authentication, the user will be unable to authenticate successfully. [ZF-15563]
- If a backslash is used in the user password for an Open/Web Auth WLAN, the user will be unable to authenticate successfully. [ZF-15563]
- If a backslash is used as the WLAN name in a Guest Access WLAN, users will be unable to access the guest pass generation page. [ZF-15554]
- If a backslash is used in the password, clients will be unable to associate to an 802.1X WLAN. [ZF-15553]

R710/T710 Access Points

- The R710/T710 AP does not honor the idle timeout setting as received in the RADIUS access accept message. [SCG-48133]
- R710 will always request 25W through LLDP in order to run full power mode. [SCG-50538]
- SFP EPON/GPON fiber module model name information is not displayed on the web interface. [SCG-49330]
- The R710 can be powered by an 802.3at-compliant (25.5W) Power over Ethernet (PoE) switch or PoE injector -- *or* -- an 802.3af-compliant PoE switch or PoE injector.

  Note that the AP can operate off of 802.3af power, but the feature set is reduced, as follows:

  - The USB port is disabled
  - The non-PoE (eth1) Ethernet port is disabled
  - The 2.4 GHz radio is reduced to two transmit streams (2x4 MIMO) with aggregate transmit power up to 22dBm (subject to country limits).
- The T710 does NOT support 802.3af PoE power. Power must be supplied using either the Ruckus supplied PoE injector, or an 802.3at PoE switch/injector, or AC power.
- If using the PoE OUT port on the T710/T710s, it is MANDATORY to use the custom Ruckus supplied 60W PoE injector (part #902-0180-XX00), or to use AC power.
- If using a PoE switch to supply power to the T710, the PoE switch must be capable of supporting a PoE+ (802.3at) powered device. It is recommended to reserve 30W for the T710 on the switch, to account for inefficiencies and losses.
- Failure to ensure a PoE+ (802.3at) supply to the access point may result in unpredictable operation of the access point. Additionally, if using a PoE switch, the T710's PoE OUT port cannot be used to power additional devices.

EoL APs

- After upgrading ZoneDirector to 9.13 with EoL APs connected as Root APs (e.g., ZF 7363, which is no longer supported as of 9.13), any Mesh APs that were previously meshed to an EoL AP will be isolated and unable to join. [ZF-15521]

  Workaround: Power off any EoL APs before upgrading to avoid this issue.

Interoperability Information 5

ZoneDirector Controller and SmartZone Controller Interoperability

To ensure reliable network operations, it is recommended that ZoneDirector controllers and SmartZone controllers (SmartCell gateway and SmartZone controllers) not be deployed on the same IP subnet or in such a way as the controllers share the same DHCP address scopes and domain name servers (DNS) as there may be limitations or restrictions in AP controller discovery capabilities. An effective network segmentation strategy should be developed when ZoneDirector and SmartZone controllers co-exist in the same network.

Redeploying ZoneFlex APs with SmartZone Controllers

Note that a supported ZoneFlex AP configured to operate with ZoneDirector will require an upgrade to a compatible SmartZone controller approved software release prior to interoperating with a SmartZone controller. Once the AP firmware is updated, the AP will no longer be able to communicate with its old ZoneDirector controller. The AP must be reset to factory-default setting before attempting to configure the AP from the SmartZone controller.

NOTE: There are established ZD to SZ controller migration tools and procedures. Contact support.ruckuswireless.com for the latest available procedures and utilities.

ZoneFlex Release 9.9 and AP Standalone Mode and FlexMaster Managed Mode Operation

Starting January 1, 2015 the default image that ships from the factory on Ruckus access points (APs) will change from ZoneFlex Release 9.8.x to ZoneFlex Base Image Release 100.0.x. Most customers will not notice any difference in AP operation. The APs will continue to support standalone mode and FlexMaster managed mode operations and will automatically discover and connect to ZoneDirector or SmartZone controllers.

Beginning in ZoneFlex Release 9.9 and higher, the AP has a new behavior: once an AP connects to a controller the AP will no longer support standalone mode and FlexMaster managed mode operation after the controller completes the necessary AP firmware update during initialization.

An AP removed from a controller managed network may be restored to operate in standalone mode and FlexMaster managed mode operation by updating the AP firmware back to ZoneFlex Base Image Release 100.0.x or to a ZoneFlex-AP Release 9.8.x or lower.

These software images are available on the Ruckus support site, see support.ruckuswireless.com for more information.

AP Interoperability

APs with ordering number prefix 901- (example 901-T300-WW81), may now be supplied with an AP base image release 100.0. or higher.

The AP base image is optimized for controller-discovery compatibility to support all Ruckus Wireless controller products including ZoneDirector, SCG, vSCG, SmartZone and SAMS.

Once the AP discovers and joins a controller (for example ZoneDirector), the AP is updated to the compatible controller-specific AP firmware version. The updated AP firmware version becomes the factory-default image. The updated AP firmware version (for example ZoneFlex 9.9) will remain persistent on the AP after reset to factory defaults.

An AP configured with base image release 100.0 may be managed by the FlexMaster management tool or may be used in standalone controller-less operation if controller discovery is disabled on the AP web UI.

FlexMaster Interoperability

Due to new SSL certificates, ZoneDirector 9.13 will be unable to register with the following FlexMaster releases:

- 9.10.0
- 9.10.1
- 9.12.0
- 9.12.1

If you are running one of the above FM releases, you must upgrade to either FM 9.10.2, FM 9.12.2, or FM 9.13 before upgrading ZD to 9.13, or ZD will be unable to register with FM. [ZF-15529]

Client Interoperability

ZoneDirector and ZoneFlex APs use standard protocols to interoperate with third-party Wi-Fi devices. Ruckus Wireless 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 10.11.3

Smart Phone/Tablet OS:

- iOS (6.1, 7.0, 7.1, 8.1, 8.4, 9.2, 9.3)
- 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)
- Windows Phone (7, 8, 8.1, 10)
- BlackBerry OS (10, 10.3.2)

- Chrome OS (47.0, 49.0)

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)
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)
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

Table 1. Zero-IT Compatibility

	WPA2 WLAN			802.1x EAP (external Radius Server)		
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	Y	Y	Y	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 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]

350 West Java Dr. Sunnyvale, CA 94089. USA
www.ruckuswireless.com