

Ruckus Wireless[™] ZoneDirector[™] Command Line Interface

Reference Guide

Part Number 800-70258-001 Published September 2010

www.ruckuswireless.com

Contents

About This Guide

Document Conventions	iii
Documentation Feedback	iv

1 Understanding the ZoneDirector Command Line Interface

What Is the CLI?
Accessing the Command Line Interface1
Requirements 1
Step 1: Connecting the Administrative Computer to ZoneDirector
Step 2: Start and Configure the Telnet/SSH Client
Step 3: Log Into the CLI 5
Using the Help Command6
Using the ? Command

2 Viewing Current Configuration

Show Commands Overview	9
Show AAA Commands	9
Show Access Point Commands	10
Show L2 Access Control List Commands	15
Show System Configuration Commands	16
Show System Information Commands	21
Show Technical Support Commands	22
Show WLAN Commands	28
Show WLAN Group Commands	31

3 Configuring Controller Settings

Configuration Commands Overview	33
Configure AAA Server Settings	33
Configure AAA Server Type Commands	33
Configure AAA Network Addressing Commands	36
Configure AAA RADIUS Commands	37
Configure Administration Preferences	41

4 Using Debug Commands

Deauthorizing a Device	123
Restarting a Device	124

Index

About This Guide

This Ruckus Wireless ZoneDirector Command Line Interface Reference Guide contains the syntax and commands for configuring and managing ZoneDirector from a command line interface.

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



NOTE: If a release note is shipped with your Ruckus Wireless product and the information there differs from the information in this guide, follow the instructions in the release note.

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

http://support.ruckuswireless.com/

Document Conventions

<u>Table 1</u> and <u>Table 2</u> list the text and notice conventions that are used throughout this guide.

Convention	Description	Example	
monospace	Represents information as it appears on screen	[Device name]>	
monospace bold	Represents information that you enter	[Device name]> set ipaddr 10.0.0.12	
default font bold	Keyboard keys, software buttons, and field names	On the Start menu, click All Programs .	
italics	Screen or page names	Click Advanced Settings . The <i>Advanced Settings</i> page appears.	
{text}	Text within curly braces represents a variable or information that the user must supply to complete	To display information about a specific device based on its MAC address, use the following command:	
	the command.	show ap mac {mac address}	

Table 1. Text Conventions

Table 2. Notice Convention:

lcon	Notice Type	Description
i	Information	Information that describes important features or instructions
Ĩ	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device
4	Warning	Information that alerts you to potential personal injury

Documentation Feedback

Ruckus Wireless is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Ruckus Wireless at:

docs@ruckuswireless.com

When contacting us, please include the following information:

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

For example:

- Ruckus Wireless ZoneDirector Command Line Interface Reference Guide
- Part number: 800-70258-001
- Page 88

Please note that we can only respond to comments and questions about Ruckus Wireless product documentation at this email address. Questions related to technical support or sales should be directed in the first instance to your network supplier.

Understanding the ZoneDirector Command Line Interface

In This Chapter

What Is the CLI?	1
Accessing the Command Line Interface	1
Using the Help Command	6
Using the ? Command	7

What Is the CLI?

The Ruckus Wireless ZoneDirector command line interface (CLI) is a software tool that enables you to configure and manage ZoneDirector, Ruckus Wireless's wireless LAN controller.

Using the command line interface, you can issue commands from an operating system prompt, such as the Microsoft Windows command prompt (C:\) or a Linux operating system terminal. Each command performs a specific action for configuring device settings or returning information about the status of a specific device feature.

Accessing the Command Line Interface

This section describes the requirements and the procedure for accessing the ZoneDirector CLI.

Requirements

To access the ZoneDirector CLI, you will need the following:

- A computer that you want to designate as the administrative computer
- An RS-232 cable (type depends on the ZoneDirector model):
 - If you are using ZoneDirector 3000, you need an RS-232 to Ethernet cable.
 - If you are using ZoneDirector 1000, you need an RS-232 to RS-232 cable.
- A Telnet or SSH (secure shell) client program

Step 1: Connecting the Administrative Computer to ZoneDirector

The steps for connecting the administrative computer to ZoneDirector depend on the ZoneDirector model that you are using. Refer to the relevant section below.

- Connecting ZoneDirector 1000
- Connecting ZoneDirector 3000



NOTE: Before continuing, make sure that both the administrative computer and ZoneDirector are both powered on.

Connecting ZoneDirector 1000

- Connect one end of the RS-232 cable to the port labeled Console on ZoneDirector.
- **2.** Connect the other end to the RS-232 cable to a COM port on the administrative computer.

Connecting ZoneDirector 3000

- 1. Connect the RS-232 end of the cable to the port labeled **Console** on ZoneDirector.
- **2.** Connect the Ethernet end of the cable to an Ethernet port on the administrative computer.

Step 2: Start and Configure the Telnet/SSH Client

Before starting this procedure, make sure that a Telnet/SSH client is already installed on the administrative computer.



NOTE: The following procedure uses PuTTY, a free and open source Telnet/SSH client, for accessing the ZoneDirector CLI. If you are using a different Telnet/SSH client, the procedure may be slightly different (although the connection settings should be the same). For more information on PuTTY, visit www.putty.org.

To start and configure the Telnet/SSH client

- **1.** Start PuTTY. The PuTTY Configuration dialog box appears, showing the *Session* screen.
- 2. In Connection type, click Serial.

Understanding the ZoneDirector Command Line Interface

Accessing the Command Line Interface

- Session	Basic options for you	ur PuTTY session
Logging Terminal Keyboard Features Window Appearance Behaviour Translation Selection Colours Connection Proxy Telnet Rlogin SSH Serial	Specify the destination you was Serial line COM1 Connection type: C Raw C Telnet C Rid Load, save or delete a stored Saved Sessions Default Settings Close window on exit: C Always C Never C	ant to connect to Speed 9600 ogin C SSH © Serial session Load Save Delete

- **3.** Under *Category*, click **Connection** > **Serial**. The serial connection options appear on the right side of the dialog box, displaying PuTTY's default serial connection settings.
- Figure 2. PuTTY's default serial connection settings



Figure 1. Click Serial as the connection type

Accessing the Command Line Interface

- 4. Configure the serial connection settings as follows:
 - Serial line to connect to: Type the COM port name to which you connected the RS-232 cable.
 - Bits per second: 115200
 - Data bits: 8
 - Parity: None
 - Stop bits: 1
 - Flow control: None

Fiaure 3.	PuTTY's serial	connection se	ttinas for co	onnectina to .	ZoneDirector

RuTTY Configuration		×
Category:		
E. Session	Options controlling	g local serial lines
⊡ Terminal	Select a serial line Serial line to connect to	COM1
Bell	Configure the serial line	
- Window	Speed (baud)	9600
···· Appearance ···· Behaviour	Data bits	8
···· Translation ···· Selection	Stop bits	1
Colours	Fanty Flow control	XON/XOFF
- Data		
Telnet		
⊡ Riogin ⊡ · SSH	z	
I Serial		
About	(Open Cancel

5. Click **Open**. The PuTTY console appears and displays the login prompt.

Understanding the ZoneDirector Command Line Interface

Accessing the Command Line Interface



Figure 4. The PuTTY console displaying the login prompt

You have completed configuring the Telnet/SSH client to connect to ZoneDirector.

Step 3: Log Into the CLI

- 1. At the Please login prompt, type **admin**, and then press <Enter>.
- 2. At the Password prompt, type **admin**, and then press <Enter>. The Ruckus Wireless ZoneDirector CLI welcome message and the ruckus prompt appears.

You are now logged into the ZoneDirector CLI as a user with limited privileges.

As a user with limited privileges, you can view a history of commands that were previously executed and ping a device. If you want to run more commands, you can switch to privileged mode by entering **enable** at the root prompt.

To view a list of commands that are available at the root level, enter **help** or?.



NOTE: You can tell if you logged into the CLI in limited or privileged mode by looking at the ruckus prompt. If you are in limited mode, the prompt appears as ruckus> (with a *greater than* sign). If you are in privileged mode, the prompt appears as ruckus# (with a pound sign).

Using the Help Command

To display all commands that the Ruckus Wireless CLI supports, use the ${\tt help}$ command.



CAUTION: Entering the help command into the CLI prints a long list of commands on the screen. If you only want to view the commands that are available from within a specific context, use the ? command. See <u>"Using the ? Command"</u> below for more information.

Example

Using the ? Command

To display commands that are available within a specific context, use the ? command.

To display commands ruckus# debug ruckus(debug)# ?	within the debug context, enter the following command:
help	Shows available commands.
history	Shows a list of previously run commands.
quit	Exits the debug context.
delete	Contains commands that can be executed from within the context.
restart	Contains commands that can be executed from within the context.

Viewing Current Configuration

In This Chapter
Show Commands Overview
Show AAA Commands
Show Access Point Commands
Show L2 Access Control List Commands 15
Show System Configuration Commands 16
Show System Information Commands
Show Technical Support Commands 22
Show WLAN Commands
Show WLAN Group Commands

Show Commands Overview

Show commands display the controller's current settings, including its status and system settings, and those of its AAA servers, access points, WLANs, and WLAN groups.



NOTE: You can only run show commands at the root prompt.

Show AAA Commands

Use the show aaa commands to display information about the authentication and accounting servers (AAA) servers that have been added to the controller.

show aaa all

To display a list of all AAA servers that have been added to the controller, use the following command:

show aaa all

Syntax Description	about	Display information	
	SHOW	Display information	
	aaa	Display AAA server information	
	all	All AAA servers	
Defaults	None.		
Example	- ruckus# show	y aaa all	
	AAA:		
	ID:		
	1:		
	Name=	Local Database	
	Туре=	local	
	2:		
	Name= 0	Guest Accounts	
	Type= o	guestpass	

Related Commands show aaa name

show aaa name

To display information about a specific AAA server that has been added to the controller, use the following command:

show aaa name {AAA server name}

Syntax Description	show	Display information	
	aaa name	Display information about a specific AAA server name	
	{AAA server n	ame } Name of the AAA server	
Defaults	- None.		
Example	_ ruckus# show aaa name Ruckus-Radius		
	AAA:		
	ID:		
	3:		
	Name= Ruo	ckus-Radius	
	Type= rad	lius-auth	
	Primary RADIUS:		
	IP Add	ress= 192.168.0.33	
	Port= 1812		
	Secret= testing123		
	Secondary	Y RADIUS:	
	Status	= Disabled	

Related Commands show aaa all

Show Access Point Commands

Use the show ap commands to display the current settings of managed devices, including their network address settings, device names, radio settings, and others.

show ap all

To display a summary of all devices that have been approved, use the following command:

show ap all

Syntax Description

show	Display information
ap	Show device information

Viewing Currer

Show Access Pc

Defaults

Example

all	All devices that have been approved by the cont
None.	
ruckus# sho w	ap all
AP:	-
ID:	
1:	
MAC Ad	dress= 00:1f:41:2a:cb:c0
Model=	z£2942
Approv	ed= Yes
Device	Name= RuckusAP
Descri	ption=
Locati	on=
GPS=	
Radio	b/g/n:
Chan	nel= Auto
TX P	ower= Use Global Configuration
WLAN	Group Name= Default
Networ	k Setting:
Devi	ce IP Settings= Keep AP's Setting
IP A	ddress= 192.168.1.105
Netm	ask= 255.255.255.0
Gate	wav= 192.168.1.3

Primary DNS Server= 172.17.17.5 Secondary DNS Server= 172.17.17.15

MAC Address= 00:22:7f:3d:db:50

TX Power= Use Global Configuration

WLAN Group Name= Default

Mesh:

2:

Status= Disabled

Device Name= RuckusAP

Model= zf7942 Approved= Yes

Description= Location= GPS=

Radio b/g/n: Channel= Auto

11

```
Network Setting:

Device IP Settings= Keep AP's Setting

IP Address= 192.168.1.101

Netmask= 255.255.255.0

Gateway= 192.168.1.3

Primary DNS Server= 172.17.17.5

Secondary DNS Server= 172.17.17.15

Mesh:

Status= Disabled
```

Related Commands	show ap devname

show ap mac

show ap devname

To display information about a specific device based on its device name, use the following command:

show ap devname {device name}

Syntax Description				
Syntax Description	show	Display information		
	ap devname	Show information about a specific device name		
	{device name}	The name of the device		
Defaults	- None.			
Example	- ruckus# show ap devname RuckusAP			
	AP:			
	ID:			
	1:			
	MAC Address	s= 00:1f:41:2a:cb:c0		
	Model= zf29	942		
	Approved= N	les		
	Device Name	e= RuckusAP		
	Description	1=		
	Location=			
	GPS=			
	Radio b/g/r	1:		
	Channel=	3		
	TX Power	= Use Global Configuration		
	WLAN Grou	up Name= Default		
	Network Set	ting:		

Show Access Point Commands

```
Device IP Settings= Keep AP's Setting
IP Address= 192.168.1.105
Netmask= 255.255.255.0
Gateway= 192.168.1.3
Primary DNS Server= 172.17.17.5
Secondary DNS Server= 172.17.17.15
Mesh:
Status= Disabled
```

2:

MAC Address= 00:22:7f:3d:db:50 Model= zf7942 Approved= Yes Device Name= RuckusAP Description= Location= GPS= Radio b/g/n: Channel= 3 TX Power= Use Global Configuration WLAN Group Name= Default Network Setting: Device IP Settings= Keep AP's Setting IP Address= 192.168.1.101 Netmask= 255.255.255.0 Gateway= 192.168.1.3 Primary DNS Server= 172.17.17.5 Secondary DNS Server= 172.17.17.15 Mesh: Status= Disabled

Related Commands show ap devname

show ap mac

show ap mac

To display information about a specific device based on its MAC address, use the following command:

show ap mac {MAC address}

```
Syntax Description
```

show

Display information

Show Access Point Commands

	ap mac	Display information about a specific device based on its MAC address		
	{MAC address}	The MAC address of the device		
Defaults	None.			
Example	ruckus# show ap	mac 00:22:7f:3d:db:50		
	AP:	AP:		
	ID:			
	2:			
	MAC Addres	s= 00:22:7f:3d:db:50		
	Model= zf7942			
	Approved= Yes			
	Device Name= RuckusAP			
	Description=			
	Location=			
	GPS=			
	Radio b/g/n:			
	Channel= 3			
	TX Power	= Use Global Configuration		
	WLAN Gro	up Name= Default		
	Network Se	tting:		
	Device I	P Settings= Keep AP's Setting		
	IP Addre	ss= 192.168.1.101		
	Netmask= 255.255.255.0			
	Gateway= 192.168.1.3			
	Primary DNS Server= 172.17.17.5			
	Secondar	y DNS Server= 172.17.17.15		
	Mesh:			
	Status=	Disabled		

Related Commands

show ap devname

show ap mac

Show L2 Access Control List Commands

Use the show 12ac1 commands to display Layer 2 access control list rules that have been added to the controller.

show l2acl all

12acl

To display all Layer 2 access control list (ACL) rules that have been added to the controller and their settings, use the following command:

show 12acl all

Syntax Description	-			
	show	Display information		
	12acl	Display L2 ACL information		
	all	All L2 ACL		
	-			
Defaults	None.			
Example	- ruckus# show l2acl all L2/MAC ACL:			
	ID:			
	1:			
	Name= System	1		
	Description=	System		
	Restriction:	Deny only the stations listed below		
	Stations:			
	2:			
	Name= blocked-sta-list			
	Description= blocked-sta-list			
	Restriction:	Deny only the stations listed below		
	Stations:			
	show I2acl name			
	To display the settings of a specific L2 ACL rule that has been added to the controller, use the following command:			
	show l2acl nam	e {L2 ACL rule name}		
Syntax Description	show	Display information		

Display L2 ACL information

 name
 Display information about a specific L2 ACL rule name

 {L2 ACL rule name}
 Name of the L2 ACL rule

 Defaults
 None.

 Example
 To display the L2 ACL rule settings of blocked-sta-list, enter the following command: ruckus# show l2acl name blocked-sta-list

 L2/MAC ACL:
 ID: 2: Name= blocked-sta-list

 Description= blocked-sta-list

 Restriction: Deny only the stations listed below Stations:

Show System Configuration Commands

Use the show config commands to display the controller's system configuration settings.

show config

To display current system configuration settings, including network addressing, management VLAN, country code, logging, AAA servers, WLAN services, WLAN groups, AP list, SNMP, and ACLs, use the following command:

show config

Syntax Description	show	Display information		
	config	Display system configuration settings		
Defaults	None.			
Example	- ruckus# show	config		
	Device IP Address:			
	Mode= DHCP			
	IP Address=	192.168.1.139		
	Netmask= 25	5.255.255.0		
	Gateway Add	ress= 192.168.1.3		
	Primary DNS	= 172.17.17.5		
	Secondary D	NS= 172.17.17.15		

Show System Configuration Commands

```
Management VLAN:
  Status= Disabled
  VLAN ID=
Country Code:
  Code= United States
Identity:
  Name= ruckus
NTP:
  Status= Enabled
  Address= ntp.ruckuswireless.com
Log:
  Status= Disabled
  Address=
AAA:
  ID:
    1:
      Name= Local Database
      Type= local
    2:
      Name= Guest Accounts
      Type= guestpass
    3:
      Name= Ruckus-Radius
      Type= radius-auth
      Primary RADIUS:
        IP Address= 192.168.0.33
        Port= 1812
        Secret= testing123
      Secondary RADIUS:
        Status= Disabled
Administrator Name/Password:
  Name= admin
```

```
Password= admin
Auth Mode= Authenticate using the admin name and password
```

```
AP:
  ID:
    1:
      MAC Address= 00:1f:41:2a:cb:c0
      Model= zf2942
      Approved= Yes
      Device Name= RuckusAP
      Description=
      Location=
      GPS=
      Radio b/g/n:
        Channel= 3
        TX Power= Use Global Configuration
        WLAN Group Name= Default
      Network Setting:
        Device IP Settings= Keep AP's Setting
        IP Address= 192.168.1.105
        Netmask= 255.255.255.0
        Gateway= 192.168.1.3
        Primary DNS Server= 172.17.17.5
        Secondary DNS Server= 172.17.17.15
      Mesh:
        Status= Disabled
    2:
      MAC Address= 00:22:7f:3d:db:50
      Model= zf7942
      Approved= Yes
      Device Name= RuckusAP
      Description=
      Location=
      GPS=
      Radio b/g/n:
        Channel= 3
        TX Power= Use Global Configuration
        WLAN Group Name= Default
      Network Setting:
        Device IP Settings= Keep AP's Setting
        IP Address= 192.168.1.101
```

Show System Configuration Commands

```
Netmask= 255.255.255.0
        Gateway= 192.168.1.3
        Primary DNS Server= 172.17.17.5
        Secondary DNS Server= 172.17.17.15
      Mesh:
        Status= Disabled
Smart Redundancy:
  Status= Disabled
  Peer IP Address=
  Shared Secret=
Management Interface:
  Status= Disabled
  IP Address=
 Netmask=
 VLAN=
L2/MAC ACL:
  ID:
    1:
      Name= System
      Description= System
      Restriction: Deny only the stations listed below
      Stations:
    2:
      Name= blocked-sta-list
      Description= blocked-sta-list
      Restriction: Deny only the stations listed below
      Stations:
SNMP Agent:
  Status= Disabled
 Contact=
  Location=
  RO Community= public
  RW Community= private
SNMP Trap:
```

```
Status= Disabled
  Address=
WLAN Service:
  ID:
    1:
      SSID= Ruckus-Wireless-1
      Description= Ruckus-Wireless-1
      Authentication= open
      Encryption= none
      Web Authentication= Disabled
      Authentication Server= Disabled
      Accounting Server= Disabled
      Tunnel Mode= Disabled
      Max Clients= 100
      Client Isolation= Disabled
      Zero-IT Activation= Enabled
      Load Balancing= Disabled
      VLAN= Disabled
      Dynamic VLAN= Disabled
      Closed System= Disabled
      L2/MAC= No ACLS
      L3/L4/IP Address= No ACLS
WLAN Group:
  ID:
    1:
      Name= Default
      Description= Default WLANs for Access Points
      VLAN Override:
        Status= Disabled
      WLAN Service:
        SSID= Ruckus-Wireless-1; VLAN=
```

Related Commands show sysinfo

Show System Information Commands

Use the show sysinfo commands to display the controller's system information.

show sysinfo

To display an overview of the system, including its devices, usage summary, user activities, system activities, used access points, and support information, use the following command:

show sysinfo

Syntax Description				
	show	Display information		
	sysinfo	Display an overview of various system statuses		
	-			
Defaults	None.			
Example	ruckus# show sysinfo			
	System Overview:			
	Name= ruckus			
	IP Address= 192.168.1.139			
	MAC Address= 00:25:C4:3D:66:0E			
	Uptime= 22m			
	Model= ZD1006			
	Licensed APs= 6			
	Serial Number= 031003000320			
	Version= 9.	0.0.0 build 55		
	Devices Overv	iew:		
	Number of APs= 2			
	Number of Client Devices= 0			
	Number of R	ogue Devices= 93		
	Usage Summary	:		
	Usage of 1	hr:		
	Max Concurrent Users= 0			
	Bytes Transmitted= 2.57M			
	Number of Rogue Devices= 93			
	Usage of 24 hr:			
	Max Concu	rrent Users= 0		
	Bytes Tra	nsmitted= 2.57M		
	Number of	Rogue Devices= 93		

```
Memory Utilization:
Used Bytes= 28659712
Used Percentage= 45%
Free Bytes= 34779136
Free Percentage= 55%
```

Related Commands show config

Show Technical Support Commands

Use the following commands to display information that Ruckus Wireless may need when providing technical support.

show techsupport

To display system information required by Technical Support, use the following command:

show techsupport

Syntax Description			
	show	Display information	
	techsupport	Display information about the controller that may be required by Ruckus Wireless Technical Support	
Defaults	- None.		
Example	- ruckus# show techsupport		
	System Overview:		
	- Name= ruckus		
	IP Address= 192.168.1.139		
	MAC Address= 00:25:C4:3D:66:0E		
	Uptime= 22m		
	Model= ZD1006		
	Licensed APs= 6		
	Serial Number= 031003000320		
	Version= 9.0.0	0.0 build 55	
	Devices Overview:		
	Number of APs= 2		
	Number of Client Devices= 0		
	Number of Rogue Devices= 93		

Show Technical Support Commands

Usage Summary: Usage of 1 hr: Max Concurrent Users= 0 Bytes Transmitted= 2.57M Number of Rogue Devices= 93 Usage of 24 hr: Max Concurrent Users= 0 Bytes Transmitted= 2.57M Number of Rogue Devices= 93 Memory Utilization: Used Bytes= 28696576 Used Percentage= 45% Free Bytes= 34742272 Free Percentage= 55% Device IP Address: Mode= DHCP IP Address= 192.168.1.139 Netmask= 255.255.255.0 Gateway Address= 192.168.1.3 Primary DNS= 172.17.17.5 Secondary DNS= 172.17.17.15 Management VLAN: Status= Disabled VLAN ID= Country Code: Code= United States Identity: Name= ruckus NTP: Status= Enabled Address= ntp.ruckuswireless.com Log: Status= Disabled Address=

```
AAA:
  ID:
    1:
      Name= Local Database
      Type= local
    2:
      Name= Guest Accounts
      Type= guestpass
    3:
      Name= Ruckus-Radius
      Type= radius-auth
      Primary RADIUS:
        IP Address= 192.168.0.33
        Port= 1812
        Secret= testing123
      Secondary RADIUS:
        Status= Disabled
Administrator Name/Password:
  Name= admin
  Password= admin
 Auth Mode= Authenticate using the admin name and password
AP:
  ID:
    1:
      MAC Address= 00:1f:41:2a:cb:c0
      Model= zf2942
      Approved= Yes
      Device Name= RuckusAP
      Description=
      Location=
      GPS=
      Radio b/g/n:
        Channel= 3
        TX Power= Use Global Configuration
        WLAN Group Name= Default
      Network Setting:
        Device IP Settings= Keep AP's Setting
```

Show Technical Support Commands

```
IP Address= 192.168.1.105
  Netmask= 255.255.255.0
  Gateway= 192.168.1.3
  Primary DNS Server= 172.17.17.5
  Secondary DNS Server= 172.17.17.15
Mesh:
  Status= Disabled
```

2:

```
MAC Address= 00:22:7f:3d:db:50
      Model= zf7942
      Approved= Yes
      Device Name= RuckusAP
      Description=
      Location=
      GPS=
      Radio b/g/n:
        Channel= 3
        TX Power= Use Global Configuration
        WLAN Group Name= Default
      Network Setting:
        Device IP Settings= Keep AP's Setting
        IP Address= 192.168.1.101
        Netmask= 255.255.255.0
        Gateway= 192.168.1.3
        Primary DNS Server= 172.17.17.5
        Secondary DNS Server= 172.17.17.15
      Mesh:
        Status= Disabled
Smart Redundancy:
  Status= Disabled
  Peer IP Address=
  Shared Secret=
Management Interface:
```

Status= Disabled IP Address= Netmask= VLAN=

```
L2/MAC ACL:
  TD:
    1:
      Name= System
      Description= System
      Restriction: Deny only the stations listed below
      Stations:
    2:
      Name= blocked-sta-list
      Description= blocked-sta-list
      Restriction: Deny only the stations listed below
      Stations:
SNMP Agent:
  Status= Disabled
 Contact=
  Location=
  RO Community= public
  RW Community= private
SNMP Trap:
  Status= Disabled
  Address=
WLAN Service:
  ID:
    1:
      SSID= Ruckus-Wireless-1
      Description= Ruckus-Wireless-1
      Authentication= open
      Encryption= none
      Web Authentication= Disabled
      Authentication Server= Disabled
      Accounting Server= Disabled
      Tunnel Mode= Disabled
      Max Clients= 100
      Client Isolation= Disabled
      Zero-IT Activation= Enabled
      Load Balancing= Disabled
      VLAN= Disabled
```

Show Technical Support Commands

```
Dynamic VLAN= Disabled

Closed System= Disabled

L2/MAC= No ACLS

L3/L4/IP Address= No ACLS

WLAN Group:

ID:

1:

Name= Default

Description= Default WLANs for Access Points

VLAN Override:

Status= Disabled

WLAN Service:

SSID= Ruckus-Wireless-1; VLAN=
```

Related Commands show config

Show WLAN Commands

Use the following commands to display information about available WLANs on the controller.

show wlan all

To display information about all available WLAN services (SSIDs), use the following command:

show wlan all

Syntax Description	-				
	snow				
	wlan	Display WLAN services (SSIDs) settings			
	all	All available WLANs/SSIDs			
Defaults	None.				
Example	- ruckus# show wlan all				
	WLAN Service:				
	ID:				
	1:				
	SSID= Ruckus-Wireless-1				
	Description= Ruckus-Wireless-1				
	Authentication= open				
	Encryption= none				
	Web Authentication= Disabled				
	Authentication Server= Disabled				
	Accounting Server= Disabled				
	Tunnel Mode= Disabled				
	Max Cl	ients= 100			
	Client	Isolation= Disabled			
	Zero-IT Activation= Enabled				
	Load Balancing= Disabled				
	VLAN= Disabled				
	Dynamic VLAN= Disabled				
	Closed System= Disabled				
	L2/MAC= NO ACLS				
	L3/L4/	IP Address= No ACLS			
Related Commands		<u>e</u>			

show wlan name stations

show wlan name

To display information about a specific WLAN service (SSID), use the following command:

show wlan name {WLAN name}

Syntax Description	show	Display information			
	wlan name	Display information about a specific WI AN name			
	(WI AN name)				
	{WLAN Hame}				
Defaults	None.				
Example	- To display information about a WLAN called <i>corporate</i> , enter the following command:				
	ruckus# show wlan name corporate				
	WLAN Service:				
	ID:				
	1:				
	SSID= con	rporate			
	Description= Ruckus-Wireless-1				
	Authentication= open				
	Encryption= wpa				
	Algorithm= aes				
	Passphrase= test1234				
	Web Authentication= Disabled				
	Authentication Server= Disabled				
	Accounting Server= Disabled				
	Tunnel Mode= Disabled				
	Backgrou	nd Scanning= Enabled			
	Max Clier	nts= 100			
	Client Is	solation= None			
	Zero-IT A	Activation= Disabled			
	Priority= High				
	Load Bala	ancing= Enabled			
	Dynamic 1	PSK= Disabled			
	Rate Lim:	iting Uplink= Disabled			
	Rate Lim:	iting Downlink= Disabled			
	VLAN= Dis	sabled			
	Dynamic V	/LAN= Disabled			
	Closed Sy	ystem= Disabled			
	L2/MAC= I	No ACLS			
L3/L4/IP Address= No ACLS

Related Commands show wlan all show wlan name stations

show wlan name stations

To display a list of wireless stations associated with a specific WLAN service, use the following command:

show wlan name {WLAN name} stations

Syntax Description			
	show	Display information	
	wlan name	Display information about a specific WLAN name	
	{WLAN name}	The name of the WLAN	
	stations	Display stations associated with the WLAN	
Defaults	- None.		
Example	 To display a list of wireless stations associated with the WLAN called <i>corporate</i>, enter the following command: 		
	ruckus# show wlan name corporate station		
	Clients List:		
	Client:		
	MAC Address= 00:24:d6:95:a7:4c		
	User Name=		
	IP Address= 172.17.16.91		
	Access Point= 00:1f:41:2a:cb:c0		
	WLAN= corporate		
	Channel= 3		
	Signal (dB) = 70		
Related Commands	show wlan all		
	show wlan name		

Show WLAN Group Commands

Use the following commands to display information about the WLAN groups that exist on the controller.

show wlan-group all

To display a list of existing WLAN groups, use the following command:

show wlan-group all

Syntax Description			
	show	Display information	
	wlan-group	Display information about a specific WLAN group	
	all	Show all WLAN groups	
	- 		
Defaults	None.		
Example	- ruckus# show wlan-group all		
	WLAN Group:		
	ID:		
	1:		
	Name= Default		
	Description= Default WLANs for Access Points		
	VLAN Override:		
	Status= Disabled		
	WLAN Service:		
	SSID= corporate; VLAN=		
	SSID= x	steven-open; VLAN=	
Related Commands	show wlan-group name		
	show wlan-grou	up name	
	To display information about a specific WLAN group name, use the following		
	command:		
	show wlan-gr	oup name {WLAN group name}	
Syntax Description			
- ,	show	Display information	
	wlan-group nam	e Display information about a specific WLAN group name	
	{WLAN group nam	The name of the WLAN group	
Defaulte	- None		
Deraults	none.		

Example	ruckus# show wlan-group name Default
	WLAN Group:
	ID:
	1:
	Name= Default
	Description= Default WLANs for Access Points
	VLAN Override:
	Status= Disabled
	WLAN Service:
	SSID= corporate; VLAN=
	SSID= xsteven-open; VLAN=

Related Commands show wlan-group all

In This Chapter	
Configuration Commands Overview	33
Configure AAA Server Settings	33
Configure Administration Preferences	41
Configure Device's System Information	45

Configuration Commands Overview

This chapter describes the commands that you can use to configure the different settings on the controller. Commands are divided into sections, including:

- <u>Configure AAA Server Settings</u>
- <u>Configure Administration Preferences</u>
- <u>Configure Device's System Information</u>

Configure AAA Server Settings

The config aaa context contains commands for configuring the AAA server settings. AAA server settings are classified into the following command types:

- Configure AAA Server Type Commands
- Configure AAA Network Addressing Commands
- <u>Configure AAA RADIUS Commands</u>

Configure AAA Server Type Commands

Use the aaa-type commands to set the type of AAA server that is used by the controller for authentication purposes.

type ad

To set the AAA server type to Active Directory, use the following command:

type ad

Syntax Description	- 		
Syntax Description	type ad	Set the AAA server type to ActiveDirectory	
	<u>-</u>		
Defaults	None.		
Example	- ruckus# config	r	
	<pre>ruckus(config)# aaa Ruckus-Auth-02</pre>		
	The AAA server server, type '	'Ruckus-Auth-02' has been created. To save the AAA end' or 'exit'.	
	ruckus(config-	aaa)#	
	ruckus(config-	aaa)# type ad	
	The command wa 'end' or 'exit	s executed successfully. To save the changes, type '.	
Related Commands	type ad		
	type radius		
	type radius-acct		
	type Idap		
	To set the AAA server type to 'LDAP', use the following command:		
	type ldap		
Suntax Description			
Syntax Description	type ldap	Set the AAA server type to LDAP	
Defaults	None.		
 Fxample	ruckus # confi c	r	
	ruckus(config)	# aaa Ruckus-Auth-02	
	The AAA server server, type '	'Ruckus-Auth-02' has been created. To save the AAA end' or 'exit'.	
	ruckus(config-	aaa)#	
	ruckus(config-	aaa)# type ldap	
	The command wa 'end' or 'exit	s executed successfully. To save the changes, type '.	
Related Commands	type ad		
	type radius		
	type radius-acct		

type radius

To set the AAA server type to 'RADIUS', use the following command

type radius

Suntax Description	•			
Syntax Description	type radius	Set the AAA server type to RADIUS		
	-			
Defaults	None.			
Example	ruckus# config			
	ruckus(config)# aaa Ruckus-Auth-02			
	The AAA server 'Ruckus-Auth-02' has been created. To save the AAA server, type 'end' or 'exit'. ruckus(config-aaa)# ruckus(config-aaa)# type radius			
	The command was 'end' or 'exit'.	executed successfully. To save the changes, type		
Related Commands	type ad			
	type Idap			
	ture a ve alive a set			
	type radius-acct			
	type radius-acc	t		
	To set the AAA serve	• er type to 'RADIUS Accounting' use the following command:		
		er type to rabios accounting, use the following command.		
	type radius-	acct		
Syntax Description				
	type radius-aco	Set the AAA server type to RADIUS Accounting		
Defaults	None.			
Example	ruckus# config			
•	ruckus(config)#	aaa Ruckus-Auth-02		
	The AAA server ' server, type 'er	Ruckus-Auth-02' has been created. To save the AAA nd' or 'exit'.		
	ruckus(config-aa	aa)#		
	ruckus(config-aa	aa)# type radius-acct		
	The command was 'end' or 'exit'.	executed successfully. To save the changes, type		

Related Commands type ad

<u>type Idap</u>

type radius

no AAA {WORD}

To delete an AAA server from the list of AAA servers, use the following command: no aaa {WORD}

Syntax Description				
, ,	no aaa	Delete an AAA server		
	{WORD}	Name of the AAA server to be deleted		
Defaults	None.			
Example	ruckus(config)# no aaa Ruckus-Radius			
	The AAA serve	r 'Ruckus-Radius' has been deleted.		
	ruckus(config) #		
Related Commands	type ad			
	<u>type Idap</u>			
	type radius			
	Configure AAA Network Addressing Commands			
	Use the ip-addu	r commands to set the network address settings of AAA servers that		
	the controller is u	using.		
	ip-addr			
	To set the AAA s	erver's IP address, use the following command:		
	ip-addr {]	IP address}		
Syntax Description				
	ip-addr {IP address}	Set the AAA server IP address to this IP address		
Defeaths				
Defaults	None.			
Example	ruckus# confi	g		
	ruckus(config)# aaa Ruckus-Auth-02		
	The AAA serves server, type	r 'Ruckus-Auth-02' has been created. To save the AAA 'end' or 'exit'.		
	ruckus(config	-aaa)#		

Configure AAA Server Settings

	ruckus(config-aaa) The command was ex 'end' or 'exit'.	<pre># ip-addr 192.168.0.200 xecuted successfully. To save the changes, type</pre>
Related Commands	ip-addr port ip-addr port ip-addr port To set the AAA server's	s IP address and port number, use the following command:
	ip-addr {IP ad	dress} port {port number}
Syntax Description	ip-addr {IP address}	Set the AAA server IP address to this IP address
	port {port number	} Set the AAA server to this port number to this port
Defaults	None.	
Example	ruckus# config ruckus(config)# a The AAA server 'Ru server, type 'end' ruckus(config-aaa) ruckus(config-aaa) The command was ex 'end' or 'exit'.	<pre>aa Ruckus-Auth-02 uckus-Auth-02' has been created. To save the AAA ' or 'exit'. # # ip-addr 192.168.0.2 port 1812 wecuted successfully. To save the changes, type</pre>
Related Commands	ip-addr port	
	Configure AA Use the radius comm radius-secret To set the RADIUS serv radius-secret	A RADIUS Commands nands to configure additional RADIUS server settings. ver's shared secret, use the following command: {RADIUS secret}
Syntax Description	radius-secret	Set the RADIUS server secret
	{RADIUS secret}	Set the RADIUS server secret to this secret
Defaults	None.	

Example	ruckus# config		
	ruckus(config)# aaa Ruckus-Auth-02 The AAA server 'Ruckus-Auth-02' has been created. To save the AAA server, type 'end' or 'exit'.		
	Tuckus (contriged	aa) # laulus-secret 12345	
	'end' or 'exit	'.	
Related Commands	type radius		
	Backup RADI	US Settings Commands	
	Use the backup co	ommands to enable the backup (or secondary) RADIUS server	
	backup		
	To enable the contr	oller to use a backup or secondary RADIUS server, use the following	
	command:	,	
	backup		
Syntax Description	backup	Enable the controller to use the backup RADII IS server if	
	backap	the primary RADIUS server is unreachable	
Defaults	None.		
Example	ruckus(config-aaa)# backup		
·	The command was executed successfully. To save the changes, type 'end' or 'exit'.		
	no backup		
	To disable the backup or secondary RADIUS server, use the following command:		
	no backup		
Syntax Description	ne heeluur	Dischla the healtup PADULS conter The controller will use	
	по раскир	only the primary RADIUS server to process authentication requests.	
Defaults	None.		
Example	ruckus(config-a	aaa)# no backup	

Configure AAA Server Settings

The command was executed successfully. To save the changes, type 'end' or 'exit'.

backup-ip-addr {IPADDR}

To set the IP address of the backup RADIUS server on the controller, use the following command:

backup-ip-addr {IPADDR}



NOTE: Use this command if the backup RADIUS server is using port 1812 (standard RADIUS port). If the RADIUS server is using a different port, use the <u>"backup-ip-addr"</u> <u>(IPADDR) port {PORT}"</u> command.

Syntax Description	-		
Syntax Description	backup-ip-addr	Set the IP address of the backup RADIUS server.	
	{IPADDR}	Set to this IP address	
Defector	-		
Defaults	None.		
Example	- ruckus(config-aaa)# backup-ip-addr 192.168.0.3		
-	The command was executed successfully. To save the changes, type 'end' or 'exit'.		
	backup-ip-addr {IPADDR} port {PORT}		
	To set the IP address and port number of the backup RADIUS server on the controller, use the following command:		
	backup-ip-addr {I	PADDR} port {PORT}	
Syntax Description	- 	Set the ID address of the health PADILIS conver	
	backup-1p-addr		
	{IPADDR}	Set to this IP address	
	port	Set the port number of the backup RADIUS server	
	{PORT}	Set to this port number	
Dofaulte	- Nono		
Delauits	None.		
Example	- ruckus(config-aaa	a)# backup-ip-addr 192.168.0.3 port 12345	
	The command was e 'end' or 'exit'.	executed successfully. To save the changes, type	

backup-radius-secret {SECRET}

To set the backup RADIUS server's shared secret, use the following command:

backup-radius-secret {SECRET}

	-		
Syntax Description	backup-radius- secret	Set the backup RADIUS server secret	
	{SECRET}	Set the backup RADIUS server secret to this secret	
Defaults	None.		
Example	ruckus(config-aaa The command was e 'end' or 'exit'.)# backup-radius-secret testing123 executed successfully. To save the changes, type	
Related Commands	radius-secret		
	request-timeout {NUMBER}		
	To set the timeout value for RADIUS requests, use the following command:		
	request-timeout {NUMBER}		
	Timeout value can rar	nge from 2 and 20 seconds.	
Syntax Description	-	Set the RADILIS request timeout value	
	{NUMBER}	Set the timeout value to this number (in seconds)	
Defaults	None.		
Example	- ruckus(config-aaa)# request-timeout 10 The command was executed successfully. To save the changes, type 'end' or 'exit'.		
Related Commands	retry-count {NUMBER	1	
	retry-count {NUMBER} To set the allowed number of retries for RADIUS requests, use the following command: retry-count {NUMBER} Retry count can range from 2 to 10.		

Configure Administration Preferences

	-		
Syntax Description	retry-count	Set the allowed number for retries for RADIUS requests.	
	{NUMBER}	Set the retry count to this number (number of times)	
	-		
Defaults	None.		
Example	- ruckus(config-aaa)# retry-count 10		
	The command was 'end' or 'exit'	executed successfully. To save the changes, type .	
Related Commands	request-timeout {N	UMBER}	
	reconnect-primary-interval {NUMBER}		
	To set the reconnec	t primary interval (in minutes), use the following command:	
	reconnect-primary-interval {NUMBER}		
	Reconnect primary	interval can range from 1 and 86400 minutes.	
Syntax Description	-		
Syntax Description	reconnect-prima interval	ry- Set the reconnect primary interval.	
	{NUMBER}	Set the interval to this number (in minutes)	
Defaults	None.		
Example	ruckus(config-aaa)# reconnect-primary-interval 120 The command was executed successfully. To save the changes, type 'end' or 'exit'.		
Related Commands	request-timeout {N	UMBER}	
	Configure	Administration Preferences	
	← The config admi	n context contains commands for configuring and viewing	
		5 5 5	

- administrator login and authentication settings.
- Configure Admin Login Commands
- <u>Configure Admin Authentication Commands</u>
- Display Administrator Account Settings

Configure Admin Login Commands

Use the admin-name commands to set the admin user name and password.

name

To set the administrator user name, use the following command: name {admin name}

	-	
Syntax Description	name	Configure the admin name setting
	{admin name}	Set the admin name to this name
Defaults	admin	
Example	ruckus(config)#	admin
	ruckus(config-ac The command was	<pre>imin)# name admin executed successfully.</pre>
Related Commands	name password	
	To set the admin name {admin	me and password at the same time, use the following command: name} password {password}
Syntax Description	name	Configure the admin name setting
	{admin name}	Set the admin name to this name
	password	Configure the admin password
	{password}	Set the admin password to this password
Defaults	admin	
Example	ruckus(config)# ruckus(config-ad The command was	admin dmin)# name admin password admin executed successfully.
Related Commands	name	

Configure Admin Authentication Commands

Use the auth-server commands to set the administrator authentication options with an external authentication server.

no auth-server

To disable administrator authentication with a remote server, use the following command:

no auth-server

Syntax Description	no suth correct	Disable admin authentication with an external conver
	no auch-server	
Defaults	None.	
Example	ruckus(config-admi The command was ex 'end' or 'exit'.	n)# no auth-server recuted successfully. To save the changes, type
Related Commands	auth-server auth-server with fallbac	<u>.k</u>
	auth-server To enable administrato authentication server, u auth-server {se	r authentication with a remote server and set the use the following command: erver name}
Syntax Description	auth-server	Admin authentication with an external server
	{server name}	Set the authentication server to this server
Defaults	None.	
Example	ruckus(config-admi The command was ex 'end' or 'exit'.	n)# auth-server Ruckus-a Auth-02 secuted successfully. To save the changes, type
Related Commands	no auth-server	
	auth-server with fallbac	<u>k</u>

auth-server with fallback

To enable fallback authentication (for use when the remote server is unavailable), use the following command:

auth-server with fallback

	_			
Syntax Description	auth-server	Admin authentication with an external server		
	{server name}	Set the auth-server to this server		
	with fallback	Enable fallback authentication if the remote authentication server is unavailable		
Defaults	_ None.			
Example	- ruckus(config-adm The command was on 'end' or 'exit'.	min)# auth-server Ruckus-Auth-02 with-fallback executed successfully. To save the changes, type		
Related Commands	_ no auth-server			
	auth-server			
	Display Administrator Account Settings			
	Use the admin show command to display the administrator account settings.			
	admin show			
	To display the curren	t admin user name and password, use the following command:		
	admin show			
Syntax Description				
- ,	admin	Admin setting		
	show	Show current administrator settings		
Defaults	- None.			
Example	_ ruckus(config-adm	min)# show		
•	Administrator Name/Password:			
	Name= admin			
	Password= admin	n		
	Auth Mode= Auth 02'	nenticate with authentication server 'Ruckus-Auth-		

Configure Device's System Information

Related Commands

name

name password

Configure Device's System Information

Use the ap commands to configure the device's system information, including the device name, description, and location.

ар

Setting the device's system information requires that first enter the config-ap context. To enter the config-ap context, enter the following command:

ap {MAC address}

Syntax Description			
	ap	Access point	
	{MAC address}	MAC address of the access point for configuration	
Defaults	None.		
Example	- ruckus(config)# ap 00:22:7f:3d:db:50		
	The AP '00:22:7f:3d:db:50' has been loaded. To save the AP, type 'end' or 'exit'.		
	ruckus(config-ap) #	
Related Commands	devname		
	description		
	location		
	devname		
	To set the device name, use the following command:		
	devname {device name}		
Syntax Description		Davias nome	
	devname		
	{device name}	Set the device name to this name	
Defaults	None.		
Example	ruckus(config-ap)	#devname Ruckus-AP	

The command was executed successfully. To save the changes, type 'end' or 'exit'.

Related Commands	ap	
	description	
	location	
	description	
	To set the device des	cription, use the following command:
	description {	description}
Syntax Description	description	Device description
	{description}	Set the device description to this text
Defaults	None.	
Example	ruckus # config ruckus(config) # a ruckus(config-ap The command was a 'end' or 'exit'.	<pre>ap 00:13:92:00:33:1C b) # description this-is-the-device-description executed successfully. To save the changes, type</pre>
Related Commands	<u>ap</u> devname location	
	location To set the device loca location {loc	ation, use the following command: ation}
Syntax Description	location	Device location
	{location}	Set the device location to this address
Defaults	None.	
Example	To set the device loca ruckus# config	ation to Sunnyvale-Office, run this command:

ruckus(config)# ap 00:13:92:00:33:1C
ruckus(config-ap)# location Sunnyvale-Office
The command was executed successfully. To save the changes, type
'end' or 'exit'.

Related Commands

<u>ap</u> devname

.

description

Configure Device Network Addressing Commands

Use the config ap ip-addr commands to configure the device's IP address, netmask, gateway, and IP addressing mode.

ip addr

To set the device's IP address and netmask, use the following command:

ip addr {IP address} {netmask}

Use a space () to separate the IP address and netmask.

Syntax Description			
Syntax Description	ip addr	IP address	
	{IP address}	Set the IP address to this address	
	{netmask}	Set the netmask to this address	
Defaults	None.		
Example	ruckus# config		
	ruckus(config)# a	p 00:13:92:00:33:1C	
	ruckus(config-ap)	# ip addr 192.168.0.33 255.255.255.0	
	The command was end 'end' or 'exit'.	xecuted successfully. To save the changes, type	
Related Commands	ip addr gateway		
	<u>ip mode</u>		
	ip name-server		
	ip addr gateway		
	To set the device's IP a the following comman	ddress, netmask, and gateway IP address at the same time, use Id:	

ip addr {IP address} {netmask} gateway {gateway IP address}

Configure Device's System Information

Syntax Description	ip addr	IP address	
	{IP address}	Set the IP address to this address	
	{netmask}	Set the netmask to this address	
	gateway	Gateway IP address	
	{gateway IP address}	Set the gateway IP address to this address	
Defaults	None.		
Example	ruckus# config ruckus(config)# ruckus(config-a 192.168.0.1	ap 00:13:92:00:33:1C p)# ip addr 192.168.0.33 255.255.255.0 gateway	
	The command was 'end' or 'exit'.	executed successfully. To save the changes, type	
Related Commands	ip addr		
	ip mode		
	ip name-server		
	ip mode To set the device's IF ip mode {dhc ₁	P address mode setting, use the following command: p static keep}	
Syntax Description	ip mode	IP address mode	
	{dhcp}	Set the device's IP address mode to DHCP	
	{static}	Set the device's IP address mode to static	
	{keep}	Leave the IP address mode unchanged	
Defaults	None.		
Example	To set the device's IF ruckus# config ruckus(config)# ruckus(config-a) The command was	<pre>P address mode to 'static', run this command: ap 00:13:92:00:33:1C p) # ip mode static executed successfully. To save the changes, type</pre>	
	'end' or 'exit'.		

Configure the 2.4GHz Radio Commands

Related Commands ip addr

ip addr gateway

ip name-server

ip name-server

To set the device's DNS servers, use the following command:

ip name-server {NS1} {NS2}

Use a space () to separate the primary and secondary DNS servers.

Syntax Description	ip name-server	Nameserver IP addresses
	{NS1}	Set the primary nameserver to this IP address
	{NS2}	Set the secondary nameserver to this IP address
Defaults	None.	
Example	ruckus# config ruckus(config)# ag ruckus(config-ap) The command was ex	<pre>p 00:13:92:00:33:1C # ip name-server 192.168.0.2 192.168.0.3 xecuted successfully. To save the changes, type</pre>
Related Commands	ip addr gateway	
	ip mode Configure th	ne 2.4GHz Radio Commands
	Use the radio 2.4 c	ommands to configure the 2.4GHz radio settings of a device.

radio 2.4 channel

To set the 2.4GHz radio to use a specific channel, use the following command: radio 2.4 channel {channel number}

To run these commands, you must first enter the config-ap context.

char	nnel	Radio channel
{cha	annel number}	Set the radio channel to this number

Defaults	None.	
Example	To set the 2.4Ghz r ruckus# config ruckus(config); ruckus(config-a The command was 'end' or 'exit	<pre>radio to channel 1, enter this command: # ap 00:13:92:00:33:1C ap)# radio 2.4 channel 1 s executed successfully. To save the changes, type '.</pre>
Related Commands	radio 2.4 channel a radio 2.4 tx-power radio 2.4 tx-power radio 2.4 tx-power	<u>auto</u> up
	radio 2.4 chan To set the 2.4GHz radio 2.4 c	nel auto radio to use 'Auto' channel, use the following command: [:] hannel auto
Syntax Description	radio 2.4	2.4GHz radio settings
	channel	Radio channel
	auto	Set the radio channel to 'auto'
Defaults	None.	
Example	ruckus# config ruckus(config); ruckus(config- The command was 'end' or 'exit	<pre># ap 00:13:92:00:33:1C ap)# radio 2.4 channel auto s executed successfully. To save the changes, type '.</pre>
Related Commands	radio 2.4 channel	
	radio 2.4 tx-power	
	radio 2.4 tx-power	auto
	radio 2.4 wlan-grou	up
		—

radio 2.4 tx-power

To set the 2.4GHz radio to use a specific TX power setting, use the following command:

Configure the 2.4GHz Radio Commands

radio 2.4 tx-power {TX power} Syntax Description 2.4GHz radio settings radio 2.4 tx-power TX power setting Set the TX power to this number {TX power} Defaults None. Example To set the TX power to 1, run this command: ruckus# config ruckus(config)# ap 00:13:92:00:33:1C ruckus(config-ap)# radio 2.4 tx-power 1 The command was executed successfully. To save the changes, type 'end' or 'exit'. **Related Commands** radio 2.4 channel radio 2.4 channel auto radio 2.4 tx-power auto radio 2.4 wlan-group radio 2.4 tx-power auto To set the 2.4GHz radio to use auto TX power setting, use the following command: radio 2.4 tx-power auto Syntax Description radio 2.4 2.4GHz radio settings TX power setting tx-power Set the TX power to auto auto Defaults None. Example ruckus# config ruckus(config)# ap 00:13:92:00:33:1C ruckus(config-ap)# radio 2.4 tx-power auto The command was executed successfully. To save the changes, type 'end' or 'exit'. Related Commands radio 2.4 channel

radio 2.4 channel auto

radio 2.4 tx-power

radio 2.4 wlan-group

radio 2.4 wlan-group

To ass sign the 2.4GHz radio to the specific WLAN group, use the following command: radio 2.4 wlan-group {WLAN group name}

Syntax Description			
Syntax Description	radio 2.4	2.4GHz radio settings	
	wlan-group	WLAN group	
	{WLAN group name}	Assign the radio to this WLAN group	
Defaults	None.		
Example	To assign the 2.4GHz radio to a WLAN group named <i>Default</i> , run this command:		
	ruckus# config		
	ruckus(config)# ap 00:13:92:00:33:1C		
	<pre>ruckus(config-ap)# radio 2.4 wlan-group Default</pre>		
	The command was exe 'end' or 'exit'.	ecuted successfully. To save the changes, type	
Related Commands	radio 2.4 channel		
	radio 2.4 channel auto		
	radio 2.4 tx-power		
	radio 2.4 tx-power auto		
	Configure the 5GHz Radio Commands		
	Use the radio 5 commands to configure the 5GHz radio settings		
	of a device. To run these commands, you must first enter the config-ap context.		
	radio 5 channel		
	To set the 5GHz radio to a specific channel, use the following command:		
	radio 5 channel	{channel number}	
Syntax Description	·		
	radio 5	5GHz radio settings	
	channel	Radio channel	

Configure the 5GHz Radio Commands

	{channel number}	Set the radio channel to this number
Defaults	None.	
	- -	
Example	lo set the 5GHz chanr	nel to 1, run this command:
	ruckus# config	
	ruckus(config)# a	p 00:13:92:00:33:1C
	The command was end 'end' or 'exit'.	* radio 5 channel 1 xecuted successfully. To save the changes, type
Polatod Commands	radio 5 channel auto	
Related Commands		
	radio 5 tx-power	
	<u>radio 5 tx-power auto</u>	
	<u>radio 5 wlan-group</u>	
	radio 5 channel a To set the 5GHz radio radio 5 channe	uto to use 'Auto' channel, use the following command: auto
Syntax Description	radio 5	5GHz radio settings
	rhannal	Padia shannal
	auto	Set the radio channel to 'auto'
Defaults	None.	
Example	<pre>ruckus# config ruckus(config)# ap 00:13:92:00:33:1C ruckus(config-ap)# radio 5 channel auto The command was executed successfully. To save the changes, type 'end' or 'exit'.</pre>	
Related Commands	radio 5 channel	
	<u>radio 5 tx-power</u>	
	radio 5 tx-power auto	
	radio 5 wlan group	
	radio 5 man-group	

radio 5 tx-power

To set the 5GHz radio to use a specific TX power setting, use the following command: radio 5 tx-power {TX power}

	-	
Syntax Description	radio 5	5GHz radio settings
	tx-power	TX power settings
	{TX power}	Set the TX power to this number
Defaults	None.	
Example	 To set the 5GHz ra	idio TX power to 1, enter this command:
	ruckus# config	
	ruckus(config)	# ap 00:13:92:00:33:1C
	ruckus(config-a	ap)# radio 5 tx-power 1
	The command was 'end' or 'exit	s executed successfully. To save the changes, type '.
Related Commands	radio 5 channel	
	radio 5 channel au	ito
	radio 5 tx-power a	
	radio 5 wlan-grour	
		2
	radio 5 tx-pow	ver auto
	To set the 5GHz ra	idio to use auto TX power setting, use the following command:
	radio 5 tx-	power auto
Syntax Description		
• j	radio 5	5GHz radio settings
	tx-power	TX power settings
	auto	Set the TX power to auto
Defaults	None.	
Example	- ruckus# config	r
·	ruckus(config)	# ap 00:13:92:00:33:1C
	ruckus(config-a	ap)# radio 5 tx-power auto
	The command was 'end' or 'exit	s executed successfully. To save the changes, type '.

Configure the 5GHz Radio Commands

Related Commands radio 5 channel

radio 5 channel auto

radio 5 tx-power

radio 5 wlan-group

radio 5 wlan-group

To assign the 5GHz radio to the specific WLAN group, use the following command: radio 5 wlan-group {WLAN group name}

Suntax Description		
Syntax Description	radio 5	Configure the 5GHz radio settings
	wlan-group	WLAN group settings
	{WLAN group name}	Assign the radio to this WLAN group
Defaults	None.	
Example	To assign the 5GHz radi ruckus# config ruckus(config)# ap	io to a WLAN group named <i>Default</i> , enter this command: 00:13:92:00:33:1C
	ruckus(config-ap)# The command was exe 'end' or 'exit'.	radio 5 wlan-group Default ecuted successfully. To save the changes, type
Related Commands	radio 5 channel	
	radio 5 channel auto	
	radio 5 tx-power	
	radio 5 tx-power auto	

Configure Management VLAN Commands

Use the config ap management vlan commands to configure and display the management VLAN settings.

ap-management-vlan

To enable the device's policy VLAN and update the VLAN ID to the specified ID number, use the following command:

ap-management-vlan {vlan id}

Curatas Decemination	- 	
Syntax Description	ap-management- vlan	Management VLAN settings
	{vlan id}	Set the management VLAN ID to this value
Defaults	Disabled.	
Example	ruckus(config)# a	p-management-vlan 3
	The AP management ruckus(config)#	VLAN has been updated.
Related Commands	vlan	
	Configure Lay	yer 2 Access Control Commands
	Use the layer2 acc Control List settings. To context.	ess control commands to configure the Layer 2 Access orun these commands, you must first enter the config-l2acl
	To enter the config- ruckus# config	12ac1 context, run this command:
	ruckus(config)# 1	2acl L2ACL-policy
	ruckus(config-12a	cl-L2ACL-policy)#
	exit	
	To save changes, and command:	then exit the config-12ac1 context, use the following
	exit	
Syntax Description		Save changes and exit the config=12ac1 context
Defaults	None.	

Configure the 5GHz Radio Commands

Example	ruckus(config-12acl)# exit
	Your changes have been saved.
Related Commands	- show
	show
	To displays the L2 ACL settings, use the show command. You must run this command from within the config-12ac1 context.
	show
Syntax Description	
, , , , , , , , , , , , , , , , , , ,	show Display the Layer 2 access control list settings
Defeulte	-
Defaults	None.
Example	- ruckus(config)# 12acl L2ACL-policy
	The L2 ACL entry 'L2ACL-policy' has been loaded. To save the L2 ACL entry, type 'end' or 'exit'.
	ruckus(config-l2acl)# show
	L2/MAC ACL:
	ID:
	3:
	Name= L2ACL-policy
	Description=
	Restriction: Deny only the stations listed below
	Stations:

Related Commands exit

no acl

To delete an L2 ACL, use the following command:

no acl {ACL name}

	-	
Syntax Description	no acl	Delete an existing ACL
	{ACL name}	Delete this ACL
	_	
Defaults	None.	
Example	- ruckus# config	r
	ruckus(config)	# no acl L2_ACL_NAME
	The L2 ACL 'L2_	ACL_NAME' has been deleted.
Related Commands	- acl	
	<u>abort</u>	
	end	
	exit	
	quit	
	<u></u>	
	acl	
	To create a new L2 /	ACL entry or update an existing entry, use the following command:
	acl {ACL nav	me}
Syntax Description	acl	Create a new ACL
	{ACL name}	Assign this name to the new ACL
	-	
Defaults	None.	
Example	- ruckus# config	,
-	ruckus(config)	# 12ac1 L2_ACL_NAME
	The L2 ACL entr	ry 'L2_ACL_NAME' has been created.
	ruckus(config-1	L2acl-L2_ACL_NAME)#
Related Commands	<u>acl</u>	
	abort	
	end	

Configure the 5GHz Radio Commands

<u>exit</u>

<u>quit</u>

abort

To exit the config-l2acl-{ACL name} context without saving changes, use the following command:

acl {ACL name} abort

Syntax Description	acl	ACL context
	{ACL name}	Name of the ACL context
	abort	Exit the context without saving changes
Defaults	None.	
Example	ruckus# config	
	ruckus(config)#	12acl L2_ACL_NAME
	The L2 ACL entr	y 'L2_ACL_NAME' has been created.
	ruckus(config-1	2acl-L2_ACL_NAME)# abort
	No changes have	been saved.
Related Commands	no acl	
	acl	
	end	
	exit	
	quit	
	end	
	To save changes, a	nd then exit the config-l2acl-{ACL, name} context, use the
	following command	d:
	acl {ACL nam	ne} end
Syntax Description		
Syntax Description	acl	ACL context
	{ACL name}	Name of the ACL context
	end	Exit the context without saving changes
Defaults	None	
Deraults		

Example	ruckus# config
	<pre>ruckus(config)# 12acl L2_ACL_NAME</pre>
	The L2 ACL entry 'L2_ACL_NAME' has been created.
	ruckus(config-l2acl-L2_ACL_NAME)# end
	Your changes have been saved.

Related Commands	<u>no acl</u>
	acl
	<u>abort</u>
	<u>exit</u>
	<u>quit</u>

exit

To save changes, and then exit the config-l2acl-{ACL <code>name}</code> context, use the following command:

acl {ACL name} exit

Syntax Description	Syntax	Description
--------------------	--------	-------------

,	acl	ACL context	
	{ACL name}	Name of the ACL context	
	exit	Exit the context without saving changes	
Defaults	None.		
Example	ruckus# config ruckus(config)#	12acl L2_ACL_NAME	
	ruckus(config-]	.2acl-L2 ACL NAME' has been created.	
	Your changes ha	ave been saved.	
Related Commands	no acl		
	acl		

<u>abort</u> <u>end</u> <u>quit</u>

quit

To exit the config-l2acl-{ACL name} context without saving changes, use the following command:

acl {ACL name} quit

acl ACL context {ACL name} Name of the ACL context quit Exit the context without saving changes Defaults None. Example ruckus# config ruckus (config) # 12acl L2_ACL_NAME The L2 ACL entry 'L2_ACL_NAME' has been created. ruckus (config-12acl-L2_ACL_NAME) # quit Your changes have been saved. Related Commands no acl acl abort end exit acl name To recome an L2 ACL entry use the following command:	
{ACL name} Name of the ACL context quit Exit the context without saving changes Defaults None. Example ruckus# config ruckus(config)# 12acl L2_ACL_NAME The L2 ACL entry 'L2_ACL_NAME' has been created. ruckus(config-12acl-L2_ACL_NAME)# quit Your changes have been saved. Related Commands no acl acl abort end exit acl name To recome ap 12 ACL entry use the following command:	
quit Exit the context without saving changes Defaults None. Example ruckus# config ruckus(config)# 12acl L2_ACL_NAME The L2 ACL entry 'L2_ACL_NAME' has been created. ruckus(config-12acl-L2_ACL_NAME)# quit Your changes have been saved. Related Commands no acl acl abort end exit acl name To renome on 12 ACL entry use the following command:	
Defaults None. Example ruckus# config ruckus(config)# 12acl L2_ACL_NAME The L2 ACL entry 'L2_ACL_NAME' has been created. ruckus(config-12acl-L2_ACL_NAME)# quit Your changes have been saved. Related Commands no acl acl abort end exit acl name Tr represe on L2 ACL entry use the following command:	
Example ruckus# config ruckus(config)# 12acl L2_ACL_NAME The L2 ACL entry 'L2_ACL_NAME' has been created. ruckus(config-12acl-L2_ACL_NAME)# quit Your changes have been saved. Related Commands no acl acl abort end exit Acl name To renome on L2 ACL entry use the following command:	
Example ruckus# config ruckus (config) # 12ac1 L2_ACL_NAME The L2 ACL entry 'L2_ACL_NAME' has been created. ruckus (config-12ac1-L2_ACL_NAME) # quit Your changes have been saved. Related Commands no acl acl abort end exit Acl name To rename an L2 ACL entry use the following command:	
ruckus (config) # 12acl L2_ACL_NAME The L2 ACL entry 'L2_ACL_NAME' has been created. ruckus (config-12acl-L2_ACL_NAME) # quit Your changes have been saved. Related Commands no acl acl abort end exit acl name To renzeme on L2 ACL entry use the following command:	
The L2 ACL entry 'L2_ACL_NAME' has been created. ruckus(config-12acl-L2_ACL_NAME)# quit Your changes have been saved. Related Commands no acl acl abort end exit acl name To rename an L2 ACL entry use the following command:	
ruckus (config-12acl-L2_ACL_NAME) # quit Your changes have been saved. Related Commands no acl acl abort end exit abort end exit acl name To represe on L2 ACL entry use the following command:	
Your changes have been saved. Related Commands no acl acl abort end exit acl name To represe on L2 ACL entry use the following command:	
Related Commands no acl acl abort end exit acl name To repromo an U2 ACL opting uppet the following command:	
acl abort end exit acl name	
abort end exit acl name	
end exit acl name	
exit acl name	
acl name	
To rename an 12 ACL entry use the following command:	
to rename an LZ ACL entry, use the following command:	
acl {ACL name} name	
Syntax Description	
{ACL name} Name of the ACL context	
name {new name} Rename the ACL to {new name}	
Defaults None.	
Example ruckus# config	
ruckus(config)# 12ac1 L2_ACL_NAME	
The L2 ACL entry 'L2_ACL_NAME' has been created.	
ruckus(config-l2acl-L2_ACL_NAME)# name L2_ACL_New_Name	

The command was executed successfully.

Related Commands acl name

acl description add mac mode allow mode deny no mac

acl description

To set the description of an L2 ACL entry, use the following command: description {description}

Syntax Description	description {description} Set the L2 ACL description to {description}
Defaults	None.
Example	ruckus# config ruckus(config)# l2acl L2_ACL_NAME The L2 ACL entry 'L2_ACL_NAME' has been created. ruckus(config-l2acl-L2_ACL_NAME)# description Description-123 The command was executed successfully.
Related Commands	acl name acl description add mac mode allow mode deny
	add mac To add a MAC address to the L2 ACL, use the following command: add mac {MAC address}
Syntax Description	add mac Add a MAC address to the ACL
	{MAC address} Add this MAC address

Configure the 5GHz Radio Commands

Defaults	None.			
Example	<pre>ruckus# config ruckus(config)# l2acl L2_ACL_NAME The L2 ACL entry 'L2_ACL_NAME' has been created. ruckus(config-l2acl-L2_ACL_NAME)# add mac 00:11:22:33:44:55 The station '00:11:22:33:44:55' has been added to the ACL.</pre>			
Related Commands	acl name acl description mode allow mode deny no mac mode allow To set the ACL mode to 'allow', use the following command: mode allow			
Syntax Description	mode allow Set the ACL mode to allow			
Defaults	None.			
Example	ruckus# config ruckus(config)# 12acl L2_ACL_NAME The L2 ACL entry 'L2_ACL_NAME' has been created. ruckus(config-12acl-L2_ACL_NAME)# mode allow The command was executed successfully.			
Related Commands	acl name acl description add mac mode deny no mac mode deny To set the ACL mode to 'deny', use the following command: mode deny			

Configure the 5GHz Radio Commands

Syntax Description	mode allow	Set the ACL mode to deny
Defaults	None.	
Example	ruckus# config	
	The L2 ACL entry	12aCI L2_ACL_NAME
	ruckus(config-12	acl-L2 ACL NAME) # mode deny
	The command was	executed successfully.
Related Commands	acl name	
	acl description	
	add mac	
	mode allow	
	no mac	
	To delete a MAC adv	drass from an 12 ACL use the following command:
	no mac {MAC add	address}
Syntax Description		Delete a MAC address from the ACI
	{MAC address}	Delete {MAC address}
Defaults	- None.	
Example	- ruckus# config	
	ruckus(config)#	12acl L2_ACL_NAME
	The L2 ACL entry	'L2_ACL_NAME' has been created.
	ruckus(config-12)	$acl-L2_ACL_NAME) \#$ no mac 00:11:22:33:44:55
		11.22.33.44.33 has been added to the Ach.
Related Commands	acl name	
	acl description	
	add mac	
	<u>mode deny</u>	
	mode allow	

Configure NTP Client Commands

Use the ntp commands to configure the controller's NTP client settings. To run these commands, you must first enter the config-sys context.

no ntp

To disable the NTP client, use the following command:

no ntp

	-			
Syntax Description	no ntp	Disable the NTP client on the controller.		
Defaults	Enabled. The default NTP server address is <pre>ntp.ruckuswireless.com.</pre>			
Example	_ ruckus# config			
	ruckus(config)# system			
	ruckus(config-s	ys)# no ntp		
	NTP has been di	sabled.		
	The command was	executed successfully.		
Related Commands	ntp			
	nto			
	To enable the NTP client, use the following command:			
	ntn /MTD server address)			
Syntax Description	-			
	ntp	Enable the NTP client		
	{NTP server}	Set the NTP server address to this IP address		
Defaults	None.			
Example	- ruckus# config			
	ruckus(config)# system			
	ruckus(config-sys)# ntp 192.168.0.3			
	NTP has been end	abled. The NTP server address is '192.168.0.3'.		
	The command was	executed successfully.		
Related Commands	no ntp			
Configure Smart Redundancy Commands

The Smart Redundancy feature allows two ZoneDirector devices to be configured as a redundant pair, with one unit actively managing your ZoneFlex network while the other serves as a backup in standby mode, ready to take over if the first unit fails or loses power.

Each ZoneDirector will either be in active or standby state. If the active ZoneDirector fails, the standby device becomes active. When the original active device recovers, it automatically assumes the standby state as it discovers an already active ZoneDirector on the network.

The ZoneDirector in active state manages all APs and client connections. The ZoneDirector in standby state is responsible for monitoring the health of the active unit and periodically synchronizing its settings to match those of the active device. The ZoneDirector in standby state will not respond to Discovery requests from APs and changing from active to standby state will release all associated APs.

When failover occurs, all associated APs will continue to provide wireless service to clients during the transition, and will associate to the newly active ZoneDirector within approximately one minute.



NOTE: This feature is only available using two ZoneDirector devices of the same model and number of licensed APs. You can not enable Smart Redundancy using a ZoneDirector 3000 as the primary and a ZoneDirector 1000 as the backup unit, for example.

Use the smart-redundancy commands to configure the smart redundancy settings. To use these commands, you must first enter the config-sys-smart-redundancy context.

peer-ip-addr {IPADDR}

To set the controller's peer (redundant) device, use the following command:

peer-ip-addr {IPADDR}

Syntax Description		
Syntax Description	peer-ip-addr	Set the IP address of the peer ZoneDirector device
	{IPADDR}	Set the IP address to this address
Defaults	None.	
Example	- ruckus# config ruckus(config)#	system
	ruckus(config-sy ruckus(config-sy	s)# smart-redundancy s-smart-redundancy)# peer-ip-addr 192.168.0.44

Configure Smart Redundancy Commands

The command was executed successfully. To save the changes, type 'end' or 'exit'.

Related Commandssecret {SECRET}

no smart redundancy

secret {SECRET}

Peer ZoneDirector devices use a shared secret (up to 15 alphanumeric characters) to secure the communication between them. Use the following command to configure the shared secret between two peer ZoneDirector devices:

secret {SECRET}

Syntax Description	-		
Syntax Description	secret	Set the shared secret between peer ZoneDirector devices	
	{SECRET}	Set the shared secret to this secret	
Defaults	None.		
Example	ruckus# config		
	ruckus(config)# system		
	ruckus(config-	-sys)# smart-redundancy	
	ruckus(config-	-sys-smart-redundancy)# secret testing123	
	The command wa 'end' or 'exit	as executed successfully. To save the changes, type	
Related Commands	peer-ip-addr {IPA	DDR}	
	no smart redundancy		
	no smart redu	Indancy	
	Use the following	command to disable smart redundancy:	
	no smart r	edundancy	
Syntax Description			
Syntax Description	no smart redur	ndancy Disable smart redundancy on the controller	
Defaults	Disabled.		
Example	ruckus# confi	g	
	ruckus(config)	# system	
	ruckus(config-	-sys)# no smart-redundancy	

The command was executed successfully. To save the changes, type <code>'end'</code> or <code>'exit'</code>.

Related Commands pee

peer-ip-addr {IPADDR}

secret {SECRET}

Configure Management Interface Commands

The additional management interface is created for receiving or transmitting management traffic only. The management IP address can be configured to allow an administrator to access ZoneDirector remotely from a different subnet from the AP network.



NOTE: The management interface can also be used for Smart Redundancy. When redundant ZoneDirectors are deployed, you can create a separate management interface to be shared by both devices.

To run these commands, you must first enter the config-sys-mgmt-if context.

ip addr {IPADDR} {NETMASK}

To set the controller's management IP address and netmask, use the following command:

ip addr {IPADDR} {NETMASK}

Use a space () to separate the IP address and netmask.

Syntax Description			
Syntax Description	ip addr	Set the management IP address of the controller	
	{IPADDR}	Set the management IP address to this address	
	{NETMASK}	Set the netmask to this address	
Defaults	None.		
Example	- ruckus# config		
	ruckus(config)# system		
	ruckus(config-sys)# mgmt-if		
	ruckus(config-sys-mgmt-if)# ip addr 192.168.0.33 255.255.255.0		
	The command was 'end' or 'exit	s executed successfully. To save the changes, type '.	
Related Commands	ip addr {IPADDR}	[NETMASK]	

Configure Management Interface Commands

no mgmt-if

vlan {VLAN-ID}

<u>no vlan</u>

no mgmt-if

Use the following command to disable the management interface and management VLAN settings:

no mgmt-if

	_	
Syntax Description	no mgmt-if	Disable the management interface
Defaults	Disabled.	
Example	ruckus# config ruckus(config); ruckus(config-s The command was 'end' or 'exit	# system sys)# no mgmt-if s executed successfully. To save the changes, type '.
Related Commands	ip addr {IPADDR} { no mgmt-if vlan {VLAN-ID} no vlan vlan {VLAN-ID } To enable the man	NETMASK} agement VLAN and set the VLAN ID, use the following command:
Syntax Description		
Syntax Description	vlan {VLAN-ID}	Enable the management VLAN Set the VLAN ID to this ID number
Defaults	None.	
Example	ruckus# config ruckus(config); ruckus(config-s ruckus(config-s	# system sys)# mgmt-if sys-mgmt-if)# vlan 111

The command was executed successfully. To save the changes, type 'end' or 'exit'.

Related Commands	ip addr {IPADDR} {NETMASK}		
	<u>no mgmt-if</u>		
	vlan {VLAN-ID}		
	<u>no vlan</u>		
	no vlan To disable the management VLAN, use the following command:		
	no vlan		
Syntax Description			
	no vlan Disable the management VLAN		
Defaults	None		
Deraults			
Example	ruckus# config		
	ruckus(config)# system		
	ruckus(config-sys)# mgmt-if		
	ruckus(config-sys-mgmt-if)# no vlan		
	The command was executed successfully. To save the changes, type 'end' or 'exit'.		
Related Commands	ip addr {IPADDR} {NETMASK}		
	<u>no mgmt-if</u>		
	vlan {VLAN-ID}		
	<u>no vlan</u>		
	Configure SNMP Agent Commands		
	Use the snmp-agent commands to configure the SNMP agent on the controller. To		
	use these commands, you must first enter the config-sys context.		
	no snmp-agent		
	To disable the SNMP agent, use the following command:		
	no snmp-agent		
Suntau Deceriation	·		

Syntax Description

no snmp-agent Disables the SNMP agent

Configure SNMP Agent Commands

Defaults	None.
Example	ruckus# config ruckus(config)# system ruckus(config-sys)# no snmp-agent The SNMP client and trap settings have been updated.
Related Commands	no snmp-agent no snmp-trap contact location ro-community rw-community snmp-trap
Syntax Description	no snmp-trap To disable the SNMP trap notifications, use the following command: no snmp-trap no snmp-trap Disables SNMP trap notifications
Defaults	None.
Example	ruckus# config ruckus(config)# system ruckus(config-sys)# no snmp-trap The SNMP trap settings have been updated. ruckus(config-sys)#
Related Commands	no snmp-agent contact location ro-community rw-community snmp-trap

contact

To enable SNMP trap notification and set the system contact, use the following command:

contact {contact name}

This command must be entered from within the snmp-agent context.

Syntax Description	aontaat	Configure the SNMP contact		
	{contact name}	Set the SNMP contact to this value		
Defaults	None.			
Example	ruckus# config			
	ruckus(config)# s	ystem		
	ruckus(config-sys)# snmp-agent			
	<pre>ruckus(config-sys-snmp-agent)# contact Joe-User</pre>			
	The command was e	xecuted successfully.		
Related Commands	no snmp-agent			
	no snmp-trap			
	location			
	<u>ro-community</u>			
	<u>rw-community</u>			
	snmp-trap			
	location			
	To set the system location, use the following command:			
	location {location name}			
	e entered from within the snmp-agent context.			
	-			
Syntax Description	location	Configure the SNMP location		
	{location name}	Set the SNMP location to this value		
	-			
Defaults	None.			
Example	ruckus# config			
	ruckus(config)# system			
	ruckus(config-sys) # snmp-agent		

Configure SNMP Agent Commands

ruckus(config-sys-snmp-agent)# location Sunnyvale
The command was executed successfully.

Related Commands <u>no snmp-agent</u>

no snmp-trap contact ro-community rw-community snmp-trap

ro-community

To set the read-only (RO) community name, use the following command: ro-community {RO community}

This command must be entered from within the snmp-agent context.

Suntax Description			
Syntax Description	ro-community	Configure the read-only community name	
	{RO community}	Set the read-only community name to this value	
Defaults	None.		
Example	ruckus(config-sys The command was e	-snmp-agent)# ro-community private-123 executed successfully	
Related Commands	no snmp-agent		
	no snmp-trap		
	<u>contact</u>		
	location		
	rw-community		
	snmp-trap		
	rw-community		
	To set the read-write (RW) community name, use the following command:		
	This command must be entered from within the snmp-agent context.		
Syntax Description	rw-community	Configure the read-write community name	

	{RW community}	Set the read-write community name to this value
Defaults	None.	
Example	ruckus(config-sys The command was e	-snmp-agent)# rw-community public-123 executed successfully
Related Commands	no snmp-agent	
	no snmp-trap	
	<u>contact</u>	
	location	
	ro-community	
	snmp-trap	
	To enable SNMP trap command: snmp-trap {tra	notification and set the trap server address, use the following ap server address}
Syntax Description	snmp-trap	Enable SNMP trap notifications
	{trap server address}	Set the trap server address to this IP address or host name
Defaults	None.	
Example	ruckus# config	
	ruckus(config)# s ruckus(config-sys	ystem)# snmp-trap 192.168.0.3
Related Commands	no snmp-agent	
	no snmp-trap	
	<u>contact</u>	
	location	
	ro-community	
	rw-community	

Configure Syslog Settings Commands

Use the syslog commands to configure the controller's syslog notification settings. To run these commands, you must first enter the config-sys context.

no syslog

To disable syslog notification, use the following command:

no syslog

Syntax Description			
	no syslog	Disable syslog notification	
Defaults	Disabled.		
Example	ruckus# config		
	ruckus(config)	# system	
	ruckus(config-	sys)# no syslog	
	The command wa	s executed successfully.	
Related Commands	syslog		
	syslog		
	To enable syslog notifications and set the syslog server address, use the following		
	command:		
	syslog {sys	<pre>slog address}</pre>	
Syntax Description	-		
	syslog	Enable syslog notification	
	{syslog IP add	ress} Send syslog notifications to this IP address or host name	
Defaults	Disabled.		
Example	ruckus# config	1	
	ruckus(config)# system		
	ruckus(config-	sys)# syslog 192.168.0.1	
	The command wa	s executed successfully.	
Related Commands	no syslog		

Configure Controller's Country Setting Command

Use the dot11-country-code commands to configure the controller's country settings. To run these commands, you must first enter the config-sys context.

dot11-country-code

To set the controller's country code, use the following command:

dot11-country-code {country code}

	-	
Syntax Description	dot11-country- code	Configure the controller's country code setting
	{country code}	Set the country code to this value
Defaults	None.	
Example	To set the country code ruckus# config ruckus(config)# sy ruckus(config-sys) The command was ex	e to US, enter the following command: ystem # dot11-country-code US secured successfully.
Related Commands	None.	
	Configure Con Use the ip commands commands, you must f ip route gateway To set the controller's g ip route gatew	ntrolller's IP Address Commands to configure the controller's IP address settings. To run these first enter the config-sys-if context. gateway IP address, use the following command: ay {gateway IP address}
Syntax Description	ip route gateway {gateway IP address}	Configure the controller's gateway IP address Set the controller' gateway IP address to this value
Defaults	None.	
Example	ruckus# config ruckus(config)# sy	ystem

Configure Syslog Settings Commands

ruckus(config-sys)# interface
ruckus(config-sys-if)# ip route gateway 192.168.0.1
The command was executed successfully.

Related Commands	ip name-server ip addr		
	<u>ip mode</u>		
	show		
	ip name-server To set the controller's DNS servers, use the ip name-server command. Use a space to separate the primary and secondary DNS servers.		
	ip name-serve	r {DNS server}	
Syntax Description	ip name-server	Configure the controller's DNS server address or addresses	
	{DNS server}	Set the DNS server address to this value. If entering primary and secondary DNS server addresses, use a space to separate the two addresses.	
Defaults	None.		
Example	ruckus# config		
	ruckus(config)# system		
	ruckus(config-sys)# interface		
	The command was e	xecuted successfully.	
Related Commands	ip route gateway		
	ip mode		
	<u>show</u>		
	ip addr To set the controller's ip addr {IP ac Use a space to separa	IP address and netmask, use the following command: ddress} {netmask} ite the IP address and netmask.	

Syntax Description	-			
- ,	ip addr	Contigure the controller's IP address and netmask		
	{IP address}	Set the controller's IP address to this value		
	{netmask}	Set the controller's netmask to this value		
Defaults	None.			
Example	_ ruckus# config			
	ruckus(config)#	system		
	ruckus(config-sy	vs)# interface		
	ruckus(config-sy	rs-if)# ip addr 192.168.0.1 255.255.255.0		
	The command was	executed successfully.		
Related Commands	ip route gateway			
	<u>ip name-server</u>			
	ip mode			
	show			
	<u>show</u> ip mode To set the controller	's IP address mode, use the following command:		
Syntax Description	show ip mode To set the controller ip mode {dhc	's IP address mode, use the following command: p static}		
Syntax Description	show ip mode To set the controller ip mode {dhc ip mode	's IP address mode, use the following command: p static} Configure the controller's IP address mode		
Syntax Description	show ip mode To set the controller ip mode {dhc {dhcp}	's IP address mode, use the following command: p static} Configure the controller's IP address mode Set the controller's IP address mode to DHCP		
Syntax Description	<pre>show ip mode To set the controller ip mode {dhc {dhcp} {static}</pre>	's IP address mode, use the following command: p static} Configure the controller's IP address mode Set the controller's IP address mode to DHCP Set the controller's IP address mode to static		
Syntax Description	<pre>show ip mode To set the controller ip mode {dhc {dhcp} {static} None.</pre>	's IP address mode, use the following command: p static} Configure the controller's IP address mode Set the controller's IP address mode to DHCP Set the controller's IP address mode to static		
Syntax Description Defaults Example	<pre>show ip mode To set the controller ip mode {dhc ip mode {dhcp} {static} None. To set the controller ruckus# config ruckus(config)# ruckus(config-sy The command was</pre>	<pre>'s IP address mode, use the following command: p static} Configure the controller's IP address mode Set the controller's IP address mode to DHCP Set the controller's IP address mode to static 's IP address mode to DHCP, enter the following command: system rs)# interface rs-if)# ip mode dhcp executed successfully.</pre>		
Syntax Description Defaults Example Related Commands	<pre>show ip mode To set the controller ip mode {dhc ip mode {dhcp} {static} None. To set the controller ruckus# config ruckus(config)# ruckus(config-sy ruckus(config-sy The command was ip route gateway</pre>	<pre>'s IP address mode, use the following command: p static} Configure the controller's IP address mode Set the controller's IP address mode to DHCP Set the controller's IP address mode to static 's IP address mode to DHCP, enter the following command: system rs)# interface rs-if)# ip mode dhcp executed successfully.</pre>		

Configure Syslog Settings Commands

<u>ip addr</u>

show

show

To display the current management interface settings, use the following command: show

Syntax Description	show	Display the current management interface settings
Defaults	None.	
Example	ruckus(conf	ig-sys-if)# show
	Device IP A	ddress:
	Mode= DHC	P
	IP Addres	s= 192.168.1.139
	Netmask=	255.255.255.0
	Gateway A	ddress= 192.168.1.3
	Primary D	NS= 172.17.17.5
	Secondary	DNS= 172.17.17.15
	Management	VLAN:
	Status= D	isabled
	VLAN ID=	
Related Commands	ip route gatew	<u>ay</u>
	<u>ip name-serve</u>	<u>r</u>
	ip addr	
	<u>ip mode</u>	
	Configur	e WLAN Settings Commands

Use the config wlan commands to configure the WLAN settings, including the WLAN's description, SSID, and its security settings. To run these commands, you must first enter the config-wlan context.

description

To set the WLAN service description, use the following command:

```
description {WLAN description}
```

Syntax Description			
eyntax Desenption	description	Configure the WLAN description	
	{WLAN description}	Set the WLAN description this value	
Defaults	None.		
Example	ruckus# config	an randu-wlansuc-01-open	
	The WLAN service 'randy-wlansvc-01-open' has been created. To save the WLAN service, type end or exit.		
	ruckus(config-wlan-	randy-wlansvc-01-open)#	
Related Commands	description		

Configure Syslog Settings Commands

ssid

To set the WLAN service's SSID or network name, use the following command:

ssid {SSID}

	-	
Syntax Description	ssid	Configure the WLAN service's SSID
	{SSID}	Set the SSID to this value
	- -	
Defaults	None.	
Example	ruckus# conf	ig
	ruckus(config)# wlan randy-wlansvc-01-open
	The WLAN serv	vice 'randy-wlansvc-01-open' has been created. To save
	the WLAN serv	vice, type end or exit.
	ruckus(config open-ENC-Non	g-wlan-randy-wlansvc-01-open)# description Auth-
	The command w 'end' or 'exi	vas executed successfully. To save the changes, type it'.
	ruckus(config	J-wlan-randy-wlansvc-01-open)#
Related Commands	description	
	open none To set the auther following comm open none	ntication method to 'open' and encryption method to 'none', use the and:
Syntax Description	open	Set the authentication method to 'open'
	none	Set the encryption method to 'none'
Defaults	None.	
Example	ruckus(config The WLAN serv the WLAN serv ruckus(config The command w 'end' or 'exi	<pre>g)# wlan randy-wlansvc-01-open rice 'randy-wlansvc-01-open' has been created. To save rice, type end or exit. g-wlan-randy-wlansvc-01-open)# open none vas executed successfully. To save the changes, type it'.</pre>
Related Commands	open wpa passp	phrase {PASSPHRASE} algorithm AES

open wpa passphrase {PASSPHRASE} algorithm TKIP open wpa2 passphrase {PASSPHRASE} algorithm AES open wpa2 passphrase {PASSPHRASE} algorithm TKIP open wep-64 key {KEY} key-id {KEY-ID} open wep-128 key {KEY} key-id {KEY-ID}

open wpa passphrase {PASSPHRASE} algorithm AES

To set the authentication method to 'open', encryption method to 'WPA', and algorithm to 'AES', use the following command:

open wpa passphrase {passphrase} algorithm AES

Syntax Description	open	Set the authentication method to open	
	wpa	Set the encryption method to WPA	
	passphrase {passphrase}	Set the WPA passphrase to {passphrase}	
	algorithm AES	Set the encryption algorithm to AES	
Defaults	None.		
Example	 ruckus(config)# •	wlan randy-wlansvc-01-open	
	The WLAN service 'randy-wlansvc-01-open' has been created. To save the WLAN service, type end or exit.		
	ruckus(config-wlan-randy-wlansvc-01-open)# open wpa passphrase 12345678 algorithm AES		
	The command was e 'end' or 'exit'.	executed successfully. To save the changes, type	
Related Commands	open none		
	open wpa passphrase	e {PASSPHRASE} algorithm TKIP	
	open wpa2 passphra	se {PASSPHRASE} algorithm AES	
	open wpa2 passphra	se {PASSPHRASE} algorithm TKIP	
	open wep-64 key {KE	Y} key-id {KEY-ID}	
	open wep-128 key {K	EY} key-id {KEY-ID}	

open wpa passphrase {PASSPHRASE} algorithm TKIP

To set the authentication method to 'open', encryption method to 'WPA', and algorithm to 'TKIP', use the following command:

open wpa passphrase {passphrase} algorithm TKIP

Syntax Description	-		
Syntax Description	open	Set the authentication method to open	
	wpa	Set the encryption method to WPA	
	passphrase {passphrase}	Set the WPA passphrase to {passphrase}	
	algorithm TKIP	Set the encryption algorithm to TKIP	
Defaults	None.		
Example	- ruckus(config)# wlan randy-wlansvc-01-open		
	The WLAN service 'randy-wlansvc-01-open' has been created. To save the WLAN service, type end or exit.		
	ruckus(config-wlan-randy-wlansvc-01-open)# open wpa passphrase 12345678 algorithm TKIP		
	The command was e 'end' or 'exit'.	executed successfully. To save the changes, type	
Related Commands	open none		
	open wpa passphrase {PASSPHRASE} algorithm AES		
	open wpa2 passphrase {PASSPHRASE} algorithm AES		
	open wpa2 passphras	e {PASSPHRASE} algorithm TKIP	
	open wep-64 key {KE`	Y} key-id {KEY-ID}	
	open wep-128 key {Kl	EY} key-id {KEY-ID}	

open wpa passphrase {PASSPHRASE} algorithm auto

To set the authentication method to 'open', encryption method to 'WPA', and algorithm to 'auto', use the following command:

open wpa passphrase {passphrase} algorithm auto

Syntax Description	- 			
	open	Set the authentication method to open		
	wpa	Set the encryption method to WPA		
	passphrase {passphrase}	Set the WPA passphrase to {passphrase}		
	algorithm auto	Set the encryption algorithm automatically		
Defaults	None.			
Example	 ruckus(config)# v	vlan randy-wlansvc-01-open		
	The WLAN service the WLAN service,	'randy-wlansvc-01-open' has been created. To save type end or exit.		
	ruckus(config-wla 12345678 algorit	n-randy-wlansvc-01-open)# open wpa passphrase . hm auto		
	The command was e 'end' or 'exit'.	executed successfully. To save the changes, type		
Related Commands	open none			
	open wpa passphrase {PASSPHRASE} algorithm AES			
	open wpa2 passphrase {PASSPHRASE} algorithm AES			
	open wpa2 passphrase {PASSPHRASE} algorithm TKIP			
	open wep-64 key {KEY} key-id {KEY-ID}			
	open wep-128 key {KEY} key-id {KEY-ID}			
	open wpa2 passphrase {PASSPHRASE} algorithm AES To set the authentication method to 'open', encryption method to 'WPA2', and algorithm to 'AES', use the following command:			
	open wpa2 pas	sphrase {passphrase} algorithm AES		
Syntax Description	open	Set the authentication method to open		
	wpa2	Set the encryption method to WPA2		
	passphrase {passphrase}	Set the WPA2 passphrase to {passphrase}		
	algorithm AES	Set the encryption algorithm to AES		

Defaults	None.			
Example	<pre>ruckus(config)# wlan randy-wlansvc-01-open The WLAN service 'randy-wlansvc-01-open' has been created. To save the WLAN service, type end or exit. ruckus(config-wlan-randy-wlansvc-01-open)# open wpa2 passphrase 12345678 algorithm AES</pre>			
	The command was e 'end' or 'exit'.	xecuted successfully. To save the changes, type		
Related Commands	open none			
	<u>open wpa passphrase</u>	{PASSPHRASE} algorithm AES		
	<u>open wpa2 passphras</u>	e {PASSPHRASE} algorithm TKIP		
	open wpa2 passphras	e {PASSPHRASE} algorithm TKIP		
	open wep-64 key {KE`	Y} key-id {KEY-ID}		
	open wep-128 key {KE	EY} key-id {KEY-ID}		
Syntax Description		Set the authentication method to open		
		Set the approximation method to Open		
	passphrase {passphrase}	Set the WPA2 passphrase to {passphrase}		
	algorithm TKIP	Set the encryption algorithm to TKIP		
Defaults	None.			
Example	ruckus(config)# w The WLAN service the WLAN service,	r lan randy-wlansvc-01-open 'randy-wlansvc-01-open' has been created. To save type end or exit.		
	ruckus(config-wlan-randy-wlansvc-01-open)# open wpa2 passphrase 12345678 algorithm TKIP			
	The command was e 'end' or 'exit'.	xecuted successfully. To save the changes, type		
Related Commands	open none			

open wpa passphrase {PASSPHRASE} algorithm AES open wpa2 passphrase {PASSPHRASE} algorithm TKIP open wpa2 passphrase {PASSPHRASE} algorithm AES open wep-64 key {KEY} key-id {KEY-ID} open wep-128 key {KEY} key-id {KEY-ID}

open wpa2 passphrase {PASSPHRASE} algorithm auto

To set the authentication method to 'open', encryption method to 'WPA2', and algorithm to 'auto', use the following command:

open wpa2 passphrase {passphrase} algorithm auto

Cuntary Description	-		
Syntax Description	open	Set the authentication method to open	
	wpa2	Set the encryption method to WPA2	
	passphrase {passphrase}	Set the WPA2 passphrase to {passphrase}	
	algorithm auto	Set the encryption algorithm automatically	
Defaults	None.		
Example	- ruckus(config)# wlan randy-wlansvc-01-open		
	The WLAN service 'randy-wlansvc-01-open' has been created. To save the WLAN service, type end or exit.		
	ruckus(config-wlan-randy-wlansvc-01-open)# open wpa2 passphrase 12345678 algorithm auto		
	The command was e 'end' or 'exit'.	executed successfully. To save the changes, type	
Related Commands	open none		
	<u>open wpa passphrase</u>	{PASSPHRASE} algorithm AES	
	open wpa2 passphrase {PASSPHRASE} algorithm TKIP		
	open wpa2 passphrase {PASSPHRASE} algorithm AES		
	open wep-64 key {KEY} key-id {KEY-ID}		
	open wep-128 key {KEY} key-id {KEY-ID}		
	open wep-64 key	۲ {KEY} key-id {KEY-ID}	
	To set the authenticat index, and WEP key, u	ion method to 'open', encryption method to 'WEP-64', key use the following command:	
	open wep-64 k	ey {key} key-id {key ID}	

Suntax Description				
Syntax Description	open	Set the authentication method to open		
	wep-64	Set the encryption method to WEP 64-bit		
	key {key}	Set the WEP key to {key}		
	key-id {key ID}	Set the WEP key ID to {key ID}		
Defaults	None.			
Example	ruckus(config)# w	lan randy-wlansvc-01-open		
	The WLAN service ' the WLAN service,	randy-wlansvc-01-open' has been created. To save type end or exit.		
	ruckus(config-wla: 1234567890 key-i	n-randy-wlansvc-01-open)# open wep-64 key d 1		
	The command was ex 'end' or 'exit'.	xecuted successfully. To save the changes, type		
Related Commands	open none			
	<u>open wpa passphrase</u>	{PASSPHRASE} algorithm AES		
	open wpa2 passphrase {PASSPHRASE} algorithm TKIP			
	open wpa2 passphrase {PASSPHRASE} algorithm AES			
	open wpa2 passphrase {PASSPHRASE} algorithm TKIP			
	open wep-128 key {KEY} key-id {KEY-ID}			
	open wep-128 key {KEY} key-id {KEY-ID} To set the authentication method to 'open', encryption method to 'WEP-128', key index, and WEP key, use the following command: open wep-128 key {key} key-id {key ID}			
Syntax Description	open	Set the authentication method to open		
	wep-128	Set the encryption method to WEP 128-bit		
	key {key}	Set the WEP key to {key}		
	key-id {key ID}	Set the WEP key ID to {key ID}		
Defaults	None.			
Example	ruckus(config)# w	lan randy-wlansvc-01-open		
	The WLAN service ' the WLAN service,	randy-wlansvc-01-open' has been created. To save type end or exit.		

ruckus(config-wlan-randy-wlansvc-01-open)# open wep-128 key 12345678901234567890123456 key-id 1

The command was executed successfully. To save the changes, type 'end' or 'exit'.

Related Commands open none

open wpa passphrase {PASSPHRASE} algorithm AES open wpa2 passphrase {PASSPHRASE} algorithm TKIP open wpa2 passphrase {PASSPHRASE} algorithm AES open wpa2 passphrase {PASSPHRASE} algorithm TKIP open wep-64 key {KEY} key-id {KEY-ID}

mac none auth-server

To set the authentication method to 'MAC Address' and encryption method to 'none', use the following command:

mac none auth-server {auth server}

mac	Set the authentication method to 'MAC Address'	
none	Set the encryption method to 'none'	
auth-server {auth server}	Set the authorization server address to {auth server}	
None.		
<pre>- ruckus(config-wlan-randall-wlansvc-01)# mac none auth-server Ruckus-Auth-01</pre>		
The command was exe 'end' or 'exit'.	ecuted successfully. To save the changes, type	
mac wpa passphrase {P/	ASSPHRASE} algorithm AES auth-server {AUTHSVR-NAME}	
mac wpa passphrase {PASSPHRASE} algorithm TKIP auth-server {AUTHSVR-NAME}		
mac wpa2 passphrase {PASSPHRASE} algorithm AES auth-server {AUTHSVR-NAME}		
mac wpa2 passphrase {PASSPHRASE} algorithm TKIP auth-server {AUTHSVR-NAME}		
mac wep-64 key {KEY} k	ey-id {KEY-ID} auth-server {AUTHSVR-NAME}	
mac wep-128 key {KEY}	key-id {KEY-ID} auth-server {AUTHSVR-NAME}	
	<pre>mac none auth-server {auth server} None. ruckus(config-wlan- Ruckus-Auth-01 The command was exe 'end' or 'exit'. mac wpa passphrase {P/ mac wpa passphrase</pre>	

mac wpa passphrase {PASSPHRASE} algorithm AES auth-server {AUTHSVR-NAME}

To set the authentication method to 'MAC Address', encryption method to 'WPA', and algorithm to 'AES', use the following command:

mac wpa passphrase {passphrase} algorithm AES auth-server
{AUTHSVR-NAME}

mac	Set the authentication method to 'MAC Address'		
wpa	Set the encryption method to 'WPA'		
passphrase {passphrase}	Set the WPA passphrase to {passphrase}		
algorithm AES	Set the encryption algorithm to 'AES'		
auth-server {AUTHSVR-NAME}	Set the authorization server address to ${AUTHSVR-NAME}$		
None.			
ruckus(config-wlan-randall-wlansvc-01)# mac wpa passphrase 12345678 algorithm AES auth-server Ruckus-Auth-01			
The command was ('end' or 'exit'.	executed successfully. To save the changes, type		
mac none auth-server			
mac wpa passphrase {PASSPHRASE} algorithm TKIP auth-server {AUTHSVR-NAME}			
mac wpa2 passphrase {PASSPHRASE} algorithm AES auth-server {AUTHSVR-NAME}			
mac wpa2 passphrase {PASSPHRASE} algorithm TKIP auth-server {AUTHSVR-NAME}			
mac wep-64 key {KE}	/} key-id {KEY-ID} auth-server {AUTHSVR-NAME}		
mac wep-128 key {KE	TY key-id {KEY-ID} auth-server {AUTHSVR-NAME}		
mac wpa passphrase {PASSPHRASE} algorithm TKIP auth- server {AUTHSVR-NAME}			
To set the authentication method to 'MAC Address', encryption method to 'WPA', and algorithm to 'TKIP', use the following command:			
mac wpa passp {AUTHSVR-NAME	whrase {PASSPHRASE} algorithm TKIP auth-server }}		
mac wpa	Set the authentication method to 'MAC Address' and		
	mac wpa passphrase {passphrase} algorithm AES auth-server {AUTHSVR-NAME} None. ruckus(config-wl. 12345678 algorid The command was of 'end' or 'exit'. mac none auth-server mac wpa passphrase mac wpa2 passphrase mac wpa		

	passphrase {passphrase}	Set the WPA passphrase to {passphrase}		
	algorithm TKIP	Set the encryption algorithm to 'TKIP'		
	auth-server {AUTHSVR-NAME}	Set the authorization server address to {AUTHSVR-NAME}		
Defaults	None.			
Example	ruckus(config-wlan-randall-wlansvc-01)# mac wpa passphrase 12345678 algorithm TKIP auth-server Ruckus-Auth-01			
	The command was end 'end' or 'exit'.	xecuted successfully. To save the changes, type		
Related Commands	mac none auth-server			
	mac wpa passphrase {	PASSPHRASE} algorithm AES auth-server {AUTHSVR-NAME}		
	mac wpa2 passphrase {PASSPHRASE} algorithm AES auth-server {AUTHSVR-NAME}			
	mac wpa2 passphrase {PASSPHRASE} algorithm TKIP auth-server {AUTHSVR-NAME}			
	mac wep-64 key {KEY} key-id {KEY-ID} auth-server {AUTHSVR-NAME}			
	mac wep-128 key {KEY} key-id {KEY-ID} auth-server {AUTHSVR-NAME}			
	mac wpa passphrase {PASSPHRASE} algorithm auto auth- server {AUTHSVR-NAME} To set the authentication method to 'MAC Address', encryption method to 'WPA',			
	and algorithm to 'auto', use the following command:			
	mac wpa passphrase {PASSPHRASE} algorithm auto auth-server {AUTHSVR-NAME}			
Syntax Description				
	mac wpa	Set the authentication method to 'MAC Address' and encryption method to 'WPA'		
	passphrase {passphrase}	Set the WPA passphrase to {passphrase}		
	algorithm auto	Set the encryption algorithm automatically		
	auth-server {AUTHSVR-NAME}	Set the authorization server address to {AUTHSVR-NAME}		
Defaults	None.			
Example	ruckus(config-wla 12345678 algorit	n-randall-wlansvc-01)# mac wpa passphrase hm auto auth-server Ruckus-Auth-01		

Configure Syslog Settings Commands

The command was executed successfully. To save the changes, type 'end' or 'exit'.

Related Commands mac none auth-server

mac wpa passphrase {PASSPHRASE} algorithm AES auth-server {AUTHSVR-NAME} mac wpa2 passphrase {PASSPHRASE} algorithm AES auth-server {AUTHSVR-NAME} mac wpa2 passphrase {PASSPHRASE} algorithm TKIP auth-server {AUTHSVR-NAME} mac wep-64 key {KEY} key-id {KEY-ID} auth-server {AUTHSVR-NAME} mac wep-128 key {KEY} key-id {KEY-ID} auth-server {AUTHSVR-NAME}

mac wpa2 passphrase {PASSPHRASE} algorithm AES authserver {AUTHSVR-NAME}

To set the authentication method to 'MAC Address', encryption method to 'WPA2', and algorithm to 'AES', use the following command:

mac wpa2 passphrase {PASSPHRASE} algorithm AES auth-server
{AUTHSVR-NAME}

C			
Syntax Description	mac wpa2	Set the authentication method to 'MAC Address' and encryption method to 'WPA2'	
	passphrase {PASSPHRASE}	Set the WPA2 passphrase to {passphrase}	
	algorithm AES	Set the encryption algorithm to 'AES'	
	auth-server {AUTHSVR-NAME}	Set the authorization server address to {AUTHSVR-NAME}	
Defaults	None.		
Example	ruckus(config-wla 12345678 algorit	an-randall-wlansvc-01)# mac wpa2 passphrase chm AES auth-server Ruckus-Auth-01	
	The command was e 'end' or 'exit'.	executed successfully. To save the changes, type	
Related Commands	mac none auth-serve	<u>r</u>	
	<u>mac wpa passphrase</u>	{PASSPHRASE} algorithm AES auth-server {AUTHSVR-NAME}	
	mac wpa passphrase {PASSPHRASE} algorithm TKIP auth-server {AUTHSVR-NAME}		
	mac wpa2 passphrase {PASSPHRASE} algorithm TKIP auth-server {AUTHSVR-NAME}		
	mac wep-64 key {KEY} key-id {KEY-ID} auth-server {AUTHSVR-NAME}		
	mac wep-128 key {KE	Y} kev-id {KEY-ID} auth-server {AUTHSVR-NAME}	

mac wpa2 passphrase {PASSPHRASE} algorithm TKIP authserver {AUTHSVR-NAME}

To set the authentication method to 'MAC Address', encryption method to 'WPA2', and algorithm to 'TKIP', use the following command:

mac wpa2 passphrase {PASSPHRASE} algorithm TKIP auth-server
{AUTHSVR-NAME}

Sumton Description	<u> </u>		
Syntax Description	mac wpa2	Set the authentication method to 'MAC Address' and encryption method to 'WPA2'	
	passphrase {PASSPHRASE}	Set the WPA2 passphrase to {passphrase}	
	algorithm TKIP	Set the encryption algorithm to 'TKIP'	
	auth-server {AUTHSVR-NAME}	Set the authorization server address to {AUTHSVR-NAME}	
Defaults	None.		
Example	ruckus(config-wla 12345678 algorit	an-randall-wlansvc-01)# mac wpa2 passphrase Chm TKIP auth-server Ruckus-Auth-01	
	The command was e 'end' or 'exit'.	executed successfully. To save the changes, type	
Related Commands	mac none auth-server	<u>_</u>	
	mac wpa passphrase {PASSPHRASE} algorithm AES auth-server {AUTHSVR-NAME}		
	mac wpa passphrase {PASSPHRASE} algorithm TKIP auth-server {AUTHSVR-NAME}		
	mac wpa2 passphrase	e {PASSPHRASE} algorithm AES auth-server {AUTHSVR-NAME}	
	mac wep-64 key {KEY	} key-id {KEY-ID} auth-server {AUTHSVR-NAME}	
	mac wep-128 key {KE	Y} key-id {KEY-ID} auth-server {AUTHSVR-NAME}	
	mac wpa2 passphrase {PASSPHRASE} algorithm auto auth- server {AUTHSVR-NAME}		
	To set the authenticat and algorithm to 'aut	tion method to 'MAC Address', encryption method to 'WPA2', o', use the following command:	
	mac wpa2 pass {AUTHSVR-NAME	phrase {PASSPHRASE} algorithm auto auth-server }	
Syntax Description	-		
-	mac wpa2	encryption method to 'WPA2'	

	passphrase {PASSPHRASE}	Set the WPA2 passphrase to {passphrase}	
	algorithm auto	Set the encryption algorithm automatically	
	auth-server {AUTHSVR-NAME}	Set the authorization server address to {AUTHSVR-NAME}	
Defaults	None.		
Example	ruckus(config-wla 12345678 algorit The command was e 'end' or 'exit'.	n-randall-wlansvc-01)# mac wpa2 passphrase hm auto auth-server Ruckus-Auth-01 xecuted successfully. To save the changes, type	
Related Commands	mac none auth-server		
	mac wpa passphrase	[PASSPHRASE] algorithm AES auth-server {AUTHSVR-NAME}	
	mac wpa passphrase	[PASSPHRASE] algorithm TKIP auth-server {AUTHSVR-NAME}	
	mac wpa2 passphrase {PASSPHRASE} algorithm AES auth-server {AUTHSVR-NAME}		
	mac wep-64 key {KEY} key-id {KEY-ID} auth-server {AUTHSVR-NAME}		
	mac wpa-mixed auth-server {AUT To set the authenticat Mixed', and algorithm	Dassphrase {PASSPHRASE} algorithm AES HSVR-NAME} ion method to 'MAC Address', encryption method to 'WPA- n to 'AES', use the following command:	
	mac wpa-mixed passphrase {PASSPHRASE} algorithm AES auth-server {AUTHSVR-NAME}		
Syntax Description	mac wpa-mixed	Set the authentication method to 'MAC Address' and encryption method to 'WPA-Mixed'	
	passphrase {PASSPHRASE}	Set the WPA2 passphrase to {passphrase}	
	algorithm AES	Set the encryption algorithm to 'AES'	
	auth-server {AUTHSVR-NAME}	Set the authorization server address to {AUTHSVR-NAME}	
Defaults	None.		
Example	ruckus(config-wla 12345678 algorit	n-randall-wlansvc-01)# mac wpa-mixed passphrase hm AES auth-server Ruckus-Auth-01	

The command was executed successfully. To save the changes, type <code>'end'</code> or <code>'exit'</code>.

Related Commands <u>mac none auth-server</u>

mac wpa-mixed passphrase {PASSPHRASE} algorithm TKIP auth-server {AUTHSVR-NAME}

mac wpa-mixed passphrase {PASSPHRASE} algorithm auto auth-server {AUTHSVR-NAME}

mac wpa-mixed passphrase {PASSPHRASE} algorithm TKIP auth-server {AUTHSVR-NAME}

To set the authentication method to 'MAC Address', encryption method to 'WPA-Mixed', and algorithm to 'TKIP', use the following command:

mac wpa-mixed passphrase {PASSPHRASE} algorithm TKIP auth-server
{AUTHSVR-NAME}

Suntax Description		
Syntax Description	mac wpa-mixed	Set the authentication method to 'MAC Address' and encryption method to 'WPA-Mixed'
	passphrase {PASSPHRASE}	Set the WPA2 passphrase to {passphrase}
	algorithm TKIP	Set the encryption algorithm to 'TKIP'
	auth-server {AUTHSVR-NAME}	Set the authorization server address to {AUTHSVR-NAME}
Defaults	None.	
Example	ruckus(config-wla 12345678 algorit	n-randall-wlansvc-01)# mac wpa-mixed passphrase hm TKIP auth-server Ruckus-Auth-01
	The command was e 'end' or 'exit'.	executed successfully. To save the changes, type
Related Commands	mac none auth-server	-
	mac wpa-mixed pass NAME}	ohrase {PASSPHRASE} algorithm AES auth-server {AUTHSVR-
	mac wpa-mixed pass NAME}	ohrase {PASSPHRASE} algorithm auto auth-server {AUTHSVR-

mac wpa-mixed passphrase {PASSPHRASE} algorithm auto auth-server {AUTHSVR-NAME}

To set the authentication method to 'MAC Address', encryption method to 'WPA-Mixed', and algorithm to 'auto', use the following command:

mac wpa-mixed passphrase {PASSPHRASE} algorithm auto auth-server
{AUTHSVR-NAME}

	-		
Syntax Description	mac wpa-mixed	Set the authentication method to 'MAC Address' and encryption method to 'WPA-mixed'	
	passphrase {PASSPHRASE}	Set the WPA2 passphrase to {passphrase}	
	algorithm auto	Set the encryption algorithm automatically	
	auth-server {AUTHSVR-NAME}	Set the authorization server address to {AUTHSVR-NAME}	
Defaults	None.		
Example	- ruckus(config-wlan-randall-wlansvc-01)# mac wpa-mixed passphrase 12345678 algorithm auto auth-server Ruckus-Auth-01		
	The command was e 'end' or 'exit'.	xecuted successfully. To save the changes, type	
Related Commands	mac none auth-server		
	mac wpa-mixed passphrase {PASSPHRASE} algorithm AES auth-server {AUTHSVR-		
	NAME}		
	mac wpa-mixed passp NAME}	hrase {PASSPHRASE} algorithm TKIP auth-server {AUTHSVR-	
	mac wep-64 key NAME}	{KEY} key-id {KEY-ID} auth-server {AUTHSVR-	
	To set the authentication method to 'MAC Address', encryption method to 'WEP-64', key index, and WEP key, use the following command:		
	mac wep-64 key	<pre>{KEY} key-id {KEY-ID} auth-server {AUTHSVR-NAME}</pre>	
Suntax Description			
Syntax Description	mac	Set the authentication method to MAC address	
	wep-64	Set the encryption method to WEP 64-bit	
	key {KEY}	Set the WEP key to {KEY}	
	key-id {KEY-ID}	Set the WEP key ID to {KEY-ID}	

auth-server	Set the authorization server address to {AUTHSVR-NAME}
{AUTHSVR-NAME}	

Defaults	None.		
Example	ruckus(config-wla 15791BD8F2 key-id	n-randy-wlansvc-01-wpa2)# mac wep-64 key 1 2 auth-server Ruckus-Auth-01	
	The command was ex 'end' or 'exit'.	xecuted successfully. To save the changes, type	
Related Commands	mac none auth-server		
	mac wpa passphrase {PASSPHRASE} algorithm AES auth-server {AUTHSVR-NAME}		
	mac wpa passphrase {PASSPHRASE} algorithm TKIP auth-server {AUTHSVR-NAME}		
	mac wpa2 passphrase	{PASSPHRASE} algorithm AES auth-server {AUTHSVR-NAME}	
	mac wpa2 passphrase	{PASSPHRASE} algorithm TKIP auth-server {AUTHSVR-NAME}	
	mac wep-128 key (KE)	() key-id {KEY-ID} auth-server {ALITHSVR-NAME}	
	<u></u>	,,	
	mac wep-128 key	{KEY} key-id {KEY-ID} auth-server {AUTHSVR-	
	To set the authentication	on method to 'MAC Address', encryption method to 'WEP-128',	
	key index, and WEP key, use the following command:		
	mac wep-128 key	<pre>{ {KEY} key-id {KEY-ID} auth-server {AUTHSVR-NAME}</pre>	
	-		
Syntax Description	mac	Set the authentication method to MAC address	
	wep-128	Set the encryption method to WEP 128-bit	
	key {KEY}	Set the WEP key to {key}	
	key-id {KEY-ID}	Set the WEP key ID to {key ID}	
	auth-server {AUTHSVR-NAME}	Set the authorization server address to {AUTHSVR-NAME}	
Defaults	None.		
	_		
Example	ruckus(config-wlan 15715791BD8F21234	n-randy-wlansvc-01-wpa2)# mac wep-128 key 45691BD8F2 key-id 2 auth-server Ruckus-Auth-01	
	The command was e: 'end' or 'exit'.	xecuted successfully. To save the changes, type	
Related Commands			

Configure Syslog Settings Commands

mac wpa passphrase {PASSPHRASE} algorithm AES auth-server {AUTHSVR-NAME} mac wpa passphrase {PASSPHRASE} algorithm TKIP auth-server {AUTHSVR-NAME} mac wpa2 passphrase {PASSPHRASE} algorithm AES auth-server {AUTHSVR-NAME} mac wpa2 passphrase {PASSPHRASE} algorithm TKIP auth-server {AUTHSVR-NAME} mac wep-64 key {KEY} key-id {KEY-ID} auth-server {AUTHSVR-NAME}

shared wep-64 key {KEY} key-id {KEY-ID}

To set the authentication method to 'Shared', encryption method to 'WEP-64', key index, and WEP key, use the following command:

shared wep-64 key {KEY} key-id {KEY-ID}

	-		
Syntax Description	shared	Set the authentication method to 'Shared'	
	wep-64	Set the encryption method to WEP 64-bit	
	key {KEY}	Set the WEP key to {key}	
	key-id {KEY-ID}	Set the WEP key ID to {KEY-ID}	
Defaults	None.		
Example	ruckus(config-wla The command was e 'end' or 'exit'.	n)# shared wep-64 key 15791BD8F2 key-id 2 xecuted successfully. To save the changes, type	
Related Commands	shared wep-128 key {KEY} key-id {KEY-ID}		
	<pre>shared wep-128 key {KEY} key-id {KEY-ID} To set the authentication method to 'Shared', encryption method to 'WEP-128', key index, and WEP key, use the following command: shared wep-128 key {KEY} key-id {KEY-ID}</pre>		
Contro Decemention			
Syntax Description	shared	Set the authentication method to 'Shared'	
	wep-128	Set the encryption method to WEP 128-bit	
	key {KEY}	Set the WEP key to {key}	
	key-id {KEY-ID}	Set the WEP key ID to {KEY-ID}	
Defaults	None.		

The command was executed successfully. To save the change 'end' or 'exit'. Related Commands shared wep-64 key (KEY) key-id (KEY-ID) dot1x wpa algorithm AES auth-server {AUTHSVR-NAME} To set the authentication method to '802.1x EAP', encryption method to ''algorithm to 'AES', use the following command: dot1x wpa algorithm AES auth-server {AUTHSVR-NAME} Syntax Description dot1x Set the authentication method to '802.11x' wpa Set the encryption method to WPA algorithm AES Set the algorithm to AES auth-server Set the auth server to {AUTHSVR-NAME} None. Defaults None. Example ruckus (config-wlan-wlansvc-012)# dot1x wpa algorithm AES server Ruckus-Auth-01 The command was executed successfully. To save the change	s, type NPA', and		
Related Commands shared wep-64 key {KEY} key-id {KEY-ID} dot1x wpa algorithm AES auth-server {AUTHSVR-NAME} To set the authentication method to '802.1x EAP', encryption method to 'algorithm to 'AES', use the following command: dot1x wpa algorithm AES auth-server {AUTHSVR-NAME} Syntax Description dot1x Set the authentication method to '802.11x' wpa Set the authentication method to '802.11x' wpa Set the encryption method to '802.11x' wpa Set the authentication method to '802.11x' wpa Set the encryption method to WPA algorithm AES Set the algorithm to AES auth-server (AUTHSVR-NAME} Set the auth server to {AUTHSVR-NAME} Defaults None. Example ruckus (config-wlan-wlansvc-012) # dot1x wpa algorithm AES server Ruckus-Auth-01 The command was executed successfully. To save the change	NPA', and		
dot1x wpa algorithm AES auth-server {AUTHSVR-NAME} To set the authentication method to '802.1x EAP', encryption method to 'algorithm to 'AES', use the following command: dot1x wpa algorithm AES auth-server {AUTHSVR-NAME} Syntax Description dot1x Set the authentication method to '802.11x' wpa Set the encryption method to '802.11x' wpa algorithm AES Set the algorithm to AES auth-server (AUTHSVR-NAME) Defaults None. Example ruckus(config-wlan-wlansvc-012)# dot1x wpa algorithm AES server Ruckus-Auth-01 The command was executed successfully. To save the change	WPA', and		
dot1x wpa algorithm AES auth-server {AUTHSVR-NAME} Syntax Description dot1x Set the authentication method to '802.11x' wpa Set the encryption method to WPA algorithm AES Set the algorithm to AES auth-server Set the auth server to {AUTHSVR-NAME} Defaults None. Example ruckus(config-wlan-wlansvc-012)# dot1x wpa algorithm AES server Ruckus-Auth-01 The command was executed successfully. To save the change			
Syntax Description dot1x Set the authentication method to '802.11x' wpa Set the encryption method to WPA algorithm AES Set the algorithm to AES auth-server Set the auth server to {AUTHSVR-NAME} Defaults None. Example ruckus(config-wlan-wlansvc-012)# dot1x wpa algorithm AES server Ruckus-Auth-01 The command was executed successfully. To save the change			
wpa Set the addictined to the definition of the definiti			
algorithm AES Set the algorithm to AES auth-server Set the auth server to {AUTHSVR-NAME} Defaults None. Example ruckus(config-wlan-wlansvc-012)# dot1x wpa algorithm AES server Ruckus-Auth-01 The command was executed successfully. To save the change			
auth-server Set the auth server to {AUTHSVR-NAME} Defaults None. Example ruckus(config-wlan-wlansvc-012)# dot1x wpa algorithm AES server Ruckus-Auth-01 The command was executed successfully. To save the change			
Defaults None. Example ruckus(config-wlan-wlansvc-012)# dot1x wpa algorithm AES server Ruckus-Auth-01 The command was executed successfully. To save the change			
Example ruckus(config-wlan-wlansvc-012)# dot1x wpa algorithm AES server Ruckus-Auth-01 The command was executed successfully. To save the change			
The command was executed successfully. To save the change	ruckus(config-wlan-wlansvc-012)# dot1x wpa algorithm AES auth- server Ruckus-Auth-01		
'end' or 'exit'.	s, type		
Related Commands dot1x wpa algorithm TKIP auth-server {AUTHSVR-NAME}			
<pre>dot1x wpa2 algorithm AES auth-server {AUTHSVR-NAME}</pre>			
<pre>dot1x wpa2 algorithm TKIP auth-server {AUTHSVR-NAME}</pre>	dot1x wpa2 algorithm TKIP auth-server {AUTHSVR-NAME}		
<pre>dot1x wep-64 auth-server {AUTHSVR-NAME}</pre>	dot1x wep-64 auth-server {AUTHSVR-NAME}		
<pre>dot1x wep-128 auth-server {AUTHSVR-NAME}</pre>	dot1x wep-128 auth-server {AUTHSVR-NAME}		
dot1x wpa algorithm TKIP auth-server {AUTHSVR-NAME To set the authentication method to '802.1x EAP', encryption method to '' algorithm to 'TKIP', use the following command:	dot1x wpa algorithm TKIP auth-server {AUTHSVR-NAME} To set the authentication method to '802.1x EAP', encryption method to 'WPA', and algorithm to 'TKIP', use the following command:		
dot1x wpa algorithm TKIP auth-server {AUTHSVR-NAME}			
Syntax Description dot1x Set the authentication method to '802.11x'			
wpa Set the encryption method to WPA			

	algorithm TKIP	Set the algorithm to TKIP	
	auth-server {AUTHSVR-NAME}	Set the auth server to {AUTHSVR-NAME}	
Defaults	None.		
Example	ruckus(config-wla server Ruckus-Au	n-wlansvc-012)# dot1x wpa algorithm TKIP auth- th-01	
	'end' or 'exit'.	Accured Successfully. To save the changes, type	
Related Commands	dot1x wpa algorithm ,	AES auth-server {AUTHSVR-NAME}	
	dot1x wpa2 algorithm	AES auth-server (AUTHSVR-NAME)	
	<u>dot1x wpa2 algorithm</u>	TKIP auth-server {AUTHSVR-NAME}	
	<u>dot1x wep-64 auth-se</u>	rver {AUTHSVR-NAME}	
	dot1x wep-128 auth-server {AUTHSVR-NAME}		
Syntax Description		Set the authentication method to '902 11v'	
	WDa	Set the appropriate method to WPA	
	algorithm auto	Set the algorithm automatically	
	auth-server {AUTHSVR-NAME}	Set the auth server to {AUTHSVR-NAME}	
Defaults	None.		
Example	- ruckus(config-wla server Ruckus-Au	n-wlansvc-012)# dot1x wpa algorithm auto auth- th-01	
	The command was e 'end' or 'exit'.	xecuted successfully. To save the changes, type	
Related Commands	dot1x wpa algorithm ,	AES auth-server {AUTHSVR-NAME}	
	dot1x wpa2 algorithm AES auth-server {AUTHSVR-NAME}		
	<pre>dot1x wpa2 algorithm TKIP auth-server {AUTHSVR-NAME}</pre>		

dot1x wep-64 auth-server {AUTHSVR-NAME}
dot1x wep-128 auth-server {AUTHSVR-NAME}

dot1x wpa2 algorithm AES auth-server {AUTHSVR-NAME}

To set the authentication method to '802.1x EAP', encryption method to 'WPA2', and algorithm to 'AES', use the following command:

dot1x wpa2 algorithm AES auth-server {AUTHSVR-NAME}

dot1x	Set the authentication method to '802.11x'	
wpa2	Set the encryption method to WPA2	
algorithm AES	Set the algorithm to AES	
auth-server {AUTHSVR-NAME}	Set the auth server to {AUTHSVR-NAME}	
None.		
ruckus(config-wla AES auth-server	n-randy-wlansvc-01-open)# dot1x wpa2 algorithm Ruckus-RADIUS	
The command was e 'end' or 'exit'.	xecuted successfully. To save the changes, type	
<pre>dot1x wpa algorithm TKIP auth-server {AUTHSVR-NAME}</pre>		
dot1x wpa2 algorithm TKIP auth-server {AUTHSVR-NAME}		
dot1x wep-64 auth-server {AUTHSVR-NAME}		
dot1x wep-128 auth-server {AUTHSVR-NAME}		
dot1x wpa2 algorithm TKIP auth-server {AUTHSVR-NAME}		
To set the authentication method to '802.1x EAP', encryption method to 'WPA2', and algorithm to 'TKIP', use the following command:		
<pre>dot1x wpa2 algorithm TKIP auth-server {AUTHSVR-NAME}</pre>		
dot1x	Set the authentication method to '802.11x'	
wpa2	Set the encryption method to WPA2	
algorithm TKIP	Set the algorithm to TKIP	
auth-server	Set the auth server to {AUTHSVR-NAME}	
	dot1x wpa2 algorithm AES auth-server {AUTHSVR-NAME} None. ruckus(config-wla AES auth-server The command was e 'end' or 'exit'. dot1x wpa algorithm dot1x wpa algorithm dot1x wpa2 algorithm dot1x wep-64 auth-se dot1x wep-128 auth-se dot1x wpa2 algorithm to 'TKIP', us dot1x wpa2 algorithm dot1x wpa2 algorithm dot1x wpa2 algorithm dot1x wpa2 algorithm dot1x wpa2 algorithm dot1x wpa2 algorithm to 'TKIP', us dot1x wpa2 algorithm to 'TKIP', us dot1x mpa2 algorithm to 'TKIP', us	

Defaults	None.	
Example	ruckus(config-wlan-wlansvc-012)# dot1x wpa2 algorithm TKIP auth- server Ruckus-Auth-01	
	The command was end 'end' or 'exit'.	xecuted successfully. To save the changes, type
Related Commands	dot1x wpa algorithm AES auth-server {AUTHSVR-NAME}	
	dot1x wpa algorithm TKIP auth-server {AUTHSVR-NAME}	
	dot1x wpa2 algorithm AES auth-server {AUTHSVR-NAME}	
	<pre>dot1x wep-64 auth-server {AUTHSVR-NAME}</pre>	
	<pre>dot1x wep-128 auth-server {AUTHSVR-NAME}</pre>	
	dot1x wpa2 algo To set the authenticati algorithm to 'auto', us dot1x wpa2 alg	rithm auto auth-server {AUTHSVR-NAME} on method to '802.1x EAP', encryption method to 'WPA2', and e the following command: gorithm auto auth-server {AUTHSVR-NAME}
Syntax Description	dot1x	Set the authentication method to '802.11x'
	wpa2	Set the encryption method to WPA2
	algorithm auto	Set the algorithm automatically
	auth-server {AUTHSVR-NAME}	Set the auth server to {AUTHSVR-NAME}
Defaults	None.	
Example	ruckus(config-wlan-wlansvc-012)# dot1x wpa2 algorithm auto auth- server Ruckus-Auth-01	
	The command was executed successfully. To save the changes, type 'end' or 'exit'.	
Related Commands	dot1x wpa algorithm AES auth-server {AUTHSVR-NAME}	
	dot1x wpa algorithm TKIP auth-server {AUTHSVR-NAME}	
	dot1x wpa2 algorithm AES auth-server {AUTHSVR-NAME}	
	dot1x wep-64 auth-server {AUTHSVR-NAME}	
	<pre>dot1x wep-128 auth-server {AUTHSVR-NAME}</pre>	
dot1x wpa-mixed algorithm AES auth-server {AUTHSVR-NAME}

To set the authentication method to '802.1x EAP', encryption method to 'WPA-Mixed', and algorithm to 'AES', use the following command:

dot1x wpa-mixed algorithm AES auth-server {AUTHSVR-NAME}

<u> </u>	-		
Syntax Description	dot1x	Set the authentication method to '802.11x'	
	wpa-mixed	Set the encryption method to WPA-Mixed	
	algorithm AES	Set the algorithm to AES	
	auth-server {AUTHSVR-NAME}	Set the auth server to {AUTHSVR-NAME}	
Defaults	None.		
Example	ruckus(config-wla rithm AES auth-s	un-randy-wlansvc-01-open)# dot1x wpa-mixed algo- erver Ruckus-RADIUS	
	The command was e		
Related Commands	dot1x wpa-mixed algo	orithm TKIP auth-server {AUTHSVR-NAME}	
	dot1x wpa-mixed algorithm auto auth-server {AUTHSVR-NAME}		
	To set the authenticati and algorithm to 'TKII dot1x wpa-mixe	on method to '802.1x EAP', encryption method to 'WPA-Mixed', P', use the following command: ed algorithm TKIP auth-server {AUTHSVR-NAME}	
Syntax Description	dot1x	Set the authentication method to '802.11x'	
	wpa-mixed	Set the encryption method to WPA2	
	algorithm TKIP	Set the algorithm to TKIP	
	auth-server {AUTHSVR-NAME}	Set the auth server to {AUTHSVR-NAME}	
Defaults	None.		
Example	ruckus(config-wla auth-server Ruck	n-wlansvc-012)# dot1x wpa-mixed algorithm TKIP ru s-Auth-01	
	The command was e 'end' or 'exit'.	executed successfully. To save the changes, type	

Configure Syslog Settings Commands

Related Commands <u>dot1x wpa-mixed algorithm AES auth-server {AUTHSVR-NAME}</u> dot1x wpa-mixed algorithm auto auth-server {AUTHSVR-NAME}

dot1x wpa-mixed algorithm auto auth-server {AUTHSVR-NAME}

To set the authentication method to '802.1x EAP', encryption method to 'WPA-Mixed', and algorithm to 'auto', use the following command:

dot1x wpa-mixed algorithm auto auth-server {AUTHSVR-NAME}

Syntax Description	dot1x	Set the authentication method to '802.11x'	
	wpa-mixed	Set the encryption method to WPA2	
	algorithm auto	Set the algorithm automatically	
	auth-server {AUTHSVR-NAME}	Set the auth server to {AUTHSVR-NAME}	
Defaults	None.		
Example	- ruckus(config-wlan-wlansvc-012)# dot1x wpa-mixed algorithm auto auth-server Ruckus-Auth-01		
	The command was exe 'end' or 'exit'.	ecuted successfully. To save the changes, type	
Related Commands			
	dot1x wpa-mixed algorithm TKIP auth-server {AUTHSVR-NAME}		
	dot1x wep-64 autl To set the authenticatio key index, and WEP key dot1x wep-64 au	h-server {AUTHSVR-NAME} n method to '802.1x EAP', encryption method to 'WEP-64', , use the following command: .th-server {AUTHSVR-NAME} {auth server}	
Syntax Description	dot1x	Set the authentication method to '802.11x'	
	wep-64	Set the encryption method to WEP 64-bit	
	<pre>auth-server {auth server}</pre>	Set the auth server to {auth server}	
Defaults	None.		

Example	ruckus(config-wlan-wlansvc-012)# dot1x wep-64 auth-server { AUTHSVR-NAME} Ruckus-Auth-01		
	The command was executed successfully. To save the changes, type 'end' or 'exit'.		
Related Commands	dot1x wpa algorithm AES auth-server {AUTHSVR-NAME}		
	<u>dot1x wpa algorithm TKIP auth-server {AUTHSVR-NAME}</u> dot1x wpa2 algorithm AES auth-server {AUTHSVR-NAME}		
	dot1x wpa2 algorithm TKIP auth-server {AUTHSVR-NAME}		
	dot1x wep-128 auth-server {AUTHSVR-NAME}		
	dot1x wep-128 auth-server {AUTHSVR-NAME} To set the authentication method to '802.1x EAP', encryption method to 'WEP-128', key index, and WEP key, use the following command: dot1x wep-128 auth-server {AUTHSVR-NAME}		
Syntax Description	dot.1x Set the authentication method to '802.11x'		
	wep-128 Set the encryption method to WEP 128-bit		
	auth-server {auth Set the auth server to {auth server} server}		
Defaults	- None.		
Example	- ruckus(config-wlan-wlansvc-012)# dot1x wep-128 auth-server {AUTHSVR-NAME} Ruckus-Auth-01		
	The command was executed successfully. To save the changes, type 'end' or 'exit'.		
Related Commands			
	dot1x wpa algorithm TKIP auth-server {AUTHSVR-NAME}		
	dot1x wpa2 algorithm AES auth-server {AUTHSVR-NAME}		
	dot1x wpa2 algorithm TKIP auth-server {AUTHSVR-NAME}		
	dot1x wep-64 auth-server {AUTHSVR-NAME}		
	client-isolation local		
	To prevent wireless clients that are associated with the same AP from communicating with each other, enable <i>local</i> client isolation using the following command: client-isolation local		

Configure Syslog Settings Commands

Syntax Description	- 		
Syntax Description	client-isolation	Enable client isolation	
	local	Prevent clients that are associated with the same AP from communicating with each other. These clients will be able to communicate with other clients that are associated with another AP.	
Defaults	None.		
Example	ruckus(config-wlan	-randy-wlansvc-01-open)# client-isolation	
	The command was ex 'end' or 'exit'.	ecuted successfully. To save the changes, type	
Related Commands	no client-isolation		
	client-isolation local		
	client-isolation full		
	To completely prevent with they are associated with using the following con client-isolatic	• vireless clients from communicating with other clients (whether h the same AP or with another AP), enable <i>full</i> client isolation nmand: on full	
Syntax Description	client-isolation	Enable client isolation	
	full	Prevent clients from communicating with other clients (regardless whether they are associated with the same AP or a different AP).	
Defaults	None.		
Example	ruckus(config-wlan The command was ex 'end' or 'exit'.	-randy-wlansvc-01-open)# client-isolation full ecuted successfully. To save the changes, type	
Related Commands	no client-isolation		
	client-isolation local		

no client-isolation

To disable wireless client isolation, use the following command:

no client-isolation

Suntax Description	-		
Syntax Description	no client-isolation Disable client isolation		
Defaults	None.		
Example	ruckus# config		
	ruckus(config_wlan_wlan_123) # no glient_isolation		
	The command was executed successfully. To save the changes, type 'end' or 'exit'.		
Related Commands	client-isolation local		
	client-isolation full		
	no web-auth To disable Web authentication, use the following command: no web-auth		
Syntax Description	no web-auth Disable Web authentication		
Defaults	None.		
Example	ruckus# config		
	ruckus(config)# wlan wlan-123		
	<pre>ruckus(config-wlan-wlan-123)# no web-auth</pre>		
	The command was executed successfully. To save the changes, type 'end' or 'exit'.		
Related Commands	web authentication		
	no acct-server		
	To disable the AAA server, use the following command:		
	no acct-server		

Configure Syslog Settings Commands

Syntax Description			
Syntax Description	no acct-server Disable AAA server authentication		
Defaults	None.		
Example	ruckus# config		
	ruckus(config)# wlan wlan-123		
	<pre>ruckus(config-wlan-wlan-123)# no acct-server</pre>		
	The command was executed successfully. To save the changes, type 'end' or 'exit'.		
Related Commands	acct-server		
	acct-server interim-update		
	no vlan		
	To disable the management VLAN, use the following command:		
	no vlan		
Syntax Description	no. vlan Disable the management VI AN		
Defaults	None.		
Example	ruckus# config		
	ruckus(config)# wlan wlan-123		
	ruckus(config-wlan-wlan-123)# no vlan		
	The command was executed successfully. To save the changes, type 'end' or 'exit'.		
Related Commands	- vlan		
	wian vian override none		
	wan vlan override untag		
	wan vlan override tag		
	no tunnel-mode		
	To disable the tunnel mode, use the following command:		
	no tunnel-mode		
Syntax Description	no_tunnel_modeDisable the tunnel mode		

Defaults	None.		
Example	<pre>ruckus# config ruckus(config)# wlan wlan-123 ruckus(config-wlan-wlan-123)# no tunnel-mode The command was executed successfully. To save the changes, type 'end' or 'exit'.</pre>		
Related Commands	<u>tunnel-mode</u>		
	no l2 access control To disable the L2 ACL, use the following command: no l2 access control		
Syntax Description	no 12 access Disable L2 access control		
Defaults	None.		
Example	<pre>ruckus# config ruckus(config)# wlan wlan-123 ruckus(config-wlan-wlan-123)# no l2 access control The command was executed successfully. To save the changes, type 'end' or 'exit'.</pre>		
Related Commands	no I3 access control acl I2 {L2ACL-NAME} acl I3 {L2ACL-NAME} no I3 access control To disable the L3/L4/IP ACL, use the following command:		
Syntax Description	no 13 access control no 13 access Disable L3 access control		
Defaults	None.		

Configure Syslog Settings Commands

	<u>.</u>					
Example	ruckus# config ruckus(config)# wlan wlan-123					
	ruckus(config-wla	n-wlan-123)# no 13 access control				
	The command was e 'end' or 'exit'.	xecuted successfully. To save the changes, type				
Related Commands	no l2 access control					
	acl I2 {L2ACL-NAME}					
	acl 13 {L2ACL-NAME} web authentication To enable Web authentication, use the following command: web-auth {AUTHSVR-NAME}					
				Svntax Description	- 	
				· · · · · · · · · · · · · · · · · · ·	web-auth	Enable Web authentication
					{AUTHSVR-NAME}	The AAA server to use for Web authentication
Defaults	None.					
Example	ruckus # config					

ruckus(config)# wlan wlan-123 ruckus(config-wlan-wlan-123)# web authentication Ruckus-RADIUS The command was executed successfully. To save the changes, type rtekus@eonexgtwlan-wlan-123)# ruckus(config-wlan-wlan-123)#

Rolatod Commande no web-auth **Related Commands**

-

_

. .

no web-auth

acct-server

ASSET SREVIN server, use the following command: To set the AAA server we the following command:

acct-server {AAA server}

Syntax Description		
Syntax Description	acce perver	
Syntax Description	{AAA server}	Configure the AAA server Set the AAA server to this address
	{AAA server}	Set the AAA server to this address
Defaulte	None	
Defaults	None.	
Framnla	ruckus# config	
Example		

	ruckus(config)#	wlan wlan-123
	ruckus(config-v	vlan-wlan-123)# acct-server Ruckus-Acct-01
	The command was 'end' or 'exit'	s executed successfully. To save the changes, type
Related Commands	no acct-server	
	acct-server interim	-update
	acct-server inte	erim-update
	To configure the in following comman	terim update frequency (in minutes) of the AAA server, use the d:
	acct-server	{AAA name} interim-update {minutes}
Syntax Description	acct-server {A name}	AA Configure the interim update frequency of the AAA server
	<pre>interim-update {minutes}</pre>	Set the update frequency to this value (in minutes)
Defaults	5 (minutes)	
Example	ruckus# config ruckus(config)# ruckus(config-w update 5 The command was 'end' or 'exit.'	<pre># wlan wlan-123 vlan-wlan-123)# acct-server Ruckus-Acct-01 intrim- s executed successfully. To save the changes, type '.</pre>
Related Commands	no acct-server	
	vlan To enable the man vlan {VLAN	agement VLAN and set the VLAN ID, use the following command: ID}
Syntax Description	vlan	Enable management VLAN
	{VLAN ID}	Set the VLAN ID to this value
Defaults	None.	

Configure Syslog Settings Commands

Example	ruckus# config ruckus(config)# wlan wlan-123		
	ruckus(config-wlan-wlan-123)# vlan 12		
	The command was executed successfully. To save the changes, type 'end' or 'exit'.		
Related Commands	vlan		
	<u>no vlan</u>		
	hide-ssid		
	To hide an SSID from wireless users, use the following command. Wireless users who know the SSID will still be able to connect to the WLAN service. hide-ssid		
Syntax Description	hide-ssid Hide SSID from wireless users		
Defaults	None.		
Example	ruckus# config ruckus(config)# wlan wlan-123 ruckus(config-wlan-wlan-123)# hide-ssid The command was executed successfully. To save the changes, type 'end' or 'exit'.		
Related Commands	no hide-ssid		
	no hide-ssid To unhide or broadcast an SSID to wireless users, use the following command: no hide-ssid		
Syntax Description	no hide-ssid Broadcast SSID to wireless users		
Defaults	None.		
Example	ruckus# config ruckus(config)# wlan wlan-123 ruckus(config-wlan-wlan-123)# no hide-ssid		

The command was executed successfully. To save the changes, type 'end' or 'exit'.

Related Commands hide-ssid

tunnel-mode

To enable tunnel mode, use the following command:

tunnel-mode

Syntax Description		
Syntax Description	tunnel-mode	Enable tunnel mode
Defaults	None.	
Example	- ruckus# config ruckus(config)# wlan wlan-123 ruckus(config-wlan-wlan-123)# tunnel-mode	
	The command was 'end' or 'exit'.	executed successfully. To save the changes, type
Related Commands	no tunnel-mode	
	max-clients {NU To set the maximum command: max-clients	IMBER} In number of clients for a specific WLAN, use the following {NUMBER}
Syntax Description	max-clients	Configure the maximum number of clients that the WLAN can support
	{NUMBER}	Set the maximum clients to this value
Defaults	None.	
Example	To set the maximum ruckus# config ruckus(config)# ruckus(config-w] The command was 'end' or 'exit'.	wlan wlan-123 Ian-wlan-123)# max-clients 50 executed successfully. To save the changes, type

Configure Syslog Settings Commands

Related Commands <u>no client-isolation</u>

acl I2 {L2ACL-NAME}

To configure the L2 ACL, use the following command:

acl 12 {L2ACL-NAME}

Syntax Description	-		
Syntax Description	acl 12	Configure the L2 ACL	
	{L2ACL-NAME}	The name of the L2 ACL that you want to configure	
Defaults	None.		
Example	ruckus# config ruckus(config)#	wlan wlan-123	
	ruckus(config-wl	an-wlan-123)# acl 12 L2-ACL-name	
	The command was 'end' or 'exit'.	executed successfully. To save the changes, type	
Related Commands	no 12 access control		
	no I3 access control		
	acl 3 {L2ACL-NAME}		
	acl I3 {L2ACL-NAME}		
	To configure the L3/L4/IP ACL, use the following command:		
	acl 13 {L2ACI	L-NAME }	
Syntax Description		Configure the 13 ACI	
	{L2ACL-NAME}	The name of the L3 ACL that you want to configure	
Defaults	None.		
Example	- ruckus# config		
•	- ruckus(config)# wlan wlan-123		
	ruckus(config-wlan-wlan-123)# acl 13 L3-ACL-name		
	The command was 'end' or 'exit'.	executed successfully. To save the changes, type	
Related Commands	no I2 access control		

no I3 access control

acl I2 {L2ACL-NAME}

show

To display the WLAN settings, use the following command: show

Defaults None. Example ruckus(config)# show wlan WLAN Service: ID: 1: SSID= corporate Description= Ruckus-Wireless-1 Authentication= open Authentication= open Encryption= wpa Algorithm= aes Passphrase= test1234 Web Authentication= Disabled Aucounting Server= Disabled Accounting Server= Disabled Tunnel Mode= Disabled Background Scanning= Enabled Max Clients= 100 Client Isolation= None Zero-IT Activation= Disabled Priority= High Load Balancing= Enabled Rate Limiting Uplink= Disabled Rate Limiting Uplink= Disabled Rate Limiting Downlink= Disabled Rate Limiting Uplink= Disabled VLAN= Disabled Dynamic VLAN= Disabled L3/L4/IP Address= No ACLS L3/L4/IP Address= No ACLS	Syntax Description	show	Display WLAN settings
Example ruckus(config) # show wlan WLAN Service: ID: 1: SSID= corporate Description= Ruckus-Wireless-1 Authentication= open Encryption= wpa Algorithm= aes Passphrase= test1234 Web Authentication= Disabled Authentication Server= Disabled Authentication Server= Disabled Accounting Server= Disabled Background Scanning= Enabled Max Clients= 100 Client Isolation= None Zero-IT Activation= Disabled Priority= High Load Balancing= Enabled Dynamic PSK= Disabled Rate Limiting Uplink= Disabled VLAN= Disabled Dynamic VLAN= Disabled L2/MAC= No ACLS	Defaults	- None.	
<pre>WLAN Service: ID: 1: SSID= corporate Description= Ruckus-Wireless-1 Authentication= open Encryption= wpa Algorithm= aes Passphrase= test1234 Web Authentication= Disabled Authentication= Disabled Authentication Server= Disabled Authentication Server= Disabled Tunnel Mode= Disabled Background Scanning= Enabled Max Clients= 100 Client Isolation= None Zero-IT Activation= Disabled Priority= High Load Balancing= Enabled Dynamic PSK= Disabled Rate Limiting Downlink= Disabled Rate Limiting Downlink= Disabled VLAN= Disabled Closed System= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS</pre>	Example	_ ruckus(confi	.g)# show wlan
ID: 1: SSID= corporate Description= Ruckus-Wireless-1 Authentication= open Encryption= wpa Algorithm= aes Passphrase= test1234 Web Authentication= Disabled Authentication Server= Disabled Authentication Server= Disabled Accounting Server= Disabled Tunnel Mode= Disabled Background Scanning= Enabled Max Clients= 100 Client Isolation= None Zero-IT Activation= Disabled Priority= High Load Balancing= Enabled Dynamic PSK= Disabled Rate Limiting Uplink= Disabled Rate Limiting Downlink= Disabled VLAN= Disabled Closed System= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS		WLAN Service	2:
1: SSID= corporate Description= Ruckus-Wireless-1 Authentication= open Encryption= wpa Algorithm= aes Passphrase= test1234 Web Authentication= Disabled Authentication Server= Disabled Authentication Server= Disabled Tunnel Mode= Disabled Background Scanning= Enabled Max Clients= 100 Client Isolation= None Zero-IT Activation= Disabled Priority= High Load Balancing= Enabled Dynamic PSK= Disabled Rate Limiting Dowlink= Disabled Rate Limiting Dowlink= Disabled VLAN= Disabled Dynamic VLAN= Disabled Losed System= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS		ID:	
SSID= corporate Description= Ruckus-Wireless-1 Authentication= open Encryption= wpa Algorithm= aes Passphrase= test1234 Web Authentication= Disabled Authentication Server= Disabled Accounting Server= Disabled Tunnel Mode= Disabled Background Scanning= Enabled Max Clients= 100 Client Isolation= None Zero-IT Activation= Disabled Priority= High Load Balancing= Enabled Dynamic PSK= Disabled Rate Limiting Dowlink= Disabled Rate Limiting Dowlink= Disabled VLAN= Disabled Dynamic VLAN= Disabled Log System= Disabled L2/MAC= No ACLS		1:	
Description= Ruckus-Wireless-1 Authentication= open Encryption= wpa Algorithm= aes Passphrase= test1234 Web Authentication= Disabled Authentication Server= Disabled Authentication Server= Disabled Accounting Server= Disabled Tunnel Mode= Disabled Background Scanning= Enabled Max Clients= 100 Client Isolation= None Zero-IT Activation= Disabled Priority= High Load Balancing= Enabled Dynamic PSK= Disabled Rate Limiting Uplink= Disabled Rate Limiting Downlink= Disabled VLAN= Disabled Closed System= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS		SSID=	corporate
Authentication= open Encryption= wpa Algorithm= aes Passphrase= test1234 Web Authentication= Disabled Authentication Server= Disabled Accounting Server= Disabled Tunnel Mode= Disabled Background Scanning= Enabled Max Clients= 100 Client Isolation= None Zero-IT Activation= Disabled Priority= High Load Balancing= Enabled Dynamic PSK= Disabled Rate Limiting Uplink= Disabled Rate Limiting Downlink= Disabled VLAN= Disabled Dynamic VLAN= Disabled Closed System= Disabled L2/MAC= No ACLS		Descr	ption= Ruckus-Wireless-1
Encryption= wpa Algorithm= aes Passphrase= test1234 Web Authentication= Disabled Authentication Server= Disabled Accounting Server= Disabled Tunnel Mode= Disabled Background Scanning= Enabled Max Clients= 100 Client Isolation= None Zero-IT Activation= Disabled Priority= High Load Balancing= Enabled Dynamic PSK= Disabled Rate Limiting Uplink= Disabled Rate Limiting Uplink= Disabled VLAN= Disabled ULAN= Disabled Closed System= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS		Auther	ntication= open
Algorithm= aes Passphrase= test1234 Web Authentication= Disabled Authentication Server= Disabled Accounting Server= Disabled Tunnel Mode= Disabled Background Scanning= Enabled Max Clients= 100 Client Isolation= None Zero-IT Activation= Disabled Priority= High Load Balancing= Enabled Dynamic PSK= Disabled Rate Limiting Uplink= Disabled Rate Limiting Downlink= Disabled VLAN= Disabled Dynamic VLAN= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS		Encryp	otion= wpa
Passphrase= test1234 Web Authentication= Disabled Authentication Server= Disabled Accounting Server= Disabled Tunnel Mode= Disabled Background Scanning= Enabled Max Clients= 100 Client Isolation= None Zero-IT Activation= Disabled Priority= High Load Balancing= Enabled Dynamic PSK= Disabled Rate Limiting Uplink= Disabled Rate Limiting Downlink= Disabled VLAN= Disabled Dynamic VLAN= Disabled Closed System= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS		Algori	thm= aes
Web Authentication= Disabled Authentication Server= Disabled Accounting Server= Disabled Tunnel Mode= Disabled Background Scanning= Enabled Max Clients= 100 Client Isolation= None Zero-IT Activation= Disabled Priority= High Load Balancing= Enabled Dynamic PSK= Disabled Rate Limiting Uplink= Disabled Rate Limiting Downlink= Disabled VLAN= Disabled Dynamic VLAN= Disabled Closed System= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS		Passpl	nrase= test1234
Authentication Server= Disabled Accounting Server= Disabled Tunnel Mode= Disabled Background Scanning= Enabled Max Clients= 100 Client Isolation= None Zero-IT Activation= Disabled Priority= High Load Balancing= Enabled Dynamic PSK= Disabled Rate Limiting Uplink= Disabled Rate Limiting Downlink= Disabled VLAN= Disabled Dynamic VLAN= Disabled Closed System= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS		Web Au	thentication= Disabled
Accounting Server= Disabled Tunnel Mode= Disabled Background Scanning= Enabled Max Clients= 100 Client Isolation= None Zero-IT Activation= Disabled Priority= High Load Balancing= Enabled Dynamic PSK= Disabled Rate Limiting Uplink= Disabled Rate Limiting Downlink= Disabled VLAN= Disabled Dynamic VLAN= Disabled Closed System= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS		Auther	ntication Server= Disabled
Tunnel Mode= Disabled Background Scanning= Enabled Max Clients= 100 Client Isolation= None Zero-IT Activation= Disabled Priority= High Load Balancing= Enabled Dynamic PSK= Disabled Rate Limiting Uplink= Disabled Rate Limiting Downlink= Disabled VLAN= Disabled Dynamic VLAN= Disabled Closed System= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS		Accour	nting Server= Disabled
Background Scanning= Enabled Max Clients= 100 Client Isolation= None Zero-IT Activation= Disabled Priority= High Load Balancing= Enabled Dynamic PSK= Disabled Rate Limiting Uplink= Disabled Rate Limiting Downlink= Disabled VLAN= Disabled Dynamic VLAN= Disabled Closed System= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS		Tunne	Mode= Disabled
Max Clients= 100 Client Isolation= None Zero-IT Activation= Disabled Priority= High Load Balancing= Enabled Dynamic PSK= Disabled Rate Limiting Uplink= Disabled Rate Limiting Downlink= Disabled VLAN= Disabled Dynamic VLAN= Disabled Closed System= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS		Backgı	cound Scanning= Enabled
Client Isolation= None Zero-IT Activation= Disabled Priority= High Load Balancing= Enabled Dynamic PSK= Disabled Rate Limiting Uplink= Disabled Rate Limiting Downlink= Disabled VLAN= Disabled Dynamic VLAN= Disabled Closed System= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS		Max C	ients= 100
Zero-IT Activation= Disabled Priority= High Load Balancing= Enabled Dynamic PSK= Disabled Rate Limiting Uplink= Disabled Rate Limiting Downlink= Disabled VLAN= Disabled Dynamic VLAN= Disabled Closed System= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS		Client	: Isolation= None
Priority= High Load Balancing= Enabled Dynamic PSK= Disabled Rate Limiting Uplink= Disabled Rate Limiting Downlink= Disabled VLAN= Disabled Dynamic VLAN= Disabled Closed System= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS		Zero-1	T Activation= Disabled
Load Balancing= Enabled Dynamic PSK= Disabled Rate Limiting Uplink= Disabled Rate Limiting Downlink= Disabled VLAN= Disabled Dynamic VLAN= Disabled Closed System= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS		Priori	ty= High
Dynamic PSK= Disabled Rate Limiting Uplink= Disabled Rate Limiting Downlink= Disabled VLAN= Disabled Dynamic VLAN= Disabled Closed System= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS		Load H	Balancing= Enabled
Rate Limiting Uplink= Disabled Rate Limiting Downlink= Disabled VLAN= Disabled Dynamic VLAN= Disabled Closed System= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS		Dynam	c PSK= Disabled
Rate Limiting Downlink= Disabled VLAN= Disabled Dynamic VLAN= Disabled Closed System= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS		Rate I	Jimiting Uplink= Disabled
VLAN= Disabled Dynamic VLAN= Disabled Closed System= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS		Rate I	imiting Downlink= Disabled
Dynamic VLAN= Disabled Closed System= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS		VLAN=	Disabled
Closed System= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS		Dynam	c VLAN= Disabled
L2/MAC= No ACLS L3/L4/IP Address= No ACLS		Closed	d System= Disabled
L3/L4/IP Address= No ACLS		L2/MAG	C= No ACLS
		L3/L4,	'IP Address= No ACLS

Configure Syslog Settings Commands

2:

SSID= xsteven-open Description= Authentication= open Encryption= none Web Authentication= Disabled Authentication Server= Disabled Accounting Server= Disabled Tunnel Mode= Disabled Background Scanning= Enabled Max Clients= 100 Client Isolation= None Zero-IT Activation= Disabled Priority= High Load Balancing= Enabled Rate Limiting Uplink= Disabled Rate Limiting Downlink= Disabled VLAN= Disabled Dynamic VLAN= Disabled Closed System= Disabled L2/MAC= No ACLS L3/L4/IP Address= No ACLS

3:

SSID= randy-wlansvc-01-open Description= Auth-open-ENc-None Authentication= open Encryption= none Web Authentication= Enabled Authentication Server= Ruckus-Auth-02 Accounting Server= Ruckus-Acct-01 Interim-Update= 5 Tunnel Mode= Disabled Background Scanning= Enabled Max Clients= 50 Client Isolation= None Zero-IT Activation= Disabled Priority= High Load Balancing= Disabled Rate Limiting Uplink= Disabled Rate Limiting Downlink= Disabled VLAN= Enabled; VLAN-ID= 12

Dynamic VLAN= Disabled Closed System= Disabled L2/MAC= L2_ACL_New_Name L3/L4/IP Address= No ACLS

Related Commands show

Configure WLAN Group Settings Commands

Use the wlan-group commands to configure the settings of a particular WLAN group.

wlan-group

To create a new WLAN group or update an existing WLAN group, use the following command:

wlan-group {WLAN group name}

Syntax Description		
,	wlan-group	Configure the WLAN group
	{WLAN group name}	Create or edit this WLAN group
Defaults	None.	
Example	ruckus# config	
	ruckus(config)# wl	an-group wlangrp-01
	The WLAN group has or exit.	been created. To save the WLAN group, type end
Related Commands	<u>abort</u>	
	end	
	<u>exit</u>	
	quit	
	abort	
	To exit the wlan-group	p context without saving changes, use the abort command.
	Enter this command fro	m within the context of the WLAN group that you are
	configuring.	
	abort	
Syntax Description		
-,	abort	Exit the WLAN group without saving changes

Configure WLAN Group Settings Commands

Defaults	None.		
Example	<pre>ruckus# config ruckus(config)# wlan-group wlangrp-01 ruckus(config-wlangrp-wlangrp-01)# abort No changes have been saved.</pre>		
Related Commands	wlan-group		
	<u>end</u>		
	exit		
	quit		
	end		
	To save changes to the WLAN group settings and exit the wlan-group context, use the following command. Enter this command from within the context of the WLAN group that you are configuring. end		
Syntax Description	end Save changes, and then exit the WLAN group		
Defaults	None.		
Example	ruckus# config ruckus(config)# wlan-group wlangrp-01 ruckus(config-wlangrp-wlangrp-01)# end The WLAN group 'hello-wlangrp' has been undated		
	Your changes have been saved.		
Related Commands	wlan-group abort exit quit		
	exit To save changes to the WLAN group settings and exit the wlan-group context, use the exit command. Enter this command from within the context of the WLAN group that you are configuring. exit		

Syntax Description		
	exit	Save changes, and then exit the WLAN group
Defaults	None.	
Example	- ruckus# con	fig
	ruckus(conf	ig)# wlan-group wlangrp-01
	ruckus(conf	ig-wlangrp-wlangrp-01)# exit
	The WLAN gro	oup 'hello-wlangrp' has been updated.
	Your changes	s have been saved.
Related Commands	wlan-group	
	abort	
	<u>end</u>	
	quit	
	To exit the wla Enter this com configuring. quit	n-group context without saving changes, use the following command. mand from within the context of the WLAN group that you are
Syntax Description	quit	Exit the WLAN group without saving changes
Defaults	None.	
Example	ruckus# con ruckus(conf: ruckus(conf: No changes]	fig ig)# wlan-group wlangrp-01 ig-wlangrp-wlangrp-01)# quit have been saved.
Related Commands	wlan-group abort end	
	<u>exit</u>	

name

To set the WLAN group name, use the following command. Enter this command from within the context of the WLAN group that you are configuring.

name {WLAN group name}

	-		
Syntax Description	name	Configure the WLAN group name	
	{WLAN group name}	Set the WLAN group name to this value	
	-		
Defaults	None.		
Example	- ruckus# config		
	ruckus(config)# wl	an-group wlangrp-01	
	ruckus(config-wlang	grp-wlangrp-01)# name hello-wlangrp	
	The command was exe 'end' or 'exit'.	ecuted successfully. To save the changes, type	
Related Commands	description		
	description		
	To set the WLAN group description, use the following command. Enter this command from within the context of the WLAN group that you are configuring.		
	description {WL	AN group description}	
Syntax Description			
Syntax Description	description	Configure the WLAN group description	
	{WLAN group description}	Set the WLAN group description to this value	
	_		
Defaults	None.		
Example	- ruckus# config		
-	ruckus(config)# wlan-group wlangrp-01		
	<pre>ruckus(config-wlangrp-wlangrp-01)# description my-description- 123</pre>		
	The command was exe 'end' or 'exit'.	ecuted successfully. To save the changes, type	
	-		
Related Commands	name		

no wlan

To delete a WLAN service, use the following command. Enter this command from within the context of the WLAN group that you are configuring.

no wlan {WLAN name to be deleted}

Syntax Description			
\$	no wlan	Delete an existing WLAN service	
	{WLAN name to be	Delete the WLAN service with this name	
	deleted}		
Defaults	None.		
Example	- ruckus# config		
-	<pre>ruckus(config)# wlan-group wlangrp-01</pre>		
	ruckus(config-wlan	grp-wlangrp-01)# no wlan wlansvc-012	
	The command was ex 'end' or 'exit'.	ecuted successfully. To save the changes, type	
Related Commands	<u>wlan</u>		
	wlan vlan override none	2	
	<u>wlan vlan override unta</u>	<u>a</u>	
	<u>wlan vlan override tag</u>		
	wlan		
	To add a WLAN service command from within t	to the WLAN group, use the following command. Enter this he context of the WLAN group that you are configuring.	
	wlan {WLAN name	e to be created}	
Syntax Description	-	Create a WI ANI service	
	{WLAN name to be created}		
	-		
Defaults	None.		
Example	ruckus# config		
	ruckus(config)# wl	an-group wlangrp-01	
	ruckus(config-wlan	grp-wlangrp-01)# wlan wlansvc-012	
	The command was ex 'end' or 'exit'.	ecuted successfully. To save the changes, type	

Configure WLAN Group Settings Commands

Related Commands	no wlan			
	wlan vlan override none			
	wlan vlan override untag			
	wlan vlan override tag			
	wlan vlan override none To add a WLAN service to the WLAN group and set the VLAN tag to 'No Change'.			
	use the following command. Enter this command from within the context of the WLAN group that you are configuring.			
	wlan {WLAN name} vlan override none			
Syntax Description	wlan {WLAN name} Add the {WLAN name} to the WLAN group			
	vlan override none Set the VLAN tag of {WLAN name} to No Change			
Defaults	None.			
Example	ruckus# config ruckus(config)# wlan-group wlangrp-01 ruckus(config-wlangrp-wlangrp-01)# wlan wlansvc-012 vlan override			
	The command was executed successfully. To save the changes, type 'end' or 'exit'.			
Related Commands	no wlan			
	<u>wlan</u>			
	wlan vlan override untag			
	wlan vlan override tag			
	wlan vlan override untag To add a WLAN service to the WLAN group and set the VLAN tag to 'Untag', use the following command:			
	wlan {WLAN name} vlan override untag			
Syntax Description	wlan {WLAN name} Add the {WLAN name} to the WLAN group			
	vlan override untag Set the VLAN tag of {WLAN name} to Untagged			
Defaults	None.			

Example	ruckus# config			
	<pre>ruckus(config)# wlan-group wlangrp-01 ruckus(config-wlangrp-wlangrp-01)# wlan wlansvc-012 vlan override untag</pre>			
	The command was executed successfully. To save the changes, type 'end' or 'exit'.			
Related Commands	no wlan			
	<u>wlan</u>			
	wlan vlan override none			
	wlan vlan override tag			
	wlan vlan override tag To add a WLAN service to the WLAN group and set the VLAN tag to 'Tag', use the following command: wlan {WLAN name} vlan override tag {vlan ID}			
Syntax Description	-			
Syntax Description	wlan {WLAN name} Add the {WLAN name} to the WLAN group			
	vlan override tag Set the VLAN tag of {WLAN name} to Tagged for {vlan ID} {vlan ID}			
Defaults	None.			
Example	ruckus# config			
	ruckus(config)# wlan-group RW-group			
	The WLAN group 'RW-group' has been created. To save the WLAN group, type end or exit.			
	<pre>ruckus(config-wlangrp-RW-group)# wlan corporate vlan override tag 33</pre>			
	The WLAN service (SSID) 'corporate' has been added.			
	ruckus(config-wlangrp-RW-group)#			
Related Commands	no wlan			
	<u>wlan</u>			
	wlan vlan override none			
	wlan vlan override untag			
	wlan vlan override tag			

Using Debug Commands

In This Chapter	
Deauthorizing a Device	123
Restarting a Device	124

Deauthorizing a Device

Deauthorizing a device refers to removing it from the list of devices that have been approved to join the controller.

delete-station {MAC address}

To deauthorize the station with a specific MAC address, use the following command: delete-station {MAC address}

Syntax Description	-	
Syntax Description	delete-station	Delete the station with a specific MAC address
	{MAC address}	The MAC address of the station that will be deleted
Defaults	None.	
Example	ruckus# debug	lete-station 00:10:77:01:00:01
	The command was es	kecuted successfully.
Related Commands		ess}

Restarting a Device

Use the restart command to restart a device that is reporting to the controller.

restart-ap {MAC address}

To restart the device with a specific MAC address, use the restart <code>ap</code> command:

restart-ap {MAC address}

Syntax Description		
•)	restart-ap	Restart the device with a specific MAC address
	{MAC address}	The MAC address of the device to be restarted
Defaults	None.	
Example	ruckus# debug ruckus(debug)# re	estart-ap 00:13:92:EA:43:01
Related Commands	delete-station {MAC	address}

Index

Α

aaa all, 9 aaa name, 10 abort, 116 access control I2, 113 access control I3, 113 acct-server, 109 acct-server interim-update, 110 acl, 58 acl abort, 59 acl end, 59 acl exit, 60 acl name, 61 acl quit, 61 add mac, 62 admin show, 44 ap all, 10 ap devname, 12 ap mac, 13 ap-management-vlan, 56 auth-server, 43

С

client isolation, 104–105 config wlan dot1x authentication encryption wpa2 algorithm TKIP auth-server, 100–103 configuring NTP client, 65 configuring SNMP agent, 70 contact, 72 country code, 76 creating a WLAN, 120

D

delete station, 123 description, 46, 62, 79, 119 devname, 45 disabling NTP client, 65 disabling SNMP agent, 70 disabling SNMP traps, 71 displaying interface settings, 79 dot11-country-code, 76 dot1x, 104 dot1x authentication encryption wep-64 auth-server, 103 dot1x authentication encryption wpa algorithm AES auth-server, 98 dot1x authentication encryption wpa algorithm TKIP auth-server, 98–99 dot1x authentication encryption wpa2 algorithm AES auth-server, 100, 102

E

enabling NTP client, 65 end, 117 exit, 56, 117

G

gateway, 76

Н

hide ssid, 111

L

ip addr, 47, 77 ip addr gateway, 47 IP address, 77 IP address mode, 78 ip mode, 48, 78 ip name-server, 49, 77 ip route gateway, 76 ip-addr, 36 ip-addr port, 37

L

location, 46, 72

Μ

mac authentication encryption none authserver, 88 mac authentication encryption wep-128 key key-id auth-server, 96 mac authentication encryption wep-64 key key-id auth-server, 95 mac authentication encryption wpa passphrase algorithm AES auth-server, 89 mac authentication encryption wpa passphrase algorithm TKIP auth-server, 89-90 mac authentication encryption wpa2 passphrase algorithm AES auth-server, 91, 93 mac authentication encryption wpa2 passphrase algorithm TKIP auth-server, 92, 94 - 95max clients, 112 mode allow, 63 mode deny, 63

Ν

name, 42, 119 name password, 42 no acct-server, 106 no acl. 58 no auth-server, 43 no client isolation, 106 no hide ssid. 111 no l2 access control, 108 no I3 access control, 108 no mac, 64 no ntp, 65 no snmp-agent, 70 no snmp-trap, 71 no syslog, 75 no tunnel mode, 107 no vlan, 107 no web authentication, 106 ntp, 65

0

open authentication encryption wep-128 key key-id, 87 open authentication encryption wep-64 key key-id, 86 open authentication encryption wpa passphrase {passphrase} algorithm AES, 82 open authentication encryption wpa passphrase {passphrase} algorithm TKIP, 83–84 open authentication encryption wpa pass-

phrase algorithm AES, 82

- open authentication encryption wpa passphrase algorithm TKIP, 83–84
- open authentication encryption wpa2 passphrase algorithm AES, 84

open authentication encryption wpa2 passphrase algorithm TKIP, 85–86 open none, 81

Q

quit, 118

R

radio 2.4 channel, 49 radio 2.4 channel auto, 50 radio 2.4 tx-power, 51 radio 2.4 tx-power auto, 51 radio 2.4 wlan-group, 52 radio 5 channel, 52 radio 5 channel auto, 53 radio 5 tx-power, 54 radio 5 tx-power auto, 54 radio 5 wlan-group, 55 radius-secret, 37 read-only community, 73 read-write community, 73 restart, 124 ro-community, 73 rw-community, 73

S

shared authentication encryption wep-128 key key-id, 97 shared authentication encryption wep-64 key key-id, 97 show, 57, 79, 114 SNMP agent contact, 72 SNMP agent location, 72 SNMP RO, 73 SNMP RW, 73 snmp-trap, 74 ssid, 81 sysinfo, 16 syslog, 75 syslog notifications, 75 syslog server address, 75 sysstats, 21

Ζ

ZoneDirector gateway, 76 IP address, 77 IP address mode, 78 name server, 77

т

techsupport, 22 trap server, 74 tunnel mode, 112 type ad, 33 type Idap, 34 type radius, 35 type radius-acct, 35

V

vlan, 110

W

web authentication, 109 wlan, 120 wlan all, 28 WLAN description, 79 wlan name, 29 WLAN SSID, 81 wlan vlan override none, 121 wlan vlan override tag, 122 wlan vlan override untag, 121 wlan-group, 116 wlan-group all, 31 wlan-group name, 31