COMMSCOPE®
RUCKUS®

RUCKUS ZoneDirector 10.5.1 Syslog Event Message Reference Guide

Supporting ZoneDirector 10.5.1

Copyright, Trademark and Proprietary Rights Information

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

Limitation of Liability

Trademarks

Contents

Preface

Contacting RUCKUS Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using https://support.ruckuswireless.com, or go to https://www.ruckuswireless.com and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.

- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.

- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.

- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871

- Canada: 1-855-782-5871

- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.

- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The RUCKUS Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents
- Community Forums—https://forums.ruckuswireless.com/ruckuswireless/categories
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

Document Feedback

RUCKUS is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to RUCKUS at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

RUCKUS Product Documentation Resources

Visit the RUCKUS website to locate related documentation for your product and additional RUCKUS resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

White papers, data sheets, and other product documentation are available at https://www.ruckuswireless.com.

Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at https://commscopeuniversity.myabsorb.com/.

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

Convention	Description	Example
`monospace`	Identifies command syntax examples	`device(config)# interface ethernet 1/1/6`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *RUCKUS Small Cell Release Notes* for more information.

Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

> **NOTE**
> A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

> **ATTENTION**
> An ATTENTION statement indicates some information that you must read before continuing with the current action or task.

> **CAUTION**
> **A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.**

> **DANGER**
> *A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.*

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional.
	Default responses to system prompts are enclosed in square brackets.
{**x**| **y**| **z**}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x|**y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

About This Guide

Introduction

The *RUCKUS ZoneDirector Syslog Event Message Reference Guide* provides descriptions and suggested actions for ZoneDirector version 10.5.1 syslog event messages.

This guide is written for service operators and system administrators who are responsible for managing, configuring, and troubleshooting RUCKUS devices. Consequently, it assumes a basic working knowledge of local area networks, wireless networking and wireless devices.

> **NOTE**
> If release notes are shipped with your RUCKUS product and the information there differs from the information in this guide, follow the instructions in the release notes.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the RUCKUS Support site at:

https://support.ruckuswireless.com/documents.

Changes in This Version

This section lists the changes in syslog event messages between ZoneDirector release 10.5 and 10.5.1.

For a list of changes between 10.4.1 and earlier releases, see the *ZoneDirector 10.4 Syslog Event Message Reference Guide,* available from https://support.ruckuswireless.com.

TABLE 2 Syslog event message changes between versions 10.5 and 10.5.1

New	Old	Change
None	None	None

Related Documentation

In addition to this *Reference Guide,* each ZoneDirector documentation set includes the following:

- *Release Notes*: Provide information about the current software release, including new features, enhancements, and known issues.
- *User Guide*: Provides instructions for setup, configuration and management of ZoneDirector and ZoneFlex access points.
- *Online Help*: Provides a web-based subset of the information contained in the User Guide. The online help is accessible from the web interface and is searchable.
- *Command Line Interface Reference Guide*: Provides a list of available CLI commands along with syntax information and examples to aid in administering ZoneDirector via command line.
- *SNMP Reference Guide*: Provides a list of SNMP MIB objects supported in this release.
- *Upgrade Guide*: Provides information on upgrading ZoneDirector to this release.

Syslog Event Messages

Syslog Event Messages

This document lists the syslog warning and event messages that ZoneDirector sends to a syslog server, along with their severity level and recommended actions, where applicable.

The syslog event messages are current as of ZoneDirector firmware version 10.5.1.

Enabling Syslog Message Delivery

To configure ZoneDirector to send event messages to a syslog server, go to **System** > **System Settings** on the ZoneDirector web interface and scroll down to the **Log Settings** section. Click **Enable reporting to remote syslog server at _____ (IP address)** and enter the IP address of the destination server in the field provided.

FIGURE 1 Enabling syslog event message delivery
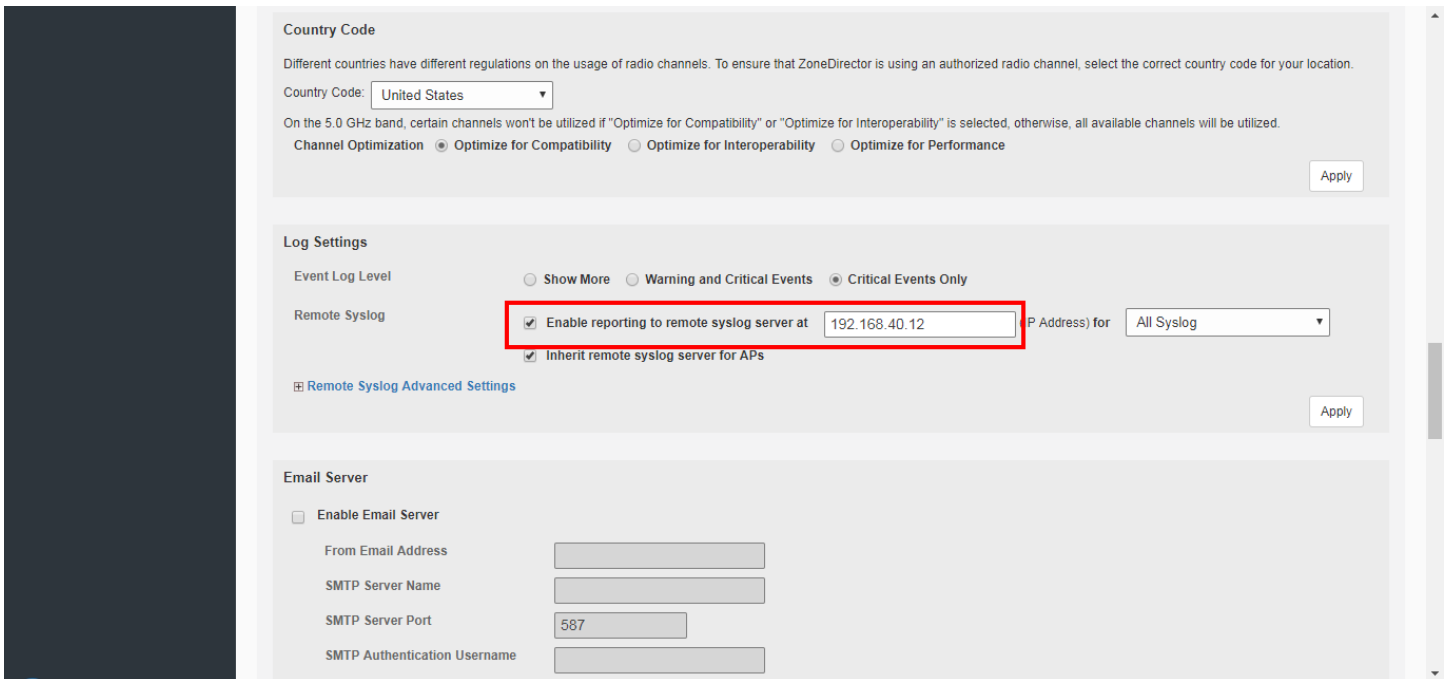
Select the event log level that you would like to receive and click **Apply** to save changes.

Debug Log Settings

You can also select which debug log components should be sent to the syslog server from the **Troubleshooting** > **Diagnostics** page, **Debug Logs** section.

FIGURE 2 Setting debug logs
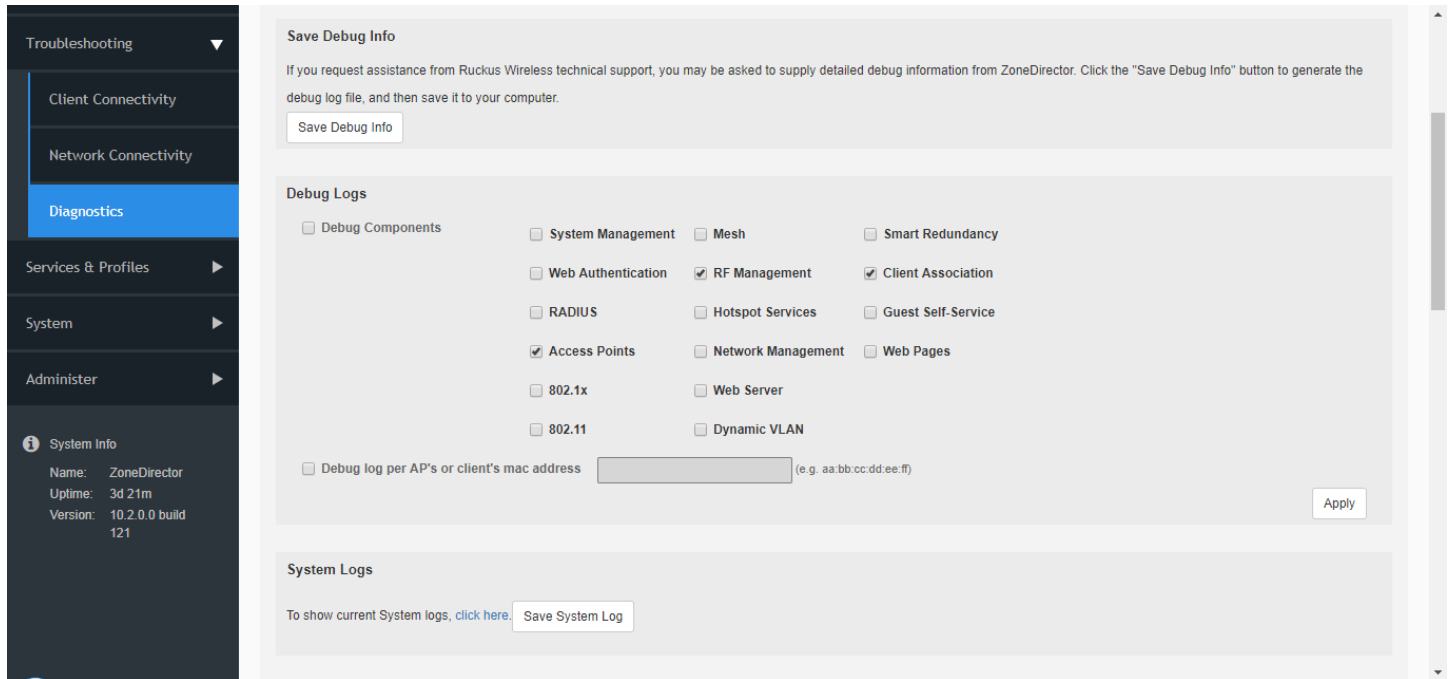
> **NOTE**
> These debug messages are not listed in the following table, which lists ZoneDirector event messages only.

Configuring Remote Syslog Advanced Settings

Advanced Syslog settings allow you to override the default Facility Name and Priority Level of messages sent to the syslog server. In this way, users can separate different kinds of syslogs according to the facility name on the syslog server side.

To configure remote syslog advanced settings:

1. Go to **System** > **System Settings**.

2. Scroll down to **Log Settings**, and expand the **Remote Syslog Advanced Settings** section.

3. In **ZoneDirector Settings**, set the facility name as follows:

    - Keep Original: Retain the original facility name.

    - local0 - local7: Specify facility name.

4. Set the priority level as follows:

    - All: Include all syslog messages.

    - 0(emerg), 1(alert), 2(crit), 3(err), 4(warning), 5(notice), 6(info), 7(debug): Lower numbers indicate higher priority. The syslog server will only receive logs whose priority levels are the same as or lower than the configured level.

5. Repeat step 4 for **Managed AP Settings**. ZoneDirector and Access Points can use different facility and priority settings. All managed APs share the same facility and priority settings.

ZoneDirector Syslog Event Messages

The event messages are a subset of the full syslog and are displayed on the **System** > **All Events/Activities** page.

The options in **System** > **System Settings** > **Log Settings** control the content of the Events/Activities viewer only and not the full syslog (configured in **Troubleshooting** > **Diagnostics**).

Below is a listing of Event log messages.

TABLE 3 ZoneDirector Syslog event messages

ZoneDirector Syslog Message	Severity Level	Action	Explanation
System restarted	Warning	No action required.	ZoneDirector system was restarted.
ZoneDirector service restarted	Warning	No action required.	One of the ZD processes was restarted.
System warm restarted with {reason}	Warning	No action required.	ZD system restart/reboot.
System cold restarted	Warning	Contact Ruckus Technical Support if this message appears frequently.	ZD went through a power-cycle.
System interface {ifindex} linkdown,admin status{ifadmin},adminoper{ifoper}.	Show More	Contact Ruckus Technical Support if this message appears frequently.	ZD's interface (ethernet/bridge) went down.
System interface {ifindex} linkup,admin status{ifadmin},adminoper{ifoper}.	Show More	No action required.	ZD's interface (ethernet/bridge) came back up.
System restarted by administrator.	Show More	No action required.	ZD restarted from GUI/CLI by administrator.
System shutdown by administrator.	Show More	No action required.	ZD shutdown from GUI/CLI by administrator.
System upgraded.	Show More	No action required.	ZD system upgraded to a different software release.
AP patch upgraded.	Show More	No action required.	A new AP model patch has been applied.
SSL certificate replaced by administrator.	Show More	No action required.	ZD's SSL certificate replaced by administrator.
Intermediate certificate added by administrator.	Show More	No action required.	ZD's intermediate certificate added by admin
SSL certificate and private key replaced by administrator for Smart Redundancy.	Show More	No action required.	ZD's SSL certificate and private key replaced by administrator for Smart Redundancy
ZD/AP Ruckus PKI certificates installation started by administrator.	Show More	No action required.	ZD/AP certificate upgrade to Ruckus PKI certificates started.
Private key and SSL certificate renewed by administrator.	Show More	No action required.	ZD's SSL certificate and private key renewed by administrator
Failed to install ZD/AP Ruckus PKI certificates.	Warning	Try again. If you encounter this message frequently, contact Ruckus Technical Support.	Failed to install Ruckus PKI certificate
{zd}/AP Ruckus PKI certificates successfully installed on {zd}.	Warning	No action required.	ZD/AP certificate upgrade to Ruckus PKI certificates successful.
System configuration restored by administrator.	Show More	No action required.	ZD's system configuration restored by administrator
System configuration restored to factory default by administrator.	Show More	No action required.	ZD's system default configuration restored by administrator.
System uses DHCP to obtain IP address.	Show More	No action required.	ZD is using DHCP to obtain system IP address.

TABLE 3 ZoneDirector Syslog event messages (continued)

ZoneDirector Syslog Message	Severity Level	Action	Explanation
System uses Auto Configuration to obtain IPv6 address.	Show More	No action required.	ZD is using IPv6 auto-configuration to obtain system IP address.
System IP mode is set to {ipmode}.	Show More	No action required.	ZD system IP mode set.
System IP address is set to {ip}.	Warning	No action required.	ZD's system IP address was set by administrator.
System IP address is set to {ip}.	Show More	No action required.	ZD's system IP address was set by administrator.
IPv6 address of the system is set to {ipv6}.	Show More	No action required.	ZD's system IP address (IPv6) was set by administrator.
System name is set to {hostname}.	Show More	No action required.	ZD's system name is set/changed.
Admin password changed from {ip}.	Show More	No action required.	ZD's admin password has changed.
Admin has completed the Installation Wizard.	Show More	No action required.	Administrator has completed the installation wizard.
ZD image has been upgraded from {old-version} to {new-version}	Warning	No action required.	ZD's image has been upgraded from <version-1> to <version-2>.
ZD upgrade failed rollback to {old-version}	Warning	Try again. If you encounter this message frequently, contact Ruckus Technical Support.	ZD's image failed to rollback to version mentioned.
ZD upgrade failed, a system reboot is required to rollback to {old-version}	Warning	Reboot ZoneDirector and try again. If you encounter this message frequently, contact Ruckus Technical Support.	ZD's image upgrade failed, system reboot is required to rollback to version mentioned.
ZD upgrade failed, please try again	Warning	Try again. If you encounter this message frequently, contact Ruckus Technical Support.	ZD's image upgrade failed, please try again.
ZD {image} image integrity check passed.	Show More	No action required.	ZD's image integrity check passed.
ZD {image} image is corrupted, use Software Upgrade to repair	Warning	Try again. If you encounter this message frequently, contact Ruckus Technical Support.	ZD's image appears corrupted,please try software upgrade menu to repair system to known image state.
ZD auto-recovery successful	Show More	No action required.	ZD's auto-recovery succeeded.
ZD auto-recovery failed	Critical	Contact Ruckus Technical Support.	ZD's auto-recovery failed.
ZD's dhcp pool is full	Show More	Expand the DHCP pool or remove clients from the existing pool.	ZD's current DHCP pool is full, no new clients can be admitted unless existing clients are removed or pool is expanded.
ZD's dhcp pool is abundant	Show More	No action required.	ZD's current DHCP pool has enough entries to service clients.
UMM logs in from {ip}	Show More	No action required.	Login by UMM specified was successful and was from IP address in message.
UMM logs in failure from {ip}	Show More	Try again. If you encounter this message frequently, contact Ruckus Technical Support.	Login attempt by UMM failed.
{admin} logs in from {ip}	Show More	No action required.	ZD's admin logged in from IP address specified.
{admin} logs in failure from {ip}	Show More	Try again. If you encounter this message frequently, contact Ruckus Technical Support.	ZD's admin login failed.
Unable to authenticate {admin} from {ip} using the specified authentication server (connection error or timeout)	Warning	Try again. If you encounter this message frequently, contact Ruckus Technical Support.	ZD:Unable to authenticate admin (from IP address) using specified authentication server.

TABLE 3 ZoneDirector Syslog event messages (continued)

ZoneDirector Syslog Message	Severity Level	Action	Explanation
{admin} is locked out for 1 hour (20 failed login attempts in 5 minutes)	Warning	Try again. If you encounter this message frequently, contact Ruckus Technical Support.	ZD:Admin is locked out for 1 hour from logging in.
{admin} logged out from {ip}	Show More	No action required.	ZD:Admin has logged out (from IP address)
All clients disconnected by admin	Show More	No action required.	ZD: All clients disconnected by administrator.
Administrator initiates an active scan from all AP's	Show More	No action required.	ZD admin initiates a scan request for all AP's.
Administrator initiates an active scan from {ap}	Show More	No action required.	ZD admin initiates a scan request for specified AP.
Temporary license {name} has expired and all features of this license are disabled	Critical	Contact Ruckus Technical Support to acquire a permanent license.	ZD: temp license has expired and all features dependent on this are disabled.
Temporary license {name} will expire within one day	Warning	Contact Ruckus Technical Support to acquire a permanent license.	ZD: temp license will expire in 1 day.
Temporary license {name} will expire within two days	Show More	Contact Ruckus Technical Support to acquire a permanent license.	ZD: temp license will expire in 2 days.
URL Filtering license {name} with {apnum} APs support will expire within {days} days	Warning	Contact Ruckus Technical Support to acquire a permanent license.	URL filtering license is about to expire.
URL Filtering license {name} has expired	Warning	Contact Ruckus Technical Support to acquire a permanent license.	URL filtering license has expired.
Rogue DHCP server detector enabled	Show More	No action required.	ZD: Rogue DHCP server detector process enabled
Rogue DHCP server detector disabled	Show More	No action required.	ZD: Rogue DHCP server detector process disabled
Rogue DHCP server detector detected	Show More	Locate the rogue DHCP server and disconnect it from the network.	ZD: A rogue DHCP server detected.
Rogue DHCP server detected on {ip}	Critical	Locate the rogue DHCP server and disconnect it from the network.	ZD: Rogue DHCP server detected at IP address specified.
DHCP server enabled with IP range from {ip-start} to {ip-end}	Show More	No action required.	ZD: DHCP server enabled with IP range specified.
Failed to enable DHCP server	Warning	Recheck your DHCP server settings.	Failed to enable DHCP server.
DHCP server disabled	Show More	No action required.	ZD: DHCP server disabled.
UMM management enabled from {url}	Show More	No action required.	ZD: UMM management enabled from specified URL.
UMM management disabled	Show More	No action required.	ZD: UMM management disabled.
SNMP agent v2c enabled with RO-community {ro-community} and RW-community {rw-community}	Show More	No action required.	ZD: SNMP agent version 2 enabled with Read-Only community and Read-Write community specified.
SNMP agent v2c and v3 disabled	Show More	No action required.	ZD: SNMP agent version 2 and version 3 disabled
SNMP v2 Trap enabled with server {trap-ip}	Show More	No action required.	ZD: SNMP version 2 Trap enabled with server IP specified
SNMP v2c and v3 Trap disabled	Show More	No action required.	ZD: SNMP version 2 and version 3 Trap disabled
Set AP management VLAN to {vlan} by admin from {ip}	Show More	No action required.	ZD: AP management VLAN was set by admin from IP address specified.
AP management VLAN setting disabled by admin from {ip}	Show More	No action required.	ZD: AP management VLAN setting was disabled by admin from IP address specified.

TABLE 3 ZoneDirector Syslog event messages (continued)

ZoneDirector Syslog Message	Severity Level	Action	Explanation
AP management VLAN enabled with AP settings by admin from {ip}	Show More	No action required.	ZD: AP management VLAN enabled with AP settings by administrator from IP address specified.
ZoneDirector management VLAN enabled with {vlan} by admin from {ip}	Show More	No action required.	ZD: ZoneDirector management VLAN enabled with VLAN by admin from IP address specified.
ZoneDirector management VLAN disabled by admin from {ip}	Show More	No action required.	ZD: ZoneDirector management VLAN disabled by admin from IP address specified.
Admin from {ip} change to provision all AP's with primary ZoneDirector {ip1} and secondary ZoneDirector {ip2}	Show More	No action required.	ZD: Administrator provisioned all AP's with primary ZoneDirector [IP] and secondary ZoneDirector [IP]
Admin from {ip} change to provision all AP's with primary ZoneDirector {ip1}	Show More	No action required.	ZD: Administrator provisioned all AP's with primary ZoneDirector IP address.
Admin from {ip} remove AP's primary and secondary ZoneDirector settings	Show More	No action required.	ZD: Administrator removed AP's primary and secondary ZoneDirector settings
Additional management interface {ip} created	Show More	No action required.	ZD: Additional management interface with IP address specified was created
Additional management interface {ip} removed	Show More	No action required.	ZD: Additional management interface with IP address specified was removed.
Additional management interface {ip} updated	Show More	No action required.	ZD: Additional management interface with IP address specified was updated.
Additional IPV6 management interface {ipv6} created	Show More	No action required.	ZD: Additional IPV6 management interface specified was created.
Additional IPV6 management interface {ipv6} removed	Show More	No action required.	ZD: Additional IPV6 management interface specified was removed.
Additional IPV6 management interface {ipv6} updated	Show More	No action required.	ZD: Additional IPV6 management interface specified was updated.
Smart Redundancy is {type}	Show More	No action required.	ZD: Smart Redundancy is enabled or disabled.
[Smart Redundancy] Peer Device IP Address changed by Administrator	Show More	No action required.	ZD:Ip Address of active OR standby ZD has been changed by administrator.
[Smart Redundancy] Shared Secret changed by Administrator	Show More	No action required.	ZD: Smart Redundancy Shared Secret (required to establish SR Connection) changed by Administrator
{admin} tried to perform an unauthorized task	Show More	Try again. If you encounter this message frequently, contact Ruckus Technical Support.	ZD: Administrator does not have permission to perform this task.
Enable remote syslog with server {srvip} by admin from {ip}	Show More	No action required.	ZD: Administrator has enabled the remote logging of syslog message.
Disable remote syslog by admin from {ip}	Show More	No action required.	ZD: Administrator has disabled the remote logging of syslog message.
SpeedFlex service is disabled by {username} from {ip}	Show More	No action required.	SpeedFlex service disabled.
SpeedFlex service is enabled by {username} from {ip}	Show More	No action required.	SpeedFlex service enabled.
SNMP request from user-name {user-name} failed authentication	Critical	Try again. If you encounter this message frequently, contact Ruckus Technical Support.	SNMP authentication failed when initiated by {user-name}
SNMP agent v3 enabled, register user {v3-user-name} with role of {v3-user-role}	Show More	No action required.	snmpv3 agent enabled.

TABLE 3 ZoneDirector Syslog event messages (continued)

ZoneDirector Syslog Message	Severity Level	Action	Explanation
SNMP agent started: v2c {v2-eanble},v3 {v3-enable}	Show More	No action required.	snmpv3 and v2c agents started.
SNMP v3 Trap enabled with server {trap-ip} security user {name}	Show More	No action required.	snmpv3 trap is enabled. ZD will sent notification to SNMP server.
System is recovered from failure	Critical	No action required.	System is recovered from some process failure...
Bonjour service enabled	Show More	No action required.	Bonjour service has been enabled.
Bonjour service disabled	Show More	No action required.	Bonjour service has been disabled.
Enable Telnet service	Show More	No action required.	ZD: Administrator has enabled Telnet service on ZD.
Bonjour service is disabled when Bonjour Gateway is enabled	Show More	No action required.	Bonjour service disabled when Bonjour Gateway enabled.
Disable Telnet service	Show More	No action required.	ZD: Administrator has disabled Telnet service on ZD.
LBS ZD sent Start {cn} Location Service: apgroup={apg-name}, venue={venue}	Show More	No action required.	Location service enabled.
MSG_admin_disable_location=LBS ZD sent Stop {cn} Location Service: apgroup={apg-name}, venue={venue}	Show More	No action required.	Location service disabled.
MSG_lbs_ZD_LS_connection_up=LBS the connection becomes up between ZD and LS: url={ls-url}, port={ls-port}	Show More	No action required.	Location service connection is up.
MSG_lbs_ZD_LS_connection_down=LBS the connection becomes down between ZD and LS: url={ls-url}, port={ls-port}, reason={down-reason}	Show More	No action required.	Location service connection is down.
MSG_lbs_receive_cmd_footfall=LBS ZD receives passive tracking footfall command: parameters={parameters}	Show More	No action required.	ZD receives passive tracking footfall command.
MSG_lbs_receive_cmd_calibration=LBS ZD receives passive tracking calibration command: parameters={parameters}	Show More	No action required.	ZD receives passive tracking calibration command.
MSG_lbs_no_response_from_LS=LBS ZD did not receive response from LS: url={ls-url}, port={ls-port}	Show More	No action required.	ZD did not receive response from LS.
MSG_lbs_bridge_auth_failed=LBS ZD-LS authentication failed: url={ls-url}, port={ls-port}	Show More	No action required.	ZD-LS authentication failed.
MSG_lbs_connection_dropped=LBS ZD-LS connection dropped: url={ls-url}, port={ls-port}	Show More	No action required.	ZD-LS connection dropped.
Mesh name changed by admin from {ip}	Show More	No action required.	Mesh SSID has been changed by admin.
Mesh passphrase changed by admin from {ip}	Show More	No action required.	Mesh passphrase changed by admin from IP(address).
Enable global client isolation by admin from {ip}	Show More	No action required.	Enabling of global client isolation by admin from IP (address).
Disable global client isolation by admin from {ip}	Show More	No action required.	Disabling of global client isolation by admin at IP(address).
Enable mesh packet forwarding filter by admin from {ip}	Show More	No action required.	Admin has enabled mesh packet forwarding filter.

TABLE 3 ZoneDirector Syslog event messages (continued)

ZoneDirector Syslog Message	Severity Level	Action	Explanation
Disable mesh packet forwarding filter by admin from {ip}	Show More	No action required.	Admin has disabled mesh packet forwarding filter.
Modify rules of mesh packet forwarding filter by admin from {ip}	Show More	No action required.	Admin has modified mesh packet forwarding filter.
Enable ARP broadcast filter with rate limiting threshold {range} by admin from {ip}	Show More	No action required.	Admin has enabled the AP to limit the ARP broadcast on network. This will help reduce flooding of ARP packets on network.
Disable ARP broadcast filter by admin from {ip}	Show More	No action required.	Enable ARP broadcast filter with rate limiting threshold
{authsvr} modified by admin from {ip}	Show More	No action required.	Authentication server (Radius Server) details is modified by admin.
{authsvr} created by admin from {ip}	Show More	No action required.	Authentication server (Radius Server) details is added by admin.
{authsvr} deleted by admin from {ip}	Show More	No action required.	Authentication server (Radius Server) details is deleted by admin.
all AAA servers RADIUS statistics recorded {period} are reseted from {ip}	Show More	No action required.	All Radius statistics reset by user.
AAA server {svr-name} RADIUS statistics recorded {period} are reseted from {ip}	Show More	No action required.	Radius statistics for specific server reset by user.
AAA server {svr-name} {role} RADIUS statistics recorded the AAA server {svr-name} {svr-ip} RADIUS statistics recorded {period} are reseted from {ip}{period} are reseted from {ip}	Show More	No action required.	Radius statistics for specific Radius server and specific time period reset by user.
all WLANs RADIUS statistics recorded {period} are reseted from {ip}	Show More	No action required.	All WLANs Radius statistics for a specific time period reset by user.
WLAN {wlan-name} RADIUS statistics recorded {period} are reseted from {ip}	Show More	No action required.	Specific WLAN Radius statistics for a specific time period reset by user.
{user-name} from {ip} failed to log in for guest pass generation	Show More	No action required.	Login for guest pass generation is failed.
{user-name} from {ip} failed to log in for wireless access provisioning	Show More	No action required.	User login from IP address specified failed.
{user} from {ip} failed to log in. No permission or incorrect credentials.	Show More	No action required.	User login failed due to lack of permission or incorrect credentials.
{user} failed to log in. No permission or incorrect credentials.	Show More	No action required.	User login failed due to lack of permission or incorrect credentials.
Unable to authenticate {user-name} from {ip} using the specified authentication server (connection error or timeout)	Warning	Try again. If you encounter this message frequently, contact Ruckus Technical Support.	User authentication failed from radius server specified. Check the user name and password.
Radius server {server} has not responded to multiple requests. {reason}.	Warning	Check the RADIUS server settings.	Radius server has not responded to multiple requests. Check if the radius server is up or not. Capture the packets at radius server to verify whether server is receiving the request message.
{user} from {wlan} at {ap} failed to verify the access token for {oauth-server}, detail error: {err-msg}	Warning	Check user social media login credentials.	Error message detailing OAuth social media login failure.
{user} from {wlan} at {ap} failed to match the host domain for {oauth-server}, detail error: {err-msg}	Warning	Check user social media login credentials.	Error message detailing OAuth host domain login failure.

TABLE 3 ZoneDirector Syslog event messages (continued)

ZoneDirector Syslog Message	Severity Level	Action	Explanation
Registering wlan {guestsvc-name} to Facebook.	Show More	No action required.	WLAN registration with facebook.com started.
Register wlan {guestsvc-name} to Facebook success.	Show More	No action required.	WLAN registration with facebook.com successful.
Register wlan {guestsvc-name} to Facebook failed.	Warning	Retry. Ensure connectivity to facebook.com	WLAN registration with facebook.com failed.
Please click "here" below "Facebook WiFi" to configure settings on Facebook.com	Show More	Facebook settings have not yet been configured.	Click the "Configure" button on the side of "Facebook" Social Media Login to configure settings on Facebook.com.
The maximum number of Facebook WiFi profiles in one {zd} is {num}.	Warning	Reduce the number of Facebook WiFi profiles and try again.	Facebook WiFi profiles not created because the max number of Facebook WiFi profiles has been reached.
Receive reauth response from Facebook failed, need to delete all stations in this request.	Warning	No action required.	No reauthorization response received from Facebook.com. All stations in this request will be deleted.
Delete User{sta-mac} from {wlan} at {ap} due to facebook WiFi wlan time out.	Warning	No action required.	Facebook WiFi user timeout; station deleted.
{user} from {ip} approved for guest access (guest pass was generated by {created-by})	Show More	No action required.	User from IP (address) has been approved for guest access.
Guest from {ip} approved for guest access	Show More	No action required.	User has been approved for guest access.
There is no credit, please recharge your account.	Show More	Recharge your account.	Credit exhausted, recharge your account.
{ap} is assigned to {apgroup}	Warning	No action required.	AP is moved to a specified AP group.
{ap} initial provisioning {apgroup} is undefined; AP assigned to system default group	Warning	No action required.	AP group specified not found, hence default AP group has been assigned.
{ap} joins with uptime {uptime} s	Warning	No action required.	AP Joined ZD with uptime specified in secs.
{ap} joins with uptime {uptime} s and last disconnected reason {reason}	Warning	No action required.	AP Joined ZD with uptime secs and last disconnected reason Heartbeat loss/ application reboot/power cycle/Release AP Cmd/reset button/
{ap} fails to join	Warning	Factory reset the AP and try again.	AP fails to join ZD. Trying factory reset of AP may enable it to join ZD.
Model{model} is not supported; connection request from {ap} refused	Warning	This AP model is not supported with this version of ZoneDirector. Downgrade ZoneDirector to a version that supports this AP model, or upgrade AP to a supported model."	AP model unsupported. ZD refused connection request.
Discover request from {ap} is ignored for unsupported model {model} or image	Warning	Upgrade or apply a new AP model patch to support the new AP.	Discover request from AP was ignored due to unsupported AP model or firmware image.
Discover request from {ap} refused; AP limit reached.	Warning	Delete APs from the list to allow new APs to join.	Discover request from AP failed since AP limit has been reached.
Connection request from {ap} refused; AP limit reached.	Warning	Delete APs from the list to allow new APs to join.	Connection request from AP failed since AP limit has been reached.
Discover request from {ap} refused; M510 AP cannot act as a member AP.	Warning	Remove M510 member AP.	Discover request from AP failed because the M510 AP cannot act as a member AP.
Connection request from {ap} is refused;AP limit reached in URL Filtering license.	Warning	Increase URL filtering license AP limit or reduce number of APs.	AP connection request refused because URL filtering license AP limit has been reached.

TABLE 3 ZoneDirector Syslog event messages (continued)

ZoneDirector Syslog Message	Severity Level	Action	Explanation
{num} AP's URL Filtering licenses are needed to enable this feature. Please purchase and renew, and then try again.	Warning	Upgrade URL filtering license to use this feature.	URL filtering license is needed to enable this feature.
No valid license here. Please purchase and renew, and then try again.	Warning	Upgrade URL filtering license to use this feature.	URL filtering license is needed to enable this feature.
Connection request from {ap} refused; country code mismatch.	Warning	Set the AP country code to the same code used by ZoneDirector and try again.	Connection request failed from AP, due to country code mismatch.
{ap} Configuration update request failed.	Critical	Verify connectivity between AP and ZoneDirector.	AP request for configuration update failed.
Hardware problem detected during {ap} attempt to join {reason}.	Critical	Contact Ruckus Technical Support.	ZD discovered number of radio supported on AP is ZERO, so join failed.
{ap} heartbeats lost	Warning	If you encounter this message frequently, contact Ruckus Technical Support.	AP has not received echo(heartbeat) response from ZD.
Lost contact with {ap}	Critical	Check the AP uplink connection (wired or mesh).	ZD is getting Ping request from AP.
{user}	Show More	No action required.	All user PII data has been removed.
{ap} cold boot successfully	Show More	If you encounter this message frequently, contact Ruckus Technical Support.	Power Cycle boot.
{ap} warm boot successfully,last reboot reason {reason}.	Show More	No action required.	Reboot command from AP CLI.
{ap}'s CPU utilization exceeds threshold.	Warning	If you encounter this message frequently, contact Ruckus Technical Support.	AP's CPU utilization exceeds normal thresholds.
{ap}'s Memory utilization exceeds threshold.	Warning	If you encounter this message frequently, contact Ruckus Technical Support.	AP's Memory utilization exceeds normal thresholds.
{ap}'s CPU clear warning that cpu utilization is too high.	Warning	No action required.	AP's CPU is getting overloaded, service may be impacted.
{ap}'s MEM clear warning that mem utilization is too high.	Warning	No action required.	AP's memory utilization is getting overloaded, service may be impacted.
{ap}'s online client number is {value} which exceeds threshold(	Show More	No action required.	Number of clients on AP have exceeded threshold limits indicating AP is getting overloaded.
{ap} can not support DFS channel {channel}.	Warning	Set channels to non-DFS channels.	AP does support DFS channel specified.
{ap} can not support C-Band channel {channel}.	Warning	No action required.	AP does not support C-Band channels (149 – 161).
{ap} download USB Software Package Vendor-ProdID-Version {vid_pid} failed.	Warning	If you encounter this message frequently, contact Ruckus Technical Support.	USB software package download failed.
{ap} downloaded USB Software Package Vendor-ProdID-Version {vid_pid} successfully.	Show More	No action required.	USB software package download was successful.
the USB Software Package Vendor-ProdID-Version {vid_pid} on {ap} is overridden.	Show More	No action required.	USB software package overriden successfully.
{ap} state set to {new-state} with downlink {downlink-state}	Show More	No action required.	AP in new state <state> with downlink <state>. AP could be failing to join due to incorrect configuration. Remove its record from the system.
{ap} state set to {new-state} on channel {channel-radio} with downlink {downlink-state}	Show More	No action required.	AP new state (RAP/ISLAND/MAP WAITING/MAP/e-MAP/Down/(Mesh/eMesh Forming), on channel <xx> with down link Enabled/Disabled.

TABLE 3 ZoneDirector Syslog event messages (continued)

ZoneDirector Syslog Message	Severity Level	Action	Explanation
{ap} state set to {new-state} uplinks to {meshap} across {hops} hops with downlink {downlink-state}	Show More	No action required.	AP new state (RAP/ISLAND/MAP WAITING/MAP/e-MAP/Down/(Mesh/eMesh Forming), on channel <xx> with down link Enabled/Disabled.
{ap} state set to {new-state} uplinks to {meshap} across {hops} hops on channel {channel-radio} with downlink {downlink-state}	Show More	No action required.	AP new state (RAP/ISLAND/MAP WAITING/MAP/e-MAP/Down/(Mesh/eMesh Forming), uplink to mesh AP(name) with number of hops on channel <xx> with down link Enabled/Disabled.
Mesh {ap} connects to Mesh {meshap} with RSSI {rssi} across {mesh-depth} links	Show More	No action required.	Mesh AP connected to another Mesh AP with RSSI <x> and hops <y>
Mesh {ap} connects to Root {rootap} with RSSI {rssi} across {mesh-depth} links	Show More	No action required.	Mesh AP connected to Root AP with RSSI <rssi> and hops <x>
Mesh {ap} accepts Mesh {meshap} connection	Show More	No action required.	Mesh AP accepted connection from another Mesh AP
Root {ap} accepts Mesh {meshap} connection	Show More	No action required.	Root AP accepted connection from another Mesh AP
Mesh {meshap} fails to connect to {ap} (authentication invalid)	Show More	Check the authentication settings on the uplink AP.	Mesh AP failed authenticating to Root AP
Mesh {meshap} disconnects from {ap}	Show More	If you encounter this message frequently, contact Ruckus Technical Support.	Mesh AP disconnected from Root AP
Mesh {ap} disconnects from uplink {meshap}	Critical	If you encounter this message frequently, contact Ruckus Technical Support.	Mesh AP disconnected from uplink Mesh AP
Isolated Mesh {ap} detected	Show More	See User Guide for instructions on isolated Mesh AP recovery.	Isolated /unconnected Mesh AP detected
eMesh {ap} connects to Mesh {meshap} across {mesh-depth} links {rea}	Critical	No action required.	eMesh AP connected to Mesh AP across hops <x>
Mesh {ap} connects to eMesh {linkap} with RSSI {rssi} across {mesh-depth} links {rea}	Critical	No action required.	Mesh AP connected to eMesh AP with RSSI <rssi> across hops <x>
Mesh {ap} accepts eMesh {linkap} connection	Show More	No action required.	Mesh AP accepted connection from eMesh AP
eMesh {ap} accepts Mesh {meshap} connection	Show More	No action required.	eMesh AP accepted connection from Mesh AP
eMesh {ap} disconnects from uplink Mesh {meshap}	Critical	Check the connection to the uplink AP.	eMesh AP disconnected from uplink Mesh AP
Mesh {ap} disconnects from uplink eMesh {linkap}	Critical	Check the connection to the uplink AP.	Mesh AP disconnected from uplink eMesh AP
eMesh {linkap} disconnects from Mesh {ap}	Critical	Check the connection to the uplink AP.	eMesh AP disconnected from Mesh AP specfied
Mesh {meshap} disconnects from eMesh {ap}	Critical	Check the connection to the uplink AP.	Mesh AP disconnected from eMesh AP specified.
{ap} accepts Mesh {meshap} with {hops} hops (hop count exceeds the threshold {threshold} hops).	Warning	Place more wired APs to reduce the number of hops.	Root AP accepted connection from Mesh AP - but hop count exceeded
{ap} accepts Mesh {meshap} and current AP's downlinks {fanout} exceeds threshold {threshold}.	Warning	Place more wired APs to reduce the number of hops.	Root AP accepted connection from Mesh AP - but downlink hop count exceeded
{ap} deleted by administrator	Show More	No action required.	AP deleted by Admin
{ap} restarted by administrator	Show More	No action required.	AP restated by Admin

TABLE 3 ZoneDirector Syslog event messages (continued)

ZoneDirector Syslog Message	Severity Level	Action	Explanation
{ap} is removed from ZD for Migration by administrator	Warning	No action required.	AP removed by Admin for migration.
{ap} released by administrator	Warning	No action required.	AP released by Admin
{ap} reset to factory default by administrator	Show More	No action required.	AP reset to factory default by administrator
{ap} reset to enable mesh function	Show More	No action required.	AP has been reset to enable mesh function
{ap} reset to disable mesh function	Warning	No action required.	AP has been reset to disable mesh function
{ap} reset due to country code change	Show More	No action required.	AP reset due to country code change
{ap} reset due to channel compatibility change	Show More	No action required.	AP reset due to channel compatibility change
{ap} reset due to management vlan change	Show More	No action required.	AP reset due to management vlan change
{ap} reset due to valid work time expired	Warning	No action required.	AP reset due to valid work time expiration
{ap} reset due to IP address change	Warning	No action required.	AP reset due to IP address change
{ap} radio band change from {ori_band} to {new_band}	Warning	No action required.	AP radio band change occurred
{ap} reset due to radio band change from {ori_band} to {new_band}	Warning	No action required.	AP radio band change occurred
{ap} joins with radio band {ap-band}, set to {zd-band}	Warning	No action required.	AP radio band change occurred
{ap} reset due to mesh mode change	Warning	No action required.	AP reset due to mesh mode change
{ap} reset due to WLAN migration	Warning	No action required.	AP reset due to WLAN migration
The IP type of {ap} is PPPoE, which does not support mesh.	Warning	Set the AP IP type to non-PPPoE.	The IP type of AP is PPPoE, which does not support mesh
{ap} reset because its configuration is out of sync with ZoneDirector	Show More	No action required.	AP reset because its configuration is out of sync with ZoneDirector
A new {ap} requests to join and is automatically approved	Show More	No action required.	AP requests to join and is automatically approved
A new {ap} requests to join, pending approval of administrator	Warning	Approve the AP join request.	AP requests to join, pending approval of administrator
{ap} fails to join because of incorrect configuration; unable to authenticate this AP.	Warning	Factory reset the AP and allow it to rejoin.	AP fails to join because of incorrect configuration; unable to authenticate this AP.
An previously known {ap} fails to join due to incorrect configuration. Remove its record from the system.	Warning	Delete the AP from the AP list and allow it to rejoin.	A previously known AP fails to join due to incorrect configuration. Remove its record from the system.
An {ap} fails to join because uplink Mesh {meshap} not found.	Warning	Check the status of the uplink Mesh AP.	AP fails to join because uplink Mesh AP not found.
Allow {ap} to join and its uplink {meshap} is not found.	Warning	Check the status of the uplink Mesh AP.	AP was allowed to join but its uplink AP is not found.
{ap} detects interference on radio {radio} and switches from channel {from-channel} to channel {to-channel}.	Show More	No action required.	AP detects interference on radio band and switches channels
Provision {ap} with primary ZoneDirector {primary-ip}	Warning	No action required.	AP is provisioning with primary ZoneDirector
Provision {ap} with primary ZoneDirector {primary-ip} and AP Group {group}	Warning	No action required.	AP is provisioning with primary ZoneDirector in specific AP Group
Provision {ap} with primary ZoneDirector {primary-ip} and secondary ZoneDirector {secondary-ip}	Warning	No action required.	AP is provisioning with primary and secondary ZoneDirectors

TABLE 3 ZoneDirector Syslog event messages (continued)

ZoneDirector Syslog Message	Severity Level	Action	Explanation
Provision {ap} with primary ZoneDirector {primary-ip}, secondary ZoneDirector {secondary-ip} and AP Group {group}	Warning	No action required.	AP is provisioning with primary and secondary ZoneDirectors in specific AP group
{ap} has been moved to primary ZoneDirector {primary-ip}	Warning	No action required.	AP has been moved to primary ZoneDirector
{ap} has been moved to primary ZoneDirector {primary-ip} and secondary ZoneDirector {secondary-ip}	Warning	No action required.	AP moved to primary ZoneDirector and secondary ZoneDirector
Delete {ap} move-ap action	Warning	No action required.	No information available.
{ap} has moved to primary ZoneDirector {primary-ip}	Warning	No action required.	AP has been moved to primary ZoneDirector
{ap} has incomplete primary addr/secondary addr settings when ZoneDirector keeps AP's primary and secondary addresses settings.	Show More	Check the primary/secondary ZoneDirector address settings on the AP, or configure Limited ZD Discovery to not keep AP's primary/secondary address settings.	AP has incomplete primary and secondary address settings from the ZD
The Channelfly {ap} detects interference on radio {radio} and switches from channel {from-channel} to channel {to-channel}.	Show More	No action required.	The ChannelFly AP detects interference on radio band and switches channels
{ap} detects radar burst on radio {radio} and channel {dfs-channel} goes into non-occupancy period.	Show More	No action required.	AP detects radar burst on radio channel and shuts channel for non-occupancy interval.
{ap} non-occupancy period expires on radio {radio} and switches back to channel {to-channel}.	Show More	No action required.	AP non-occupancy period expires on radio channel and service is restored
{ap} detects interference on radio {radio} and changes transmit power from {from-tx} power to {to-tx} power.	Show More	No action required.	AP detects interference on radio channel and lowers transmit power accordingly
{ap} detects less interference on radio {radio} and changes transmit power from {from-tx} power to {to-tx} power.	show More	No action required.	AP detects less interference on radio channel and raises transmit power accordingly
SpeedFlex: {ap} to {apto} - downlink {downlink}, uplink {uplink}	Show More	No action required.	SpeedFlex: AP to AP down link and uplink throughput results
SpeedFlex: {ap} to {apto} - downlink {downlink}	Show More	No action required.	SpeedFlex: AP to AP downlink throughput results
SpeedFlex: {ap} to {apto} - uplink {uplink}	Show More	No action required.	SpeedFlex: AP to AP uplink throughput results
SpeedFlex: {ap} to ZoneDirector - downlink {downlink}, uplink {uplink}	Show More	No action required.	SpeedFlex: AP to ZD down link and uplink throughput results
SpeedFlex: {ap} to ZoneDirector - downlink {downlink}	Show More	No action required.	SpeedFlex: AP to ZD downlink throughput results
SpeedFlex: {ap} to ZoneDirector - uplink {uplink}	Show More	No action required.	SpeedFlex: AP to ZD uplink throughput results
{ap} Cable Modem interface is down.	Critical	Reboot the Cable Modem interface. If you encounter this message frequenty, contact Ruckus Technical Support.	Cable Modem interface is down
{ap} Cable Modem restarted by administrator.	Show More	No action required.	Cable Modem restarted by admin.
ZD {ip} sends heartbeat to NMS periodically.	Warning	No action required.	ZD sent message to Network Management System (SNMP trap)
A new {rogue} with {ssid} is detected	Critical	Locate the rogue AP and disconnect it from the network.	Rogue AP detected with specific SSID

TABLE 3 ZoneDirector Syslog event messages (continued)

ZoneDirector Syslog Message	Severity Level	Action	Explanation
{rogue}/{ip} with {ssid} is detected by {ap} on the local wired network	Critical	Locate the rogue AP and disconnect it from the network.	Rogue AP(IP) detected with specific SSID on wired network
A new ad-hoc network {adhoc} with {ssid} is detected	Warning	Locate the rogue AP and disconnect it from the network.	An ad-hoc, SSID-spoofing, MAC-spoofing, Same-Network or User-Defined Rogue AP is identified as a Rogue AP and is rejected.
A new user blocked {rogue} with {ssid} is first detected by {ap}.	Warning	Locate the rogue AP and disconnect it from the network.	Same as above.
A new SSID-spoofing {rogue} with {ssid} is first detected by {ap}	Critical	Locate the rogue AP and disconnect it from the network.	Same as above.
A new MAC-spoofing {rogue} with {ssid} is first detected by {ap}	Critical	Locate the rogue AP and disconnect it from the network.	Same as above.
A new Same-Network {rogue} with {ssid} is first detected by {ap}	Warning	Locate the rogue AP and disconnect it from the network.	Same as above.
A {rogue} with {ssid} interferes with {ap} on channel {channel}.	Warning	Locate the rogue AP and disconnect it from the network.	Rogue AP is detected and rejected by RW AP.
Spectrum analysis failed in {ap}	Warning	Check whether the AP supports spectrum analysis.	Spectrum analysis failed.
A Malicious {rogue} detection by {ap} goes away	Critical	No action required.	ZD uses a malicious rogue AP list to store the bssid of malicious AP
{ap} detects excessive probe requests on radio {radio}.	Warning	Possible DoS attack.	Possible attack, notification to 802.11 trace mgmt
{ap} detects excessive 802.11 management frames on radio {radio}.	Warning	Possible DoS attack.	Possible attack, notification to 802.11 trace mgmt
{ap} joins with different firmware/custom file version and is being upgraded.	Warning	No action required.	AP joins with different firmware version and is being upgraded.
{ap} image has been upgraded from {old-ver} to {new-ver}	Show More	No action required.	AP image has been upgraded from <version1> to <version2>
{ap} image has been upgraded from {old-ver} to {new-ver} after {err-cnt} retries.	Show More	No action required.	AP image has been upgraded from <version1> to <version2> after <count> retries.
Failed to upgrade {ap} image from {old-ver} to {new-ver}	Show More	Try again. If you encounter this message frequently, contact Ruckus Technical Support.	AP version upgrade failed. Try again.
Failed to upgrade {ap} image from {old-ver} to {new-ver}, possibly due to incorrect IP address on AP.	Show More	Check the AP's IP address settings.	AP version upgrade failed.
Failed to upgrade {ap} image from {old-ver} to {new-ver} after {err-cnt} retries	Show More	Try again. If you encounter this message frequently, contact Ruckus Technical Support.	AP version upgrade failed. Try again.
{ap} backup image has been upgraded from {old-ver} to {new-ver}	Show More	No action required.	AP backup image has been upgraded from <version1> to <version2> successfully.
{ap} backup image has been upgraded from {old-ver} to {new-ver} after {err-cnt} retries.	Show More	No action required.	AP backup image upgraded successfully.
{ap} backup image has been upgraded from {old-ver} to {new-ver} after {err-cnt} retries.	Show More	No action required.	AP backup image upgraded successfully after x number of retries.
Failed to upgrade {ap} backup image from {old-ver} to {new-ver}	Show More	Try again. If you encounter this message frequently, contact Ruckus Technical Support.	AP backup image upgrade failed. Try again.

TABLE 3 ZoneDirector Syslog event messages (continued)

ZoneDirector Syslog Message	Severity Level	Action	Explanation
Failed to upgrade {ap} backup image from {old-ver} to {new-ver}, possibly due to incorrect IP address on AP.	Show More	Check the AP's IP address settings.	AP backup image upgrade failed.
Failed to upgrade {ap} backup image from {old-ver} to {new-ver} after {err-cnt} retries	Show More	Try again. If you encounter this message frequently, contact Ruckus Technical Support.	AP backup image upgrade failed. Try again.
{ap} custom file has been upgraded to {new-custom}.	Show More	No action required.	AP custom file has been upgraded successfully.
Fail to upgrade {ap} custom file to {new-custom}.	Show More	Try again. If you encounter this message frequently, contact Ruckus Technical Support.	custom file upgrade failed. Try again.
Ruckus PKI certificate of {ap} upgraded.	Show More	No action required.	AP's Ruckus PKI certificate installed or upgraded.
Failed to upgrade Ruckus PKI certificate of {ap}.	Show More	Try again. If you encounter this message frequently, contact Ruckus Technical Support.	AP's Ruckus PKI certificate upgrade failed.
Receiving System Info from {ap}	Show More	No action required.	ZD received system info from AP
Receiving Cable Modem Info from {ap}	Show More	No action required.	ZD received cable modem info from AP
Failed to initialize the configuration of all APs because AP limit exceeded.	Critical	Delete APs from the list to allow new APs to join.	Too many AP's tried to join to ZD. Exceeded AP limit.
Receiving RF Info from {ap}	Show More	No action required.	ZD received RF info from AP
Imported {ap-cnt} APs from backup configuration, {new-apg-cnt} of them AP-group mismatch, {new-wlg-cnt} of them wlan-group mismatch	Show More	No action required.	Imported configuration (from backup) has too many AP's.
{apgrp} modified by admin from {ip}	Show More	No action required.	AP group is modified by an admin
{apgrp} created by admin from {ip}	Show More	No action required.	AP group is created by an admin
{apgrp} deleted by admin from {ip}	Show More	No action required.	AP group is deleted by an admin
{apgrp} of the imported backup configuration is undefined.	Show More	Create the relevant AP Group and import again.	AP group imported from backup configuration undefined.
{wlan} modified by admin from {ip}	Show More	No action required.	Wlan is modified by an admin.
{wlan} created by admin from {ip}	Show More	No action required.	Wlan is created by an admin.
{wlan} deleted by admin from {ip}	Show More	No action required.	Wlan is deleted by an admin.
{wlan} enabled by administrator.	Show More	No action required.	WLAN is enabled by admin.
{wlan} disabled by administrator.	Show More	No action required.	WLAN is disabled by admin.
{wlan} enabled according to service schedule.	Show More	No action required.	WLAN is enabled by service schedule.
{wlan} disabled according to service schedule.	Show More	No action required.	WLAN is disabled by service schedule.
The role {role} is modified by admin, so disconnect the station in this role.	Show More	No action required.	Role is modified by admin, all currently connected stations with this role disconnected.
{role} enabled by administrator.	Show More	No action required.	Role is enabled by admin.
{role} disabled by administrator.	Show More	No action required.	Role is disabled by admin.
{role} enabled according to time range.	Show More	No action required.	Role is enabled by time range.
{role} disabled according to time range.	Show More	No action required.	Role is disabled by time range.
{wlangrp} modified by admin from {ip}	Show More	No action required.	Wlan group is modified by an admin.

TABLE 3 ZoneDirector Syslog event messages (continued)

ZoneDirector Syslog Message	Severity Level	Action	Explanation
{wlangrp} created by admin from {ip}	Show More	No action required.	Wlan group is created by an admin.
{wlangrp} deleted by admin from {ip}	Show More	No action required.	Wlan group is deleted by an admin.
{wlangrp} of the imported backup configuration is undefined.	Show More	Create the relevant WLAN Group and import again.	Wlan group imported from a backup configuration is undefined.
Warning about online client numbers from {ap} exceed threshold {value} is cleared.	Show More	No action required.	AP Warning about the online client number exceeding threshold is cleared
{ap} is online.	Show More	No action required.	AP is online
{ap} wireless interface experienced high reception error.	Show More	Reboot the AP. If you encounter this message frequently, contact Ruckus Technical Support.	AP wireless interface experienced high reception errors.
System CPU utilization {util} exceeds threshold {value}, {count} times.	Warning	Disable debug mode or stop Real Time Monitoring to free resources.	System CPU utilization exceeded threshold<count> times.
System memory utilization {util} exceeds threshold {value}, {count} times.	Warning	Disable debug mode or stop Real Time Monitoring to free resources.	System memory utilization exceeded threshold <count> times.
System CPU utilization {util} is less than threshold {value}, and clears warning {count} times.	Warning	No action required.	System CPU utilization less than threshold warning cleared <count> times.
System memory utilization {util} is less than threshold {value}, and clears warning {count} times.	Warning	No action required.	System memory utilization less than threshold warning cleared <count> times.
System bandwidth utilization {util} exceeds threshold {value}.	Warning	Reduce bandwidth utilization.	System bandwidth utilization exceeded threshold <value>.
System packet-drop rate {util} exceeds threshold {value}.	Warning	Check client connectivity.	System packet drop rate exceeded threshold.
{ap} fails to synchronize clock with ZoneDirector	Warning	If you encounter this message frequently, contact Ruckus Technical Support.	AP clock synchronization with ZD failed.
Radio {radio} of {ap} has switched wlan group from {old-group} to {new-group}	Show More	No action required.	AP radio has switched wlan group from <group1> to <group2>.
[Smart Redundancy] Peer {zd}{peer-ip} has upgraded AP patch.	Show More	No action required.	A new AP model patch has been applied to the peer ZD.
[Smart Redundancy] AP patch upgrading command received from peer {zd}{peer-ip}	Show More	No action required.	The peer ZD has sent a request for a new AP model patch.
[Smart Redundancy] Peer ZoneDirector{peer-ip} has been restored.	Critical	No action required.	[Smart Redundancy] Peer ZD configuration has been restored.
[Smart Redundancy] System is being upgraded per command from peer ZoneDirector{peer-ip}	Critical	No action required.	[Smart Redundancy] System received upgrade command from peer ZD.
[Smart Redundancy] System restored command received from peer ZoneDirector{peer-ip}	Critical	No action required.	[Smart Redundancy] System received configuration restore command from peer ZD.
[Smart Redundancy] Could not retrieve necessary file from peer ZoneDirector{peer-ip}. Operation aborted.	Critical	Try again. If you encounter this message frequently, contact Ruckus Technical Support.	[Smart Redundancy] System could not retrieve necessary file from peer ZD. Operation aborted.
[Smart Redundancy] Peer ZoneDirector{peer-ip} image has been upgraded from {old-version} to {new-version}. System is being upgraded.	Warning	No action required.	[Smart Redundancy] Peer ZD image has been upgraded successfully. System is being upgraded
[Smart Redundancy] System upgraded, peer ZoneDirector upgrade pending.	Critical	No action required.	[Smart Redundancy] System has been upgraded and peer ZD upgrade is pending.

TABLE 3 ZoneDirector Syslog event messages (continued)

ZoneDirector Syslog Message	Severity Level	Action	Explanation
[Smart Redundancy] System upgraded, peer ZoneDirector upgrade pending.	Critical	No action required.	
[Smart Redundancy] Peer ZoneDirector{peer-ip} upgrade failed.	Critical	Try again. If you encounter this message frequently, contact Ruckus Technical Support.	[Smart Redundancy] Peer ZD upgrade failed.
[Smart Redundancy] Sync configuration to peer ZoneDirector{peer-ip}	Critical	No action required.	[Smart Redundancy] System sync configuration to peer ZD.
[Smart Redundancy] System ready to sync configuration from peer ZoneDirector{peer-ip}	Critical	No action required.	[Smart Redundancy] System is about to sync configuration from peer ZD.
[Smart Redundancy] Sync configuration from peer ZoneDirector{peer-ip}	Show More	No action required.	[Smart Redundancy] System finished configuration sync from peer ZD.
[Smart Redundancy] Standby ZoneDirector has more recent configuration than the active ZoneDirector	Critical	Do not make configuration changes on the standby ZoneDirector.	[Smart Redundancy] Standby ZD has more recent configuration than the active ZD.
[Smart Redundancy] Failed to sync configuration from peer ZoneDirector{peer-ip} due to {lmsg}	Show More	Try again. If you encounter this message frequently, contact Ruckus Technical Support.	[Smart Redundancy] System failed to sync configuration from peer ZD with reason.
[Smart Redundancy] Admin forces a failover to peer ZoneDirector{peer-ip}	Critical	No action required.	[Smart Redundancy] Admin forced a failover to peer ZD.
[Smart Redundancy] Received failover command to change state to {to-state} from peer ZoneDirector{peer-ip}	Critical	No action required.	[Smart Redundancy] System received failover command from peer ZD to change state.
[Smart Redundancy] Failed! Firmware version mismatch	Critical	Ensure that both peers in a Smart Redundancy configuration have the same firmware version.	[Smart Redundancy] System detected mismatch of peer ZD firmware version.
[Smart Redundancy] Failed! AP Firmware version mismatch	Warning	Ensure that any new AP model patch files that have been imported into one ZD have also been applied to the peer.	[Smart Redundancy] System detected a mismatch of peer ZD's AP firmware version.
[Smart Redundancy] New SR has lower licensed APs	Warning	Ensure that you have enough AP licenses for your APs on both SR peers.	[Smart Redundancy] The New SR peer device has a lower number of AP licenses.
[Smart Redundancy] New SR has lower licensed APs	Warning		[Smart Redundancy] The New SR peer device has a lower number of AP licenses.
[Smart Redundancy] Model mismatch (i.e. ZD1000 cannot pair with ZD3000)	Critical	Ensure that both peers in a Smart Redundancy configuration are the same model.	[Smart Redundancy] System detected mismatch of peer ZD model (i.e. ZD1000 cannot pair with ZD3000).
[Smart Redundancy] Connection from peer {zd} IP address is different from that configured	Critical	Check the IP address of the peer ZoneDirector.	[Smart Redundancy] System detected IP address from peer ZD connection is different from that configured.
[Smart Redundancy] Received unrecognized command from peer ZoneDirector{peer-ip}, it may be caused by Shared Secret mismatch	Critical	Ensure that the Shared Secret is the same on both Smart Redundancy peers.	[Smart Redundancy] System received unrecognized command from peer ZD that could be caused by shared scret mismatch.
[Smart Redundancy] System state changed to {state} due to {reason}	Critical	No action required.	[Smart Redundancy] System state changed with reason.
[Smart Redundancy] Peer ZoneDirector{peer-ip} not found, system changed to active state.	Critical	Check connectivity between Smart Redundancy peers.	[Smart Redundancy] Peer ZD connection lost, system changed to active state.
[Smart Redundancy] Peer ZoneDirector{peer-ip} connected, system is in active state.	Critical	No action required.	[Smart Redundancy] Peer ZD connected, system is in active state.

TABLE 3 ZoneDirector Syslog event messages (continued)

ZoneDirector Syslog Message	Severity Level	Action	Explanation
[Smart Redundancy] Peer ZoneDirector{peer-ip} connected, system is in standby state.	Critical	No action required.	[Smart Redundancy] Peer ZD connected, system is in standby state.
[Smart Redundancy] Lost connection to peer ZoneDirector{peer-ip}, system is in active state.	Critical	Check connectivity between Smart Redundancy peers.	[Smart Redundancy] Lost connection to peer ZD, system is in active state.
[Smart Redundancy] Lost connection to peer ZoneDirector{peer-ip}, system is in standby state.	Critical	Check connectivity between Smart Redundancy peers.	[Smart Redundancy] Lost connection to peer ZD, system is in standby state.
[Smart Redundancy] System is currently being upgraded; disconnected from peer ZoneDirector.	Critical	No action required.	[Smart Redundancy] System is currently being upgraded; disconnect from peer ZD.
[Smart Redundancy] Peer ZoneDirector is being upgraded.	Critical	No action required.	[Smart Redundancy] Peer ZD is being upgraded.
[Smart Redundancy] Peer ZoneDirector did not reconnect after upgrade or restore configuration. Local Upgrade is aborted, please check the peer ZoneDirector.	Warning	No action required.	[Smart Redundancy] Peer ZD did not reconnect after upgrade. System is being upgraded automatically.
[Smart Redundancy] System received command {cmd} from peer ZoneDirector but the command has been completed already due to connection timeout.	Critical	No action required.	[Smart Redundancy] System completed upgrade due to timeout in connection to peer ZD without waiting for upgrade command sent from peer ZD.
[Smart Redundancy] Peer ZoneDirector{peer-ip} is being upgraded by administrator to sync up firmware version.	Critical	No action required.	[Smart Redundancy] Peer ZD is being upgraded by administrator to sync up firmware version.
[Smart Redundancy] System is being upgraded by administrator to sync up firmware version.	Critical	No action required.	[Smart Redundancy] System is being upgraded by administrator to sync up firmware version.
[Smart Redundancy] Peer ZoneDirector{peer-ip} is lost after upgrade. Please check the status of Peer ZoneDirector.	Critical	Check the status of the peer ZoneDirector.	[Smart Redundancy] Peer ZD IP address lost after upgrade. Please check the status of the peer ZD.
Administrator decide to use {higher} Smart Redundancy license.	Show More	No action required.	[Smart Redundancy] The admin has selected a higher number of combined AP licenses.
{ap} is reset for Smart Redundancy.	Critical	No action required.	AP reboot due to Smart Redundancy.
Upgrade or Restore is pending... Please wait about 10-15 minutes to try again.	Critical	Try again after 10-15 minutes.	Upgrade or restore pending.
{wlan} has been deployed on radio {radio} of {ap} with {vap}	Show More	No action required.	Wlan has been deployed on Radio of of AP with VAP
{wlan} with {vap} has been removed from radio {radio} of {ap}	Show More	No action required.	Wlan with VAP has been removed from Radio of AP.
{wlan} with {vap} configuration has been updated on radio {radio} of {ap}	Show More	No action required.	Wlan with VAP configuration has been updated on Radio of AP.
{wlan} with {vap} has been deployed on radio {radio} of {ap} after retry.	Show More	No action required.	Wlan with VAP has been deployed on Radio of AP after retry.
{wlan} with {vap} configuration has been updated on radio {radio} of {ap} after retry	Show More	No action required.	Wlan with VAP configuration has been updated on Radio of AP after retry.
{wlan} with {vap} has been removed from radio {radio} of {ap} after retry	Show More	No action required.	Wlan with VAP has been removed from Radio of AP after retry.
Failed to deploy {wlan} on radio {radio} of {ap}	Show More	Reboot the AP. If you encounter this message frequently, contact Ruckus Technical Support.	Failure to deploy Wlan on Radio of Ap.

TABLE 3 ZoneDirector Syslog event messages (continued)

ZoneDirector Syslog Message	Severity Level	Action	Explanation
Failed to remove {wlan} from radio {radio} of {ap}	Show More	Reboot the AP. If you encounter this message frequently, contact Ruckus Technical Support.	Failure to remove Wlan from Radio of AP.
Failed to update {wlan} configuration of radio {radio} of {ap}	Show More	Reboot the AP. If you encounter this message frequently, contact Ruckus Technical Support.	Failure to update Wlan configuration of Radio of AP.
Failed to deploy {wlan} on radio {radio} of {ap}, try again.	Show More	Reboot the AP. If you encounter this message frequently, contact Ruckus Technical Support.	Failure to deploy Wlan on Radio of AP.
Failed to update {wlan} configuration of radio {radio} of {ap},try again.	Show More	Reboot the AP. If you encounter this message frequently, contact Ruckus Technical Support.	Failure to update Wlan configuration of Radio of AP.
Failed to remove {wlan} configuration of radio {radio} of {ap},try again.	Show More	Reboot the AP. If you encounter this message frequently, contact Ruckus Technical Support.	Failure to remove Wlan configuration of Radio of AP.
{wlan} cannot be deployed to radio {radio} of {ap} because this WLAN is only bound to radio {bound_radio}.	Show More	No action required.	WLAN cannot be deployed to the AP's radio because the bound radio is unavailable on this AP.
{wlan} cannot be deployed to radio {radio} of {ap} because its suiteb192 WLAN and AP mode {model} does not support it.	Show More	No action required.	WLAN cannot be deployed to the AP because this AP model does not support Suite B 192-bit profile for TLS.
Wired {user} joins {port} from {ap}	show More	No action required.	Wired client joins port at AP.
Wired {user} disconnected by admin from {port} at {ap}	Show More	No action required.	Wired client disconnected by admin from port at AP.
Wired {user} leave from {port} at {ap}	Show More	No action required.	Wired client leaves from port at AP.
Wired {user} IEEE 802.1X authentication failed from {port} at {ap}	Show More	Check authentication settings on AP port and wired client.	IEEE 802.1X authentication failed on wired client from port at AP.
{user} joins {wlan} from {ap}	Show More	No action required.	Client joined WLAN from AP.
{user} with {vlan} joins {wlan} from {ap}	Show More	No action required.	Client with VLAN joined WLAN from AP.
{user} rejoins {wlan} from {ap}	Show More	No action required.	Client rejoins WLAN from AP.
{user} with {vlan} rejoins {wlan} from {ap}	Show More	No action required.	Client with VLAN rejoins WLAN from AP.
{user} fails to join {wlan} from {ap}	Show More	Check user authentication credentials.	Client failed to join WLAN from AP.
{user} is refused access to {wlan} from {ap} because there are too many users on that AP, WLAN, or Radio.	Show More	Increase APs to provide additional capacity.	Client refused to join WLAN from ap because there are too many users on that AP, WLAN, or Radio.
{user} fails to join {wlan} from {ap} due to authentication failure	Show More	Check user authentication credentials.	Client failed to join WLAN from AP due to authentication failure.
{user} idle timeout and disconnected from {wlan} at {ap}	Show More	No action required.	Client idle timeout and disconnected from WLAN at AP.
{user} disconnects from {wlan} at {ap}	Show More	No action required.	Client disconnected from WLAN at AP.
{ap} radio {radiofrom} detects {user} in {wlan} roams out to {apto}	Show More	No action required.	AP (from) radio detected client in WLAN roams out to AP(to).
{ap} radio {radioto} detects {user} in {wlan} roams from {apfrom}	Show More	No action required.	AP(to) radio detected client in WLAN roams from AP(from).
{user} disconnected by admin from {wlan} at {ap}	Show More	No action required.	Client disconnected by admin from WLAN at AP.
{user} logged out by user from {wlan} at {ap}	Show More	No action required.	User logged out from WLAN at AP.
{user} disconnected by timebased rule from {wlan} at {ap}	Show More	No action required.	Client disconnected by timebased rule from WLAN at AP.

TABLE 3 ZoneDirector Syslog event messages (continued)

ZoneDirector Syslog Message	Severity Level	Action	Explanation
{user} disassociated from {wlan} due to timeout waiting for AP to add station.	Show More	No action required.	Client disassociated from WLAN due to timeout waiting for AP to add station.
{user} joins {wlan} from {ap} with {rssi} and client's rssi is below threshold {rssi-threshold}	show More	No action required.	Client joined WLAN from AP with rssi and client's rssi is below rssi-threshold.
{user} leave {wlan} at {ap} with {session_time} {rx_bytes} {tx_bytes}	Show More	No action required.	Client leaves WLAN at AP with session_time, rx_bytes, and tx_bytes.
The Authorization of {user} is changed by Radius CoA	Show More	No action required.	User authorization status changed due to CoA (change of authorization) message from RADIUS.
{user} disassociated from {wlan} at {ap} due to timeout during authentication.	Show More	Check user authentication credentials.	Client disassociated from WLAN at AP due to timeout during authentication.
User{sta-mac} disassociated from {wlan} at {ap} due to force DHCP timeout. User IP {sta-ip}, {vlan}, DHCPassigned-IP {sta-dhcp-ip}, DHCP lease time {sta-dhcplease}.	Show More	No action required.	User disassociated due to force DHCP timeout.
{user} tries to connect to an unauthorized {wlan}	Warning	No action required.	Client tried to connect to an unauthorized WLAN.
{user} session time limit exceeded; session terminated	Show More	No action required.	client session time limit exceeded; session terminated.
{user} of {wlan} is authorized at {ap}	Show More	No action required.	Client of WLAN is authorized at AP.
{user} repeatedly fails authentication when joining {wlan} at {ap}.	Warning	Check user authentication credentials.	Client repeatedly failed authentication when joining WLAN at AP.
{user} fails authentication too many times in a row when joining {wlan} at {ap}. {user} is temporarily blocked from the system for {block}.	Critical	Check user authentication credentials.	Client failed authentication too many times in a row when joining WLAN at AP. Client is temporarily blocked from system for some time.
{user} fails to login {wlan} at {ap} too many times and is temporarily blocked from login for {block}.	Warning	Check user authentication credentials.	Client failed to login WLAN at AP too many times and is temporarily blocked from login for some time.
{mac} attempts to login to {wlan} at {ap} too many times and is temporarily blocked from login for {block}.	Warning	Check user authentication credentials.	Device with mac address attempted to login to WLAN at AP too many times and is temporarily blocked from login.
Temporary blocking of User{user-name} unblocked.	Warning	No action required.	Temporary blocking of username (client) unblocked.
Temporary blocking of {mac} unblocked.	Warning	No action required.	Temporary blocking of device with mac address unblocked.
User{user-name} has acquired a new Dynamic PSK.	Show More	No action required.	Client has acquired a new Dynamic PSK.
Administrator has acquired batch generation of {num} new Dynamic PSKs.	Show More	No action required.	Administrator has acquired batch generation of # new Dynamic PSKs.
{user}'s access is restricted because of an expired Dynamic PSK.	Show More	Create a new Dynamic PSK for this user. If you encounter this message frequently, increase Dynamic PSK expiration value.	Client access is restricted because of an expired Dynamic PSK.
{user} has renewed a Dynamic PSK.	Show More	No action required.	Client has renewed a Dynamic PSK.
{user} reconnects to {ap} within grace period. No additional authentication is required.	Show More	No action required.	Client reconnected to AP within grace period. No additional authentication is required.
DPSKs of WLAN{wlan-name} are deleted.	Show More	No action required.	DPSKs deleted for a WLAN.

TABLE 3 ZoneDirector Syslog event messages (continued)

ZoneDirector Syslog Message	Severity Level	Action	Explanation
{user} of {wlan} can not be allowed temporarily due to internal error	Show More	No action required.	Client is temporarily blocked due to an internal error.
UMM {url} sends a bad {file} file.	Critical	Try again. If you encounter this message frequently, contact Ruckus Technical Support.	System received a bad file from UMM.
UMM {url} issues image upgrade command.	Show More	No action required.	System received image upgrade command from UMM.
UMM {url} issues restart command.	Show More	No action required.	System received restart command from UMM.
UMM {url} issues restore command {action}.	Show More	No action required.	System received restore command from UMM.
ZoneDirector contacts UMM {status}.	Show More	No action required.	System contacted UMM failed/successfully.
UMM {url} issues command to write configuration template.	Show More	No action required.	System received command(write configuration template) from UMM.
ZoneDirector successfully writes configuration template successfully cmdkey {cmdkey}.	Critical	No action required.	System wrote configuration template successfully with cmdkey from UMM.
Write template fail due to {err} cmdkey {cmdkey}.	Critical	Try again. If you encounter this message frequently, contact Ruckus Technical Support.	System failed to write configuration template. Error indicated for cmdkey which failed.
ZoneDirector fails to retrieve template file from UMM{url} cmdkey {cmdkey}.	Show More	Try again. If you encounter this message frequently, contact Ruckus Technical Support.	System failed to retrieve template file from UMM with cmdkey.
ZoneDirector file download from UMM{url} timeout cmdkey {cmdkey}.	Show More	Check connectivity between ZoneDirector and UMM.	System timeout downloading file from UMM with cmdkey.
UMM {url} changes the UMM monitoring event list.	Show More	No action required.	UMM changed the monitoring event list.
ZoneDirector is not Active and skips UMM {url} command cmdkey {cmdkey}.	Show More	No action required.	System is not in active state and skips UMM command.
SMTP server {name} unavailable.	Warning	Check connectivity between ZoneDirector and SMTP server.	System is unable to connect to SMTP server.
RADIUS authentication server {ip} unavailable.	Warning	Check connectivity between ZoneDirector and RADIUS server.	RADIUS authentication server unavailable.
RADIUS accounting server {ip} unavailable.	Warning	Check connectivity between ZoneDirector and RADIUS server.	RADIUS accounting server unavailable.
SSID{id} RADIUS authentication server {change} to {server}.	Warning	No action required.	Reconnect/Failover to Radius authentication server
SSID{id} RADIUS accounting server {change} to {server}.	Warning	No action required.	Reconnect/Failover to Radius accounting server.
RADIUS authentication server {change} to {server}.	Warning	No action required.	Reconnect/Failover to Radius authentication server.
Bonjour Gateway automatically reboot for the following reason:{reason}.	Warning	No action required.	Bonjour Gateway service rebooted.
Bonjour Gateway is started.	Show More	No action required.	Bonjour Gateway service started.
Bonjour Gateway is stopped.	Show More	No action required.	Bonjour Gateway service stopped.
Bonjour Gateway restart.	Show More	No action required.	Bonjour Gateway service restarted.
Sensor {desc} status is {status}	Critical	No action required.	Sensor description and it's status
Turn On the the {ap}'s ChannelFly according to {apgrp} setting.	Show More	No action required.	ChannelFly enabled for this AP based on AP Group settings.

TABLE 3 ZoneDirector Syslog event messages (continued)

ZoneDirector Syslog Message	Severity Level	Action	Explanation
Turn Off the the {ap}'s ChannelFly according to {apgrp} setting.	Show More	No action required.	ChannelFly disabled for this AP based on AP Group settings.
Spectrum analysis of {ap} is enabled	Show More	No action required.	AP Spectrum Analysis feature enabled.
Spectrum analysis of {ap} is disabled	Show More	No action required.	AP Spectrum Analysis feature disabled.
Support Entitlement file has been downloaded from the {cn} Entitlement Server.	Warning	No action required.	Support Entitlement file has been downloaded from the Ruckus Entitlement Server.
Failed to download the Support Entitlement file from the {cn} Entitlement Server.	Critical	Try again. If the problem persists, check your connection to the entitlement server, and check the status of your entitlements.	Failed to download the Support Entitlement file from the Ruckus Entitlement Server.
Synchronized the URL Filtering License file from the {cn} Server	Show More	No action required.	URL filtering license file synchronized.
Failed to download the URL Filtering License file from the {cn} Server	Warning	Try again. If the problem persists, check your connection to the URL filtering license server, and check the status of your URL filtering license.	Failed to download the URL filtering license file from the Ruckus license server.
URL Filtering is disabled due to insufficient license	Warning	Update URL filtering license file.	URL filtering disabled due to insufficient license.
The URL Filtering licenses entitled to {1} APs on this Wireless Controller appear to expire in {2} days. Please contact Support for further assistance.	Warning	No action required.	URL filtering license about to expire.
The URL Filtering licenses on this Wireless Controller appear to have expired,valid licenses are:{1}-less than connected APs,this feature is disabled. Please contact Support for further assistance.	Warning	No action required.	URL filtering license expired.
The URL filtering will be enabled for 90 days using temporary license. Within these 90 days, a valid URL filtering license must be loaded. Otherwise, URL filtering will be disabled until a valid license is loaded.	Warning	No action required.	Temporary URL filtering license valid for 90 days.
Radio {radioindex} of {ap} is ON	Warning	No action required.	AP radio has been turned on.
{radioindex} of {ap} is OFF	Warning	No action required.	AP radio has been turned off.
User{pppoe-user} connected with PPPOE server successfully	Show More	No action required.	PPPoE user successfully connected to PPPoE server.
User{pppoe-user} disconnected from PPPOE server	Show More	No action required.	PPPoE user disconnected from PPPoE server.
PPPeE Client authentication failure	Warning	Check client login credentials.	PPPoE client authentication failure.
Start client connectivity troubleshooting for station {mac}	Warning	No action required.	Client connectivity troubleshooting started.
Stop client connectivity troubleshooting for station {mac}	Warning	No action required.	Client connectivity troubleshooting stopped.
External gateway status change from {old-status} to {new-status}	Warning	No action required.	External gateway status change detected.
Hello {system-id}!	Show More	No action required.	Hello system message.
Social Login for WiFi Access	Show More	No action required.	Social Media login.
Welcome to the WeChat login page	Show More	No action required.	WeChat login.
Remove preload image fail! {reason}	Warning	Examine the reason for the failure.	ZoneDirector failed to remove preloaded image due to {reason}.

TABLE 3 ZoneDirector Syslog event messages (continued)

ZoneDirector Syslog Message	Severity Level	Action	Explanation
start ad server for 802.1X {search-base} {server1} {host-device-name} {admin-dn}.	Show More	No action required.	Active Directory for 802.1X server started.
stop ad server for 802.1X.	Show More	No action required.	Active Directory for 802.1X server stopped.
Unknown Error	Warning	No action required.	An unknown error has occurred.

COMMSCOPE®
RUCKUS®