

Ruckus Wireless ZoneFlex 9.1.2 (FlexMaster, ZoneDirector and ZoneFlex Access Points) Release Notes

October 18, 2011



Contents

1	Introduction	4
2	What's New in This Release	4
3	Supported Platforms	4
4	Enhancements and Resolved Issues in This Release	5
4.1	FlexMaster	5
4.2	ZoneDirector	5
4.3	ZoneFlex Access Points	10
5	Caveats, Limitations and Known Issues	11
5.1	FlexMaster	11
	Installation	11
	Licenses	11
	Network Environment/Firewall	11
	TR069 Limitations	11
	Web Interface	12
	Device View	12
	Provisioning	12
	User Security	13
	AP-related Issues	14
	Reports	14
	SpeedFlex	14
	VLANs	14
	Other Caveats	15
5.2	ZoneDirector	15
	General	15
	Web Interface	16
	SpeedFlex	17
	SNMP	17
	CLI	17
	Ethernet Ports and Port-based VLAN	18
	VLAN, Dynamic VLAN, and Tunnel Mode	18
	DHCP Option 12	19
	AAA Servers	19
	Smart Redundancy	19
	Smart Mesh Networking	20

WLAN Service Schedule	20
Band Steering	21
Dynamic PSKs	21
Guest Access	22
Captive Portal.....	22
WISPr (Hotspot Service)	22
Voice	23
Real-Time Monitoring	23
Email Alarm.....	23
Bradford Network Access Control (NAC) Server.....	23
SSL Certificates	23
Traffic Shaping	23
5.3 ZoneFlex Access Points.....	24
General	24
ZoneFlex Access Points.....	24
ZoneFlex 7025	25
Interoperability with PoE Switches.....	25
6 Upgrading to This Version.....	26
6.1 ZoneDirector	26
ZoneDirector 1100.....	27
6.2 ZoneFlex Access Points.....	27
6.3 Changed Behavior.....	27
Upgrading to releases 9.1.2-and-later:	27
From release 9.1 to 9.1.2.0.8:.....	28
From release 9.1.0.0.23 to 9.1.0.0.38-and-later:.....	28
Between releases prior-to-8.2 and releases 8.2-and-later:	28
7 Interoperability Information.....	28

1 Introduction

Ruckus Wireless ZoneDirector is a WLAN access point controller that is capable of operating at both Layer 2 and Layer 3. ZoneDirector 1000/1100 supports up to 50 ZoneFlex access points (APs) and is developed specifically for small-to-medium enterprises (SMEs) and hotzone operators. ZoneDirector 3000, on the other hand, supports up to 500 ZoneFlex APs and is intended for larger enterprise environments. FlexMaster is a centralized management system that can manage ZoneDirector devices, as well as standalone ZoneFlex APs and Bridges, on a global scale.

This document provides release information on FlexMaster, ZoneDirector, supported ZoneFlex platforms, known issues, caveats, workarounds, upgrades, and interoperability information for version 9.1.2.

2 What's New in This Release

For a list of features that have been added in this release, visit:

<http://support.ruckuswireless.com/documents>

3 Supported Platforms

Release 9.1.2 supports the following platforms:

- FlexMaster 9.1.1.0.20 supports the ZoneDirector and ZoneFlex AP models listed below. FlexMaster 9.1 also supports the MediaFlex product line (not included in Release 9.1).
- ZoneDirector 1000 version 9.1.2.0.8
- ZoneDirector 1100 version 9.1.2.0.8
- ZoneDirector 3000 version 9.1.2.0.8
- ZoneFlex 2741 802.11g Outdoor Access Point build 9.1.2.0.8 (both main and backup)
- ZoneFlex 2942 802.11g Access Point build 9.1.2.0.8 (both main and backup)
- ZoneFlex 7025 802.11n Wired/Wireless Wall Switch build 9.1.2.0.8 (both main and backup)
- ZoneFlex 7341 2.4GHz 802.11n Smart Wi-Fi Access Point build 9.1.2.0.8 (both main and backup)
- ZoneFlex 7343 2.4GHz 802.11n Smart Wi-Fi Access Point build 9.1.2.0.8 (both main and backup)
- ZoneFlex 7363 Dual Band 802.11n Smart Wi-Fi Access Point build 9.1.2.0.8 (both main and backup)
- ZoneFlex 7762 Dual-band 802.11n Outdoor Access Point build 9.1.2.0.8 (both main and backup)
- ZoneFlex 7762-S Dual-band 802.11n Outdoor Access Point with Sector Antenna build 9.1.2.0.8 (both main and backup)
- ZoneFlex 7762-T Dual-band 802.11n Outdoor Access Point with Omni Antenna build 9.1.2.0.8 (both main and backup)
- ZoneFlex 7942 802.11n Access Point build 9.1.2.0.8 (both main and backup)
- ZoneFlex 7962 Dual-band 802.11n Access Point build 9.1.2.0.8 (both main and backup)

Starting from ZoneDirector Release 8.2, ZoneDirector does not support ZoneFlex 2925 Access Point. Therefore, the 2925 cannot be upgraded to Release 9.1. Moreover, upgrading a ZoneDirector that is managing a 2925 AP to this release will result in the 2925 AP becoming unmanaged and unable to rejoin ZoneDirector.

4 Enhancements and Resolved Issues in This Release

This section lists enhancements that have been added and issues from previous releases that have been resolved in this release.

4.1 FlexMaster

- 4.1.1 Firmware Task creation now has a search box to find devices. (ID 15912).
- 4.1.2 Most result tables now have a “10 more records” option to show more results (ID 16020).
- 4.1.3 Drop down selection boxes are now sorted alphabetically (ID 16233).
- 4.1.4 Resolved display issue in Device View for Firefox (ID 16363).
- 4.1.5 Support for new product models ZoneFlex 7025, 7341, 7762-S, and 7762-T.
- 4.1.6 GPS coordinates are automatically calculated from Location Field information.
- 4.1.7 Mesh display issue with Google Maps (ID 15606).
- 4.1.8 Added options for configuring the four front-facing Ethernet ports on ZoneFlex 7025. These four ports can be configured individually as either VLAN Trunk Ports or Access Ports. VLAN-based QoS configuration is also available in FlexMaster.

4.2 ZoneDirector

4.2.1 ZoneDirector 1100

A new ZoneDirector model, ZoneDirector 1100 is now available. The ZoneDirector 1100 shares the same form factor as the ZoneDirector 1000 but includes increased memory to support more AP types, including the ZoneFlex 7025.

4.2.2 New AP model support

Release 9.1 supports the ZoneFlex 7025 wired/wireless wall switch and the ZoneFlex 7762-S Outdoor Access Point with Sector Antenna.

With release 9.1.1 and later, the ZoneFlex 7762-T Dual Band 802.11n Outdoor Access Point with Omni Antenna and the ZoneFlex 7341 2.4GHz Indoor Access Point are also supported.

4.2.3 Ethernet port configuration

ZoneDirector provides new tools for configuring AP Ethernet ports, allowing administrators to set ports as either access ports or trunk ports, to assign VLANs to ports, or to disable ports entirely from the ZoneDirector Web interface.

4.2.4 Single SSID for multiple WLANs

This release provides the ability to configure multiple WLANs with the same SSID. For instance, a WLAN defined with Open authentication can use the same SSID as a WLAN defined with 802.1X authentication. Alternatively, a WLAN configured with walled garden URLs specific for one location can use the same SSID as a WLAN configured with walled garden URLs specific to a different location. This allows network operators to market a single SSID to different user types or at different locations.

4.2.5 Dynamic PSK and Zero-IT for Apple iPad and Android OS Platforms

Starting with software release 9.1, ZoneDirector supports Dynamic PSK and Zero-IT on Apple iPad and Android OS platforms. Support for iPad and Android platforms is in addition to the previous support of Windows 7, Windows XP, Windows Vista, Windows Mobile, Windows CE, Apple Mac, and Apple iPhone.

As of release 9.1.1, the following Android OS versions are supported: 1.5, 1.6, 2.0, 2.1, 2.2, 2.3, 2.3.3.

4.2.6 SNMPv3

With this release, ZoneFlex Access Points and ZoneDirector can be managed using SNMPv3 in addition to SNMPv2.

4.2.7 External Antenna Gain

With this release, administrators can indicate the gain of an antenna attached externally to ZoneFlex Access Points. ZoneFlex APs with connectors for an external antenna include the 2942, 2741, 7762, and 7762-S. The conducted transmit power of the AP is adjusted to maximize the Effective Isotropic Radiated Power (EIRP) allowed by regulations. Valid antenna gain values range from 0 to 90 (0 is disabled).

4.2.8 RADIUS Accounting can now be enabled on WLANs that use Open, Shared, or MAC Addresses for authentication (ID 8825, 14019).

RADIUS Accounting, available in release 8.2.2.0.7, was not available for these WLAN types in 9.0. If you enabled RADIUS Accounting in 8.2.2.0.7, you were unable to upgrade to 9.0. You can upgrade from 8.2.2.0.7 to 9.1 without losing RADIUS Accounting capabilities for these WLAN types.

4.2.9 RADIUS enhancements

Username used in RADIUS authentication supports up to 128 characters.

The following enhancements or fixes were made for RADIUS Accounting:

- Acct-Interim-Interval is now correctly honored by ZoneDirector (ID 12772).
- Interim-update period can be configured for a period from 0 (disabled) to 1440 minutes.
- New attributes are included in Accounting messages Accounting-Start: Framed-IP-Address; Access-Request: Service-Type; Accounting-on/off: User-Name, Session-ID.
- New Vendor Specific Attribute: Ruckus-SSID.
- New Accounting-Stop: Acct-Terminate-Causes: User Request (1), Lost Carrier (2), Lost Service (3), Session Timeout (5), Admin Reset (6), Admin Reboot (7), Supplicant Restart (19).
- NAS-Identifier reported for WLANs using 802.1X or MAC Authentication can now be configured through the CLI to use either ZoneDirector MAC address, model name, or WLAN BSSID.
- The RADIUS Called-Station_ID attribute now includes an SSID field to be compliant with RFC 3580. Example: "00-10-A4-23-19-C0:AP1".

- 4.2.10 ZoneDirector can be configured to automatically or not automatically refresh the screen when an update event is made to the existing view. When auto-refresh is disabled, information will still be updated when browsing to a new page (ID 13220, 15841).
- 4.2.11 The Devices Overview in ZoneDirector Dashboard now shows separate statistics for number of authorized clients and number of total clients (which also include clients who have expired DPSKs or guest passes) (ID 10494).
- 4.2.12 If the Setup Wizard is used to set the Country Code, the APs now properly allow use of DFS channels. This bug did not apply to US country code (ID 15806).
- 4.2.13 ZoneDirector managed APs can be configured through CLI to advertise only OFDM rates. By not advertising CCK rates, 802.11b and 802.11g clients only capable of slower 1, 2, 5.5 and 11 Mbps rates will not be able to associate to the AP at those rates.
- 4.2.14 The period that a PMK key is kept in cache can be configured or even disabled through the CLI.
- 4.2.15 The ZoneDirector configuration can be backed up using a TFTP server. Scripts can be created to automatically backup the configuration on a periodic basis (ID 12859).
- 4.2.16 SNMP queries return the correct value for .iso.org.dod.internet.mgmt.mib-2.interfaces (.1.3.6.1.2.1.2), .iso.org.dod.internet.mgmt.mib-2.interfaces.ifNumber (.1.3.6.1.2.1.2.1) and .iso.org.dod.internet.mgmt.mib-2.system.SysObjectID (.1.3.6.1.2.1.1.2) (ID 15727, 15731, 15935, 15936)
- 4.2.17 The semicolon (;) character can now be used in passphrases for WPA or WPA2-PSK (ID 15741, 16119).
- 4.2.18 SpeedFlex events now properly display the AP device names in the Events/Activities table. (ID 16780)
- 4.2.19 Changing WLAN prioritization with active APs no longer causes AP “assertion failed” events or disconnects, and no longer requires the APs to be rebooted (ID 16204)
- 4.2.20 RADIUS Accounting server now properly receives all Accounting-Request-Start packets each time a station reconnects after having been disconnected from the WLAN. (This issue appeared in some configurations with WPA+Web Auth enabled.) (ID 16811, 16885 and 17610)
- 4.2.21 SSL Certificates (ID 16705)

The Backup Private Key feature in the SSL Certificates Advanced settings has been modified to work more seamlessly with the Smart Redundancy feature. The SSL Certificate backup and restore feature now allows you to backup and restore private keys stored in either text files or tar files.
- 4.2.22 All ZoneFlex models are now properly identified in the RUCKUS-PRODUCTS-MIB.txt file for proper SNMP product differentiation on ZoneDirector. (ID 17128)
- 4.2.23 An issue that caused some Mesh APs with very long names (including description/location/GPS coordinates) to intermittently lose mesh settings and enter dormant mode has been resolved. (ID 16762)
- 4.2.24 ZoneDirector 3000 will no longer enter a condition where no more HTTP(S) sessions are available due to connections on ports 80 and 443 that never pass any data. When no data is passed, these connections are now properly initialized with host timeout set to 30 seconds. (ID 17236)

- 4.2.25 ZoneDirector now properly deletes client MAC ACL cache entries when an admin manually deletes a client. Clients will now always send a RADIUS Access-Request packet to re-associate to the MAC Auth WLAN each time after an admin deletes the client from the Web interface. (ID 17612)
- 4.2.26 APs will no longer attempt to query meshd and flood the syslog server with error messages when mesh is not enabled. (ID 16407)
- 4.2.27 ZoneDirector will no longer crash due to a memory problem caused by APs frequently disconnecting and reconnecting. (ID 16739)
- 4.2.28 ZoneDirector now correctly displays the proper IP address on the “Restarting...” screen after changing the IP address and restarting. (ID 15247)
- 4.2.29 Client traffic tagged with management VLAN is now classified into the video queue rather than the voice queue to prevent delays in time-critical 802.11 management frames. (ID 17097)
- 4.2.30 A txq buffer leak that caused AP performance degradation in version 9.1 has been resolved. (ID 17985 and 18016)
- 4.2.31 SNMP version information is now sent with SNMP agent event messages to differentiate the SNMP version used. (ID 16614 and 17927)
- 4.2.32 AP ACK RSSI values are now displayed correctly when the command `get station stats` is run from the CLI. (ID 17053)
- 4.2.33 The WLAN Group command “Enable VLAN override” now properly overrides the VLAN for WLANs configured with tunnel mode enabled. (ID 11869)
- 4.2.34 ZoneDirector now allows the correct radio channels when the country code is set to Romania. (ID 17830)
- 4.2.35 The Configure > Alarm Settings page now prompts the user for valid email entries where required, reducing the likelihood that ZoneDirector will fail to deliver email notifications due to incomplete or improperly formatted entries. (ID 16633, 16965)
- 4.2.36 Windows XP users are no longer required to be logged in as an Administrator to be able to self-provision their clients with Zero-IT Activation.
- 4.2.37 Ethernet Port Configuration

The ZoneDirector Web interface now displays an updated AP Ethernet Port Configuration section with ports individually configurable as either VLAN Trunk Ports or Access Ports and configurable Untagged VLAN field. All Ethernet ports on APs other than the ZoneFlex 7025 are VLAN Trunk Ports by default, and the 7025’s four configurable ports are Access Ports by default.

Access Port behavior: Untagged ingress packets and tagged packets with VLAN ID equal to the default PVID will be forwarded. All other ingress packets will be dropped. Egress packets are sent untagged.

VLAN Trunk Port behavior: Untagged and tagged ingress packets will be forwarded. Egress packets will be tagged with non-default PVID.
- 4.2.38 Disabling WLAN service on the 5GHz radio no longer prevents Mesh APs from finding better uplinks on different channels. (ID 16430)

4.2.39 AP channel change interval has been reduced from 3600 to 600 seconds when blacklisting feature is enabled, allowing APs that are under ZoneDirector control to change channels more rapidly. (ID 14879, ID 15068)

4.2.40 OFDM-only and BSS-minrate support

These two new features are available only from the CLI.

- OFDM-only: Allows the user to increase management frame transmission speed from CCK rates to OFDM rates. This feature is implemented per WLAN and only affects the 2.4GHz radio.
- BSS-minrate: Allows the user to change bss rates of management frames from default rates [CCK rates for 2.4G or OFDM rate – 6Mbps for 5G] to the desired rates.

OFDM-only takes higher priority than BSS-minrate. However, OFDM-only relies on BSS-minrate to adjust its rate for management frames.

4.2.41 Rate limiting configuration (**Configure > WLANs > Create New/Edit WLAN > Advanced Options > Rate Limiting**) now allows for finer granularity in limiting uplink and downlink speeds (increments of 250Kbps).

4.2.42 When a disconnected AP rejoins ZoneDirector and is receiving WLAN and VLAN configuration from ZoneDirector, multiple clients attempting to associate at the same time no longer causes some clients to receive incorrect VLAN assignment. (ID 16398)

4.2.43 Smart Redundancy synchronization enhancements

Several issues with synchronizing configuration between active and standby ZoneDirectors in a Smart Redundancy configuration have been resolved. The standby ZoneDirector now properly displays synchronized guest pass, WLAN and AP configuration settings received from the active ZoneDirector when Smart Redundancy is re-enabled or connection is re-established. (ID 21420, 20465, 20886, 20755, 20203, 20816, 20775, 19668)

4.2.44 Clicking the “Failover” button multiple times in succession no longer results in one ZoneDirector becoming stuck in active state or being unable to deploy WLANs on the now active device. (ID 20719, 17622)

4.2.45 The WLAN Service Schedule no longer incorrectly adds a gap in service between 4:00 PM-4:15 PM on Saturday when time zone is (GMT-8). (ID 21308)

4.2.46 Resolved an issue where wireless clients failed to associate to ZoneFlex 802.11g APs because resources were reserved for unassociated clients. (ID 21287)

4.2.47 When a FlexMaster-managed ZoneDirector’s interface language is set to Simplified Chinese, rebooting the device no longer resets the language to English. (ID 21091)

4.2.48 The ZoneDirector `webs` process can now be restarted after a crash without having to restart all other processes. Additionally, a webs crash issue related to reference count overflow when burst requests occur has been resolved. (ID 20904)

4.2.49 Resolved an SNMP issue that could cause ZoneDirector to reboot. (ID 20346)

4.2.50 Resolved an XML file update timeout issue that could result in ZoneDirector losing AP's configuration. (ID 20981, 19448)

4.2.51 Resolved an issue with admin passwords using the “%” character. (ID 20005)

- 4.2.52 ZoneDirector no longer sends IGMP/MLD query messages when QueryInterval is set to zero. Additionally, the IGMP/MLD Init Query delay can no longer be set to zero via CLI.
- 4.2.53 Smart Redundancy failover events now generate SNMP alerts and email alert messages. (ID 20435)

4.3 ZoneFlex Access Points

- 4.3.1 After upgrading to release 9.1, Standalone ZoneFlex Access Points can be upgraded to future releases using a locally provided file option. In addition to TFTP, FTP, and a Web option, administrators can now download the AP image to their computer and upload this file directly to the AP through the Web UI.
- 4.3.2 Web UI will no longer become inaccessible after running continuously for long periods of time with “Enable Auto-Update” enabled. (ID 17305)
- 4.3.3 The ZoneFlex 7025 Web interface includes a Configuration > LAN Ports page, which allows configuration of the four front-facing Ethernet ports as either VLAN Trunk Ports or Access Ports. Ports can also be individually disabled, and an Untagged VLAN can be specified for each port from this page.
 - Access port behavior: Untagged ingress packets and ingress packets tagged with the VLAN ID equal to the default PVID will be forwarded. Other ingress packets will be dropped. Egress packets are sent untagged.
 - Trunk port behavior: All ingress packets (tagged and untagged) will be forwarded. Egress packets will be tagged with a non-default PVID. Untagged VLAN on LAN1-LAN4 can be configured with a PVID other than 1.
- 4.3.4 The ZoneFlex 7025 supports four priority queues (voice, video, data and background) on both the wired and wireless interfaces, allowing traffic prioritization based on VLAN ID.

VLAN QoS (802.1p prioritization) can be performed from the ZoneDirector CLI.

 - ZoneDirector CLI command: (from the directory path /ruckus/config/ap-policy):
`vlan-qos <vlanid> <traffic class> <Interface Name>`
- 4.3.5 Ethernet port speed configuration: AP Ethernet ports can be configured for connect speed using the AP CLI.
- 4.3.6 Rate limiting configuration (**Configuration > Wireless > WLAN # > Rate Limiting**) now allows for finer granularity in limiting uplink and downlink speeds (increments of 250Kbps).
- 4.3.7 External antenna disablement configuration for 5G Hz radio is ignored and the antenna setting is always enabled for 7762-S and 7762-T APs.
- 4.3.8 Improved the channel change time when the 2.4 GHz radio faces extreme interference conditions. (ID 20013)

5 Caveats, Limitations and Known Issues

This section lists the caveats, limitations, and known issues for FlexMaster, ZoneDirector and ZoneFlex Access Points in this version.

5.1 FlexMaster

Installation

5.1.1 Ruckus Wireless recommends installing FlexMaster on a Red Hat Enterprise 5.x server.

5.1.2 For APs to be able to connect to FlexMaster, the AP image must support TR069.

Licenses

5.1.3 A FlexMaster installation provides 100 licenses by default.

5.1.4 If the maximum number of devices that the FlexMaster license supports has been reached, an alert message appears on the Dashboard and on the **Administer > License** page.

5.1.5 If FlexMaster is also used to manage ZoneDirector, note that the number of license seats that ZoneDirector will consume depends on the maximum number of APs that it can support. ZoneDirector 3500 (which supports up to 500 APs), for example, will consume 500 license seats.

5.1.6 If two redundant ZoneDirector devices are deployed, the standby ZoneDirector device will also use up one license count.

Network Environment/Firewall

5.1.7 If a device is behind a NAT server, FlexMaster will be unable to communicate with it using TCP or UDP.

5.1.8 FlexMaster will only be able to communicate with the device behind a NAT server at inform intervals, at which time the device will send an inform packet to FlexMaster via HTTP and HTTPS.

5.1.9 The shortest allowed periodic inform interval is one minute, the longest is four weeks.

5.1.10 If the ZoneDirector or Access Point is behind a NAT server, port forwarding must be configured on FlexMaster and the NAT server to enable FlexMaster to communicate with the device behind the NAT server.

5.1.11 SpeedFlex does not work if the target device is behind a NAT server.

TR069 Limitations

5.1.12 FlexMaster tasks are not implemented in real time. For example, if the managed device is behind a NAT server, the administrator may need to wait for the device to communicate successfully with FlexMaster before the task can be executed.

5.1.13 If a device loses communication with FlexMaster while it is being provisioned with a task, FlexMaster will mark the task as expired if the device does not re-establish communication within three inform intervals (see exception below).


- 5.1.14 If the task is 'Firmware Upgrade' or 'Reboot', FlexMaster will mark the task as expired if the AP reboots and does not re-establish communication within 60 minutes.

Web Interface

- 5.1.15 FlexMaster release 9.1 supports the following Web browsers:

- Firefox 3.0, 3.5, and 3.6
- Internet Explorer 7 and 8
- Safari 5 .0
- Chrome 5.0 and 6.0

FlexMaster does not support Internet Explorer 6.0. Some Web interface elements may not display correctly in this browser.

- 5.1.16 The information displayed in the ZoneDirector Device View of the Dashboard is retrieved from connected ZoneDirector devices every five minutes; it may not be real-time information.
- 5.1.17 The graphs that are displayed on the Dashboard are generated from the FlexMaster database. This information is aggregated from managed ZoneDirector devices and refreshed on an hourly basis.
- 5.1.18 To show the most up-to-date information from the managed device or FlexMaster database on the Web interface, click the  (refresh) button.
- 5.1.19 If DHCP Option 43 is configured with a FlexMaster server URL that is different from the FM configuration template, the managed device will use the FlexMaster server URL that has been set in DHCP Option 43.
- 5.1.20 When FlexMaster is managing a large number of devices, the *Client Association Activity* and *Connectivity* graphs may show inconsistent data. (ID 19678).
- 5.1.21 The Clients column on the ZD Device View widget may display an incorrect number of clients. Clients that have already disassociated with managed APs for two or more hours may still be included in the client count (ID 20319).

Device View

- 5.1.22 The information displayed in the ZoneDirector Device View of the Dashboard is retrieved from connected ZoneDirector devices every five minutes; it may not be real-time information.
- 5.1.23 If any setting is changed from the AP Web interface, this change will not be reflected on the FlexMaster Web interface in real-time. The administrator may need to click the refresh button on the FlexMaster Web interface to see this change.
- 5.1.24 After applying any configuration change from the Device View, Ruckus Wireless recommends verifying that the change has been applied successfully before performing other tasks. The status appears in the Device Status area in the upper-right corner of the page.
- 5.1.25 VLAN settings in the FlexMaster Device View are virtually created before any interfaces are joined in.

Provisioning

- 5.1.26 A ZoneDirector backup file that has been used to create a ZoneDirector configuration task cannot be deleted. (ID 11411)

- 5.1.27 FlexMaster is unable to distinguish between far-end and near-end 7731 bridges if the bridge topology is modified after a task is provisioned. (ID 12889)

FlexMaster applies provisioning tasks to the 7731 bridges in the following order of priority:

1. Far-end non-root bridge
2. Far-end root bridge
3. Near-end non-root bridge
4. Near-end root bridge

Provisioning tasks to far-end bridges (those with the least number of connections within the topology) first minimizes the chances of a downtime in case errors occur during the provisioning process. However, if the topology is modified (for example, if a far-end bridge becomes a near-end bridge) after a task is provisioned, FlexMaster may be unable to detect the topology change right away and may apply the task first to the now near-end bridge.

Consider the following bridge topology:

```
FM Server -- Ethernet -- BR1 (Non-Root) -- Wireless -- BR2 (Root)
                                     -- Wireless -- BR3 (Non-Root)
```

If the administrator unplugs the Ethernet cable from Bridge 1 (BR1), and then plugs it into Bridge 3 (BR3), the bridge topology will change automatically to:

```
FM Server -- Ethernet -- BR3 (Non-Root) -- Wireless -- BR2 (Root)
                                     -- Wireless -- BR1 (Non-Root)
```

FlexMaster will not detect this topology change and will provision the task to BR3 first. If an error occurs during provisioning to BR3 and BR3 crashes, FlexMaster will no longer be able to provision to BR1 and BR2, since BR3 connects FlexMaster to these far-end bridges.

Workaround: If the bridge topology is modified after a task is provisioned, Ruckus Wireless recommends that all 7731 bridges that are part of the topology be rebooted to update FlexMaster about the new bridge topology.

- 5.1.28 Provisioning a template that updates a ZF7731 device's SSID and encryption settings will terminate its connection with its pair.
- 5.1.29 Provisioning to a ZF7731 device will fail if the template contains changes to both the device's country code and channel width.
- 5.1.30 MediaFlex 2825 templates can be provisioned to APs with different customer profiles, even if these profiles contain different settings.
- 5.1.31 If an administrator creates a template and then uses that template to provision a task, changing the template settings later on will not affect tasks that have already been provisioned. The new template settings will only be applied to new tasks.
- 5.1.32 Tasks with duplicate names can be saved.
- 5.1.33 A rule created in Auto Configuration Setup can be saved to a rule name that already exists.

User Security

- 5.1.34 FlexMaster allows multiple instances of the same user account to be logged in simultaneously.
- 5.1.35 The FlexMaster Web interface automatically logs off any user who has been inactive for five minutes (unless the page in view is the Dashboard).

- 5.1.36 Some pages of the FlexMaster Web interface that use AJAX query the status from the FlexMaster server periodically. If a user navigates to a page that uses AJAX and stays there, the HTTP session will not time out.

AP-related Issues

- 5.1.37 If a wireless client roams between managed APs, the traffic information that FlexMaster receives for that client may be inaccurate.
- 5.1.38 After importing a VeriSign certificate into FlexMaster, the FlexMaster server must be restarted.
- 5.1.39 MediaFlex 2825 and MediaFlex 7811 do not support SpeedFlex.
- 5.1.40 MediaFlex 2825 backup image can only support bare image version 4.2.0.0.6 or later.
- 5.1.41 L2TP tunneling is not supported on ZoneFlex 7025/7343/7363/7762/7762-S/7942/7962 Access Points and ZoneFlex 7731 Wireless Bridge.
- 5.1.42 If an automatic monthly report is created and the date that was set is invalid (for example, FlexMaster was configured to send the report every 31st and the current month only has 30 days), then report will be sent out on the last day of the month.
- 5.1.43 Provisioning a restricted wireless channel to an AP (using a configuration template) changes the AP's wireless mode to SmartSelect automatically (ID 8358).

For example, if the AP's country code is set to US and the administrator creates a configuration template that changes the wireless channel to 13 (a restricted channel in the US), the AP's wireless mode will change to SmartSelect when it is provisioned.
- 5.1.44 Actual AP traffic may not match the AP traffic shown on the AP Device View.
- 5.1.45 In 2-tier management mode, if the inform interval is set to one hour or longer, the AP's downtime information may be incorrect.
- 5.1.46 In a mesh environment, # of Child APs displayed on the FlexMaster Web interface may be incorrect when there are multi-hop APs. This occurs because ZoneDirector reports incorrect numDownlink to FlexMaster when there are eMAPs on the network.

Reports

- 5.1.47 The filter function may not work correctly when applied to client association or disassociation event reports. (ID 13603)
- 5.1.48 Information shown in the Top-N bar chart is inconsistent with the information in the Histogram. The information displayed in the Top-N bar chart is correct. (ID 18468)

SpeedFlex

- 5.1.49 SpeedFlex tests cannot be performed on wireless clients that are associated with standalone APs.
- 5.1.50 SpeedFlex tests cannot be run on MediaFlex 2825 (VF2825) and MediaFlex 7811 (VF7811) APs.

VLANs

- 5.1.51 When creating a VLAN configuration template, note that only the management VLAN is active by default. All other VLANs are inactive, even though they each have a unique VLAN ID by default. To activate one of these VLANs, either assign a wireless interface to it or configure the VLAN tagging of at least one Ethernet port.

- 5.1.52 The VLAN configuration pages on the FlexMaster Web interface and the AP Web interface are inconsistent with each other. On the FlexMaster Web interface, VLAN configuration templates can be saved and provisioned successfully even if no wireless interfaces are bound to any VLAN. On the AP Web interface, on the other hand, VLAN settings cannot be saved successfully unless at least one wireless interface is bound to a VLAN.

Other Caveats

- 5.1.53 This FlexMaster release does not support provisioning a VLAN template that contains 8 VLANs to APs running Release 5.x and earlier.
- 5.1.54 Post factory persistent configuration can be cleared by a factory reset task only in Release 8.0 and later.
- 5.1.55 VF2825 and VF7811 do not support clearing persistent configuration via a factory reset task.
- 5.1.56 FlexMaster currently supports only one SMTP server, but can send email alerts to multiple email recipients.
- 5.1.57 FlexMaster cannot send out email notifications if the SMTP user name and password are not set (ID 20298).
Workaround: Enter the correct SMTP user name and password on the **System Settings > SMTP** page.
- 5.1.58 Client Inventory cannot be exported to CSV successfully if it contains more than 40,000 rows (ID 20318).
Workaround: Export the Client Inventory to an Excel file instead.
- 5.1.59 If the FlexMaster installation is downgraded from 9.x to 8.2 or 8.6 or upgraded from 8.2 or 8.6 to 9.x, the FlexMaster server URL will change.
- 5.1.60 Some of the email addresses configured for alerts (on the Alert Properties page) are lost if FlexMaster is upgraded from version 9.1.0.0.103 to 9.1.1.0.12.
- 5.1.61 This FlexMaster release does not display indoor channel restrictions for outdoor APs. See "Changed Behavior" section below for more information.

5.2 ZoneDirector

General

- 5.2.1 ZoneFlex 7025 is not supported by ZoneDirector 1000
ZoneFlex 7025 Wired/Wireless Wall Switch is not supported by ZoneDirector 1000 (including 1006, 1012, 1025 and 1050). If you have a ZoneFlex 7025, you can manage the device with ZoneDirector 1100 or ZoneDirector 3000 Series, as a Standalone AP, or with FlexMaster.
- 5.2.2 Upgrade from releases prior to 8.2.2
ZoneDirector cannot be directly upgraded to 9.1 from 8.2.1, 8.2.0, 8.1 or earlier versions (ID 16432).
Workaround: upgrade to 8.2.2 or 9.0 before upgrading to 9.1.

5.2.3 AP License

A new AP license upgrade type is supported with release 9.0 or later when compared to 8.2 or earlier releases. The license increases the number of allowed APs by a particular amount (for example, by 50 APs). The previous type increased the AP license from a specific value to a specific value (for example, from 100 APs to 150 APs).

To upgrade the AP license to this new type of license, the administrator must first upgrade ZoneDirector to 9.0 or later, and then apply the new AP license. License types supported by 9.0 or later follow the format `zd_ordernumber_serialnumber_incr450ap3k.lic`.

If an AP license for 8.2 (or earlier version) has not been installed, the administrator must upgrade the AP license on ZoneDirector first, and then upgrade ZoneDirector to release 9.0 or later. License types supported by 8.2 or earlier versions follow the format `zd_ordernumber_serialnumber_12ap.lic`.

Release 9.0 or later is required to increase the AP license above 250 APs. For instance, release 9.0 or later is needed if the ZoneDirector is to be upgraded to support from 300 to 500 APs.

5.2.4 WLANs with Same SSID (ID 16733)

For multiple WLANs using the same SSID, Zero-IT and DPSK can only be enabled on one WLAN.

If ZoneDirector is upgraded from 9.0 to 9.1, and existing WLANs are to be assigned the same SSID, first ensure that Zero-IT and DPSK are disabled on all but one of these WLANs. Otherwise, this will cause problems if the WLANs use different authentication methods.

Workaround: Manually disable Zero-IT and DPSK on all WLANs with the same SSID but one.

- 5.2.5 If an additional management IP interface is used for Web UI management, the actual IP address must still be used when configuring ZoneDirector as a client for a backend RADIUS server, FlexMaster server or in any SNMP systems. If two ZoneDirectors are deployed in a Smart Redundancy configuration, both of the actual IP addresses must be used rather than the management IP. (ID 15259)
- 5.2.6 AP may not forward multicast stream from the wireless interface to the Ethernet interface if it is connected to a switch on which IGMP snooping is enabled because the switch can filter out IGMP network packets between the AP and hosts. (ID 11091)
- 5.2.7 Per node rate information is not included in support.txt output (debug file created when AP System Info button is clicked) due to Flash size limitation. This will be fixed in a future release. (ID 19311)

Web Interface

- 5.2.8 ZoneDirector release 9.1 supports the following Web browsers:

- Firefox 3.0, 3.5, and 3.6
- Internet Explorer 7 and 8
- Safari 5.0
- Chrome 5.0 and 6.0

- 5.2.9 Map View cannot be displayed on Opera browser because Opera uses its own java plug-in.

Workaround: Use Internet Explorer, Firefox, Chrome, Safari to access the ZoneDirector Web interface.

- 5.2.10 Launching the System Info tool from the Monitor > Access Points page in Safari browser causes the AP list to be emptied (ID 16453)
Workaround: None. If you encounter this problem, try using a different browser.
- 5.2.11 ZoneDirector incorrectly displays the value for PHY Errors and % Air Time (total/busy/RX/TX) on the **Monitor > Access Points > [AP MAC Address] > Access Point Information** as zero (ID 15716).
- 5.2.12 Dashboard Usage summary may show incorrect number of rogues (ID 15483).
Workaround: reboot ZoneDirector.
- 5.2.13 AP Noise Floor value is incorrect (ID 14337)
In **Monitor > Access Points > AP MAC Address**, the noise floor value displayed is incorrect.
- 5.2.14 RSSI information for the same Access Point is inconsistent between the Downlinks and Neighbor APs sections on the **Monitor > Access Points > [AP MAC Address]** page. (ID 11527)
- 5.2.15 Web UI displays some text in English when another UI language is selected. Some new or modified text strings have not yet been translated into all languages. This will be updated in a future release. (ID 18839, ID 20160).

SpeedFlex

- 5.2.16 AP device names for SpeedFlex events in the Events/Activities table may not be displayed correctly. (ID 16110)
If DHCP Option 12 is used to configure the AP device name, the full device name rather than only the first 17 characters may be displayed in the Events/Activities table.

SNMP

- 5.2.17 If the SNMP community strings are not changed from their default "private" and "public" values, ZoneDirector's SNMP daemon is susceptible to DoS attack and will terminate after a system vulnerability scan using Nessus (ID 16451, 14441)
Workaround: Do not use default community strings.
- 5.2.18 SNMP trap is not sent when a client authentication fails or is blocked (ID 14998)
- 5.2.19 MIB browsers display the speed of all interfaces on the AP as 10Mbps (ID 12548)
- 5.2.20 The free MIB browser Manage Engine is unable to compile RUCKUS-ZD-WLAN-MIB.txt (ID 16761)
- 5.2.21 SNMP ifSpeed node displays incorrect interface bandwidth when connected to GbE port on L2 switch (ID 18562)

CLI

- 5.2.22 Information for an eMAP node is not displayed using the `show mesh topology` command (ID 16245)

- 5.2.23 The `show-currently-active-clients all` command may consume excessive CPU resources on the ZoneDirector 1000 when many clients are connected, debug log is enabled and other processes are running (such as Real-Time Monitoring), resulting in ZoneDirector disconnecting APs and stations (ID 16736)

Workaround: Disable debug or Real-Time Monitoring to improve performance.

- 5.2.24 The RF statistics may show incorrect values after the AP reboots (ID 13340)

Ethernet Ports and Port-based VLAN

- 5.2.25 If the administrator needs to downgrade ZoneDirector from 9.1 to an earlier release, first undo any configuration changes made to the Access Point Ethernet Port Configuration, either Globally or to individual APs before downgrading. Ensure that all ports are “Enabled” and configured as “VLAN Trunk Port”. If these changes are not first undone, all APs will need to be factory reset. This is because earlier versions do not support the AP Ethernet port configuration features. (ID 15992)

- 5.2.26 ZoneFlex 7300 Series AP Ethernet ports can become disabled if half-duplex is forced on any port. (ID 15915)

Workarounds: Do not force half-duplex on any port; use gigabit port for uplink connection

- 5.2.27 For the ZoneFlex 7025, VLAN IDs 4091 to 4095 are reserved for hardware switch. Setting an access port to any of these VLAN IDs causes unpredictable behavior. (ID 15966)

Workaround: Do not use VLAN IDs in the range 4091 to 4095

- 5.2.28 If an AP is configured with a management VLAN, the same VLAN ID may not be used for port-based VLAN. If you configure the management VLAN and a port with the same VLAN ID, the AP will be unable to join ZoneDirector. (ID 16594)

VLAN, Dynamic VLAN, and Tunnel Mode

- 5.2.29 When configuring or updating the management VLAN settings, make sure that the same VLAN settings are applied on the **Configure > Access Points > Access Point Policies > Management VLAN** page, if APs exist on the same VLAN as ZoneDirector. (ID 11724)

- 5.2.30 If the VLAN, Dynamic VLAN, and Tunnel Mode features are all enabled and they have conflicting rules, ZoneDirector prioritizes and applies these three features in the following order:

1. Dynamic VLAN (top priority)
2. VLAN
3. Tunnel Mode

- 5.2.31 Per-user VLAN segmentation depends on the user credentials configured on the RADIUS server.

- 5.2.32 If Dynamic VLAN and Tunnel Mode are both enabled and the Dynamic VLAN attributes have not been configured on the RADIUS server, the Tunnel Mode rule will override the Dynamic VLAN rule.

- 5.2.33 If Dynamic VLAN and VLAN are both enabled and the Dynamic VLAN attributes have not been configured on the RADIUS server, the VLAN rule will override the Dynamic VLAN rule.

- 5.2.34 L3 tunnel mode voice packets incorrectly sent to data queue (ID 16755)

The new “QoS for Tunnel mode” feature sometimes incorrectly places voice packets into the data queue rather than the voice queue.

DHCP Option 12

5.2.35 If DHCP option 12 is used for naming APs, ZoneDirector will only update an AP's device name from DHCP once, and subsequent changes to the AP's hostname on the DHCP server will not be recognized by ZoneDirector. This is because AP names must be configurable from within ZoneDirector, and if DHCP server host names were to take precedence over ZoneDirector's own naming, admins would be unable to rename APs from within ZoneDirector.

Workaround: Do not rename an AP using DHCP option 12 after it has associated with ZoneDirector. If you do, then you will need to delete the AP entry and let it rejoin, or modify the hostname to RuckusAP and rejoin. (ID 15550)

5.2.36 Do not create DHCP option 12 hostnames of over 64 characters. The maximum length of AP names in ZoneDirector is 64. Therefore, if you create a name with over 64 characters on the DHCP server, ZoneDirector will fail to display the AP hostname correctly and will display the default AP name, "RuckusAP." (ID 15692)

5.2.37 When DHCP option 12 is used and the device name given includes the MAC address, syslog events will include the MAC address twice, while the Web UI will correctly display it only once. i.e.,

- Syslog -> AP[zf7962_0123456789@00:25:c4:14:b9:40]
- GUI -> AP[zf7962_0123456789]

(ID 16167)

AAA Servers

5.2.38 ZoneDirector unable to create new Active Directory or LDAP servers via MIB browser (ID 16395)
The current version does not support AD and LDAP MIBs.

Smart Redundancy

5.2.39 Smart Redundancy versus Limited ZD Discovery

Smart Redundancy supports Active/Standby redundant controller deployments. Configuration and client runtime information is automatically synchronized between controllers so that in the event the Active controller becomes unavailable, the Standby controller can seamlessly take over managing the WLAN.

Limited ZD Discovery configures connected APs with the IP addresses of a Primary and Secondary ZoneDirector that the AP should connect to when reachable. Limited ZD Discovery does not provide configuration or run-time synchronization, and APs need to reboot when joining the Secondary controller to obtain the current configuration.

Ruckus recommends deploying Smart Redundancy instead of Limited ZD Discovery. If Limited ZD Discovery was enabled previously (as with using a release earlier than 9.0), Ruckus recommends disabling it under **Configure > Access Points > Access Point Policies** prior to configuring Smart Redundancy. Limited ZD Discovery can be used concurrently with Smart Redundancy. However, in that case, the Primary and Secondary ZoneDirector IP Address must be configured with the IP Addresses of both ZoneDirectors.

5.2.40 Certificates needed on both ZoneDirectors

If you install a certificate on ZoneDirector to eliminate the browser Security warning, you should install certificates on both ZoneDirector to avoid seeing this warning when the system fails over to the Standby ZoneDirector. Using the Management IP address will not eliminate this requirement.

- 5.2.41 Clicking the “Failover” button from the active ZoneDirector in a Smart Redundancy configuration may cause the original Active ZoneDirector (now Standby) to reboot. (ID 16555)
- 5.2.42 Dashboard layout is not synchronized across ZoneDirectors
- ZoneDirector Dashboard layout – for instance, which widgets are opened, where they are positioned on the Dashboard – is not synchronized between ZoneDirector Smart Redundancy peers. If you want the Dashboard to look the same on both ZoneDirectors, manually replicate the layout on both ZoneDirectors individually.

Smart Mesh Networking

- 5.2.43 In some countries, the set of allowed channels differs between indoor and outdoor access points. Therefore, if an outdoor ZoneFlex Mesh AP is supposed to connect to an indoor AP as its uplink, the two devices can have mismatched allowed channel sets. To resolve this problem, change your backhaul link to an unrestricted channel by configuring the indoor uplink AP by going to **Configure > Access Points > [Edit AP] > Radio A/N (5.0 GHz) > Channel** and selecting a channel such as 149, 153, 157, or 161.
- If you want your mesh backhaul link to use an indoor-only channel, first ensure that all MAPs have joined the network over an unrestricted channel, then enable indoor-only channels through the AP CLI or by configuring **Configure > System > Country Code > Channel Mode** and checking “*Allow indoor channels (allows ZoneFlex Outdoor APs to use channels regulated as indoor use-only)*”. (ID 21380)
- 5.2.44 Smart Mesh networking is not supported on ZoneFlex 7025 Wired/Wireless Wall Switch.
- 5.2.45 Meshing between ZoneFlex 7962 and 7363/7762/7762-S/7762-T APs in US country code
- The ZoneFlex 7962 supports DFS channels in the US country code, while the 7363, 7762/7762-S/7762-T do not. If meshing between these APs, with the 7962 as the Root AP, the APs need to be on a channel usable by all APs. If the 7962 is set to one of the DFS channels, the 7363 and 7762 will not be able to connect to it.
- Workaround: Under **Configure > System > Country Code**, set the Channel Optimization to either *Optimize for Compatibility* or *Optimize for Interoperability*, or set the 7962 Root AP to a non-DFS channel (e.g. channels 149-165).
- 5.2.46 If an eMesh AP is 8 hops away from the RootAP, it will join the mesh, but the information displayed may not be correct (ID 13935).
- 5.2.47 With mesh enabled, ZoneDirector channel selection algorithm sometimes chooses channel 149 for ZoneFlex 7762 access points when a higher channel (161, 165) would provide better performance and stability. (ID 19672)

WLAN Service Schedule

- 5.2.48 Service Schedules, which are used to define the day and time that a WLAN is enabled, are based on the ZoneDirector’s System Time (UTC). WLANs are enabled and disabled based on the ZoneDirector’s time, regardless of where the AP is located.
- 5.2.49 If ZoneDirector is managing APs in different time zones that need the same local-time Service Schedule, create different WLANs with different Service Schedules (based on the ZoneDirector’s UTC time) and apply them to different APs based on time zone. For instance, if the ZoneDirector is in Pacific Time, create WLANPT with Service Schedule M-F, 9 am – 5pm for APs located in the Pacific time zone, and create WLANET with Service Schedule M-F, 6 am – 2 pm for APs located in the Eastern time zone.

When configuring the Service Schedule, your browser will interpret the ZoneDirector's UTC time to your PC's time. For instance, if the ZoneDirector is set to the Pacific time zone, if your PC clock is set to the local Pacific Time, you will see WLANPT configured for M-F, 9 am – 5 pm. If your PC is changed to the local Eastern Time (while ZoneDirector remains on Pacific time zone; for instance, when you travel to New York), you will see WLANPT configured for M-F, 12 pm – 8 pm.

Band Steering

5.2.50 Band steering is disabled on mesh-enabled APs.

Dynamic PSKs

5.2.51 When using an Apple iPhone 4 (iOS version 4.1), Zero-IT may not work correctly if run more than one time (ID 16117).

Workaround: Do not run Zero-IT more than one time. If you have, manually remove the old profile from the iPhone, and install a new Zero-IT provisioning file.

5.2.52 When using an Apple iPhone4 where the Dynamic PSK has expired, the user may not be automatically redirected to the Zero IT activation page to download a new DPSK, or may be prompted to manually enter the PSK even after Zero-IT has configured on the iPhone (ID 16112).

Workaround: Manually remove the old profile from the iPhone, and install a new Zero-IT provisioning file.

5.2.53 When using an Apple iPhone to connect to the ZoneDirector activation page, the Safari browser crashes if AutoFill is enabled. This is a bug in Apple's latest Safari release for iPhone.

Workaround: Disable AutoFill in the iPhone's Safari browser settings (**Settings > Safari > AutoFill**).

5.2.54 iPhone and iPad clients cannot use Zero-IT to automatically authenticate to an 802.1X WLAN if ZoneDirector is used as the authentication server (ID 15997, ID 20130)

Due to a display issue with iOS version 4.1, the Zero-IT configuration tool does not work with 802.1X WLANs using local database for EAP authentication.

5.2.55 When provisioning a Zero-IT/Dynamic Pre-Shared Key on Windows 7 clients over a wireless connection, users are not automatically reconnected to the secured SSID (ID 14960).

Workaround: the end user must manually disconnect from the SSID used to provision the DPSK, and connect to their secured SSID.

5.2.56 ZoneDirector supports dynamic PSK generation on clients running various Windows and Mac OS platforms. However, only users who have the privilege to change the client's wireless settings can run prov.exe (prov.exe is the Ruckus Wireless application that is used to generate the dynamic PSK). Moreover, any user who attempts to run prov.exe will be prompted for his password, even if he is an administrator.

5.2.57 If the maximum number of PSKs that ZoneDirector supports has been reached, the ZoneDirector Web interface may not be accessible after bootup, even if the Status LED shows green. This may be because one or more STAMGR sockets failed to initialize. Typically, this automatically resolves itself after five or so minutes.

The maximum number of PSKs that is supported is

- 1,250 on ZoneDirector 1000 and ZoneDirector 1100
- 5,000 on ZoneDirector 3000 licensed up to 250 APs
- 10,000 on ZoneDirector 3000 licensed up to 500 APs

5.2.58 When the maximum number of PSKs that ZoneDirector supports has been reached, the Web interface may be slower in responding to requests.

5.2.59 ZoneDirector does not delete expired DPSK entries when duplicate DPSK IDs are created (ID 18932).

Guest Access

5.2.60 ZoneDirector doesn't redirect client to a long URL (ID 13896)

If the URL that the user originally visited before being prompt to login with their guest pass is long, they may not be redirected there after successfully logging in.

Workaround: On the **Configure > Guest Access** page, set Redirection to *Redirect to the following URL* rather than *Redirect to the URL that the user intends to visit*.

5.2.61 Additional guest pass keys cannot be created when an exclamation point (!) is used as the first character in the guest pass key (ID 15957)

Workaround: Do not use ! as the first character in guest pass keys.

5.2.62 Batch generated guest passes can be sorted in different orders depending on the number of guest passes entered. (ID 11495)

Captive Portal

5.2.63 Guest captive portal does not work when accessed via HTTPS (ID 3816)

If the guest captive portal is accessed via HTTPS before authentication, the guest user is not redirected to the authentication server.

Workaround: Try browsing to an HTTP page.

5.2.64 Web portal based authentication does not redirect the client to the Web login page if the ZoneDirector and the AP/Client are on the same subnet, but using different VLANs. (ID 11904)

Workaround: If ZoneDirector and APs need to use different VLANs, they should also be placed on different subnets.

WISPr (Hotspot Service)

5.2.65 Cross-subnet clients connection issue with WISPr

In some cases, clients that associate with an AP that is on a different IP subnet than ZoneDirector may need to connect more than once before they can reach the WISPr captive portal. This is because ZoneDirector needs to learn the client addresses first before it can redirect them to the captive portal.

5.2.66 When an AP is connected to ZoneDirector via Layer 3 without tunnel and Hotspot service configured, clients connected to a Hotspot WLAN are not logged out after clicking the Logout button. Instead, an "Error: 404 Not Found" message is displayed and the client remains connected (ID 18904).

Voice

- 5.2.67 Multicast traffic on Vocera communication badges and Vocera App on smartphones may be delayed when a receiver roams (ID 14379).
- 5.2.68 ZoneFlex APs may occasionally be delayed in sending Broadcast or Multicast traffic from when their DTIM interval is scheduled. Devices operating in power save mode may not receive the Broadcast or Multicast traffic, as they may no longer be awake when the traffic is finally sent (ID 14383).
- 5.2.69 Some soft phones (Nortel X-lite) on a client with an Intel 5300 adapter do not work on 802.11n APs (ID 14127).

Workaround: Use 11g AP or different soft phone client

Real-Time Monitoring

- 5.2.70 Real-Time Monitoring loads the ZoneDirector CPU and may impact performance. Ruckus recommends that you run Real-Time Monitoring for only as long as necessary to provide analytical information, and disable it otherwise.
- 5.2.71 Real-Time Monitoring displays incorrect value in # of APs after a reboot (ID 16006)

The Real-Time Monitoring tool displays a period of time prior to ZoneDirector reboot during which the "# of APs" table shows 0. This is because the tool is displaying the start time as when the tool itself was started, rather than when ZoneDirector was rebooted.

Email Alarm

- 5.2.72 Alarm email notification for rogue access points does not include channel information, although it is shown on the Monitor page. (ID 10740)

Bradford Network Access Control (NAC) Server

- 5.2.73 Release 9.1 is not compatible with the Bradford NAC Server software version 4.1.1.192.P7. Instead, release 9.1 works with Bradford software version 4.1.1.252.P12. If you are upgrading ZoneDirector to release 9.1, you will also need to upgrade your Bradford NAC Server to 4.1.1.252.P12. Please contact Bradford for the software update.

SSL Certificates

- 5.2.74 The SSL Certificate authority StartSSL does not accept Certificate Signing Requests (CSRs) with MD5 hash. StartSSL requires SHA1 hashed CSRs. (ID 17636)

Workaround: use another certificate authority that allows MD5 hashed CSRs.

Traffic Shaping

- 5.2.75 When a WLAN is added or removed from a WLAN group in the ZoneDirector Web UI, the access point console displays "Cannot find device "wlan1", Command failed (null):13" error.

Workaround: Do not remove a WLAN from the default WLAN group when the AP console shows "Notice: Traffic shaping computation is still going on."

5.3 ZoneFlex Access Points

General

5.3.1 Configuration of physical ports on a ZoneDirector-controlled AP

- If VLAN tagging is configured for one or more non-tunneled WLANs on ZoneDirector, the VLAN tag will propagate to all physical ports on the access point.
- If VLAN tagging is configured on one or more WLANs (either tunneled or non-tunneled) on ZoneDirector, the VLAN tag will propagate to the physical port on ZoneDirector.

ZoneFlex Access Points

5.3.2 Channels 100 to 140 unsupported by some 802.11a and 802.11a/n clients

Some 802.11a and 802.11a/n clients (such as US-based Atheros, Broadcom, and Centrino NICs) do not support radio channels 100 to 140.

5.3.3 DFS channels support

In this release, Dynamic Frequency Selection (DFS) channels are unavailable for all APs other than ZoneFlex 7962 (restricted by ZoneDirector/AP) when the country code is set to US.

This will be fixed upon FCC approval in a later software release this year.

5.3.4 Video streaming and background scanning issue (ID 8571)

If there is a ZoneFlex 7363/7762/7762-S/T/7962 AP on the network and it is being used to stream video traffic (UDP traffic), Ruckus Wireless recommends that background scanning be disabled (on the **Configure > Services** page) to improve video performance.

Similarly, if a particular WLAN will be used primarily for voice traffic and VoIP clients are expected to roam frequently between APs, disabling background scanning can improve performance (reduce latency) when roaming occurs. In this case, Ruckus recommends disabling background scanning for this specific WLAN only (from the **Configure > WLANs** page).

5.3.5 Enabling or disabling *HTTP Access* or *HTTPS Access* on the **Administration > Management** page of the AP Web interface causes the Web interface to be inaccessible for about one (1) minute. This is because the Web service is restarted immediately after a change in HTTP or HTTPS management access is applied (ID 15753).

5.3.6 Access Ports do not drop untagged ingress packets when the tagged VLAN ID is equal to the configured untagged PVID. (ID 16883)

5.3.7 ZoneFlex 7343/7363 APs experience voice traffic packet loss when ports congested. (ID 18992)

Workaround: Do not transmit high priority (voice/video) traffic at over 20Mbps.

5.3.8 Entering a very long FlexMaster URL on the **Administration > Management** page of the AP Web UI results in incorrect display of the state of Telnet, SSH, HTTP and HTTPS access (ID 16823).

Workaround: Factory reset the AP and reconfigure it.

- 5.3.9 AP automatically reboots when an 802.11b client connects to a WLAN with bss-minrate set to 11Mbps (ID 17835).

Workaround: Do not set bss-minrate to 11Mbps for any WLAN that is expected to support 11b clients.
- 5.3.10 AP CLI command `get scanap wlanX` displays incorrect radio type in the scanned AP list (ID 18465).
- 5.3.11 AP CLI command `get qos ethX` displays incorrect filter values when TOS marking is configured (ID 18717).
- 5.3.12 ZoneFlex 7363 experiences Ethernet port instability when powered by PoE (ID 19053).
- 5.3.13 When multiple VAPs with different vapminrates are configured, the AP does not handle probe response/probe response retries correctly. (ID 20179)

ZoneFlex 7025

- 5.3.14 ZoneFlex 7025 fails to communicate with ZoneDirector 3000 when WAN port is congested. (ID 18986)

Workaround: When testing QoS via congestion, do not modify ZoneDirector configuration.
- 5.3.15 Scan and report for rogue devices is not supported on ZoneFlex 7025.
- 5.3.16 When the LAN 5/Uplink port is congested, wired stations connected to the 7025's LAN 1-LAN 4 ports are unable to pass traffic to the uplink port. (ID 19952)

Workaround: If the wired station uses DHCP and has not yet received an IP address, stop the traffic and make sure the Uplink port is not congested until the wired station gets an IP address.

Interoperability with PoE Switches

- 5.3.17 If a 10/100Mbps PoE injector is used to power a ZoneFlex 7343/7363/7942/7762/7762-S/7962 AP and the injector is connected to a switch port that supports 10/100/1000Mbps, the Ethernet connection of the AP may not work. (ID 7634)

This incompatibility is caused by the link speed negotiation between the AP and the Gigabit-Ethernet port. The AP and the Gigabit-Ethernet port can support 1000Mbps connection, but the PoE injector cannot.

Workaround: Use a Gigabit-Ethernet compliant PoE injector or a 10/100/1000Mbps PoE switch instead. Alternatively, connect the 10/100Mbps PoE injector to a 10/100Mbps switch port, or configure the Gigabit-Ethernet port of the switch to use full duplex at 100Mbps.

5.3.18 ZoneFlex APs support standard Power-over-Ethernet (802.3af). The following PoE switches were tested with ZoneFlex 2942, 2741, 7343, 7363, 7942, and 7962 APs:

- Ruckus ZoneSwitch 4124 and 4224
- Linksys 2008MP
- Linksys SRW 224P
- NetGear FS726TP
- SMC | SMC GS8P-SMART 8P+1SFP
- HP ProCurve-24 2610
- HP ProCurve 2520-8-PoE
- BayStack 470
- D-Link DES-1228P
- TrendNet TPE-S88

6 Upgrading to This Version

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

The ZoneFlex 2925 AP is not supported in this release and, therefore, cannot be upgraded.

6.1 ZoneDirector

- ZoneFlex 2925 APs cannot be upgraded to this release and, therefore, cannot be managed by ZoneDirector running on release 9.1. To continue using the 2925 APs on the network, do one of the following:
 - Cancel the upgrade to release 9.1 and continue using the current ZoneDirector version. 2925 APs can be managed by ZoneDirector releases up to 8.1.
 - Convert the 2925 AP from a ZoneDirector-managed AP to a standalone AP. Do this by resetting the AP to factory default settings. Standalone 2925 APs are supported up to release 8.1.
 - If there is a significant number of 2925 APs on the network, the administrator can provision a ZoneDirector device to manage only these 2925 APs. 2925 APs can be managed by ZoneDirector releases up to 8.1.
 - If FlexMaster exists on the network, any version of FlexMaster can be used to manage 2925 APs (running on release 8.1 or earlier) directly.
- Only ZoneDirector 1000 and ZoneDirector 3000 with firmware versions 8.2.2, 8.4 and 9.0 can be upgraded to this release. Upgrading from any other firmware versions might result in loss of configuration settings. ZoneDirectors that are using firmware version earlier than 8.2.2 (including 8.2.0 and 8.2.1) must be upgraded to 8.2.2, 8.4 or 9.0 before they can be upgraded to 9.1.
- After upgrading to ZoneDirector version 9.1, clear the Web browser cache. This will ensure that the ZoneDirector Web interface shows all the changes and enhancements that were implemented in version 9.1.
- When upgrading ZoneDirector 1000 to 9.1, the administrator may be prompted to reboot ZoneDirector manually to delete temporary files and clear the system memory. This happens when there is insufficient memory to perform the upgrade process.

ZoneDirector 1100

The time taken to upgrade a ZoneDirector 1100 may take up to 15 minutes to complete, depending on which version it is being upgraded from. Do not reset the unit until you know that the system has been successfully upgraded or approximately 15 minutes have passed. Resetting the unit while it is still being upgraded may result in the unit having to be returned as an RMA.

6.2 ZoneFlex Access Points

- Standalone ZoneFlex 2942, 7343, 7363, 7762, 7942, and 7962 units running on version 8.2 and 9.0 can be upgraded to this version
- Standalone ZoneFlex 7762 and 7962 units running on version 8.4 can be upgraded to this version
- Four new ZoneFlex models, 7025, 7762-S, 7762-T and 7341 are not compatible with versions earlier than 9.1.

6.3 Changed Behavior

Upgrading to releases 9.1.2-and-later:

Some countries restrict certain 5 GHz channels to indoor use only. For instance, Germany restricts channels in the 5.15 GHz to 5.25 GHz band to indoor use. When ZoneFlex Outdoor APs and Bridges with 5 GHz radios (ZoneFlex 7762, 7762-S, 7762-T, 7761-CM and 7731) are set to a country code where these restrictions apply, the AP or Bridge can no longer be set to an indoor-only channel and will no longer select from amongst a channel set that includes these indoor-only channels when SmartSelect or Auto Channel selection is used, unless the administrator configures the AP to allow use of these channels. For instance, if the AP is installed in a challenging indoor environment such as a warehouse, the administrator may want to allow the AP to use an indoor-only channel. These channels can be enabled for use through the AP CLI or ZoneDirector Web interface by configuring **Configure > System > Country Code > Channel Mode** and checking *“Allow indoor channels (allows ZoneFlex Outdoor APs to use channels regulated as indoor use-only)”*.

If you have a dual-band ZoneFlex Indoor AP functioning as a RAP with dual-band ZoneFlex Outdoor APs functioning as MAPs, the mesh backhaul link must initially use a channel allowed for outdoor use. Your ZoneFlex Outdoor MAPs may fail to join if the mesh backhaul link is using a restricted indoor-only channel.

From release 9.1 to 9.1.2.0.8:

If using VLAN QoS after upgrading to version 9.1.2.0.8, you will first need to factory reset ZoneDirector before configuring VLAN QoS from the CLI.

If you have configured Access Ports to use a VLAN other than 1 while running version 9.1.0.0.38, when you upgrade to 9.1.2.0.8, the PVID of all Access Ports will revert to 1. (ID 20687)

Workaround: Reapply any Access Port VLAN configurations from the ZoneDirector Web interface after upgrading to 9.1.2.0.8. ZoneDirector will deploy the configuration to all APs correctly.

From release 9.1.0.0.23 to 9.1.0.0.38-and-later:

For US Country Code, ZoneFlex 7962 and 7363 Access Points will no longer use channels 120, 124, or 128 when set to 20 MHz wide channels. The APs will no longer use channels 116, 120, 124, or 128 when set to 40 MHz wide channels.

If your APs were previously configured to “Auto” (ZoneDirector) or “SmartSelect” (Standalone AP) for the 5 GHz channel, the AP will now automatically select from among a channel set that excludes these channels. You do not need to do anything.

If your APs were manually set to one of these channels

1. Change the AP to an alternative channel before upgrading to 9.1.0.0.38 or a later release. Ruckus recommends changing to one of the following channels because these channels have the same power capabilities as channels (116), 120, 124, and 128:
52, 56, 60, 64, 100, 104, 108, 112, 132, 136, 140, 149, 153, 157, 161, 165

This is particularly important if you are using Mesh and had configured a Root AP (RAP) to channel (116), 120, 124, and 128. Using one of these channels will reduce the risk that a mesh link cannot be made due to weak signals.

2. Upgrade the AP to 9.1.0.0.38 or a later release.

Between releases prior-to-8.2 and releases 8.2-and-later:

(Applies to all Roles except the Default Role) If a Role is allowed to create guest passes (by selecting the *Allow guest pass generation* check box in **Configure > Role**), the administrator must also allow that Role to access at least one guest WLANs (under the Allow All WLANs section). Otherwise, users that are assigned this Role will be unable to generate guest passes. (ID 12607)

7 Interoperability Information

ZoneDirector 1000/1100/3000 and ZoneFlex APs use standard protocols to interoperate with third-party Wi-Fi devices. Ruckus Wireless qualifies its functionality on the most common clients.