

# Unleashed 200.7 Command Line Interface Reference Guide

Supporting Unleashed 200.7

# Copyright, Trademark and Proprietary Rights Information

© 2020 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

## Export Restrictions

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

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

## Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

## Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

## Trademarks

ARRIS, the ARRIS logo, CommScope, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, Edgelron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, and ZoneFlex are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

# Contents

---

<b>Preface.....</b>	<b>23</b>
Document Conventions.....	23
Notes, Cautions, and Warnings.....	23
Command Syntax Conventions.....	24
Document Feedback.....	24
Ruckus Product Documentation Resources.....	24
Online Training Resources.....	25
Contacting Ruckus Customer Services and Support.....	25
What Support Do I Need?.....	25
Open a Case.....	25
Self-Service Resources.....	25
<b>About This Guide.....</b>	<b>27</b>
Introduction.....	27
What's New in this Release.....	27
Unleashed CLI Setup Wizard.....	29
<b>Understanding the Unleashed Command Line Interface.....</b>	<b>33</b>
Introduction.....	33
Accessing the Command Line Interface.....	33
Requirements.....	33
Step 1: Connecting the Administrative Computer to Unleashed.....	33
Step 2: Start and Configure the SSH Client.....	33
Step 3: Log Into the CLI.....	36
Using the ? Command.....	36
Top-Level Commands.....	38
Using the Help Command.....	38
<b>Viewing Current Configuration.....</b>	<b>39</b>
Show Commands Overview.....	40
Show AAA Commands.....	41
show aaa all .....	41
show aaa name .....	42
Show DHCP Commands.....	43
show dhcp all.....	43
show dhcp name.....	43
Show Access Point Commands.....	45
show ap all.....	45
show ap devname.....	47
show ap mac.....	48
Show AP Group Commands.....	50
show ap-group all.....	50
show ap-group name.....	51
Show AP Policy Commands.....	53
show ap-policy.....	53
Show System Configuration Commands.....	54
show config.....	54
Show Performance Commands.....	56

show performance.....	56
show performance ap-radio2-4 .....	56
show performance ap-radio5.....	56
show performance station.....	57
Show System Information Commands.....	59
show sysinfo.....	59
Show Ethernet Info Commands.....	60
show ethinfo.....	60
Show Technical Support Commands.....	61
show techsupport.....	61
Show Management ACL Commands.....	63
show mgmt-acl all.....	63
show mgmt-acl name.....	63
Show WLAN Commands.....	64
show wlan.....	64
Show WLAN Group Commands.....	66
show wlan-group all.....	66
show wlan-group name.....	66
Show L2 Access Control List Commands.....	68
show l2acl all.....	68
show l2acl name.....	68
Show Whitelist Commands.....	70
show whitelist all.....	70
show whitelist name.....	70
Show L3 Access Control List Commands.....	72
show l3acl all.....	72
show l3acl name.....	72
Show Hotspot Commands.....	73
show hotspot all.....	73
show hotspot name.....	74
Show Guest Policy Commands.....	75
show guest-access-service.....	75
Show Hotspot 2.0 Operator Commands.....	76
show hs20op.....	76
Show Hotspot 2.0 Service Provider Commands.....	77
show hs20sp.....	77
Show Role Commands.....	78
show role all.....	78
show role name.....	78
Show User Commands.....	80
show user all.....	80
show user name.....	80
Show Currently Active Clients Commands.....	82
show current-active-clients all.....	82
show current-active-clients mac.....	83
Show Mesh Commands.....	84
show mesh info.....	84
show mesh topology.....	84
Show Dynamic PSK Commands.....	86
show dynamic-psks.....	86

Show Guest Pass Commands.....	87
show guest-passes.....	87
show guest-access-generation.....	88
show portal-auth-generation.....	89
Show Rogue Device Commands.....	90
show rogue-devices.....	90
Show Events and Activities Commands.....	91
show events-activities.....	91
Show Alarm Commands.....	92
show alarm.....	92
Show License Commands.....	93
show license.....	93
Show Application Policy Commands.....	94
show app-policy.....	95
show user-app-ip.....	95
show user-app-port.....	95
Show Session-Timeout Commands.....	97
show session-timeout.....	97
Show Active Wired Client Commands.....	98
show active-wired-client all.....	98
show active-wired-client mac.....	98
Show RADIUS Statistics Commands.....	99
show radius-statistics.....	99
reset radius-statistics.....	99
Show Load Balancing Commands.....	101
show load-balance.....	101
Show Station Rename Commands.....	101
show sta-rename.....	101
Show Station Favorite Commands.....	101
show sta-favorite.....	102
<b>Configuring Master Settings.....</b>	<b>103</b>
Configuration Commands Overview.....	104
General Config Commands.....	104
help.....	104
history.....	104
abort.....	104
end.....	104
exit.....	105
quit.....	105
Configure Context Show Commands.....	106
show aaa.....	106
show dhcp.....	106
show admin.....	106
show mgmt-acl.....	106
show ap.....	106
show l2acl.....	106
show l3acl.....	106
show whitelist.....	106
show prece.....	107
show dvcpcy.....	107

show app-policy.....	107
show user-app-ip.....	107
show user-app-port.....	107
show load-balancing.....	108
show wlan.....	108
show wlan-group.....	108
show role.....	108
show user.....	109
show hotspot.....	109
show guest-access-service.....	109
show guest-access-generation.....	109
show portal-auth-generation.....	109
show ap-group.....	109
show usb-software.....	109
show location-services.....	110
show sta-rename.....	110
show sta-favorite.....	110
show mdnsproxyrule.....	110
show mdnsproxy.....	110
show bonjour-policy.....	110
show bonjour-fencing.....	110
Configure AAA Server Commands.....	111
aaa.....	111
Configure DHCP Server Commands.....	114
dhcp.....	114
no dhcp.....	114
show.....	115
name.....	115
description.....	115
first.....	115
second.....	115
no second.....	115
Configure Admin Commands.....	116
admin.....	116
name.....	116
name password.....	116
show.....	118
Configure Access Points Commands.....	119
ap.....	119
no ap.....	119
devname.....	120
no devname.....	120
bonjour-gateway.....	120
no bonjour-gateway.....	120
description.....	121
no description.....	121
gps.....	121
no gps.....	122
location.....	122
no location.....	122

group.....	122
ip.....	123
ipv6.....	124
no ipv6.....	125
Radio 2.4/5 GHz Commands.....	126
radio.....	126
no radio.....	127
mesh mode.....	128
mesh uplink-selection.....	129
status-leds.....	129
no status-leds-override.....	130
usb-port.....	130
no usb-port-override.....	130
poe-out.....	130
no poe-out-override.....	131
no usb-software-override.....	131
external-antenna.....	131
no external-antenna-override.....	131
spectra-analysis 2.4GHz.....	132
spectra-analysis 5GHz.....	132
internal-heater.....	132
no internal-heater-override.....	132
cband-channels.....	132
no cband-channels-override.....	133
usb-software.....	133
no usb-software.....	133
ipmode.....	133
no ipmode-override.....	134
radio-band.....	134
no radio-band-override.....	134
venue-name.....	135
no venue-name.....	135
lldp.....	135
no lldp-override.....	136
power-mode.....	136
no power-mode-override.....	137
802.3af-txchain.....	137
no 802.3af-txchain-override.....	137
show.....	137
AP Port Setting Commands.....	139
port-setting.....	139
abort.....	141
end.....	141
exit.....	141
quit.....	141
show.....	141
lan.....	142
no lan.....	143
lan uplink.....	143
lan untag.....	144

lan member.....	144
lan opt82.....	145
lan tunnel.....	146
lan guest-vlan.....	147
lan dvlan enabled.....	147
lan dvlan disabled.....	147
lan dot1x.....	147
dot1x authsvr.....	148
dot1x acctsvr.....	148
dot1x mac-auth-bypass.....	149
dot1x supplicant username.....	149
dot1x supplicant password.....	149
dot1x supplicant mac.....	150
Configure AP Group Commands.....	151
ap-group.....	151
no ap-group.....	151
Configure Hotspot Redirect Settings.....	153
hotspot_redirect_https.....	153
no hotspot_redirect_https.....	153
no blocked-client.....	153
Configure Layer 2 Access Control Commands.....	154
acl.....	154
no acl.....	154
abort.....	155
end.....	155
exit.....	155
quit.....	155
show.....	155
name.....	156
description.....	156
add-mac.....	157
mode allow.....	157
mode deny.....	158
del-mac.....	158
Configure Layer 3 Access Control Commands.....	159
l3acl.....	159
no l3acl.....	159
l3acl-ipv6.....	160
no l3acl-ipv6.....	160
abort.....	160
end.....	160
exit.....	161
quit.....	161
show.....	161
name.....	161
description.....	162
mode allow.....	162
mode deny.....	163
rule-order.....	163
no rule-order.....	166



Layer 3 Access Control Rule Commands.....	167
end.....	167
exit.....	167
order.....	167
description.....	167
type allow.....	168
type deny.....	168
destination address.....	169
destination port.....	169
protocol.....	169
show.....	170
Layer 3 IPv6 Access Control List Commands.....	171
l3acl-ipv6.....	171
abort.....	171
end.....	171
exit.....	171
quit.....	171
name.....	171
description.....	171
mode allow.....	171
mode deny.....	171
no rule-order.....	171
rule-order.....	172
Configure L3 IPv6 Rule Commands.....	173
end.....	173
exit.....	173
order.....	173
description.....	173
type allow.....	173
type deny.....	173
destination.....	173
destination address.....	173
destination port.....	173
protocol.....	174
icmpv6-type Any.....	174
icmpv6-type number.....	174
show.....	174
Configure Precedence Policy Commands.....	175
prece.....	175
no prece.....	175
end.....	175
exit.....	175
quit.....	176
name.....	176
description.....	176
show.....	176
Configure Precedence Policy Rule Commands.....	177
rule.....	177
description.....	178
order.....	178

Configure Device Policy Commands.....	179
dvcpcy.....	179
no dvcpcy.....	180
rule.....	180
Configure Application Policy Commands.....	182
app-policy.....	182
no app-policy.....	182
description.....	183
show.....	183
Configure Application Policy Rules.....	184
rule.....	184
no rule.....	184
rule-type.....	184
application-type.....	184
category.....	185
application.....	185
Configuring User-Defined Applications.....	187
user-app-ip.....	187
no user-app-ip.....	187
abort.....	187
end.....	187
exit.....	187
destination-IP.....	187
netmask.....	188
destination-port.....	188
protocol.....	188
application-name.....	188
Configuring User-Defined Applications Based on Port Mapping.....	189
user-app-port.....	189
abort.....	189
end.....	189
exit.....	189
port.....	189
protocol.....	189
application-name.....	190
Configure Whitelist Commands.....	191
whitelist.....	191
no whitelist.....	191
name.....	191
description.....	191
Configuring Whitelist Rules.....	192
rule.....	192
no rule.....	192
description.....	192
mac.....	192
ip.....	192
Configure Band Balancing Commands.....	193
band-balancing.....	193
abort.....	193
end.....	193

exit.....	193
quit.....	193
enable.....	193
disable.....	193
Proactive.....	195
percent-2.4G <NUMBER>.....	195
show.....	195
Configure Load Balancing Commands.....	196
load-balancing.....	196
adj-threshold.....	196
weak-bypass.....	197
strong-bypass.....	197
act-threshold.....	198
new-trigger.....	198
headroom.....	199
disable wifi0.....	199
disable wifi1.....	199
enable wifi0.....	199
enable wifi1.....	200
show.....	200
Configure STP Commands.....	201
stp.....	201
no stp.....	201
Configure System Commands.....	202
system.....	202
dot11-country-code.....	202
hostname.....	203
Interface Commands.....	204
timezone.....	207
ftp-anon.....	207
no ftp-anon.....	207
ftp.....	207
no ftp.....	208
mgmt-if.....	208
Unleashed-Multi-Site-Manager.....	209
northbound.....	210
no northbound.....	211
ntp.....	211
no ntp.....	211
SNMPv2 Commands.....	213
SNMPv3 Commands.....	217
Syslog Settings Commands.....	221
Management Access Control List Commands.....	225
QoS Commands.....	228
tunnel-mtu.....	230
bonjour.....	231
no bonjour.....	231
telnetd.....	231
no telnetd.....	232
snmp-trap.....	232

no snmp-trap.....	232
no snmpv2-trap.....	233
no snmpv3-trap.....	233
no snmpv2.....	233
no snmpv3.....	234
show support-entitle.....	235
login-warning.....	235
no login-warning.....	236
event-log-level.....	236
support-entitle.....	236
session-stats-resv.....	236
no session-stats-resv.....	237
session-limit-unauth-stats.....	237
no session-limit-unauth-stats.....	237
eapol-no-retry.....	238
no eapol-no-retry.....	239
arc-data-transmission.....	240
no arc-data-transmission .....	241
master-protect.....	242
generate-token.....	245
show.....	246
Configure UPNP Settings.....	247
upnp.....	247
no upnp.....	247
Configure Zero-IT Settings.....	248
zero-it.....	248
zero-it-auth-server.....	248
Configure Dynamic PSK Expiration.....	249
dynamic-psk-expiration.....	249
Configure WLAN Settings Commands.....	250
wlan.....	250
abort.....	250
end.....	250
exit.....	250
quit.....	250
description.....	251
called-station-id-type.....	251
ssid.....	251
beacon-interval.....	252
wlan-bind.....	253
mgmt-tx-rate.....	253
name.....	253
type.....	254
type standard-usage.....	255
type guest-access.....	255
type hotspot.....	255
type hs20.....	255
type autonomous.....	255
open.....	255
mac none auth-server.....	256

mac wpa2 passphrase algorithm AES auth-server.....	256
mac wpa-mixed passphrase algorithm AES auth-server.....	257
mac wep-64 key key-id auth-server.....	258
mac wep-128 key key-id auth-server.....	258
auth-server.....	260
dot1x eap-type EAP-SIM auth-server.....	260
dot1x eap-type PEAP auth-server.....	261
dot1x wpa2 algorithm AES auth-server.....	261
dot1x wpa2 algorithm auto auth-server.....	262
dot1x wpa-mixed algorithm AES auth-server.....	263
dot1x wpa-mixed algorithm auto auth-server.....	264
dot1x authentication encryption wep-64 auth-server.....	264
dot1x wep-128 auth-server.....	265
dot1x none.....	265
dot1x-mac none.....	266
bgscan.....	266
no bgscan.....	266
ft-roaming.....	267
no ft-roaming.....	267
rrm-neigh-report.....	267
no rrm-neigh-report.....	267
https-redirect.....	267
no https-redirect.....	267
client-flow-log.....	268
no client-flow-log.....	268
client-connect-log.....	268
no client-connect-log.....	268
bypasscna.....	269
no bypasscna.....	269
client-isolation.....	269
whitelist.....	270
no whitelist.....	270
load-balancing.....	270
no load-balancing.....	270
band-balancing.....	270
no band-balancing.....	271
send-eap-failure.....	271
no send-eap-failure.....	271
pap-authenticator.....	271
no pap-authenticator.....	272
nasid-type.....	272
priority low.....	272
priority high.....	272
web-auth.....	273
no web-auth.....	273
grace-period.....	274
no grace-period.....	274
acct-server.....	274
acct-server interim-update.....	275
no acct-server.....	275

inactivity-timeout.....	276
web-auth-timeout.....	276
vlan.....	277
dynamic-vlan.....	277
no dynamic-vlan.....	278
mcast-filter.....	278
no mcast-filter.....	278
hide-ssid.....	278
no hide-ssid.....	279
ofdm-only.....	279
no ofdm-only.....	279
admission-control.....	279
no admission-control.....	279
bss-minrate.....	280
no bss-minrate.....	280
dtim-period.....	281
no dtim-period.....	282
directed-threshold.....	283
no directed-threshold.....	284
tunnel-mode.....	284
no tunnel-mode.....	284
dhcp-relay.....	285
no dhcp-relay.....	285
smart-roam.....	285
no smart-roam.....	285
force-dhcp.....	285
force-dhcp-timeout.....	286
no force-dhcp.....	286
Configuring DHCP Option 82 Sub-Option Settings.....	287
sta-info-extraction.....	288
no sta-info-extraction.....	288
zero-it-activation.....	288
no zero-it-activation.....	289
max-clients.....	289
802dot11d.....	290
no 802dot11d.....	290
arc.....	290
no arc.....	291
apply-policy-group.....	291
auto-proxy.....	291
no auto-proxy.....	292
pmk-cache.....	292
no pmk-cache.....	292
pmk-cache-for-reconnect.....	292
no pmk-cache-for-reconnect.....	292
roaming-acct-interim-update.....	292
no roaming-acct-interim-update.....	293
Configuring Dynamic PSKs.....	294
dynamic-psk enable.....	294
dynamic-psk passphrase-len.....	294

dynamic-psk type.....	294
no dynamic-psk.....	295
limit-dpsk.....	295
no limit-dpsk.....	295
dynamic-psk-expiration.....	295
no l2acl.....	296
no role-based-access-ctrl.....	296
no l3acl.....	296
no l3acl-ipv6.....	297
no dvcpcy.....	297
rate-limit.....	297
no rate-limit.....	297
no mac-addr-format.....	298
mac-addr-format.....	298
acl dvcpcy.....	298
acl prece.....	298
acl role-based-access-ctrl.....	298
qos classification.....	299
no qos classification.....	299
qos heuristics-udp.....	299
no qos heuristics-udp.....	299
qos directed-multicast.....	299
no qos directed-multicast.....	299
qos igmp-snooping.....	299
no qos igmp-snooping.....	299
qos mld-snooping.....	300
no qos mld-snooping.....	300
qos tos-classification.....	300
no qos tos-classification.....	300
qos priority high.....	300
qos priority low.....	300
qos directed-threshold.....	300
disable-dgaf.....	300
no disable-dgaf.....	301
proxy-arp.....	301
no proxy-arp.....	301
80211w-pmf.....	301
no 80211w-pmf.....	301
ignor-unauth-stats.....	301
no ignor-unauth-stats.....	301
show.....	301
Configure WLAN Group Settings Commands.....	304
wlan-group.....	304
no wlan-group.....	304
abort.....	305
end.....	305
exit.....	306
quit.....	306
name.....	307
description.....	307

wlan.....	308
no wlan.....	308
wlan vlan override none.....	309
wlan vlan override tag.....	309
show.....	310
Configure Role Commands.....	311
role.....	311
no role.....	311
abort.....	312
end.....	312
exit.....	312
quit.....	313
name.....	313
description.....	314
group-attributes.....	314
wlan-allowed.....	315
specify-wlan-access.....	315
no specify-wlan-access.....	316
guest-pass-generation.....	316
no guest-pass-generation.....	316
admin.....	317
no admin.....	317
access-ctrl.....	318
no access-ctrl.....	318
os-type-allowed all.....	319
os-type-allowed specify.....	319
specify-os-type-access.....	319
no specify-os-type-access.....	319
vlan.....	319
rate-limit uplink.....	319
rate-limit uplink downlink.....	320
no rate-limit.....	320
apply-arc-policy.....	321
no apply-arc-policy.....	322
show.....	322
Configure User Commands.....	323
user.....	323
no user.....	323
abort.....	324
end.....	324
exit.....	324
quit.....	325
user-name.....	325
full-name.....	326
password.....	326
role.....	327
show.....	327
Configure Guest Access Commands.....	329
guest-access.....	329
no guest-access.....	329



abort.....	329
end.....	329
exit.....	329
quit.....	329
guest-access-force-https-redirectio.....	330
no guest-access-force-https-redirectio.....	331
guest-access-guestpass-effective.....	332
name.....	332
self-service.....	332
no self-service.....	332
guestpass-duration.....	332
guestpass-reauth.....	332
no guestpass-reauth.....	333
guestpass-share-number.....	333
guestpass-sponsor.....	333
no guestpass-sponsor.....	333
guestpass-sponsor-auth-server.....	333
guestpass-sponsor-number.....	333
guestpass-notification.....	333
guestpass-terms-and-conditions.....	334
no guestpass-terms-and-conditions.....	334
onboarding.....	334
no onboarding.....	334
no authentication.....	335
authentication guest-pass-and-social-login.....	335
authentication only-social-login.....	336
no term-of-use.....	336
term-of-use.....	336
redirect.....	337
welcome-text.....	337
show.....	338
social-media-login.....	339
web-portal-force-https-redirectio.....	341
no web-portal-force-https-redirectio.....	342
portal-auth-force-dns-server.....	343
no portal_auth-force-dns-server.....	344
guest-access-auth-server.....	345
Configuring Guest Access Restriction Rules.....	346
no restrict-access-order.....	346
restrict-access-order.....	347
show.....	347
order.....	348
description.....	348
type allow.....	348
type deny.....	349
destination address.....	349
destination port.....	350
protocol.....	350
IPv6 Guest Restrict Access Commands.....	352
no restrict-access-order-ipv6.....	352

restrict-access-order-ipv6.....	352
show.....	353
order.....	354
description.....	354
type allow.....	355
type deny.....	355
destination address.....	356
destination port.....	356
protocol.....	356
icmpv6-type.....	357
Configure Hotspot Commands.....	358
hotspot.....	358
no hotspot.....	358
abort.....	359
end.....	359
exit.....	359
quit.....	360
show.....	360
name.....	361
smartclient.....	361
no smartclient.....	362
login-page.....	362
start-page.....	363
no session-timeout.....	363
session-timeout.....	364
no grace-period.....	364
grace-period.....	364
auth-server local.....	365
auth-server name.....	365
auth-server name no-mac-bypass.....	366
auth-server name mac-bypass.....	366
auth-server name mac-bypass mac-addr-format.....	367
acct-server.....	367
no acct-server.....	368
acct-server interim-update.....	368
client-isolation.....	369
whitelist.....	369
location-id.....	370
location-name.....	370
walled-garden.....	370
no walled-garden.....	371
Configuring Hotspot Restricted Access Rules.....	372
restrict-access-order.....	372
no restrict-access-order.....	373
restrict-access-order-ipv6.....	373
no restrict-access-order-ipv6.....	374
icmpv6-type.....	375
Hotspot Access Restriction Commands.....	376
end.....	376
exit.....	376

show.....	376
order.....	377
description.....	377
type allow.....	378
type deny.....	378
destination address.....	379
destination port.....	379
protocol.....	379
intrusion-prevention.....	380
no intrusion-prevention.....	380
Configure Hotspot 2.0 Commands.....	381
hs20op.....	381
no hs20op.....	381
Configure Hotspot 2.0 Operator Settings.....	382
hs20sp.....	391
no hs20sp.....	391
Configure Hotspot 2.0 Service Provider Settings.....	392
nai-realm.....	393
name.....	394
encoding.....	394
eap-method.....	394
eap-method eap-mthd.....	394
eap-method auth-info.....	395
Configure Mesh Commands.....	398
mesh.....	398
abort.....	398
end.....	398
exit.....	398
quit.....	398
show.....	398
ssid.....	399
passphrase.....	399
hops-warn-threshold.....	400
no detect-hops.....	400
fan-out-threshold.....	401
no detect-fanout.....	401
beacon-interval.....	401
mgmt-tx-rate.....	402
mesh-uplink-selection static.....	402
mesh-uplink-selection dynamic.....	403
mesh-radio-option.....	404
zero-touch-mesh.....	405
no zero-touch-mesh.....	406
zt-mesh-serial.....	407
no zt-mesh-serial.....	408
Configure Alarm Commands.....	409
alarm.....	409
no alarm.....	409
abort.....	409
end.....	409

exit.....	410
quit.....	410
e-mail.....	410
show.....	410
Configure Alarm-Event Settings.....	412
alarm-event.....	412
event.....	412
no event.....	414
Configure Services Commands.....	416
abort.....	416
end.....	416
exit.....	416
quit.....	417
auto-adjust-ap-power.....	417
no auto-adjust-ap-power.....	417
auto-adjust-ap-channel.....	418
no auto-adjust-ap-channel.....	418
raps.....	419
no raps.....	419
channelfly.....	419
no channelfly.....	420
background-scan.....	420
no background-scan.....	421
background-scan low-threshold.....	421
aeroscout-detection.....	423
no aeroscout-detection.....	423
ekahau.....	423
no ekahau.....	424
pif.....	424
no pif.....	425
show.....	425
Configure WIPS Commands.....	427
wips.....	427
Configure Email Server Commands.....	429
email-server.....	429
from.....	430
enable.....	431
no enable.....	431
smtp-server-name.....	431
smtp-server-port.....	432
smtp-auth-name.....	432
smtp-auth-password.....	433
smtp-wait-time.....	433
tls-smtp-encryption.....	433
no tls-smtp-encryption.....	434
Configure SMS Server Commands.....	435
sms-server.....	435
no sms-server.....	436
sns.....	436
Syntax Description.....	436

Defaults.....	437
Example.....	437
Configure Station Rename Commands.....	437
sta-rename.....	438
Configure Favorite Station Commands.....	438
sta-favorite.....	439
Configure mDNS (Bonjour) Commands.....	440
mdnsproxy.....	440
no mdnsproxy.....	440
mdnsproxyrule.....	440
no mdnsproxyrule.....	440
Configuring a Bonjour Policy.....	441
Configuring a Bonjour Fencing Policy.....	443
upload-debug.....	445
no upload-debug.....	446
<b>Using Debug Commands.....</b>	<b>447</b>
Debug Commands Overview.....	447
General Debug Commands.....	447
help.....	447
list-all.....	447
history.....	447
quit.....	447
apfw_upgrade.....	447
delete-station.....	448
restart-ap.....	449
restore.....	449
wlaninfo.....	449
save_debug_info.....	451
remote_ap_cli.....	451
save-config.....	452
emfd-malloc-stats.....	453
Show Commands.....	454
show ap.....	454
show station.....	456
show logs.....	457
show remote-troubleshooting.....	457
ps.....	458
Accessing a Remote AP CLI.....	460
remote_ap_cli.....	460
Working with Debug Logs and Log Settings.....	462
logs all.....	462
no logs all.....	462
logs comp sys-mgmt.....	463
no logs comp sys-mgmt.....	463
logs comp mesh.....	463
no logs comp mesh.....	463
logs comp web-auth.....	464
no logs comp web-auth.....	464
logs comp rf-mgmt.....	464
no logs comp rf-mgmt.....	464

logs comp radius.....	464
no logs comp radius.....	464
logs comp hotspot-srv.....	464
no logs comp hotspot-srv.....	464
logs comp aps.....	464
no logs comp aps.....	464
logs comp net-mgmt.....	464
no logs comp net-mgmt.....	465
logs comp 802.1x.....	465
no logs comp 802.1x.....	465
logs comp web-svr.....	465
no logs comp web-svr.....	465
logs comp 802.11.....	465
no logs comp 802.11.....	465
logs comp dvlan.....	465
no logs comp dvlan.....	465
logs comp smart-redundancy.....	465
no logs comp smart-redundancy.....	465
logs comp bonjour-gateway.....	466
no logs comp bonjour-gateway.....	466
logs comp mdnsd.....	466
no logs comp mdnsd.....	466
logs comp client-association.....	466
no logs comp client-association.....	466
logs mac.....	466
no logs mac.....	467
logs play.....	467
no logs play.....	468
support_tls1.0.....	468
no support_tls1.0.....	468
Remote Troubleshooting.....	469
remote-troubleshooting server.....	469
remote-troubleshooting start.....	469
remote-troubleshooting stop.....	469
radius-stats-wlan.....	470
radius-stats-authsvr.....	470
AP Core Dump Collection.....	471
collect_ap_coredump.....	471
no collect_ap_coredump.....	471
Script Execution.....	473
script.....	473
quit.....	473
list.....	473
del.....	474
info.....	474
exec.....	474
<b>Accessing the AP-Mode CLI.....</b>	<b>477</b>
Accessing the AP Mode CLI from the Unleashed CLI.....	477
Configure LTE Commands.....	477

# Preface

- Document Conventions..... 23
- Command Syntax Conventions..... 24
- Document Feedback..... 24
- Ruckus Product Documentation Resources..... 24
- Online Training Resources..... 25
- Contacting Ruckus Customer Services and Support..... 25

## Document Conventions

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

**TABLE 1** Text Conventions

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

## Notes, Cautions, and Warnings

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

### NOTE

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

### ATTENTION

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



### CAUTION

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



### DANGER

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

# Command Syntax Conventions

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

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

## Document Feedback

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

You can email your comments to Ruckus at [ruckus-docs@arris.com](mailto:ruckus-docs@arris.com).

When contacting us, include the following information:

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

For example:

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

## Ruckus Product Documentation Resources

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

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

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



## Online Training Resources

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

## Contacting Ruckus Customer Services and Support

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

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

### What Support Do I Need?

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

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

### Open a Case

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

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at <https://support.ruckuswireless.com/contact-us> and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

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

### Self-Service Resources

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

- Technical Documentation—<https://support.ruckuswireless.com/documents>

## Preface

### Contacting Ruckus Customer Services and Support

- Community Forums—<https://forums.ruckuswireless.com/ruckuswireless/categories>
- Knowledge Base Articles—<https://support.ruckuswireless.com/answers>
- Software Downloads and Release Notes—[https://support.ruckuswireless.com/#products\\_grid](https://support.ruckuswireless.com/#products_grid)
- Security Bulletins—<https://support.ruckuswireless.com/security>

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

# About This Guide

- Introduction..... 27
- What's New in this Release..... 27
- Unleashed CLI Setup Wizard..... 29

## Introduction

The *Ruckus Unleashed CLI Reference Guide* contains the syntax and commands for configuring and managing Unleashed from a command line interface.

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

### NOTE

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

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

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

## What's New in this Release

The following table lists the changes in CLI commands between this release (200.7) and the previous release (200.6).

### NOTE

In addition to the new and updated commands listed below, the 200.7 CLI also provides a new CLI-based Setup Wizard. For information, see *Unleashed CLI Setup Wizard*.

New	Old	Change
show sta-rename	None	New in 200.7
show sta-favorite	None	New in 200.7
switch-ap	None	New in 200.7
web-portal-force-https-redirect	None	New in 200.7
no web-portal-force-https-redirect	None	New in 200.7
upload-debug	None	New in 200.7
no upload-debug	None	New in 200.7
ap-group	None	New in 200.7
no ap-group	None	New in 200.7
Unleashed-Multi-Site-Manager	None	New in 200.7
No Unleashed-Multi-Site-Manager	None	New in 200.7
northbound	None	New in 200.7
no northbound	None	New in 200.7

## About This Guide

### What's New in this Release

New	Old	Change
show internet	None	New in 200.7
master-protect	None	New in 200.7
no master-protect	None	New in 200.7
cpu-reject-sta	None	New in 200.7
cpu-kickout-sta	None	New in 200.7
master-max-sta	None	New in 200.7
generate-token	None	New in 200.7
sta-rename	None	New in 200.7
event gateway-unreachable	None	New in 200.7
no event gateway-unreachable	None	New in 200.7
event ap-radio-on	None	New in 200.7
event ap-radio-off	None	New in 200.7
event master-switch	None	New in 200.7
no event master-switch	None	New in 200.7
event ap-join-with-reason	None	New in 200.7
no event ap-join-with-reason	None	New in 200.7
zt-mesh-serial	None	New in 200.7
no zt-mesh-serial	None	New in 200.7
mesh-radio-option	None	New in 200.7
background-scan low-threshold	None	New in 200.7
sta-favorite	None	New in 200.7
show sta-rename	None	New in 200.7
show sta-favorite	None	New in 200.7
wan-protection	None	New in 200.7
type <LOG TYPE>	None	New in 200.7
arc-data-transmission	None	New in 200.7
no arc-data-transmission	None	New in 200.7
client-connect-log	None	New in 200.7
no client-connect-log	None	New in 200.7
bypass cna	bypass cna	Moved from config-sys to config-wlan
no bypass cna	no bypass cna	Moved from config-sys to config-wlan
authentication guest-pass-and-social-login	authentication guest-pass	Changed "guest-pass" to "guest-pass-and-social-login"
authentication only-social-login	None	New in 200.7
None	show dynamic-certs	Removed in 200.7
None	type social-media	Removed in 200.7
None	type wechat	Removed in 200.7
social-media-login wechat	None	New in 200.7

# Unleashed CLI Setup Wizard

The CLI setup wizard allows you to quickly configure your controller with basic settings using a short series of CLI commands.

To perform Unleashed setup using CLI commands, use the following procedure:

1. When the Unleashed AP is in factory default state, associate to the "Configure.Me-xxxxxx" WLAN and connect to the Unleashed CLI using SSH (default IP address: **unleashed.ruckuswireless.com** or **10.154.231.125**), and log in using the default user name and password:

- Please login: **super**
- Password: **sp-admin**

The Unleashed CLI Wizard Configuration Tool starts automatically.

2. Follow the instructions in the setup wizard to configure your Unleashed Master AP. The following are two examples.

## Configure Unleashed AP in Bridge Mode

```
Please login: super
Password: *****
```

```
Welcome to Ruckus Wireless Unleashed CLI Setup Wizard
```

```
Would you like to start the Setup Wizard? [yes/no]: yes
```

```
Enter Administrative User Name (32 characters max) [admin]:
```

```
admin
```

```
Enter Administrator Password (4-32 characters):
```

```
*****
```

```
Re-enter Administrator Password (4-32 characters):
```

```
*****
```

```
Enter System Name (32 characters max) [Ruckus-Unleashed]:
```

```
Unleashed
```

```
Enter Country Code (or 'help' to show the list) [US]: US
```

```
Enable Mesh [yes/NO]? no
```

```
Enable Gateway Mode [yes/NO]? no
```

```
Enter WAN IP type [1]:
```

- 1: DHCP Mode;
- 2: Manual Mode;

```
1
```

```
Enable WLANs [YES/no]? yes
```

```
Enter Wireless LAN (ESSID, 1-32 characters) [Ruckus-Wireless 1]:
```

```
Unleashed-SSID
```

```
Is it an Open WLAN [yes/NO]? no
```

```
Enter the WPA2 Passphrase (8-63 characters): *****
```

```
Re-enter the WPA2 Passphrase (8-63 characters):
```

```
*****
```

```
Please review the following settings:
```

```
System Name=           Unleashed
Administrator Name=    admin
Country Code=          US
Mesh Supported=         Disable
Gateway Mode Supported= Disable
IPv4 Mode=              DHCP
WLAN ESSID=            Unleashed-SSID
Wireless Authentication= WPA2_PSK
```

## About This Guide

### Unleashed CLI Setup Wizard

Done with the Setup Wizard [yes/no]? **yes**

Save the configuration ...

It will take a few minutes to complete, do not power off the AP! This AP will reboot automatically.

Welcome to Ruckus Unleashed Network Command Line Interface  
ruckus>

## Configure Unleashed AP in Gateway Mode

Please login: **super**  
Password: **\*\*\*\*\***

Welcome to Ruckus Wireless Unleashed CLI Setup Wizard

Would you like to start the Setup Wizard? [yes/no]: **yes**

Enter Administrative User Name (32 characters max) [admin]:  
**admin**

Enter Administrator Password (4-32 characters):  
**\*\*\*\*\***

Re-enter Administrator Password (4-32 characters):  
**\*\*\*\*\***

Enter System Name (32 characters max) [Ruckus-Unleashed]:  
**Unleashed-Gateway**

Enter Country Code (or 'help' to show the list) [US]: **US**

Enable Mesh [yes/NO]? **no**

Enable Gateway Mode [yes/NO]? **yes**

Enter AP R510 WAN Port:  
1: port1, eth0, UP:  
2: port2, eth1, DOWN:  
**1**

Enter WAN IP type [1]:  
1: DHCP Mode;  
2: Manual Mode;  
3: PPPOE Mode;  
**1**

Enter LAN & WLAN IP Address [10.106.0.1]:  
**192.168.1.1**

Enter LAN & WLAN IP Netmask [255.255.0.0]:  
**255.255.255.0**

Enter Client Starting IP Address [10.106.0.2]:  
**192.168.1.2**

Enter Client Ending IP Address [10.106.7.209]:  
**192.168.1.200**

Enter Lease Time [2]:  
1: 6 hours;  
2: 12 hours;  
3: 1 day;  
4: 2 days;  
5: 1 week;  
6: 2 weeks;  
**1**

Enable WLANs [YES/no]? **yes**

Enter Wireless LAN (ESSID, 1-32 characters) [Ruckus-Wireless 1]:

**Unleashed-SSID**

Is it an Open WLAN [yes/NO]? **no**

Enter the WPA2 Passphrase (8-63 characters):

\*\*\*\*\*

Re-enter the WPA2 Passphrase (8-63 characters):

\*\*\*\*\*

Please review the following settings:

System Name=	Unleashed-Gateway
Administrator Name=	admin
Country Code=	US
Mesh Supported=	Disable
Gateway Mode Supported=	Enable
WAN Port=	port1 eth0 UP
IPv4 Mode=	DHCP
LAN Port IPv4 Address Info=	192.168.1.1/255.255.255.0
Client Starting IPv4=	192.168.1.2
Client Ending IPv4=	192.168.1.200
Lease Time=	6 hours
WLAN ESSID=	Unleashed-SSID
Wireless Authentication=	WPA2_PSK

Done with the Setup Wizard [yes/no]? **yes**

Save the configuration ...

It will take a few minutes to complete, do not power off the AP! This AP will reboot automatically.

Welcome to Ruckus Unleashed Network Command Line Interface  
ruckus>





# Understanding the Unleashed Command Line Interface

---

- Introduction..... 33
- Accessing the Command Line Interface..... 33
- Using the ? Command..... 36
- Top-Level Commands..... 38
- Using the Help Command..... 38

## Introduction

The Ruckus Unleashed Command Line Interface (CLI) is a software tool that allows you to configure and manage your Unleashed network - including the Unleashed Master AP and all currently managed member APs - using CLI commands.

Using the command line interface, you can configure Unleashed Master AP system settings, access points, wireless networks and client connection settings, or view current status information for each component of your Ruckus Unleashed wireless network. 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 Unleashed CLI.

### NOTE

The Unleashed CLI supports a maximum of 8 simultaneous SSH sessions, and a maximum 4 sessions from the same IP address.

## Requirements

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

- A computer that you will designate as the admin computer
- A network connection to the Unleashed Master AP
- An SSH (secure shell) client such as PuTTY

## Step 1: Connecting the Administrative Computer to Unleashed

The Unleashed Command Line Interface can be accessed in one of two ways:

- [Using an Ethernet Connection](#) on page 34
- [Using a Serial Connection](#) on page 34

## Step 2: Start and Configure the SSH Client

Before starting this procedure, make sure that your 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 Unleashed 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](http://www.putty.org).

### Using an Ethernet Connection

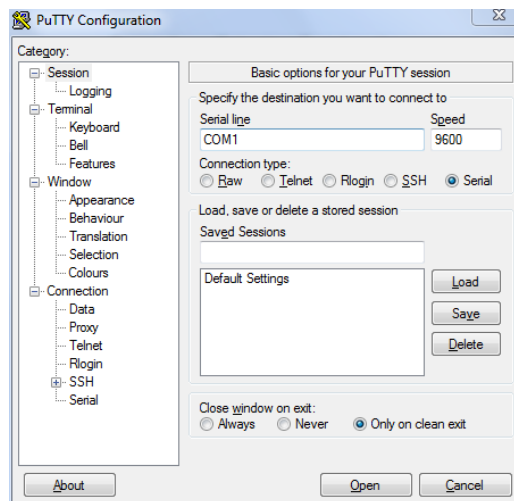
1. Ensure that Unleashed's IP address is reachable from the administrative computer. In factory default state, Unleashed's IP address is **192.168.0.1**.
2. Continue to "Step 2: Start and Configure the SSH Client".

### Using a Serial Connection

To start and configure the SSH client:

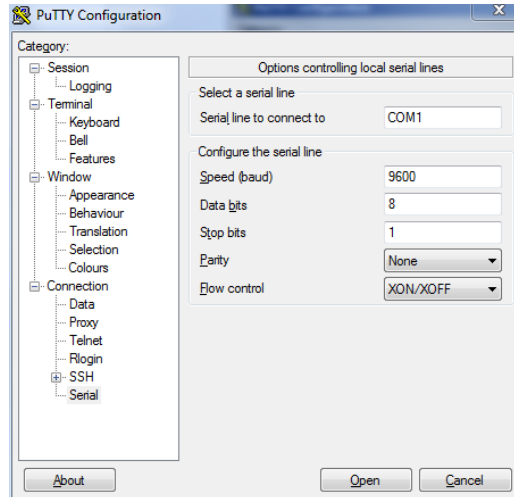
1. Start PuTTY. The PuTTY Configuration dialog box appears, showing the **Session** screen.
2. In **Connection type**, select **Serial** if you are connecting via serial cable.

**FIGURE 1** Select Serial as the connection type



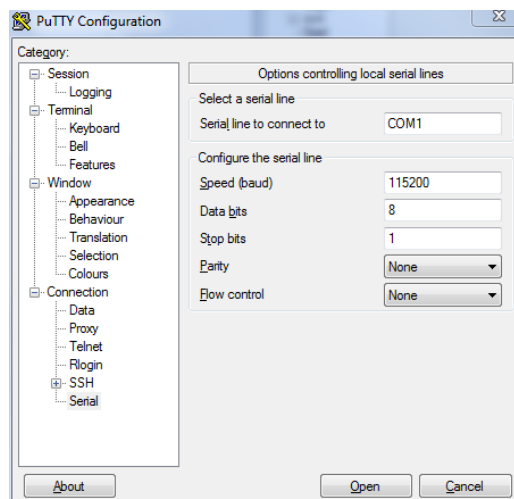
- Under **Category**, click **Connection** > **Serial**. The serial connection options appear on the right side of the dialog box, displaying PuTTY's default serial connection settings.

**FIGURE 2** PuTTY's default serial connection settings



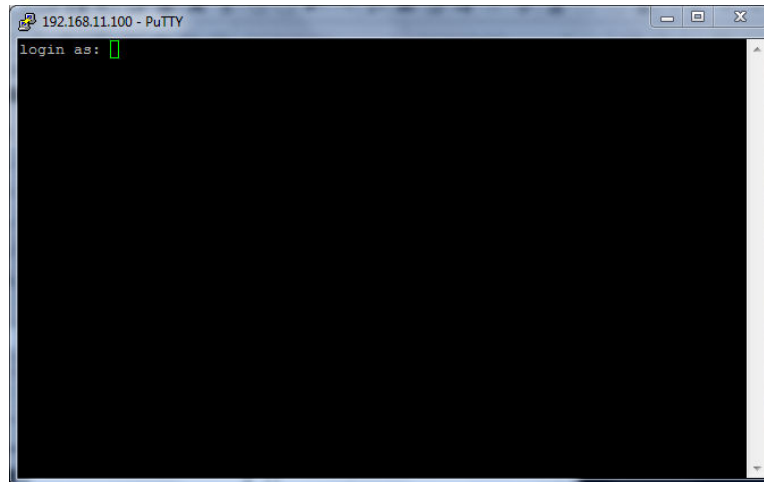
- Configure the serial connection settings as follows:
  - Serial line to connect to:** Type the COM port name to which you connected the RS-232 cable.
  - Bits per second:** 115200
  - Data bits:** 8
  - Stop bits:** 1
  - Parity:** None
  - Flow control:** None

**FIGURE 3** PuTTY's serial connection settings for connecting to Unleashed



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

**FIGURE 4** The PuTTY console displaying the login prompt



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

## Step 3: Log Into the CLI

1. At the **login as** prompt, press **<Enter>** once.
2. At the **Please login** prompt, enter the login name (default: **admin**), and then press **<Enter>**.
3. At the **Password** prompt, enter the login password (default: **admin**), and then press **<Enter>**. The Unleashed CLI welcome message and the `ruckus>` prompt appears.

You are now logged into the Unleashed 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 are 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).

To enable privileged mode when another user session is enabled, use the `<force>` option with the `enable` command to force disconnect of the previous user session. (i.e., **enable force**).

## Using the ? Command

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

## Example

To display commands within the debug context, enter the following command:

**ruckus# debug**

**ruckus(debug)# ?**

**help**

Shows available commands.

**list-all**

Lists all available commands.

**history**

Shows a list of previously run commands.

**quit**

Exits the debug context.

**fw\_upgrade**

Upgrades the controller's firmware.

**delete-station** *MAC*

Disassociates a station.

**restart-ap** *MAC*

Restarts a device.

**wlaninfo**

Configures and enables debugging of WLAN service settings.

**show**

Contains commands that can be executed from within the context.

**ps**

Displays information about all processes that are running (ps -aux).

**save\_debug\_info** *IP-ADDR FILE-NAME*

Saves debug information.

**remote\_ap\_cli**

Executes AP CLI command in remote AP.

**save-config** *IP-ADDR FILE-NAME*

Upload the configuration to the designated TFTP site.

**logs**

Contains commands that can be executed from within the context.

**no**

Contains commands that can be executed from within the context.

**remote-troubleshooting**

Troubleshooting commands group.

**collect\_ap\_coredump**

Enable AP core dump collection.

**script**

Manages system script for debug.

## Top-Level Commands

The following table lists the top-level CLI commands available in privileged mode.

exit	End the CLI session.
help	Show available commands.
quit	End the CLI session.
history	Show a list of previously run commands.
disable	Disable privileged commands.
ping <IP-ADDR/ DOMAIN-NAME>	Send ICMP echo packets to an IP/IPv6 address or domain name.
reboot	Reboot the Master.
shutdown	Shut down Unleashed, to power on Unleashed again, press the power.
set-factory	Reset the Master to factory defaults.
switch-ap	Reset the Master to factory defaults.
config	Enter the config context.
logo	Configure Ruckus logo. Options are "logo nodog" and "logo default."
debug	Enter the debug context.
show	Display system options and settings.
reset	Reset RADIUS statistics commands.
session-timeout <NUMBER>	Set the CLI session timeout.
ap-mode	Run AP CLI (set/get) in Master AP

## Using the Help Command

To display all commands that the Ruckus Wireless CLI supports, use the **help** command.

### NOTE

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 *Using the ? Command* above for more information.

# Viewing Current Configuration

---

- Show Commands Overview..... 40
- Show AAA Commands..... 41
- Show DHCP Commands..... 43
- Show Access Point Commands..... 45
- Show AP Group Commands..... 50
- Show AP Policy Commands..... 53
- Show System Configuration Commands..... 54
- Show Performance Commands..... 56
- Show System Information Commands..... 59
- Show Ethernet Info Commands..... 60
- Show Technical Support Commands..... 61
- Show Management ACL Commands..... 63
- Show WLAN Commands..... 64
- Show WLAN Group Commands..... 66
- Show L2 Access Control List Commands..... 68
- Show Whitelist Commands..... 70
- Show L3 Access Control List Commands..... 72
- Show Hotspot Commands..... 73
- Show Guest Policy Commands..... 75
- Show Hotspot 2.0 Operator Commands..... 76
- Show Hotspot 2.0 Service Provider Commands..... 77
- Show Role Commands..... 78
- Show User Commands..... 80
- Show Currently Active Clients Commands..... 82
- Show Mesh Commands..... 84
- Show Dynamic PSK Commands..... 86
- Show Guest Pass Commands..... 87
- show guest-access-generation..... 88
- show portal-auth-generation..... 89
- Show Rogue Device Commands..... 90
- Show Events and Activities Commands..... 91
- Show Alarm Commands..... 92
- Show License Commands..... 93
- Show Application Policy Commands..... 94
- Show Session-Timeout Commands..... 97
- Show Active Wired Client Commands..... 98
- Show RADIUS Statistics Commands..... 99
- Show Load Balancing Commands..... 101
- Show Station Rename Commands..... 101
- Show Station Favorite Commands..... 101

## Show Commands Overview

Show commands display the controller's current configuration and status information, such as system status and system configuration settings, along with the status and configurations of the controller's WLAN services, users, roles, AAA servers, access points, connected clients, AP groups and WLAN groups, etc.

Monitor commands allow the administrator to enter monitoring mode to view status and configuration changes as they occur.



# Show AAA Commands

Use the **show aaa** commands to display information about the authentication, authorization 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 all
```

### Syntax Description

<b>show</b>	Display AAA server information
<b>aaa</b>	Display AAA server information
<b>all</b>	All AAA servers

### Defaults

None.

### Example

```
ruckus# show aaa all
AAA:
ID:
1:

Name= Local Database
Type= Local

2:
Name= Guest Accounts
Type= Guest

3:
Name= RADIUS Accounting
Type= RADIUS Accounting server
Primary RADIUS Accounting:
IP Address= 192.168.11.7
Port= 1813
Secret= secret
Secondary RADIUS Accounting:
Status= Disabled

4:
Name= Ruckus RADIUS
Type= RADIUS server
Auth Method=
Primary RADIUS:
IP Address= 192.168.11.99
Port= 1812
Secret= secret
Secondary RADIUS:
Status= Disabled
```

## Viewing Current Configuration

### Show AAA Commands

```
5:
Name= Ruckus AD
Type= Active Directory
IP Address= 192.168.11.17
Port= 389
Windows Domain Name= domain.ruckuswireless.com
Global Catalog= Disabled
Admin DN=domain
Admin Password=password

ruckus#
```

## 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 WORD
```

### Syntax Description

#### **show**

Display information

#### **aaa name**

Display information about the specified AAA server name

#### *WORD*

Name of the AAA server

### Defaults

None.

### Example

```
ruckus# show aaa name "Ruckus RADIUS"
AAA:
ID:
4:
Name= Ruckus RADIUS
Type= RADIUS server
Auth Method=
Primary RADIUS:
IP Address= 192.168.11.99
Port= 1812
Secret= secret
Secondary RADIUS:
Status= Disabled

ruckus#
```

# Show DHCP Commands

Use the **show dhcp** commands to display the current settings for any DHCP servers configured for DHCP relay agent use.

## show dhcp all

To display a list of all DHCP servers that have been configured on the controller, use the following command:

```
show dhcp all
```

### Syntax Description

<b>show</b>	Display information
<b>dhcp</b>	Display information about the specified DHCP server name
<b>all</b>	Display a list of all DHCP servers

### Defaults

None.

### Example

```
ruckus# show dhcp all
DHCP servers for DHCP relay agent:
ID:
 1:
   Name= DHCP Server 1
   Description=
   IP Address= 192.168.11.1
   IP Address=

ruckus#
```

## show dhcp name

To display a list of all DHCP servers that have been configured on the controller, use the following command:

```
show dhcp name WORD
```

### Syntax Description

<b>show</b>	Display information
<b>dhcp</b>	Display information about the specified DHCP server name
<b>name</b>	Display the DHCP server specified

## Viewing Current Configuration

### Show DHCP Commands

*WORD*

Name of the DHCP server

### **Defaults**

None.

### **Example**

```
ruckus# show dhcp name "DHCP Server 1"
DHCP servers for DHCP relay agent:
  ID:
  1:
    Name= DHCP Server 1
    Description=
    IP Address= 192.168.11.1
    IP Address=
ruckus#
```

# 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

<b>show</b>	Display information
<b>ap</b>	Show device information
<b>all</b>	All devices that have been approved by the controller

### Defaults

None.

### Example

```
ruckus# show ap all
AP:
ID:
1:
MAC Address= 04:4f:aa:0c:b1:00
Model= zf7962
Approved= Yes
Device Name= 7962 - MAP
Description= 7962 MAP (Living Room)
Location= Living Room
GPS=
Group Name= System Default
Radio a/n:
Channelization= Auto
Channel= Auto
WLAN Services enabled= Yes
5.8GHz Channels = Disabled
Tx. Power= Auto
WLAN Group Name= Default
Radio b/g/n:
Channelization= Auto
Channel= Auto
WLAN Services enabled= Yes
5.8GHz Channels = Disabled
Tx. Power= Auto
WLAN Group Name= Default
Override global ap-model port configuration= No
Network Setting:
Protocol mode= IPv4 and IPv6
Device IP Settings= Keep AP's Setting
IP Type= DHCP
IP Address= 192.168.11.6
```

## Viewing Current Configuration

### Show Access Point Commands

```
Netmask= 255.255.255.0
Gateway= 192.168.11.1
Primary DNS Server=
Secondary DNS Server=

Device IPv6 Settings= Keep AP's Setting
IPv6 Type= Auto Configuration
IPv6 Address= fc00::1
IPv6 Prefix Length= 7
IPv6 Gateway=
IPv6 Primary DNS Server=
IPv6 Secondary DNS Server=
Mesh:
Status= Enabled
Mode= Auto
Uplink:
Status= Smart

2:
MAC Address= 00:24:82:3f:14:60
Model= zf7363
Approved= Yes
Device Name= 7363 - RAP
Description= 7363 - RAP (Study)
Location= Study
GPS=
Group Name= System Default
Radio a/n:
Channelization= Auto
Channel= Auto
WLAN Services enabled= Yes
5.8GHz Channels = Disabled
Tx. Power= Auto
WLAN Group Name= Default
Radio b/g/n:
Channelization= Auto
Channel= Auto
WLAN Services enabled= Yes
5.8GHz Channels = Disabled
Tx. Power= Auto
WLAN Group Name= Default
Override global ap-model port configuration= No
Network Setting:
Protocol mode= IPv4 and IPv6
Device IP Settings= Keep AP's Setting
IP Type= DHCP
IP Address= 192.168.11.3
Netmask= 255.255.255.0
Gateway= 192.168.11.1
Primary DNS Server= 192.168.11.1
Secondary DNS Server=

Device IPv6 Settings= Keep AP's Setting
IPv6 Type= Auto Configuration
IPv6 Address=
IPv6 Prefix Length= 7
IPv6 Gateway=
IPv6 Primary DNS Server=
IPv6 Secondary DNS Server=
Mesh:
Status= Enabled
Mode= Auto
Uplink:
Status= Smart

ruckus#
```

## show ap devname

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

```
show ap devname WORD
```

### Syntax Description

**show**

Display information

**ap devname**

Show information about the specified device name

*WORD*

The name of the device

### Defaults

None.

### Example

```
ruckus# show ap devname "7962 - MAP"
AP:
ID:
1:
MAC Address= 04:4f:aa:0c:b1:00
Model= zf7962
Approved= Yes
Device Name= 7962 - MAP
Description= 7962 MAP (Living Room)
Location= Living Room
GPS=
Group Name= System Default
Radio a/n:
Channelization= Auto
Channel= Auto
WLAN Services enabled= Yes
5.8GHz Channels = Disabled
Tx. Power= Auto
WLAN Group Name= Default
Radio b/g/n:
Channelization= Auto
Channel= Auto
WLAN Services enabled= Yes
5.8GHz Channels = Disabled
Tx. Power= Auto
WLAN Group Name= Default
Override global ap-model port configuration= No
Network Setting:
Protocol mode= IPv4 and IPv6
Device IP Settings= Keep AP's Setting
IP Type= DHCP
IP Address= 192.168.11.6
Netmask= 255.255.255.0
Gateway= 192.168.11.1
Primary DNS Server=
Secondary DNS Server=

Device IPv6 Settings= Keep AP's Setting
IPv6 Type= Auto Configuration
IPv6 Address= fc00::1
IPv6 Prefix Length= 7
```

## Viewing Current Configuration

### Show Access Point Commands

```
IPv6 Gateway=  
IPv6 Primary DNS Server=  
IPv6 Secondary DNS Server=  
Mesh:  
Status= Enabled  
Mode= Auto  
Uplink:  
Status= Smart  
  
ruckus#
```

## show ap mac

To search for the device that matches the specified MAC address, use the following command:

```
show ap mac MAC
```

### Syntax Description

#### **show**

Display information

#### **ap mac**

Display information about the device with the specified MAC address

#### *MAC*

The MAC address of the device

### Defaults

None.

### Example

```
ruckus# show ap mac 04:4f:aa:0c:b1:00  
AP:  
ID:  
1:  
MAC Address= 04:4f:aa:0c:b1:00  
Model= zf7962  
Approved= Yes  
Device Name= 7962 - MAP  
Description= 7962 MAP (Living Room)  
Location= Living Room  
GPS=  
Group Name= System Default  
Radio a/n:  
Channelization= Auto  
Channel= Auto  
WLAN Services enabled= Yes  
5.8GHz Channels = Disabled  
Tx. Power= Auto  
WLAN Group Name= Default  
Radio b/g/n:  
Channelization= Auto  
Channel= Auto  
WLAN Services enabled= Yes  
5.8GHz Channels = Disabled  
Tx. Power= Auto  
WLAN Group Name= Default  
Override global ap-model port configuration= No  
Network Setting:
```



```
Protocol mode= IPv4 and IPv6
Device IP Settings= Keep AP's Setting
IP Type= DHCP
IP Address= 192.168.11.6
Netmask= 255.255.255.0
Gateway= 192.168.11.1
Primary DNS Server=
Secondary DNS Server=

Device IPv6 Settings= Keep AP's Setting
IPv6 Type= Auto Configuration
IPv6 Address= fc00::1
IPv6 Prefix Length= 7
IPv6 Gateway=
IPv6 Primary DNS Server=
IPv6 Secondary DNS Server=
Mesh:
Status= Enabled
Mode= Auto
Uplink:
Status= Smart

ruckus#
```

# Show AP Group Commands

Use the show **ap-group** commands to display Access Point Group settings.

## show ap-group all

To display all AP groups and their settings (including the default AP group), use the following command:

```
show ap-group all
```

### Syntax Description

**show**

Display information

**ap-group**

Display access point group information

**all**

All AP groups

### Defaults

None.

### Example

```
ruckus# show ap-group all
APGROUP:
  ID:
  1:
  Name= System Default
  Description= System default group for Access Points
  Radio 11bgn:
  Channelization= Auto
  Channel= Auto
  Enable auto channel selection which select from 1,6,11= Yes
  Tx. Power= Auto
  11N only Mode= Auto
  WLAN Group= Default
  Radio 11an:
  Channelization= Auto
  Channel= Auto
  Tx. Power= Auto
  11N only Mode= Auto
  WLAN Group= Default
  Members:
  MAC= 04:4f:aa:0c:b1:00
  MAC= 00:24:82:3f:14:60
  MAC= 74:91:1a:2b:ff:a0

APGROUP:
  ID:
  2:
  Name= ap group 2
  Description=
  Radio 11bgn:
  Channelization= Auto
  Channel= Auto
  Enable auto channel selection which select from 1,6,11= Yes
  Tx. Power= Auto
```

```
11N only Mode= Auto
WLAN Group= Default
Radio 11an:
Channelization= Auto
Channel= Auto
Tx. Power= Auto
11N only Mode= Auto
WLAN Group= Default
Members:

APGROUP:
ID:
3:
Name= ap group 1
Description=
Radio 11bgn:
Channelization= Auto
Channel= Auto
Enable auto channel selection which select from 1,6,11= Yes
Tx. Power= Auto
11N only Mode= Auto
WLAN Group= Default
Radio 11an:
Channelization= Auto
Channel= Auto
Tx. Power= Auto
11N only Mode= Auto
WLAN Group= Default
Members:

ruckus#
```

## show ap-group name

To display details about a specific AP group, use the following command:

```
show ap-group name WORD
```

### Syntax Description

**show**

Display information

**ap-group name**

Display information about the AP group with the specified name

*WORD*

The name of the AP group

### Defaults

None.

### Example

```
ruckus# show ap-group name "System Default"
APGROUP:
ID:
1:
Name= System Default
Description= System default group for Access Points
Radio 11bgn:
```

## Viewing Current Configuration

### Show AP Group Commands

```
Channelization= Auto
Channel= Auto
Enable auto channel selection which select from 1,6,11= Yes
Tx. Power= Auto
11N only Mode= Auto
WLAN Group= Default
Radio 11an:
Channelization= Auto
Channel= Auto
Tx. Power= Auto
11N only Mode= Auto
WLAN Group= Default
Members:
MAC= 04:4f:aa:0c:b1:00
MAC= 00:24:82:3f:14:60
MAC= 74:91:1a:2b:ff:a0

ruckus#
```

# Show AP Policy Commands

Use the **show ap-policy** command to display global access point policies that have been configured on the controller.

## show ap-policy

**show ap-policy**

### Example

```
ruckus# show ap-policy
  Automatically approve all join requests from APs= Enabled
  Limited Unleashed Discovery:
    Status= Disabled
  Management VLAN:
    Status= Keep AP's setting
  Auto Recovery= 30 minutes
ruckus#
```

# Show System Configuration Commands

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

## show config

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

**show config**

### Syntax Description

**show**

Display information

**config**

Display system configuration settings

### Defaults

None.

### Example

```
ruckus# show config
Protocol Mode= IPv4-Only
Device IP Address:
  Mode= Manual
  IP Address= 192.168.40.100
  Netmask= 255.255.255.0
  Gateway Address= 192.168.40.1
  Primary DNS= 192.168.40.1
  Secondary DNS=

Management VLAN:
  VLAN ID= 1

Country Code:
  Code= United States

Identity:
  Name= Ruckus

NTP:
  Status= Enabled
  Address= ntp.ruckuswireless.com

Log:
  Status= Disabled
  Address= 192.168.3.10
  Facility= local0
  Priority= emerg
  AP Facility= local0
  AP Priority= emerg

Tunnel MTU:
  Tunnel MTU= 1500

Bonjour Service:
  Status= Disabled
```

```
Telnet Server:
  Status= Disabled

FTP Server:
  Status= Enabled
  Anonymous Status= Enabled

FlexMaster:
  Status= Disabled
  Address=
  Interval= 15

AAA:
  ID:
    1:
      Name= Local Database
      Type= Local

    2:
      Name= Guest Accounts
      Type= Guest
  ...
  ...
ruckus#
```

# Show Performance Commands

Use the **show performance** commands to display performance details on an AP radio or client station.

## show performance

Use the following command to display performance details:

```
show performance
```

## show performance ap-radio2-4

Use the following command to display performance details for the AP's 2.4 GHz radio.

```
show performance ap-radio2-4
```

### Syntax Description

**show**

Display information

**performance**

Display performance information

**ap-radio-2-4**

Display AP 2.4 GHz radio performance

**mac** *MAC*

The MAC address of the AP

### Defaults

None.

### Example

```
ruckus# show performance ap-radio2-4 mac c4:10:8a:1f:d1:f0
AP performance:
  1:
    Radio b/g/n:
    MAC Address= c4:10:8a:1f:d1:f0
    Estimated Capacity= 9930
    Downlink= 67
    Uplink= 0
    RF pollution= 11
    Associated clients= 1
    Other APs= 0

ruckus#
```

## show performance ap-radio5

Use the following command to display performance details for the AP's 5 GHz radio:

```
show performance ap-radio5 mac MAC
```



## Syntax Description

### **show performance**

Display performance information

### **ap-radio-5**

Display AP 5 GHz radio performance

### **mac** *MAC*

The MAC address of the AP

## Defaults

None.

## Example

```
ruckus# show performance ap-radio5 mac c4:10:8a:1f:d1:f0
AP performance:
  1:
    Radio a/n:
    MAC Address= c4:10:8a:1f:d1:f0
    Estimated Capacity= 20891
    Downlink= 77
    Uplink= 2
    RF pollution= 3
    Associated clients= 1
    Other APs= 0

ruckus#
```

## show performance station

Use the following command to display performance details for a connected client/station:

**show performance station mac** *MAC*

## Syntax Description

### **show performance**

Display performance information

### **station**

Display station performance

### **mac** *MAC*

The MAC address of the station

## Defaults

None.

## Example

```
ruckus# show performance station mac 00:22:fb:ad:1b:2e
Station performance:
  MAC Address= 00:22:fb:ad:1b:2e
```

## Viewing Current Configuration

### Show Performance Commands

```
Estimated Capacity= 61401  
Downlink= 76  
Uplink= 18  
ruckus#
```

# 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 status, including system, devices, usage summary, user activities, system activities, 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= 192.168.40.100
  MAC Address= 00:13:11:01:01:01
  Uptime= 4d 0h 18m
  Model= ZD1112
  Licensed APs= 12
  Serial Number= 000000000011
  Version= 9.8.0.0 build 112

Devices Overview:
  Number of APs= 3
  Number of Client Devices= 2
  Number of Rogue Devices= 15

Usage Summary:
  Usage of 1 hr:
    Max. Concurrent Users= 2
    Bytes Transmitted= 45.87M
    Number of Rogue Devices= 15
  Usage of 24 hr:
    Max. Concurrent Users= 3
    Bytes Transmitted= 5.90G
    Number of Rogue Devices= 50

Memory Utilization:
  Used Bytes= 61009920
  Used Percentage= 47%
  Free Bytes= 67158016
  Free Percentage= 53%

ruckus#
```

# Show Ethernet Info Commands

Use the **show ethinfo** command to display current system Ethernet status.

## show ethinfo

**show ethinfo**

### Syntax Description

**show**

Display information

**ethinfo**

Display the current system Ethernet status

### Defaults

None.

### Example

```
ruckus# show ethinfo
System Ethernet Overview:
  Port 0:
    Interface= eth0
    MAC Address= 00:13:11:01:01:01
    Physical Link= up
    Speed= 1000Mbps
  Port 1:
    Interface= eth1
    MAC Address= 00:13:11:01:01:02
    Physical Link= up
    Speed= 100Mbps

ruckus#
```

# 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
ruckus# show techsupport
System Overview:
  Name= Ruckus
  IP Address= 192.168.40.100
  MAC Address= 00:13:11:01:01:01
  Uptime= 15d 18h 44m
  Model= ZD1112
  Licensed APs= 12
  Serial Number= 000000000011
  Version= 9.7.0.0 build 155

Devices Overview:
  Number of APs= 3
  Number of Client Devices= 2
  Number of Rogue Devices= 0

Usage Summary:
Usage of 1 hr:
  Max. Concurrent Users= 2
  Bytes Transmitted= 76.66M
  Number of Rogue Devices= 0
Usage of 24 hr:
  Max. Concurrent Users= 0
  Bytes Transmitted= 2.24G
  Number of Rogue Devices= 0

Memory Utilization:
  Used Bytes= 95956992
  Used Percentage= 74%
  Free Bytes= 32210944
  Free Percentage= 26%

Protocol Mode= IPv4-Only
Device IP Address:
  Mode= Manual
  IP Address= 192.168.40.100
```

## Viewing Current Configuration

### Show Technical Support Commands

```
Netmask= 255.255.255.0
Gateway Address= 192.168.40.1
Primary DNS= 192.168.40.1
Secondary DNS=

Management VLAN:
  VLAN ID= 1

Country Code:
  Code= United States

Identity:
  Name= Ruckus
  ...
  ...
ruckus#
```

# Show Management ACL Commands

Use the **mgmt-acl** and **mgmt-acl-ipv6** commands to display information about the management access control lists configured on the controller.

## show mgmt-acl all

To display all management ACLs that have been configured on the controller, use the following command:

```
show mgmt-acl all
```

## show mgmt-acl name

To display information about a specific management ACL, use the following command:

```
show mgmt-acl name NAME
```

## Show WLAN Commands

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

### show wlan

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

```
show wlan [ all | name <WORD>]
```

### Syntax Description

<b>show</b>	Display information
<b>wlan</b>	Display WLAN services (SSIDs) settings
<b>all</b>	Display all WLAN services
<b>name &lt;WORD&gt;</b>	Display the named WLAN only

### Defaults

None.

### Example

```
ruckus# show wlan all
WLAN Service:
ID:
  1:
    NAME = Ruckus1
    Tx. Rate of Management Frame(2.4GHz) = 2.0Mbps
    Tx. Rate of Management Frame(5GHz) = 6.0Mbps
    Beacon Interval = 100ms
    SSID = Ruckus1
    Description = Ruckus1
    Type = Standard Usage
    Authentication = open
    Encryption = wpa2
    Algorithm = aes
    Passphrase = secretpassphrasegoeshere
    FT Roaming = Disabled
    802.11k Neighbor report = Disabled
    Web Authentication = Disabled
    Authentication Server = Disabled
    Accounting Server = Disabled
    Called-Station-Id type = wlan-bssid
    Tunnel Mode = Disabled
    DHCP relay = Disabled
    Max. Clients = 100
    Isolation per AP = Disabled
    Isolation across AP = Disabled
    Zero-IT Activation = Enabled
    Load Balancing = Disabled
    Band Balancing = Disabled
    Dynamic PSK = Enabled
```



```
Dynamic PSK Passphrase Length =  
Dynamic PSK Expire Time = unlimited  
Dynamic PSK Validity Period =  
Limit Dynamic PSK = Disabled  
Auto-Proxy configuration:  
  Status = Disabled  
Inactivity Timeout:  
  Status = Disabled  
VLAN-ID = 1  
Dynamic VLAN = Disabled  
Closed System = Disabled  
Https Redirection = Disabled  
OFDM-Only State = Disabled  
Multicast Filter State = Disabled  
802.11d State = Disabled  
Force DHCP State = Disabled  
Force DHCP Timeout = 0  
DHCP Option82:  
  Status = Disabled  
  Option82 sub-Option1 = Disabled  
  Option82 sub-Option2 = Disabled  
  Option82 sub-Option150 = Disabled  
  Option82 sub-Option151 = Disabled  
Ignore unauthorized client statistic = Disabled  
STA Info Extraction State = Enabled  
BSS Minrate = Disabled  
DTIM period = 1  
Directed MC/BC Threshold = 5  
Call Admission Control State = Disabled  
PMK Cache Timeout= 720 minutes  
PMK Cache for Reconnect= Enabled  
NAS-ID Type= wlan-bssid  
Roaming Acct-Interim-Update= Disabled  
PAP Message Authenticator = Enabled  
Send EAP-Failure = Disabled  
L2/MAC = No ACLS  
L3/L4/IP Address = No ACLS  
L3/L4/IPv6 Address = No ACLS  
Precedence = No ACLS  
Proxy ARP = Disabled  
Device Policy = No ACLS  
Vlan Pool = No Pools  
Role based Access Control Policy = Disabled  
SmartRoam = Disabled  Roam-factor = 1  
White List = No ACLS  
Application Recognition & Control = Disabled  
Apply ARC Policy = NO POLICY  
Wlan Bind = all  
Client Flow Data Logging = Disabled  
Client Connection Data = Disabled
```

ruckus#

## 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 the specified 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
WLAN Service:
WLAN1:
NAME= Ruckus1
VLAN=
WLAN2:
NAME= Ruckus2
VLAN=

2:
Name= Guest WLAN Group
Description= 1st floor APs only
WLAN Service:
WLAN1:
NAME= Ruckus-Guest
VLAN=

ruckus#
```

### show wlan-group name

To display information about the specified WLAN group name, use the following command:

```
show wlan-group name WORD
```

## Syntax Description

### **show**

Display information

### **wlan-group name**

Display information about the specified WLAN group name

### *WORD*

The name of the WLAN group

## Defaults

None.

## Example

```
ruckus# show wlan-group name Default
WLAN Group:
ID:
1:
Name= Default
Description= Default WLANs for Access Points
WLAN Service:
WLAN1:
NAME= Ruckus1
VLAN=
WLAN2:
NAME= Ruckus2
VLAN=

ruckus#
```

# Show L2 Access Control List Commands

Use the **show l2acl** commands to display Layer 2 access control list rules that have been added to the controller.

## show l2acl all

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 l2acl all**

### Syntax Description

<b>show</b>	Display information
<b>l2acl</b>	Display L2 ACL information
<b>all</b>	All L2 ACL

### Defaults

None.

### Example

```
ruckus# show l2acl all
L2/MAC ACL:
ID:
1:
Name= System
Description= System
Restriction: Deny only the stations listed below
Stations:
2:
Name= blocked-sta-list
Description=
Restriction: Deny only the stations listed below
Stations:
```

## show l2acl name

To display the settings of a specific L2 ACL rule that has been added to the controller, use the following command:

**show l2acl name WORD**

### Syntax Description

<b>show</b>	Display information
<b>l2acl</b>	Display L2 ACL information

**name** Display information about the specified L2 ACL rule name

*WORD*  
Name of the L2 ACL rule

## Defaults

None.

## Example

```
ruckus# show l2acl name 1
L2/MAC ACL:
ID:
2:
Name= 1
Description=
Restriction: Deny only the stations listed below
Stations:
MAC Address= 00:33:22:45:34:88
```

# Show Whitelist Commands

Use the **show whitelist** commands to display client isolation whitelists that have been added to the controller.

## show whitelist all

To display all whitelists that have been added to the controller and their settings, use the following command:

```
show whitelist all
```

### Syntax Description

<b>show</b>	Display information
<b>whitelist</b>	Display whitelist information
<b>all</b>	All whitelists

### Defaults

None.

### Example

```
ruckus# show whitelist all
White Lists:
  ID:
  1:
    Name= printer whitelist
    Description= printer
    Rules:
      1:
        Description= printer
        MAC = 12:34:56:78:90:00
        IP Address = 192.168.4.10

ruckus#
```

## show whitelist name

To display a specified whitelist that has been added to the controller by name, use the following command:

```
show whitelist name WORD
```

### Syntax Description

<b>show</b>	Display information
<b>whitelist</b>	Display whitelist information

**name** *WORD*  
Specify the name of the whitelist

## Defaults

None.

## Example

```
ruckus# show whitelist name "printer whitelist"
White Lists:
ID:
 1:
  Name= printer whitelist
  Description= printer
Rules:
 1:
  Description= printer
  MAC = 12:34:56:78:90:00
  IP Address = 192.168.4.10

ruckus#
```

## Show L3 Access Control List Commands

Use the **show l3acl** commands to display Layer 3 access control list rules that have been added to the controller.

### show l3acl all

To display all Layer 3 access control list (ACL) rules that have been added to the controller and their settings, use the following command:

```
show l3acl all
```

### show l3acl name

To display the settings of a specific L3 ACL rule that has been added to the controller, use the following command:

```
show l3acl name WORD
```



# Show Hotspot Commands

Use the **show hotspot** commands to display the controller's hotspot configuration settings.

## show hotspot all

To display a list of all hotspot services that have been created on the controller, use the following command:

```
show hotspot all
```

### Syntax Description

**show**

Display information

**hotspot**

Display hotspot information

**all**

All available hotspots

### Defaults

None.

### Example

```
ruckus# show hotspot all
Hotspot:
  ID:
    1:
      Name= Hotspot 1
      WISPr Smart Client Support:
        Status= None
      Login Page Url= http://192.168.1.12/login.htm
      Start Page= redirect to the URL that the user intends to visit
      Session Timeout:
        Status= Disabled
      Grace Period:
        Status= Disabled
      Intrusion Prevention= Enabled
      Authentication Server= Local Database
      Accounting Server:
        Status= Disabled
      Isolation per AP = Disabled
      Isolation across AP = Disabled
      White List = No ACLS
      Location ID=
      Location Name=
      Walled Garden 1= 1.1.1.1
      IPv4 Rules:

      IPv6 Rules:

ruckus#
```

## show hotspot name

To display information about the specific hotspot service, use the following command:

**show hotspot name** *WORD*

If the hotspot name includes a space, you must put the name in quotation marks (for example, "hotspot name").

### Syntax Description

**show**

Display information

**hotspot name**

Display hotspot information

*WORD*

The name of the hotspot

### Defaults

None.

### Example

```
ruckus# show hotspot name "Hotspot 1"
Hotspot:
  ID:
    1:
      Name= Hotspot 1
      WISPr Smart Client Support:
        Status= None
      Login Page Url= http://192.168.1.12/login.htm
      Start Page= redirect to the URL that the user intends to visit
      Session Timeout:
        Status= Disabled
      Grace Period:
        Status= Disabled
      Intrusion Prevention= Enabled
      Authentication Server= Local Database
      Accounting Server:
        Status= Disabled
      Isolation per AP = Disabled
      Isolation across AP = Disabled
      White List = No ACLS
      Location ID=
      Location Name=
      Walled Garden 1= 1.1.1.1
      IPv4 Rules:

      IPv6 Rules:

ruckus#
```

# Show Guest Policy Commands

Use the following commands to display guest access services.

## show guest-access-service

To display a list of guest access services or a specific service, use the following command:

```
show guest-access-service [ all | name WORD ]
```

### Example

```
ruckus# show guest-access all
Guest Access:
  Name = guestpolicy1
  Onboarding Portal:
    Aspect = Guest pass and ZeroIT
  Authentication:
    Mode = Use Guest Pass and Social login authentication
  Title = hello
  Terms of Use:
    Status = Disabled
  Redirection:
    Mode = To the URL that the user intends to visit
  Restricted Subnet Access:
    Rules:
      1:
        Description=
        Type= Deny
        Destination Address= local
        Destination Port= Any
        Protocol= Any
      2:
        Description=
        Type= Deny
        Destination Address= 10.0.0.0/8
        Destination Port= Any
        Protocol= Any
      3:
        Description=
        Type= Deny
        Destination Address= 172.16.0.0/12
        Destination Port= Any
        Protocol= Any
      4:
        Description=
        Type= Deny
        Destination Address= 192.168.0.0/16
        Destination Port= Any
        Protocol= Any
  Restricted IPv6 Access:
    Rules:
      1:
        Description=
        Type= Deny
        Destination Address= local
        Destination Port= Any
        Protocol= Any
        ICMPv6 Type= Any

ruckus#
```

## Show Hotspot 2.0 Operator Commands

Use the following commands to display Hotspot 2.0 Operators.

### show hs20op

To display a list of Hotspot 2.0 operators, use the following command:

**show hs20op** [all | name *WORD*]

### Example

```
ruckus# show hs20op all
```

# Show Hotspot 2.0 Service Provider Commands

Use the following commands to display Hotspot 2.0 Service Providers.

## show hs20sp

To display a list of Hotspot 2.0 service providers, use the following command:

**show hs20sp** [all | name *WORD*]

### Example

```
ruckus# show hs20sp all
```

# Show Role Commands

Use the **show role** commands to display details about roles that have been created on the controller.

## show role all

To display a list of all roles that have been created, use the following command:

```
show role all
```

### Syntax Description

<b>show</b>	Display information
<b>role</b>	Display role information
<b>all</b>	All roles that have been created

### Defaults

None.

### Example

```
ruckus# show role all
Role:
  ID:
    1:
      Name= Default
      Description= Allow Access to All WLANs
      Group Attributes=
      Guest Pass Generation= Allowed
      Unleashed Administration:
        Status= Disallowed
      Allow All WLANs:
        Mode= Allow access to all WLANs
      Access Control Policy= Disallowed

ruckus#
```

## show role name

To display information about the specific role, use the following command:

```
show role name WORD
```

### Syntax Description

<b>show</b>	Display information
-------------	---------------------

**role name**

Display role information

*WORD*

The name of the role

**Defaults**

None.

**Example**

```
ruckus# show role name Default
Role:
ID:
  1:
    Name= Default
    Description= Allow Access to All WLANs
    Group Attributes=
    Guest Pass Generation= Allowed
    Unleashed Administration:
      Status= Disallowed
    Allow All WLANs:
      Mode= Allow access to all WLANs
    Access Control Policy= Disallowed

ruckus#
```

# Show User Commands

Use the **show user** commands to display details about user accounts that exist on the controller.

## show user all

To display a list of all existing user accounts, use the following command:

```
show user all
```

### Syntax Description

<b>show</b>	Display information
<b>user</b>	Display user information
<b>all</b>	All existing user accounts

### Defaults

None.

### Example

```
ruckus# show user all
User:
ID:
1:
User Name= test22
Full Name= test11
Password= test1234
Role= Default
```

## show user name

To display information about the specific user, use the following command:

```
show user name user_name
```

### Syntax Description

<b>show</b>	Display information
<b>user name</b>	Display user information
<b>WORD</b>	The name of the user



## Defaults

None.

## Example

```
ruckus# show user name test22
User:
ID:
1:
User Name= test22
Full Name= test11
Password= test1234
Role= Default
```

## Show Currently Active Clients Commands

Use the **show current-active-clients** commands to display a list of wireless clients that are associated with the APs that the controller manages.

### show current-active-clients all

To display a list of all existing user accounts, use the following command:

**show current-active-clients all**

#### Syntax Description

**show**

Display information

**current-active-clients**

Display currently active wireless clients

**all**

All active wireless clients

#### Defaults

None.

#### Example

```
ruckus# show current-active-clients all
Current Active Clients:
Clients:
Mac Address= 00:22:fb:5c:e2:32
User/IP= 172.18.30.2
User/IPv6=
Access Point= 04:4f:aa:13:30:f0
BSSID= 04:4f:aa:13:30:fa
Connect Since=2011/03/01 02:48:22
Auth Method= OPEN
WLAN= 11jojoe
VLAN= None
Channel= 6
Radio= 802.
Signal= 0
Status= Authorized

Last 300 Events/Activities:
Activity:
Date/Time= 2011/03/01 02:49:05
Severity= Low
User=
Activities= User[00:22:fb:5c:e2:32] joins WLAN[11jojoe] from AP[04:4f:aa:13:30:f0]
Activity:
Date/Time= 2011/03/01 02:48:22
Severity= Low
User=
Activities= User[00:22:fb:5c:e2:32] joins WLAN[11jojoe] from AP[04:4f:aa:13:30:f0]
...
...
ruckus#
```

## show current-active-clients mac

To display information about the specific active client, use the following command:

```
show current-active-clients mac MAC
```

### Syntax Description

**show**

Display information

**current-active-clients mac**

Display currently active wireless clients

*MAC*

The MAC address of the wireless client

### Defaults

None.

### Example

```
ruckus# show current-active-clients mac 6c:62:6d:1b:e3:00
Current Active Clients:
Clients:
Mac Address= 6c:62:6d:1b:e3:00
User/IP= 192.168.11.11
User/IPv6=
Access Point= 04:4f:aa:0c:b1:00
BSSID= 04:4f:aa:0c:b1:08
Connect Since=2012/01/10 06:22:44
Auth Method= OPEN
WLAN= Ruckus1
VLAN= None
Channel= 6
Radio= 802.11gn
Signal= 53
Status= Authorized
Received from client= 20746 pkts / 6274531 bytes
Transmitted to client= 25777 pkts / 6714433 bytes
Tx. drops due to retry failure= 1 pkts

Last 300 Events/Activities:
Activity:
Date/Time= 2012/01/10 06:22:44
Severity= Low
User=
Activities= User[6c:62:6d:1b:e3:00]> joins WLAN[Ruckus1] from AP[7962 - MAP@04:4f:aa:0c:b1:00]
Activity:
Date/Time= 2012/01/09 18:52:28
Severity= Low
User=
Activities= User[6c:62:6d:1b:e3:00]disconnects from WLAN[Ruckus1] at AP[7363 - RAP@00:24:82:3f:14:60]
Activity:
Date/Time= 2012/01/08 06:08:52
Severity= Low
User=
Activities= AP[7363 - RAP@00:24:82:3f:14:60] radio [11g/n] detects User[6c:62:6d:1b:e3:00] in
WLAN[Ruckus1] roams from AP[7962 - MAP@04:4f:aa:0c:b1:00]
...
...
ruckus#
```

## Show Mesh Commands

Use the **show mesh** commands to display the controller's mesh network configuration and topology.

### show mesh info

To display a list of mesh information, use the following command:

```
show mesh info
```

### Syntax Description

<b>show</b>	Display information
<b>mesh</b>	Display mesh network information
<b>info</b>	Show mesh information

### Defaults

None.

### Example

```
ruckus# show mesh info
Mesh Settings:
  Mesh Status= Enabled
  Mesh Name (ESSID)= Mesh-951608000220
  Mesh Passphrase= bzj9Y0kEpkxOPzPXyKqLrJHZSAAntfaTm7Ebh6qps24PFpcc5MtClijGGwFZBG
  Mesh Radio Option= 5G
  Mesh Uplink Selection Algorithm = default(static)
  Mesh Hop Detection:
    Status= Disabled
  Mesh Downlinks Detection:
    Status= Disabled
  Tx. Rate of Management Frame= 2Mbps
  Beacon Interval= 200ms
  Zero-Touch-Mesh status= Enabled
Zero Touch Mesh Pre-Approved Serial Number List:
serial number = 921802014959, approved = 0, time = 0, id = 1
serial number = 441e981cf0d0, approved = 0, time = 0, id = 2
serial number = 4f1e681cf3f0, approved = 0, time = 0, id = 3
serial number = c41e781bd7c0, approved = 0, time = 0, id = 4

ruckus#
```

### show mesh topology

To display the topology of existing mesh networks, use the following command:

```
show mesh topology
```

## Syntax Description

- show**  
Display information
- mesh**  
Display mesh network information
- topology**  
Show mesh topology

## Defaults

None.

## Example

```
ruckus# show mesh topology
Mesh Topology(Mesh-951608000220):
  Root Access Points= d4:c1:9e:35:c9:50
  Signal (dB) Downlink= / Uplink=
  Description=
  Channel= 36 (11ac)
  IP Address= 192.168.0.3
  Mesh Access Points= 44:1e:98:1b:f0:d0
  Signal (dB) Downlink= 44 / Uplink= 36
  Description=
  Channel= 36
  IP Address= 192.168.0.10

ruckus#
```

## Show Dynamic PSK Commands

Use the **show dynamic-psks** commands to display information about Dynamic PSKs that have been generated. Use the following command:

### show dynamic-psks

**show dynamic-psks**

#### Syntax Description

**show**

Display information

**dynamic-psks**

Display dynamic PSKs that have been generated

#### Defaults

None.

#### Example

```
ruckus# show dynamic-psks
Generated Dynamic PSKs:
DPSK:
User= BatchDPSK_User_1
Mac Address= 00:00:00:00:00:00
Created= 2011/03/01 03:30:01
Expired= Unlimited
DPSK:
User= BatchDPSK_User_2
Mac Address= 00:00:00:00:00:00
Created= 2011/03/01 03:30:02
Expired= Unlimited
DPSK:
User= DPSK-User-2
Mac Address= 00:11:22:33:44:55
Created= 2011/03/01 03:30:47
Expired= Unlimited
```

# Show Guest Pass Commands

Use the **show guest-passes** commands to display information about guest passes that have been generated. Use the following command:

```
show guest-passes
```

## show guest-passes

```
show guest-passes
```

### Syntax Description

**show**

Display information

**guest-passes**

Display guest passes that have been generated

### Defaults

None.

### Example

```
ruckus# show guest-passes
Generated Guest Passes:
ID:
Guest Name= John Doe
Remarks=
Expires= 2012/01/11 08:32:15
Re-auth=
Creator= ruckus
Sharable= No
Wlan= Ruckus-Guest

ruckus#
```

Viewing Current Configuration  
show guest-access-generation

## show guest-access-generation

Display generation information for guest access.

### Examples

```
ruckus# show guest-access-generation
  Authentication Server: radius1
  Force HTTPS Redirection: Disabled
ruckus#
```



# show portal-auth-generation

Display generation information for portal authentication.

## Examples

```
ruckus# ruckus# show portal-auth-generation
  Force DNS server: 192.168.40.10
ruckus#
```

## Show Rogue Device Commands

Use the **show rogue-devices** commands to display information about rogue devices that the controller has detected on the network. Use the following command.

### show rogue-devices

**show rogue-devices**

#### Syntax Description

**show**

Display information

**rogue-devices**

Display rogues devices that have been detected on the network

#### Defaults

None.

#### Example

```
ruckus# show rogue-devices
Current Active Rogue Devices:
Rogue Devices:
Mac Address= 00:25:c4:52:1c:a1
Channel= 6
Radio= 802.11bg
Type= AP
Encryption= Open
SSID= V54-HOME001
Last Detected= 2011/03/01 02:03:43

Known/Recognized Rogue Devices:
```

# Show Events and Activities Commands

Use the **show events-activities** commands to display information events and network activities that have been recorded by the controller. Use the following command:

## show events-activities

**show events-activities**

### Syntax Description

**show**

Display information

**events-activities**

Display a list of events and activities records by the controller

### Defaults

None.

### Example

```
ruckus# show events-activities
ruckus# show events-activities
Last 300 Events/Activities:
Activity:
Date/Time= 2012/01/10 08:33:17
Severity= Low
User=
Activities= Admin[ruckus] logs in from [192.168.11.7]
Activity:
Date/Time= 2012/01/10 08:32:00
Severity= Low
User=
Activities= WLAN[Ruckus-Guest] with BSSID[04:4f:aa:4c:b1:08] configuration has been updated on radio
[11g/n] of AP[7962 - MAP@04:4f:aa:0c:b1:00]
Activity:
Date/Time= 2012/01/10 08:32:00
Severity= Low
User=
...
...
```

## Show Alarm Commands

Use the **show alarm** commands to display alarms that have been generated by the controller. Use the following command:

### show alarm

**show alarm**

### Syntax Description

**show**

Display information

**alarm**

Display a list of alarms that have been generated by the controller

### Defaults

None.

### Example

```
ruckus# show alarm
Last 300 Alarms:
  Alarms:
    Date/Time= 2013/03/27 15:36:59
    Name= AP Lost Contact
    Severity= High
    Activities= Lost contact with AP[7372 - MAP@c0:c5:20:3b:91:f0]
  Alarms:
    Date/Time= 2013/03/18 14:44:21
    Name= ZD warm restart
    Severity= Medium
    Activities= System warm restarted with [user reboot].
  ...
  ...
ruckus#
```

# Show License Commands

Use **the show license** commands to display the controller's license information, including the model number, the maximum number of APs that it can support, and the maximum number of wireless clients that managed APs can support. Use the following command:

## show license

```
show license
```

### Syntax Description

**show**

Display information

**license**

Display the controller's license information

### Defaults

None.

### Example

```
ruckus# show license
License:
  Model= ZD1112
  Max. AP Number= 12
  Max. Client Number= 1250
ruckus#
```

## Show Application Policy Commands

Use the following commands to display application policies, user-defined applications and application port-mapping settings.

## show app-policy

**show app-policy**

### *Syntax Description*

**show**

Display information

**app-policy**

Display application policies

### *Defaults*

None.

### *Example*

```
ruckus# show app-policy
Application Policy:
  ID:
ruckus#
```

## show user-app-ip

**show user-app-ip**

### *Syntax Description*

**show**

Display information

**license**

Display IP-based user defined applications

### *Defaults*

None.

### *Example*

```
ruckus# show user-app-ip
User defined application hasn't been found.
ruckus#
```

## show user-app-port

**show user-app-port**

## **Syntax Description**

### **show**

Display information

### **license**

Display port-based user defined applications

## **Defaults**

None.

## **Example**

```
ruckus# show user-app-port
Application based on port hasn't been found.
ruckus#
```



# Show Session-Timeout Commands

Use the **show session-timeout** command to display the current session timeout interval.

## show session-timeout

**show session-timeout**

### Syntax Description

**show**

Display information

**session-timeout**

Display the current session timeout interval

### Defaults

None.

### Example

```
ruckus# show session-timeout
Current session timeout interval is 30 minutes
ruckus#
```

# Show Active Wired Client Commands

Use the **show active-wired-client** commands to display information about currently active wired clients.

## show active-wired-client all

**show active-wired-client all**

## show active-wired-client mac

**show active-wired-client mac** *MAC*

### Syntax Description

<b>show</b>	Display information
<b>active-wired-client</b>	Display the currently active wired client information
<b>all</b>	Show all wired clients
<b>mac</b>	Show a specific client information by MAC address
<i>MAC</i>	The MAC address of the specific client

### Defaults

None.

### Example

```
ruckus# show active-wired-client all
Current Active Wired Clients:

ruckus#
```

# Show RADIUS Statistics Commands

Use the following commands to display RADIUS statistics or to reset RADIUS statistics.

## show radius-statistics

To display a list of RADIUS server statistics, use the following command:

```
show radius-statistics [ server-all | server-name WORD ] [ [ wlan-all | wlan-name NAME ] [ latest-ten-min | latest-one-hour | latest-one-day ]
```

### Syntax Description

**show radius-statistics**

Display list of RADIUS server statistics.

**server-all**

Display statistics for all servers. (Default: recorded from power on.)

**server-name** *WORD*

Display statistics for the specified server. (Default: recorded from power on.)

**wlan-all**

Display statistics for all WLANs. (Default: recorded for the last day.)

**wlan-name** *NAME*

Display statistics for the specified WLAN. (Default: recorded for the last day.)

**latest-ten-min**

Display statistics for the last 10 minutes.

**latest-one-hour**

Display statistics for the last hour.

**latest-one-day**

Display statistics for the last day.

## reset radius-statistics

To reset RADIUS statistics, use the following command:

```
reset radius-statistics [ server-all | server-name WORD ] [ master | standby ] [ latest-ten-min | latest-one-hour | latest-one-day ]
```

### Syntax Description

**reset radius-statistics**

Reset RADIUS server statistics.

**server-all**

Reset statistics for all servers to zero. (Default: recorded from power on.)

**server-name** *WORD*

Reset statistics for the specified server to zero. (Default: recorded from power on.)

**wlan-all**

Reset statistics for all WLANs. (Default: recorded for the last day.)

**wlan-name** *NAME*

Reset statistics for the specified WLAN. (Default: recorded for the last day.)

**master**

Reset statistics of the master server to zero.

**standby**

Reset statistics of the standby server to zero.

**latest-ten-min**

Reset statistics recorded for the last 10 minutes

**latest-one-hour**

Reset statistics recorded for the last hour

**latest-one-day**

Reset statistics recorded for the last day

## Show Load Balancing Commands

Use the following commands to display AP load balancing information.

### show load-balance

To display AP load balancing information, use the following command:

**show load-balance**

#### Example

```
ruckus# show load-balance
*** Show AP load balance
Radio---Enable--Scan--ActThresh---AdjThresh---WeakBypass---StrongBypass---NewActTrigger---Headroom
2GHz      0   2000      10      50      33      55      3      3
5GHz      0   2000      10      43      35      55      3      3
----MAC Address----Cli-New-Lim---Allow-----Fallbk----Adjacent 2-GHz Radios [MacAdrs FwdRssi RevRssi
SumRssi]
c4:10:8a:1f:d1:f0  1  0  0 1000000000 0000000000
c0:c5:20:3b:91:f0  2  0  0 1000000000 0000000000
----MAC Address----Cli-New-Lim---Allow-----Fallbk----Adjacent 5-GHz Radios [MacAdrs FwdRssi RevRssi
SumRssi]
c4:10:8a:1f:d1:f0  0  0  0 1000000000 0000000000
c0:c5:20:3b:91:f0  1  0  0 1000000000 0000000000
ruckus#
```

## Show Station Rename Commands

Use the **show sta-rename** command to display the current renamed station list.

### show sta-rename

To display the current renamed station list, use the following command:

**show sta-rename**

#### Example

```
ruckus# show sta-rename
Displays sta rename list.
MAC Address= 6C:AA:B3:00:00:A0
rename= my-iphone
```

```
All sta rename number: 1
```

## Show Station Favorite Commands

Use the **show sta-favorite** command to display the current favorite station list.

## show sta-favorite

To display the current favorite station list, use the following command:

**show sta-favorite**

### Example

```
ruckus# show sta-favorite
Displays sta favorite list.
  MAC Address= aa:aa:aa:aa:aa:aa
  MAC Address= bb:bb:bb:bb:bb:bb
```

```
All sta favorite number: 2
```

# Configuring Master Settings

---

• Configuration Commands Overview.....	104
• General Config Commands.....	104
• Configure Context Show Commands.....	106
• Configure AAA Server Commands.....	111
• Configure DHCP Server Commands.....	114
• Configure Admin Commands.....	116
• Configure Access Points Commands.....	119
• Radio 2.4/5 GHz Commands.....	126
• AP Port Setting Commands.....	139
• Configure AP Group Commands.....	151
• Configure Hotspot Redirect Settings.....	153
• Configure Layer 2 Access Control Commands.....	154
• Configure Layer 3 Access Control Commands.....	159
• Layer 3 Access Control Rule Commands.....	167
• Layer 3 IPv6 Access Control List Commands.....	171
• Configure L3 IPv6 Rule Commands.....	173
• Configure Precedence Policy Commands.....	175
• Configure Precedence Policy Rule Commands.....	177
• Configure Device Policy Commands.....	179
• Configure Application Policy Commands.....	182
• Configure Application Policy Rules.....	184
• Configuring User-Defined Applications.....	187
• Configuring User-Defined Applications Based on Port Mapping.....	189
• Configure Whitelist Commands.....	191
• Configuring Whitelist Rules.....	192
• Configure Band Balancing Commands.....	193
• Configure Load Balancing Commands.....	196
• Configure STP Commands.....	201
• Configure System Commands.....	202
• Configure UPNP Settings.....	247
• Configure Zero-IT Settings.....	248
• Configure Dynamic PSK Expiration.....	249
• Configure WLAN Settings Commands.....	250
• Configuring Dynamic PSKs.....	294
• Configure WLAN Group Settings Commands.....	304
• Configure Role Commands.....	311
• Configure User Commands.....	323
• Configure Guest Access Commands.....	329
• web-portal-force-https-redirectation.....	341
• no web-portal-force-https-redirectation.....	342
• portal-auth-force-dns-server.....	343
• no portal_auth-force-dns-server.....	344
• guest-access-auth-server.....	345
• Configuring Guest Access Restriction Rules.....	346
• IPv6 Guest Restrict Access Commands.....	352
• Configure Hotspot Commands.....	358
• Configuring Hotspot Restricted Access Rules.....	372
• Hotspot Access Restriction Commands.....	376

- Configure Hotspot 2.0 Commands..... 381
- Configure Mesh Commands..... 398
- Configure Alarm Commands..... 409
- Configure Alarm-Event Settings.....412
- Configure Services Commands.....416
- Configure WIPS Commands.....427
- Configure Email Server Commands..... 429
- Configure SMS Server Commands..... 435
- sns..... 436
- Configure Station Rename Commands..... 437
- Configure Favorite Station Commands..... 438
- Configure mDNS (Bonjour) Commands..... 440
- upload-debug..... 445
- no upload-debug..... 446

## Configuration Commands Overview

This section describes the commands that you can use to configure Unleashed via the **config** context. From the privileged commands context, type **config** to enter the configuration context. To show a list of commands available from within the **config** context, type **help** or **?**.

## General Config Commands

The following section describes general configuration commands can be executed from within the **config** context. To save your configuration changes and exit the **config** context, use the **end** or **exit** command. To discard your changes and exit the **config** context, use the **abort** or **quit** command.

Some sub-contexts within the **config** context do not allow the use of the **abort** or **quit** commands; you must save your changes and exit the sub-context. Many commands offer a corresponding “no” command to undo your configuration changes (for example, use “no wlan” to delete a WLAN).

### help

Shows available commands.

### history

Shows a list of previously run commands.

### abort

Exits the **config** context without saving changes. Some contexts do not allow **abort**, you must save your changes to exit the context (**end** or **exit**).

### end

Saves changes, and then exits the **config** context.



## exit

Saves changes, and then exits the **config** context.

## quit

Exits the **config** context without saving changes. Some contexts do not allow quit, you must save your changes to exit the context (**end** or **exit**).

# Configure Context Show Commands

Use the following show commands to display configured settings within the **config** context.

## show aaa

Displays a list of available AAA servers.

## show dhcp

Displays a list of available DHCP servers.

## show admin

Displays information about the administrator login settings.

### Example

```
ruckus(config)# show admin
Administrator Name/Password:
  Name= admin
  Password= *****
  Authenticate:
    Mode= Authenticate using the admin name and password

ruckus(config)#
```

## show mgmt-acl

Displays a list of all management access controls.

## show ap

Displays a list of all approved devices.

## show l2acl

Displays a list of L2 Access Control Lists.

## show l3acl

Displays a list of L3/L4/IP ACL.

## show whitelist

Displays a list of client isolation white lists.

## show prece

Displays a list of Precedence Policies.

### Defaults

Name= Default

Description= None

Attribute=vlan

- Order = AAA,Device Policy,WLAN

Attribute = rate-limit

- Order = AAA,Device Policy,WLAN

### Example

```
ruckus(config)# show prece
Precedence Policy:
  ID:
  1:
    Name= Default
    Description=
    Rules:
      1:
        Description=
        Attribute = vlan
        Order = AAA,Device Policy,WLAN
      2:
        Description=
        Attribute = rate-limit
        Order = AAA,Device Policy,WLAN
```

```
ruckus(config)#
```

## show dvcpcy

Displays a list of Device Policies.

## show app-policy

Displays the application policy settings.

## show user-app-ip

Displays the user-defined IP-based application settings.

## show user-app-port

Displays the user-defined application port mapping settings.

## show load-balancing

Displays information about Load balancing.

### Example

```
ruckus(config)# show load-balancing
Load Balancing:
  Radio 0:
    Status= Disabled
    AdjacentThreshold= 50
    WeakBypass= 33
    StrongBypass= 55
    ActivationThreshold= 10
    NewTrigger= 3
    Headroom= 3

  Radio 1:
    Status= Disabled
    AdjacentThreshold= 43
    WeakBypass= 35
    StrongBypass= 55
    ActivationThreshold= 10
    NewTrigger= 3
    Headroom= 3

ruckus(config)#
```

## show wlan

Displays a list of all WLAN services (Names).

## show wlan-group

Displays a list of existing WLAN groups.

### Example

```
ruckus(config)# show wlan-group
WLAN Group:
  ID:
    1:
      Name= Default
      Description= Default WLANs for Access Points
      WLAN Service:
        WLAN1:
          NAME= Ruckus1
          VLAN=

ruckus(config)#
```

## show role

Displays a list of roles.

## show user

Displays a list of users.

## show hotspot

Displays a list of hotspot entries.

## show guest-access-service

To display a list of guest access services, use the following command:

**show guest-access-service**

## show guest-access-generation

To display generation information for guest access, use the following command:

**show guest-access-generation**

### Example

```
ruckus(config)# show guest-access-generation
  Authentication Server: Local Database
  Force HTTPS Redirection: Disabled
ruckus(config)#
```

## show portal-auth-generation

To display generation information for portal authentication, use the following command:

**show portal-auth-generation**

### Example

```
ruckus(config)# show portal-auth-generation
  Force DNS server: Disabled
  Force Web Portal HTTPS Redirection: Enabled
ruckus(config)#
```

## show ap-group

To display all or specified AP groups, use the following command:

**show ap-group [ all | name WORD ]**

## show usb-software

Displays USB Software Package information.

## show location-services

Displays a list of configured location services.

## show sta-rename

Displays a list of renamed stations.

## show sta-favorite

Displays a list of favorite stations.

## show mdnsproxyrule

To display Mdnsproxy rules, use the following command:

**show mdnsproxyrule** *ID-From ID-to*

## show mdnsproxy

To display Mdnsproxy status, use the following command:

**show mdnsproxy** *ID-From ID-to*

## show bonjour-policy

To display Bonjour policy rules, use the following command:

**show bonjour-policy** *name*

## show bonjour-fencing

To display Bonjour Fencing rules, use the following command:

**show bonjour-fencing** *name*

# Configure AAA Server Commands

This section describes the commands that you can use to configure AAA server entries on the controller. The following commands can be executed from within the **config-aaa** context. To show a list of commands available from within the context, type **help** or **?**.

## aaa

Use the following command to configure an AAA server entry and enter the config-aaa context:

**aaa** *WORD*

### Syntax Description

#### **abort**

Exits the config-aaa context without saving changes.

#### **end**

Saves changes, and then exits the config-aaa context.

#### **exit**

Saves changes, and then exits the config-aaa context.

#### **quit**

Exits the config-aaa context without saving changes.

#### **name** *WORD*

Sets the AAA server name.

#### **show**

Displays a list of available AAA servers.

#### **CaseSensitive**

Sets the 'CaseSensitive' value of AD/LDAP server to 'enabled'.

#### **type**

Sets the type of AAA server.

#### **type ad**

Sets the AAA server type to 'Active Directory'.

#### **type ldap**

Sets the AAA server type to 'LDAP'.

#### **type ad-802.1x**

Sets the AAA server type to 'Active Directory For 802.1x'.

#### **type radius-auth**

Sets the AAA server type to 'RADIUS'.

#### **type tacplus-auth**

Sets the AAA server type to 'TACPLUS'.

#### **type radius-acct**

Sets the AAA server type to 'RADIUS Accounting'.

**radius-encryption**

Sets the AAA server encryption type.

**radius-encryption tls**

Sets the AAA server encryption type to 'TLS'.

**auth-method pap**

Sets the authentication method to PAP.

**auth-method chap**

Sets the authentication method to CHAP.

**ip-addr** *IP-ADDR*

Sets the AAA server's IP/IPv6 address.

**port** *PORT-NUM*

Sets the AAA server's port.

**tacplus-service** *WORD*

Sets TACPLUS service name with length (1-64 bytes).

**domain-name** *WORD*

Sets the windows/base domain name.

**domainServer-deviceName***WORD*

Sets the domain server device name.

**no radius-encryption**

Disables the AAA server encryption.

**no ad-global-catalog**

Disables global catalog support.

**no grp-search**

Disables group attribute lookup support.

**no encryption-TLS**

Disable the TLS Encryption

**no backup**

Disables the backup function.

**ad-global-catalog**

Enables global catalog support.

**grp-search**

Enables group attribute lookup support.

**admin-dn** *WORD*

Sets the admin domain name.

**admin-password** *WORD*

Sets the admin password.

**key-attribute** *WORD*

Sets the LDAP key attribute.

**search-filter** *WORD*

Sets the LDAP search filter.



**radius-secret** *WORD*

Sets the AAA server's shared secret.

**tacplus-secret** *WORD*

Sets the TACPLUS server's shared secret.

**encryption-TLS**

Enables the TLS Encryption

**backup**

Enables the backup function.

**backup-ip-addr** *IP-ADDR*

Sets the backup AAA server's IP/IPv6 address.

**backup-port** *PORT-NUM*

Sets the backup AAA server's port.

**backup-radius-secret** *WORD*

Sets the backup AAA server's shared secret.

**request-timeout** *NUMBER*

Sets the failover request timeout (2~20 seconds).

**retry-count** *NUMBER*

Sets the failover retry count (2~10 times).

**consecutive-drop-packet** *NUMBER*

Sets the number of consecutive dropped packet (range:1~10 , default is 1).

**reconnect-primary-interval** *NUMBER*

Sets the failover re-connect to primary interval (1~86400 minutes).

**Example**

```
ruckus(config)# aaa activedir
The AAA server 'activedir' has been created. To save the AAA server, type 'end' or 'exit'.
ruckus(config-aaa)# type ad
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-aaa)# ip-addr 192.168.10.40
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-aaa)# show
AAA:
  ID:
  :
  Name= activedir
  Type= Active Directory
  IP Address= 192.168.10.40
  Port= 389
  Windows Domain Name=
  Global Catalog= Disabled
  Admin DN=
  Admin Password=
  Group Search= Enabled
  encryption-TLS = Disabled

ruckus(config-aaa)# end
The AAA server 'activedir' has been updated and saved.
Your changes have been saved.
ruckus(config)#
```

# Configure DHCP Server Commands

This section describes the commands that you can use to configure DHCP server entries on the controller. These DHCP server entries are used by the DHCP Relay feature, if enabled for a tunneled WLAN. The following commands can be executed from within the **config-dhcp** context.

## dhcp

Use the **dhcp** command from within the **config** context to create or edit a DHCP server entry.

**dhcp** *WORD*

### Syntax Description

**dhcp**

Configure the DHCP server settings

*WORD*

Name of the DHCP server entry

### Defaults

none

### Example

```
ruckus(config)# dhcp dhcp_server_2
The DHCP server 'dhcp_server_2' has been created. To save the DHCP server, type 'end' or 'exit'.
ruckus(config-dhcp)# first 192.168.11.99
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-dhcp)# show
DHCP servers for DHCP relay agent:
  ID:
  :
  Name= dhcp_server_2
  Description=
  IP Address= 192.168.11.99
ruckus(config-dhcp)# end
The DHCP server 'dhcp_server_2' has been updated and saved.
Your changes have been saved.
ruckus(config)# show dhcp
DHCP servers for DHCP relay agent:
  ID:
  1:
  Name= DHCP Server 1
  Description=
  IP Address= 192.168.11.1
  IP Address=
  2:
  Name= dhcp_server_2
  Description=
  IP Address= 192.168.11.99
  IP Address=
ruckus(config)#
```

## no dhcp

Use the **no dhcp** command to delete a DHCP server entry.

**no dhcp** *WORD*

### Example

```
ruckus(config)# no dhcp dhcp_server_2  
The DHCP server 'dhcp_server_2' has been deleted.  
ruckus(config)#
```

## show

Displays a list of available DHCP servers.

**show**

## name

Sets the DHCP server name.

**name** *WORD*

## description

Sets the DHCP server description.

**description** *WORD*

## first

Sets the DHCP server's first IP address.

**first** *IP-ADDR*

## second

Sets the DHCP server's second IP address.

**second** *IP-ADDR*

## no second

Deletes the DHCP server's second IP address.

**no second** *IP-ADDR*

# Configure Admin Commands

Use the admin commands to enter the **config-admin** context to set the admin user name, password and admin authentication server settings.

## admin

To enter the config-admin context and configure administrator preference, use the following command:

**admin**

### Example

```
ruckus(config)# admin
ruckus(config-admin)
```

## name

To set the administrator user name, use the following command:

**name** *WORD*

### Syntax Description

**name**

Configure the admin name setting

*WORD*

Set the admin name to this name

### Defaults

admin

### Example

```
ruckus(config)# admin
ruckus(config-admin)# name admin
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-admin)# end
The administrator preferences have been updated.
Your changes have been saved.
ruckus(config)#
```

## name password

To set the admin name and password at the same time, use the following command:

**name** *WORD* password *WORD*

## Syntax Description

### **name**

Configure the admin name setting

### *WORD*

Set the admin name to this name

### **password**

Configure the admin password

### *WORD*

Set the admin password to this password

## Defaults

admin

## Example

```
ruckus(config)# admin
ruckus(config-admin)# name admin password admin
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-admin)# end
The administrator preferences have been updated.
Your changes have been saved.
ruckus(config)#
```

## show

To view the current admin login and authentication settings, use the following command:

**show**

### Example

```
ruckus(config-admin)# show
Administrator Name/Password:
  Name= admin
  Password= *****
  Authenticate:
    Mode= Authenticate using the admin name and password

ruckus(config-admin)#
```

# Configure Access Points Commands

The following commands can be used from within the config-ap context to configure a specific Access Point.

## ap

To enter the config-ap context, enter the following command:

```
ap MAC
```

### Syntax Description

<b>ap</b>	Access Point
<i>MAC</i>	MAC address of the access point for configuration

### Defaults

None.

### Example

```
ruckus(config)# ap 04:4f:aa:0c:b1:00  
The AP '04:4f:aa:0c:b1:00' has been loaded. To save the AP, type 'end' or 'exit' .  
ruckus(config-ap)#
```

## no ap

To delete an AP from the list of approved devices, use the following command:

```
no ap MAC
```

### Syntax Description

<b>no ap</b>	Delete Access Point
<i>MAC</i>	MAC address of the access point

### Defaults

None.

### Example

```
ruckus(config)# no ap 04:4f:aa:0c:b1:00  
The AP '04:4f:aa:0c:b1:00' has been deleted.  
ruckus(config)#
```

## devname

To set the device name, use the following command:

**devname** *WORD*

### Syntax Description

**devname**

Device name

*WORD*

Set the device name to this name

### Defaults

None.

### Example

```
ruckus(config)# ap 04:4f:aa:0c:b1:00
The AP '04:4f:aa:0c:b1:00' has been loaded. To save the AP, type 'end' or 'exit'.
ruckus(config-ap)# devname 7962
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-ap)# end
The device information has been updated.
Your changes have been saved.
ruckus(config)#
```

## no devname

To delete the device's name, use the following command:

**no devname**

## bonjour-gateway

To bind a bonjour gateway policy to this AP, use the following command:

**bonjour-gateway** *WORD*

### Example

```
ruckus(config-ap)# bonjour-gateway bonjour1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-ap)#
```

## no bonjour-gateway

To unbind a bonjour gateway policy, use the following command:

**no bonjour-gateway**



## Example

```
ruckus(config-ap)# no bonjour-gateway
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-ap)#
```

## description

To set the device description, use the following command:

**description** *WORD*

### Syntax Description

**description**

Device description

*WORD*

Set the device description to this text

## Defaults

None.

## Example

```
ruckus(config-ap-00:13:92:00:33:1C)# description this-is-the-device-description
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-ap)#
```

## no description

To delete the device's description, use the following command:

**no description**

## gps

To set the device GPS coordinates, use the following command:

**gps** *GPS-COORDINATE*

### Syntax Description

**gps**

Set the device GPS coordinates

*GPS-COORDINATE*

Enter the device's GPS coordinates for the latitude and longitude. Use a comma (,) to separate the latitude and longitude. The first coordinate is for the latitude. The second coordinate is for the longitude. Ex. A,B or -37,38.

## Defaults

None.

## Example

```
ruckus(config-ap)# gps 37.3,-122
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-ap)#
```

## no gps

To delete the device's GPS coordinates, use the following command:

**no gps**

## location

To set the device location, use the following command:

**location** *WORD*

## Syntax Description

### **location**

Device location

### *WORD*

Set the device location to this address

## Defaults

None.

## Example

```
ruckus(config-ap)# location sunnyvale-office
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-ap)#
```

## no location

To delete the device's location, use the following command:

**no location**

## group

To set the AP group for this AP, use the following command:

**group** [name *WORD*] | system-default]

## Syntax Description

- group**  
Set the AP group that this AP is a member of
- name**  
Set the AP to be a member of the named AP group
- WORD*  
The name of the AP group
- system-default**  
Set the AP as a member of the system default AP group

## Defaults

system-default

## Example

```
ruckus(config-ap)# group system-default  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-ap)#
```

## ip

To set the AP's IPv4 address, use the following command from within the config-ap context:

**ip** [enable | disable] addr *IP-ADDR NET-MASK* name-server *DNS-ADDR* mode [dhcp | static | keep]

## Syntax Description

- ip**  
Set the AP's IPv4 addressing
- enable**  
Enable IPv4 addressing
- disable**  
Disable IPv4 addressing
- addr**  
Set the AP's IPv4 address
- IP-ADDR*  
The IPv4 address
- NET-MASK*  
The IPv4 netmask
- name-server**  
Set the device's DNS servers. Use a space ( ) to separate primary and secondary DNS servers
- DNS-ADDR*  
The IP address of the DNS server

<b>mode</b>	Set the device's IP addressing mode (DHCP, static or "keep AP's setting")
<b>dhcp</b>	Set the device's IP address mode to DHCP
<b>static</b>	Set the device's IP address mode to static
<b>keep</b>	Set the device to use its current network settings

## Defaults

none

## Example

```
ruckus(config-ap)# ip enable mode dhcp
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-ap)#
```

## ipv6

To set the AP's IPv6 address, use the following command from within the config-ap context:

```
ipv6 [ enable ] addr IPv6-ADDR IPv6-PREFIX-LENGTH name-server DNS-ADDR mode [ auto | manual | keep ]
```

## Syntax Description

<b>ipv6</b>	Set the AP's IPv6 addressing
<b>enable</b>	Enable IPv6 addressing
<b>addr</b>	Set the AP's IPv6 address
<i>IPv6-ADDR</i>	The IPv6 address
<i>IPv6-PREFIX-LENGTH</i>	The IPv6 prefix length. Use a space ( ) to separate the IPv6 address and prefix length
<b>name-server</b>	Set the device's DNS servers. Use a space ( ) to separate primary and secondary DNS servers
<i>DNS-ADDR</i> [ <i>DNS-ADDR</i> ]	The IP address of the DNS server
<b>mode</b>	Set the device's IP addressing mode (auto, manual or "keep AP's setting")
<b>auto</b>	Set the device's IPv6 address mode to auto

**manual**

Set the device's IPv6 address mode to manual

**keep**

Set the device to use its current network settings

**Defaults**

none

**Example**

```
ruckus(config-ap)# ipv6 enable mode auto  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-ap)#
```

**no ipv6**

To disable the AP's IPv6 mode, use the following command:

**no ipv6**

# Radio 2.4/5 GHz Commands

Use the radio 2.4 or radio 5 commands to configure the 2.4/5 GHz radio settings independently.

## radio

Use the radio command from within the config-ap context to configure the 2.4GHz or 5GHz radios independently.

**radio** [ **2.4** | **5** ] *arguments*

### Syntax Description

#### 2.4

Configure the 2.4 GHz radio

#### 5

Configure the 5 GHz radio

**channelization** [ **auto** | *NUMBER* ]

Set channel width to 20 MHz, 40 MHz or Auto

**channel** [ **auto** | *NUMBER* ]

Set channel to Auto or manually set channel

**tx-power** [ **auto** | **full** | **min** | **num** *1-10* ]

Set transmit power to auto, full, min, or a number (-1dB~-10dB)

**admission-control** *VALUE*

Set the radio to use the specified call admission control airtime usage limit (%)

**channel-range** *NUMBER-LIST*

Set the allowed list of channels for the specified radio

**wlan-group** *WORD*

Set the AP radio as a member of a WLAN group

**wlan-service** [ **enable** | **disable** ]

Enable WLAN service on this radio

**wlan-service-override**

Enable the override of the WLAN service settings for this radio

**extant-gain** *NUMBER*

Set external antenna gain (on APs that support external antennas) (dBi)

### Defaults

channelization: Auto

channel: Auto

wlan-group: Default

wlan-service: Enabled

wlan-service-override: Disabled

tx-power: Auto

admission-control: Disabled  
spectralink-compatibility: Disabled

### Example

```
ruckus(config-ap)# radio 2.4 channelization auto
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-ap)# radio 2.4 channel auto
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-ap)# radio 2.4 wlan-group Default
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-ap)# radio 2.4 wlan-service
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-ap)# radio 2.4 tx-power auto
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-ap)# end
The device information has been updated.
Your changes have been saved.
ruckus(config)#
```

## no radio

Use the no radio 2.4 or no radio 5 commands from within the config-ap context to disable AP group overrides for the 2.4GHz or 5GHz radio settings.

**no radio** [ 2.4 | 5 ] *arguments*

### Syntax Description

#### **no radio**

Disable override of 2.4/5GHz radio settings

#### **2.4**

Disable 2.4GHz radio override settings

#### **5**

Disable 5GHz radio override settings

#### **wlan-service**

Disable override of WLAN service settings

#### **channel-range-override**

Disables override of channel range settings

#### **channel-override**

Disables override of channel settings

#### **channelization-override**

Disables override of 5GHz channelization settings

#### **tx-power-override**

Disables override of Tx power

#### **wlan-group-override**

Disables override of WLAN group settings

#### **admission-control**

Disables call admission control on the radio

**admission-control-override**

Disables override of call admission control settings

**wlan-service**

Disables WLAN service for the radio

**wlan-service-override**

Disables the override of the WLAN service settings for this radio.

**channel-range-override**

Disables override of channel range settings

**Example**

```
ruckus(config-ap)# no radio 2.4 tx-power-override  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-ap)#
```

## mesh mode

Use the mesh mode command from within the config-ap context to configure the AP's mesh mode settings.

**mesh mode [ auto | root-ap | mesh-ap | disable ]**

### Syntax Description

**mesh mode**

Configure the AP's mesh mode

**auto**

Set mesh mode to Auto

**root-ap**

Configure AP as a Root AP

**mesh-ap**

Configure AP as a Mesh AP

**disable**

Disable mesh

### Defaults

Auto.

### Example

```
ruckus(config-ap)# mesh mode auto  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-ap)#
```



## mesh uplink-selection

Use the mesh uplink-selection command from within the config-ap context to configure the AP's mesh uplink selection settings.

**mesh uplink-selection** [auto | manual ] *add-mac* | *del-mac* *MAC*

### Syntax Description

#### **mesh uplink-selection**

Configure the AP's mesh uplink selection mode

#### **auto**

Set mesh uplink selection to Auto

#### **manual**

Set mesh uplink selection to manual

#### **add-mac**

Add a manual uplink selection AP

#### **del-mac**

Delete a manual uplink selection AP

#### *MAC*

The MAC address of the uplink AP

### Defaults

Auto.

### Examples

```
ruckus(config-ap)# mesh uplink-selection manual add-mac 00:24:82:3f:14:60
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-ap)#
```

```
ruckus(config-ap)# mesh uplink-selection auto
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-ap)#
```

## status-leds

To enable or disable the AP's status LEDs, use the following command:

**status-leds** [enable | disable ]

### Defaults

Enabled.

### Syntax Description

#### **status-leds**

Configure status LEDs

**enable**

Override group config, enable status LEDs

**disable**

Override group config, disable status LEDs

**Example**

```
ruckus(config-ap)# status-leds disable  
ruckus(config-ap)#
```

## no status-leds-override

To disable override of status LEDs for this AP, use the following command:

**no status-leds-override**

## usb-port

To disable the override the group configuration and enable/disable the USB port for this AP, use the following command:

**usb-port [ enable | disable ]**

## no usb-port-override

To disable the override of the USB port for the specified AP model, use the following command:

**no usb-port-override**

## poe-out

To enable or disable the AP's PoE Out port, use the following command:

**poe-out [ enable | disable ]**

## Defaults

Disabled.

## Syntax Description

**poe-out**

Configure PoE Out port

**enable**

Override group config, enable PoE Out port

**disable**

Override group config, disable PoE Out port

## Example

```
ruckus(config-ap) # poe-out enable  
ruckus(config-ap) #
```

## no poe-out-override

To disable override of the PoE out port settings, use the following command:

```
no poe-out-override
```

## no usb-software-override

To disable the override of the AP USB software package, use the following command:

```
no usb-software-override
```

## external-antenna

To configure the AP's external antenna settings, use the following command:

```
external-antenna [ 2.4G | 5G ] [ enable | disable ] [ gain NUMBER ] cable-loss NUMBER [ 2-antennas | 3-antennas ]
```

## Syntax Description

### **2.4G**

Configure external 2.4GHz antenna

### **5G**

Configure external 5GHz antenna

### **enable** | **disable**

Enable/disable external antenna

### **gain**

Set external antenna gain for 2.4/5GHz radio

### **cable-loss** *NUMBER*

Enter the external antenna loss (0-90 dB)

### **2-antennas**

Select two external antennas for the specified radio

### **3-antennas**

Select three external antennas for the specified radio

## Defaults

Varies by AP model.

## no external-antenna-override

To disable the external antenna override settings, use the following command:

**no external-antenna-override**

## spectra-analysis 2.4GHz

To enable or disable the spectrum analysis feature for this radio, use the following command:

**spectra-analysis 2.4GHz [ enable | disable ]**

## spectra-analysis 5GHz

To enable or disable the spectrum analysis feature for this radio, use the following command:

**spectra-analysis 5GHz [ enable | disable ]**

## internal-heater

To enable or disable the AP's internal heater, use the following command:

**internal-heater [ enable | disable ]**

### Defaults

Disabled.

### Syntax Description

#### **internal-heater**

Configure internal heater

#### **enable**

Override group config, enable internal heater

#### **disable**

Override group config, disable internal heater

### Example

```
ruckus(config-ap)# internal-heater enable  
ruckus(config-ap)#
```

## no internal-heater-override

To disable override of the internal heater for this AP, use the following command:

**no internal-heater-override**

## cband-channels

To enable or disable the 5.8 GHz C-band channels, use the following command:

**cband-channels [ enable | disable ]**

## Defaults

Disabled.

## Syntax Description

### **cband-channels**

Configure C-band channels

### **enable**

Override group config, enable C-band channels

### **disable**

Override group config, disable C-band channels

## Example

```
ruckus(config-ap) # cband-channels enable  
ruckus(config-ap) #
```

## no cband-channels-override

To disable override of the 5.8 GHz channels, use the following command:

**no cband-channels-override**

## usb-software

To set the AP USB software package vendor ID (VID) and product ID (PID), and version, use the following command:

**usb-software** *VID-PID-VERSION*

## no usb-software

To delete a USB software package from the list of USB software packages, use the following command:

**no usb-software**

## ipmode

To set the AP's IP mode, use the following command:

**ipmode** *WORD*

## Defaults

Dual-stack IPv4/IPv6 mode

## Syntax Description

### **ipmode**

Configure IP addressing mode

<b>ipv4</b>	Set to IPv4 only mode
<b>ipv6</b>	Set to IPv6 only mode
<b>dual</b>	Set to dual-stack IPv4/IPv6 mode

### Example

```
ruckus(config-ap)# ipmode dual  
ruckus(config-ap)#
```

## no ipmode-override

To disable override of the IP mode, use the following command:

**no ipmode-override**

## radio-band

To set the radio band of the AP, use the following command:

**radio-band** *WORD*

### Syntax Description

<b>radio-band</b>	Configure radio band mode
<i>WORD</i>	Set to 2.4 or 5 GHz radio mode

### Usage Guidelines

This command is available only on APs that support band switching between 2.4GHz and 5GHz radio band modes.

### Example

```
ruckus(config-ap)# radio-band 5  
Your changes have been saved.  
ruckus(config-ap)#
```

## no radio-band-override

To disable the AP radio band override, use the following command:

**no radio-band-override**

## venue-name

To set the venue name of the AP, use the following command:

**venue-name** [ **language** ] *WORD*

### Syntax Description

**venue-name**

Set the venue name for the AP

[ **language** ]

Set the language of the venue name. Valid languages are: English, Chinese, Czech, Danish, Dutch, French, German, Japanese, Spanish, Swedish, Turkish)

*WORD*

Set the venue name to the name specified

### Example

```
ruckus(config-ap)# venue-name english venue1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-ap)#
```

## no venue-name

To remove a venue name entry, use the following command:

**no venue-name** [ **language** ]

### Example

```
ruckus(config-ap)# no venue-name english
The entry 'English' has been removed. To save the changes, type 'end' or 'exit'.
ruckus(config-ap)#
```

## Ildp

To enable, disable or configure the AP's Link Layer Discover Protocol settings, use the following Ildp commands from within the config-ap context.

### Syntax Description

**Ildp**

Configure LLDP settings.

**enable**

Enable LLDP with current settings.

**disable**

Disable LLDP with current settings.

**interval** *NUMBER*

Set packet transmit interval in second(s).

**holdtime** *NUMBER*

Set amount of time receiving device should retain the information.

**ifname eth** *NUMBER*

Enter the AP port number.

**mgmt enable**

Enable LLDP management IP address of the AP.

**mgmt disable**

Disable LLDP management IP address of the AP.

### Example

```
ruckus(config-ap)# lldp enable  
ruckus(config-ap)#
```

## no lldp-override

To disable the AP's LLDP override settings (use parent settings), use the following command:

**no lldp-override**

### Example

```
ruckus(config-ap)# no lldp-override  
ruckus(config-ap)#
```

## power-mode

To set the PoE mode of the AP, use the following command:

**power-mode** *WORD*

### Syntax Description

**power-mode**

Set the PoE power mode.

**auto**

Set the PoE power mode to auto.

**802.3af**

Set the PoE power mode to 802.3af.

**802.3at**

Set the PoE power mode to 802.3at.

### Example

```
ruckus(config-ap)# power-mode 802.3af  
ruckus(config-ap)#
```



## no power-mode-override

To disable the override of the PoE mode, use the following command:

```
no power-mode-override
```

## 802.3af-txchain

To set the number of 2.4 GHz radio transmit chains in 802.3af PoE power mode, use the following command:

```
802.3af-txchain WORD
```

### Syntax Description

#### **802.3af-txchain**

Set the number of 2.4 GHz radio transmit chains in 802.3af power mode.

- 1** Set the number of tx chains to 1.
- 2** Set the number of tx chains to 2.
- 4** Set the number of tx chains to 4.

### Example

```
ruckus(config-ap)# 802.3af-txchain 2  
ruckus(config-ap)#
```

## no 802.3af-txchain-override

To disable the override of the 2.4GHz radio transmit chains in 802.3af PoE mode, use the following command:

```
no 802.3af-txchain-override
```

### Example

```
ruckus(config-ap)# no 802.3af-txchain-override  
ruckus(config-ap)#
```

## show

To display the AP's current configuration settings, use the following command:

```
show
```

### Example

```
ruckus(config)# ap c0:8a:de:21:a8:10  
The AP 'c0:8a:de:21:a8:10' has been loaded. To save the AP, type 'end' or 'exit'.  
ruckus(config-ap)# show  
AP:
```

## Configuring Master Settings

### Radio 2.4/5 GHz Commands

```
ID:
1:
  MAC Address= c0:8a:de:21:a8:10
  Model= zf7982
  Approved= Yes
  Device Name= RuckusAP
  Description=
  Location=
  GPS=
  CERT = Complex
  Bonjour-policy=
  Bonjour-fencing= Disabled
  Group Name= System Default
  Channel Range:
    A/N= 36,40,44,48,149,153,157,161 (Disallowed= )
    B/G/N= 1,2,3,4,5,6,7,8,9,10,11 (Disallowed= )
  Radio a/n:
    Channelization= Auto
    Channel= Auto
    WLAN Services enabled= Yes
    Tx. Power= Auto
    WLAN Group Name= Default
    Call Admission Control= OFF
    Protection Mode= Auto
  Radio b/g/n:
    Channelization= Auto
    Channel= Auto
    WLAN Services enabled= Yes
    Tx. Power= Auto
    WLAN Group Name= Default
    Call Admission Control= OFF
    Protection Mode= 2
  Override global ap-model port configuration= No
  Network Setting:
    Protocol mode= Use Parent Setting
    Device IP Settings= Keep AP's Setting
    IP Type= DHCP
    IP Address= 10.10.3.51
    Netmask= 255.255.0.0
    Gateway= 10.10.0.1
    Primary DNS Server= 10.10.0.1
    Secondary DNS Server=

    Device IPv6 Settings= Keep AP's Setting
    IPv6 Type= Auto Configuration
    IPv6 Address= fc00::1
    IPv6 Prefix Length= 7
    IPv6 Gateway=
    IPv6 Primary DNS Server=
    IPv6 Secondary DNS Server=
  Mesh:
    Status= Disabled
  LLDP:
    Status = Use Parent Setting
  Venue Name List:
  LAN Port:
    0:
      Interface= eth0
      Dot1x= None
      LogicalLink= Up
      PhysicalLink= Up 100Mbps full
      Label= 10/100/1000 PoE LAN1
    1:
      Interface= eth1
      Dot1x= None
      LogicalLink= Down
      PhysicalLink= Down
      Label= 10/100/1000 LAN2

ruckus(config-ap) #
```

# AP Port Setting Commands

To override AP group configuration settings and configure the AP's Ethernet ports individually, you must first enter the **config-ap-model** context from within the **config-ap** context.

## port-setting

Use the following command to enter the config-ap-model context and override AP group settings to configure AP ports individually:

**port-setting**

### Syntax Description

**port-setting**

Configure AP port settings

**lan** *NUMBER* {Arguments}

Configure the AP LAN port

**no lan** *NUMBER*

Disable the AP LAN port

**uplink** *WORD*

Set the AP port to use the specified type (trunk, access or general)

**untag** *NUMBER*

Set the AP port to use the specified VLAN ID(1-4094)

**member** *NUMBER*

Set the AP port to use the specified members(1-4094)

**opt82** [ **enabled** | **disabled** ]

Enable the AP port DHCP Option 82 settings

**tunnel** [ **enabled** | **disabled** ]

Enable the AP port tunnel settings

**guest-vlan** *NUMBER*

Set the AP port to use the specified guest VLAN ID(1-4094)

**dvlan** [ **enabled** | **disabled** ]

Enable the AP port dynamic VLAN settings

**no dot1x** *authsvr acctsvr mac-auth-bypass*

Disable authentication server, accounting server, or MAC auth bypass for the AP's 802.1X settings

**dot1x** *authsvr acctsvr mac-auth-bypass*

Enable authentication server, accounting server, or MAC auth bypass for the AP's 802.1X settings

**authsvr** *WORD*

Enter the RADIUS server name

**acctsvr** *WORD*

Enter the RADIUS accounting server name

### **mac-auth-bypass**

Enable MAC authentication bypass for the 802.1X-enabled port

### **dot1x supplicant [ username | password ] WORD**

Set the username/password for AP 802.1X supplicant

### **dot1x supplicant mac**

Set the username and password to use AP MAC address for AP 802.1X supplicant

## **Defaults**

Enable LAN: Yes

LAN Type: trunk

Untag ID: 1

Members: 1-4094

Guest VLAN: Disabled

Dynamic VLAN: Disabled

802.1X: disabled

DHCP opt82: Disabled

Tunnel= Disabled

MLD Snooping: Disabled

IGMP Snooping: Enabled

## **Example**

```
ruckus(config-ap)# port-setting
ruckus(config-ap-model)# lan 1 uplink trunk
ruckus(config-ap-model)# show
PORTS:
  LAN ID:
    1:
      Enable LAN = Yes
      LAN Type= trunk
      Untag ID= 1
      Members= 1-4094
      Guest VLAN=
      Enable Dynamic VLAN= Disabled
      802.1X= disabled
      DHCP opt82= Disabled
      Tunnel= Disabled
      MLD Snooping= Disabled
      IGMP Snooping= Enabled
    2:
      Enable LAN = Yes
      LAN Type= trunk
      Untag ID= 1
      Members= 1-4094
      Guest VLAN=
      Enable Dynamic VLAN= Disabled
      802.1X= disabled
      DHCP opt82= Disabled
      Tunnel= Disabled
      MLD Snooping= Disabled
      IGMP Snooping= Enabled

ruckus(config-ap-model)#
```

## abort

To exit the port-setting context without saving changes, use the abort command.

**abort**

## end

To save changes, and then exit the port-setting context, use the following command:

**end**

## exit

To save changes, and then exit the config-ap-model context, use the following command:

**exit**

## quit

To exit the config-ap-model context without saving changes, use the quit command.

**quit**

## show

To display the current port settings, use the following command:

**show**

## Example

```
ruckus(config)# ap 04:4f:ab:0c:b1:00
ruckus(config-ap)# port-setting
ruckus(config-ap-model)# show
PORTS:
  LAN ID:
    1:
      Enable LAN = Yes
      LAN Type= trunk
      Untag ID= 1
      Members= 1-4094
      Guest VLAN=
      Enable Dynamic VLAN= Disabled
      802.1X= disabled
      DHCP opt82= Disabled
      Tunnel= Disabled
      MLD Snooping= Disabled
      IGMP Snooping= Enabled
    2:
      Enable LAN = Yes
      LAN Type= trunk
      Untag ID= 1
      Members= 1-4094
      Guest VLAN=
      Enable Dynamic VLAN= Disabled
      802.1X= disabled
      DHCP opt82= Disabled
      Tunnel= Disabled
```

```
MLD Snooping= Disabled
IGMP Snooping= Enabled
ruckus (config-ap-model) #
```

## lan

To enable the LAN port, use the following command:

**lan** *NUMBER*

### Syntax Description

**lan**

Enable the LAN port

*NUMBER*

Specify the LAN port to enable

**uplink** *WORD*

Sets the AP port to use the specified type(trunk,access or general).

**untag** *NUMBER*

Sets the AP port to use the specified VLAN ID(1-4094) or none.

**member** *NUMBER*

Sets the AP port to use the specified members(1-4094).

**opt82**

Sets the AP port DHCP Option 82.

**tunnel**

Sets the AP port tunnel.

**guest-vlan** *NUMBER*

Sets the AP port to use the specified guest VLAN ID(1-4094).

**dvlan**

Sets the AP port dynamic VLAN.

**dot1x**

Sets the AP port 802.1X.

### Defaults

Enable LAN = Yes

LAN Type= trunk

Untag ID= 1

Members= 1-4094

Guest VLAN=

Enable Dynamic VLAN= Disabled

802.1X= disabled

DHCP opt82= Disabled

Tunnel= Disabled  
MLD Snooping= Disabled  
IGMP Snooping= Enabled

### Example

```
ruckus(config-ap-model) # lan 1  
ruckus(config-ap-model) #
```

## no lan

To disable the LAN port, use the following command:

**no lan** *NUMBER*

### Syntax Description

**no lan**

Disable the LAN port

*NUMBER*

Specify the LAN port to disable

### Defaults

None.

### Example

```
ruckus(config-ap-model) # no lan 1  
ruckus(config-ap-model) #
```

## lan uplink

To sets the AP port type (Trunk, Access or General), use the following command:

**lan** *NUMBER uplink WORD*

### Syntax Description

**lan uplink**

Set the LAN port type

*NUMBER*

Specify the LAN port to configure

**uplink**

Set the port type to the specified type

*WORD*

LAN port type (Trunk port, Access port, General port)

## Defaults

For all APs other than 7025/7055: Trunk

For 7025/7055 LAN 5: Trunk

For 7025/7055 LAN 1-LAN 4: Access

## Example

```
ruckus(config-ap-model)# lan 1 uplink access  
ruckus(config-ap-model)#
```

## lan untag

To set the LAN port untag VLAN ID (native VLAN, for Trunk ports), use the following command:

**lan** *NUMBER* **untag** *NUMBER*

## Syntax Description

### lan untag

Set the LAN port untag VLAN ID

*NUMBER*

Specify the LAN port to configure

*NUMBER*

Set the untag VLAN ID (1~4094)

## Defaults

1

## Example

```
ruckus(config-ap-model)# lan 1 untag 1  
ruckus(config-ap-model)#
```

## lan member

To set the LAN port VLAN membership (only General ports have configurable membership; Trunk ports are members of all VLANs, and Access port membership must be the same as the Untag VLAN), use the following command:

**lan** *NUMBER* **member** *NUMBER*

## Syntax Description

### lan member

Set the LAN port VLAN membership

*NUMBER*

Specify the LAN port to configure



*NUMBER*

Set the VLAN membership (1~4094, range separated by hyphen, multiple VLANs separated by commas)

## Defaults

1

## Example

```
ruckus(config-ap-model)# lan 2 member 1-10,100,200
ruckus(config-ap-model)# show
PORTS:
  LAN ID:
    1:
      Enable LAN = Yes
      LAN Type= trunk
      Untag ID= 1
      Members= 1-4094
      Guest VLAN=
      Enable Dynamic VLAN= Disabled
      802.1X= disabled
      DHCP opt82= Disabled
      Tunnel= Disabled
      MLD Snooping= Disabled
      IGMP Snooping= Enabled
    2:
      Enable LAN = Yes
      LAN Type= general
      Untag ID= 1
      Members= 1-10,100,200
      Guest VLAN=
      Enable Dynamic VLAN= Disabled
      802.1X= disabled
      DHCP opt82= Disabled
      Tunnel= Disabled
      MLD Snooping= Disabled
      IGMP Snooping= Enabled

ruckus(config-ap-model)#
```

## lan opt82

To enable or disable DHCP option 82 for a LAN port, use the following command:

**lan** *NUMBER* **opt82** [ **enabled** | **disabled** ]

## Syntax Description

### **opt82**

Enable or disable DHCP option 82

### **enabled**

Enable option 82

### **disabled**

Disable option 82

## Defaults

Disabled

## Example

```
ruckus(config-ap-model)# lan 1 opt82 enable
ruckus(config-ap-model)#
```

## lan tunnel

To enable or disable Ethernet port tunnel mode for the port, use the following command:

```
lan NUMBER tunnel [ enabled | disabled ]
```

## Syntax Description

### **tunnel**

Enable or disable port tunnel mode

### **enabled**

Enable tunnel mode

### **disabled**

Disable tunnel mode

## Defaults

Disabled

## Example

```
ruckus(config-ap-model)# lan 1 tunnel enable
ruckus(config-ap-model)# show
PORTS:
  LAN ID:
    1:
      Enable LAN = Yes
      LAN Type= trunk
      Untag ID= 1
      Members= 1-4094
      Guest VLAN=
      Enable Dynamic VLAN= Disabled
      802.1X= disabled
      DHCP opt82= Disabled
      Tunnel= Enabled
      MLD Snooping= Disabled
      IGMP Snooping= Enabled
    2:
      Enable LAN = Yes
      LAN Type= trunk
      Untag ID= 1
      Members= 1-4094
      Guest VLAN=
      Enable Dynamic VLAN= Disabled
      802.1X= disabled
      DHCP opt82= Disabled
      Tunnel= Disabled
      MLD Snooping= Disabled
      IGMP Snooping= Enabled

ruckus(config-ap-model)#
```

## lan guest-vlan

To set the AP port to use the specified Guest VLAN ID, use the following command:

```
lan NUMBER guest-vlan NUMBER
```

## lan dvlan enabled

To enable dynamic VLAN for the port, use the following command:

```
lan NUMBER dvlan enabled
```

## lan dvlan disabled

To disable dynamic VLAN for the port, use the following command:

```
lan NUMBER dvlan disabled
```

## lan dot1x

To configure 802.1X settings for a LAN port, use the following command:

```
lan NUMBER dot1x [ disabled | supplicant | auth-port-based | auth-mac-based ]
```

### Syntax Description

#### lan dot1x

Configure 802.1X settings for this port

#### NUMBER

LAN port number to configure

#### disabled

Disable 802.1X

#### supplicant

Configure this LAN port as an 802.1X supplicant

#### supplicant username WORD

Set the username for AP 802.1X supplicant

#### supplicant password WORD

Set the password for AP 802.1X supplicant

#### supplicant mac

Set the username and password to use AP MAC address for AP 802.1X supplicant

#### auth-port-based

Configure this LAN port as an 802.1X authenticator (port-based)

#### auth-mac-based

Configure this LAN port as an 802.1X authenticator (MAC-based)

## Defaults

Disabled

## Example

```
ruckus(config-ap-model)# lan 1 dot1x supplicant  
ruckus(config-ap-model)#
```

## dot1x authsvr

To configure the 802.1X authentication server for the AP, use the following command:

**dot1x authsvr** *WORD*

### Syntax Description

#### **dot1x authsvr**

Configure 802.1X authentication server

*WORD*

Name of AAA server

## Defaults

None

## Example

```
ruckus(config-ap-model)# dot1x authsvr radius  
ruckus(config-ap-model)#
```

## dot1x acctsvr

To configure the 802.1X accounting server for the AP, use the following command:

**dot1x acctsvr** *WORD*

### Syntax Description

#### **dot1x acctsvr**

Configure 802.1X accounting server

*WORD*

Name of AAA server

## Defaults

None

### Example

```
ruckus(config-ap-model)# dot1x acctsvr radius-acct  
ruckus(config-ap-model)#
```

## dot1x mac-auth-bypass

To configure 802.1X MAC authentication bypass, use the following command:

**dot1x mac-auth-bypass**

### Syntax Description

**dot1x mac-auth-bypass**

Enable 802.1X MAC authentication bypass

### Defaults

Disabled

### Example

```
ruckus(config-ap-model)# dot1x mac-auth-bypass  
ruckus(config-ap-model)#
```

## dot1x supplicant username

To configure 802.1X supplicant user name, use the following command:

**dot1x supplicant username** *WORD*

### Syntax Description

**dot1x supplicant username**

Configure 802.1X supplicant user name

*WORD*

Set the 802.1X supplicant user name

### Defaults

None

### Example

```
ruckus(config-ap-model)# dot1x supplicant username johndoe  
ruckus(config-ap-model)#
```

## dot1x supplicant password

To configure 802.1X supplicant password, use the following command:

**dot1x supplicant password** *WORD*

### **Syntax Description**

**dot1x supplicant password**  
Configure 802.1X supplicant password

*WORD*  
Set the 802.1X supplicant password

### **Defaults**

None

### **Example**

```
ruckus(config-ap-model)# dot1x supplicant password test123  
ruckus(config-ap-model)#
```

## **dot1x supplicant mac**

To set the 802.1X supplicant user name and password as the AP's MAC address, use the following command:

**dot1x supplicant mac**

### **Syntax Description**

**dot1x supplicant mac**  
Set the supplicant user name and password as the AP's MAC address

### **Defaults**

None

### **Example**

```
ruckus(config-ap-model)# dot1x supplicant mac  
ruckus(config-ap-model)#
```

# Configure AP Group Commands

This section describes the commands that you can use to configure AP groups on the controller. The following commands can be executed from within the **config-apgrp** context. To show a list of commands available from within the context, type **help** or **?**.

## ap-group

To create a new AP group or configure an existing AP group and enter the config-apgrp context, enter the following command:

```
ap-group WORD
```

### Syntax Description

<b>ap-group</b>	Configure an AP group
WORD	Name of the AP group

### Defaults

"System Default"

### Example

```
ruckus(config)# ap-group "System Default"  
The AP group entry 'System Default' has been loaded. To save the AP group, type 'end' or 'exit'.  
ruckus(config-apgrp)#
```

## no ap-group

To delete an AP group from the list, enter the following command:

```
no ap-group WORD
```

### Syntax Description

<b>no ap-group</b>	Delete an AP group
WORD	Name of the AP group

### Defaults

None

## Configuring Master Settings

### Configure AP Group Commands

#### **Example**

```
ruckus(config)# no ap-group apgrp2  
The AP Group 'apgrp2' has been removed.  
ruckus(config)#
```



# Configure Hotspot Redirect Settings

To configure Hotspot redirect settings, use the following command:

## hotspot\_redirect\_https

To enable Hotspot redirect, use the following command:

```
hotspot_redirect_https
```

### Defaults

None.

### Example

```
ruckus(config)# hotspot_redirect_https  
/bin/hotspot_redirect_https enable  
ruckus(config)#
```

## no hotspot\_redirect\_https

To disable Hotspot redirect, use the following command:

```
no hotspot_redirect_https
```

### Defaults

None.

### Example

```
ruckus(config)# no hotspot_redirect_https  
/bin/hotspot_redirect_https disable  
ruckus(config)#
```

## no blocked-client

To remove a blocked client from the blocked clients list, use the following command:

```
no blocked-client MAC
```

### Defaults

None.

### Example

```
ruckus(config)# no blocked-client dc:2b:61:13:f7:72  
The L2 ACL 'dc:2b:61:13:f7:72' has been deleted.  
ruckus(config)#
```

# Configure Layer 2 Access Control Commands

Use the layer2 access control commands to configure the Layer 2 Access Control List settings. To run these commands, you must first enter the **config-l2acl** context.

## acl

To create a new L2 ACL entry or update an existing entry, use the following command:

**acl** *WORD*

### Syntax Description

**acl**

Create a new ACL

*WORD*

Assign this name to the new ACL

### Defaults

None.

### Example

```
ruckus(config)# l2acl l2acl1
The L2 ACL entry 'l2acl1' has been created.
ruckus(config-l2acl)#
```

## no acl

To delete an L2 ACL, use the following command:

**no acl** *WORD*

### Syntax Description

**no acl**

Delete an existing ACL

*WORD*

Delete this ACL

### Defaults

None.

### Example

```
ruckus(config)# no l2acl l2acl1
The L2 ACL 'l2acl1' has been deleted.
ruckus(config)#
```

## abort

To exit the config-l2acl context without saving changes, use the following command:

**abort**

## end

To save changes, and then exit the config-l2acl context, use the following command:

**end**

### Example

```
ruckus(config-l2acl)# end
The L2 ACL entry has saved successfully.
Your changes have been saved.
ruckus(config)#
```

## exit

To save changes, and then exit the config-l2acl context, use the following command:

**exit**

### Example

```
ruckus(config-l2acl)# exit
The L2 ACL entry has saved successfully.
Your changes have been saved.
ruckus(config)#
```

## quit

To exit the config-l2acl context without saving changes, use the following command:

**quit**

### Example

```
ruckus(config-l2acl)# quit
No changes have been saved.
ruckus(config)#
```

## show

To displays the L2 ACL settings, use the show command. You must run this command from within the config-l2acl context.

**show**

## Example

```
ruckus(config-l2acl)# show
L2/MAC ACL:
  ID:
  :
  Name= l2acl1
  Description=
  Restriction= Deny only the stations listed below
  Stations:
    MAC Address= 00:11:22:33:44:55

ruckus(config-l2acl)#
```

## name

To rename an L2 ACL entry, use the following command:

**name** *WORD*

## Syntax Description

### **name**

Sets the L2 ACL entry name.

### *WORD*

Rename the ACL to this name.

## Defaults

None.

## Example

```
ruckus(config)# l2acl l2acl1
The L2 ACL entry 'l2acl1' has been created.
ruckus(config-l2acl)# name L2-ACL-1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-l2acl)#
```

## description

To set the description of an L2 ACL entry, use the following command (multiple word text must be enclosed in quotation marks):

**description** *WORD*

## Syntax Description

### **description** *WORD*

Set the L2 ACL description.

## Defaults

None.

## Example

```
ruckus(config)# l2acl l2acl1
The L2 ACL entry 'l2acl1' has been created.
ruckus(config-l2acl)# description "L2 ACL 1"
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-l2acl)#
```

## add-mac

To add a MAC address to the L2 ACL, use the following command:

```
add-mac MAC
```

## Syntax Description

### **add mac**

Add a MAC address to the ACL

MAC

Add this MAC address

## Defaults

None.

## Example

```
ruckus(config-l2acl)# add-mac 00:11:22:33:44:55
The station '00:11:22:33:44:55' has been added to the ACL.
ruckus(config-l2acl)#
```

## 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-l2acl)# mode allow
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-l2acl)#
```

## mode deny

To set the ACL mode to 'deny', use the following command:

```
mode deny
```

### Syntax Description

```
mode deny
```

Set the ACL mode to deny

### Defaults

None.

### Example

```
ruckus(config-l2acl)# mode deny  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-l2acl)#
```

## del-mac

To delete a MAC address from an L2 ACL, use the following command:

```
del-mac MAC
```

### Syntax Description

```
del-mac
```

Delete a MAC address from the ACL

```
MAC
```

**Delete this** *MAC*

### Defaults

None.

### Example

```
ruckus(config-l2-acl)# del-mac 00:01:02:34:44:55  
The station '00:01:02:34:44:55' has been removed from the ACL.  
ruckus(config-l2-acl)# del-mac 00:01:02:34:44:55  
The station '00:01:02:34:44:55' could not be found. Please check the spelling, and then try again.
```

# Configure Layer 3 Access Control Commands

Use the **I3acl** commands to configure the Layer 3 Access Control List settings. To run these commands, you must first enter the **config-I3acl** or **config-I3acl-ipv6** context.

## I3acl

To enter the config-I3acl context, run this command:

```
I3acl WORD
```

### Syntax Description

**I3acl**

Create or configure a Layer 3 Access Control List

WORD

Name of the L3 ACL

### Defaults

None.

### Example

```
ruckus(config)# l3acl "ACL 1"  
The L3/L4/IP ACL entry 'ACL 1' has been created.  
ruckus(config-l3acl)#
```

## no I3acl

To delete an L3/L4 ACL entry, use the following command:

```
no I3acl WORD
```

### Syntax Description

**no I3acl**

Delete a Layer 3 ACL

WORD

Name of the L3 ACL

### Defaults

None.

### Example

```
ruckus(config)# no l3acl "ACL test"  
The L3/L4/IP ACL 'ACL test' has been deleted.  
ruckus(config)#
```

## I3acl-ipv6

To enter the config-l3acl-ipv6 context, run this command:

```
I3acl-ipv6 WORD
```

### Syntax Description

#### **I3acl-ipv6**

Create or configure a Layer 3 Access Control List

WORD

Name of the L3 ACL

### Defaults

None.

### Example

```
ruckus(config)# l3acl-ipv6 "ACL 2"  
The L3/L4/IPv6 ACL entry 'ACL 2' has been created.  
ruckus(config-l3acl-ipv6)#
```

## no I3acl-ipv6

To disable Layer 3/4 IPv6 ACLs, use the following command:

```
no I3acl-ipv6
```

## abort

To exit the config-l3acl context without saving changes, use the following command:

```
abort
```

### Example

```
ruckus(config-l3acl)# abort  
No changes have been saved.  
ruckus(config)#
```

## end

To save changes, and then exit the config-l3acl context, use the following command:

```
end
```

### Example

```
ruckus(config-l3acl)# end  
The L3/L4/IP ACL entry has saved successfully.  
Your changes have been saved.  
ruckus(config)#
```



## exit

To save changes, and then exit the config-l3acl context, use the following command:

**exit**

### Example

```
ruckus# config-l3acl
ruckus(config-l3acl)# exit
Your changes have been saved.
```

## quit

To exit the config-l3acl context without saving changes, use the following command:

**quit**

### Example

```
ruckus(config-l3acl)# quit
No changes have been saved.
ruckus(config)#
```

## show

To display the L3ACL settings, use the show command. You must run this command from within the config-l3acl context.

**show**

### Example

```
ruckus(config-l3acl)# show
L3/L4/IP ACL:
ID:
3:
Name= test_newname
Description= justfortestCLI
Default Action if no rule is matched= Deny all by default
Rules:
Order= 1
Description=
Type= Allow
Destination Address= Any
Destination Port= 53
Protocol= Any
Order= 2
Description=
Type= Allow
Destination Address= Any
Destination Port= 67
Protocol= Any
```

## name

To set the name of an L3/L4/IP ACL entry, use the following command:

**name WORD**

## Syntax Description

**name**  
Set the name of an L3/L4/IP ACL entry

**WORD**  
Name of the L3/L4/IP ACL entry

## Defaults

None.

## Example

```
ruckus(config-l3acl)# name test_newname  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## description

To set the description of an L3/L4/IP ACL entry, use the following command (multiple word text must be enclosed in quotes):

**description WORD**

## Syntax Description

**description**  
Set the L3/L4/IP ACL entry description

**WORD**  
Set to this description

## Defaults

None.

## Example

```
ruckus(config-l3acl)# description justfortestCLI  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## mode allow

To set the ACL mode to 'allow', use the following command:

**mode allow**

## Syntax Description

**mode**  
Set the ACL mode

### **allow**

Set the mode to 'allow'

### **Defaults**

None.

### **Example**

```
ruckus(config-l3acl)# mode allow  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## **mode deny**

To set the ACL mode to 'deny', use the following command:

**mode deny**

### **Syntax Description**

#### **mode**

Set the ACL mode

#### **deny**

Set the mode to 'deny'

### **Defaults**

None.

### **Example**

```
ruckus(config-l3acl)# mode deny  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## **rule-order**

To create or modify a rule in the L3/L4/IP ACL, use the following command:

**rule-order** *NUMBER*

### **Syntax Description**

#### **rule-order**

Create a new rule or modify an existing one

#### *NUMBER*

Create or modify this rule ID

## **Defaults**

None.

## **Example**

For example, to set the current rule as the third ACL rule to apply, use the following command:

```
ruckus(config-l3acl)# rule-order 3  
ruckus(config-l3acl-rule)#
```

## **source address**

To set the source address of a L3/L4/IP ACL rule, use the following command:

**source address <IP-ADDR/WORD>**

## **Example**

```
ruckus(config-l3acl-rule)# source address 192.168.0.1/24  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-l3acl-rule)#
```

## source port

To set the source port of a L3/L4/IP ACL rule, use the following command:

**source port** <NUMBER/WORD>

## Example

```
ruckus(config-l3acl-rule)# source port 880  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-l3acl-rule)#
```

## no rule-order

To delete a rule from the L3/L4/IP ACL, use the following command:

**no rule-order** NUMBER

## Syntax Description

### no rule-order

Delete a rule from the L3/L4/IP ACL

### NUMBER

Delete this rule ID

## Defaults

None.

## Example

```
ruckus(config-l3acl)# no rule-order 3  
The rule '3' has been removed from the ACL.
```

# Layer 3 Access Control Rule Commands

Use the **l3acl-rule** commands to configure the Layer 3/Layer 4/IP Access Control List rules. To run these commands, you must first enter the **config-l3acl-rule** context. To enter the **config-l3acl-rule** context, run this command:

**rule-order** *NUMBER*

## end

To save changes, and then exit the config-l3acl-rule context, use the following command:

**end**

## exit

To save changes, and then exit the config-l3acl-rule context, use the following command:

**exit**

## order

To set the L3/L4/IP ACL rule order, use the following command:

**order** *NUMBER*

## Example

```
ruckus(config-l3acl-rule)# order 1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-l3acl-rule)#
```

## description

To set the description of an L3/L4/IP ACL rule, use the following command (multiple word text must be enclosed in quotes):

**description** *WORD*

## Syntax Description

### **description**

Set the L3/L4/IP ACL rule description

*WORD*

Set to this description

## Defaults

None.

### Example

```
ruckus(config-l3acl-rule)# description thirdl3rule  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## type allow

To set the ACL rule type to 'allow', use the following command:

```
type allow
```

### Syntax Description

**type**

Set the ACL rule type

**allow**

Set the rule type to 'allow'

### Defaults

None.

### Example

```
ruckus(config-l3acl-rule)# type allow  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## type deny

To set the ACL rule type to 'deny', use the following command:

```
type deny
```

### Syntax Description

**type**

Set the ACL rule type

**deny**

Set the rule type to 'deny'

### Defaults

None.

### Example

```
ruckus(config-l3acl-rule)# type deny  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```



## destination address

To set the destination address of the rule, use the following command:

**destination address** *IP-ADDR/WORD*

### Syntax Description

**destination address**

Set the destination address of the rule

*IP-ADDR/WORD*

Set the destination to this IP address

### Defaults

None.

### Example

```
ruckus(config-l3acl-rule)# destination address 192.168.1.22
The destination IP address is invalid. Please enter 'Any' or check the IP address(for example:
192.168.0.1/24), and then please try again.
ruckus(config-l3acl-rule)# destination address 192.168.1.22/24
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## destination port

To set the destination port of the rule, use the following command:

**destination port** *NUMBER/WORD*

### Syntax Description

**destination port**

Set the destination port of the rule

*NUMBER/WORD*

Set the destination to this port number

### Defaults

None.

### Example

```
ruckus(config-l3acl-rule)# destination port 580
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## protocol

To set the protocol for the rule, use the following command:

**protocol** *NUMBER/WORD*

## Syntax Description

### **protocol**

Set the protocol for the rule

### *NUMBER/WORD*

Set to this protocol

## Defaults

None.

## Example

```
ruckus(config-l3acl-rule)# protocol tcp
The protocol must be a number between 0 and 254.
ruckus(config-l3acl-rule)# protocol Any
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## show

To display L3/L4/IP ACL settings, use the following command:

### **show**

## Example

```
ruckus(config-l3acl)# show
L3/L4/IP ACL:
  ID:
  :
  Name= l3acl1
  Description=
  Default Action if no rule is matched= Deny all by default
  Rules:
  1:
    Description=
    Type= Allow
    Destination Address= 192.168.1.22/24
    Destination Port= 53
    Protocol= Any
  2:
    Description=
    Type= Allow
    Destination Address= Any
    Destination Port= 67
    Protocol= Any

ruckus(config-l3acl)#
```

# Layer 3 IPv6 Access Control List Commands

Use the **l3acl-ipv6** command to configure the IPv6 Layer 3/Layer 4/IP Access Control List. To run these commands, you must first enter the **config-l3acl** context.

## l3acl-ipv6

To enter the **config-l3acl-ipv6** context, run this command:

```
l3acl-ipv6 WORD
```

## abort

Exits the **config-l3acl-ipv6** context without saving changes.

## end

Saves changes, and then exits the **config-l3acl-ipv6** context.

## exit

Saves changes, and then exits the **config-l3acl-ipv6** context.

## quit

Exits the **config-l3acl-ipv6** context without saving changes.

## name

Sets the L3/L4/IPv6 ACL entry name.

## description

Sets the L3/L4/IPv6 ACL entry description.

## mode allow

Sets the ACL mode to 'allow'.

## mode deny

Sets the ACL mode to 'deny'.

## no rule-order

Deletes a rule name from the L3/L4/IPv6 ACL.

## rule-order

Creates a new L3/L4/IPv6 ACL rule or modifies an existing entry rule.

# Configure L3 IPv6 Rule Commands

Use the **l3acl-ipv6-rule** commands to configure the IPv6 Layer 3/Layer 4/IP Access Control List rules. To run these commands, you must first enter the **config-l3acl-ipv6-rule** context. To enter the **config-l3acl-ipv6-rule** context, run this command:

**rule-order** *NUMBER*

## end

Saves changes, and then exits the config-l3acl-ipv6-rule context.

## exit

Saves changes, and then exits the config-l3acl-ipv6-rule context.

## order

Sets the L3/L4/IPv6 ACL rule order.

## description

Sets the L3/L4/IPv6 ACL rule description.

## type allow

Sets the ACL rule type to 'allow'.

## type deny

Sets the ACL rule type to 'deny'.

## destination

Contains commands that can be executed from within the context.

## destination address

Sets the destination address of a L3/L4/IPv6 ACL rule.

## destination port

Sets the destination port of a L3/L4/IPv6 ACL rule.

## protocol

Sets the protocol of a L3/L4/IPv6 ACL rule.

## icmpv6-type Any

Sets the icmpv6 type of a L3/L4/IPv6 ACL rule.

## icmpv6-type number

Sets the icmpv6 type of a L3/L4/IPv6 ACL rule.

## show

Displays L3/L4/IPv6 ACL settings.

# Configure Precedence Policy Commands

Use the **prece** commands to configure precedence policy settings. Precedence policies are used to define the order in which VLAN and rate limiting policies are applied when the WLAN settings, AAA server configuration or Device Policy settings conflict.

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

## prece

To create or modify a precedence policy, use the following command:

**prece** *WORD*

Enters the config-prece context. To save changes and exit the context, type exit or end. To exit the context without saving changes, type abort.

### Example

```
ruckus(config)# prece precedencel
The Precedence Policy entry 'precedencel' has been created.
ruckus(config-prece)#
```

## no prece

To delete a precedence policy entry, use the following command:

**no prece** *WORD*

## end

To save changes, and then exit the config-prece context, use the following command:

**end**

### Example

```
ruckus(config-prece)# end
The Precedence Policy entry has saved successfully.
Your changes have been saved.
ruckus(config)#
```

## exit

To save changes, and then exit the config-prece context, use the following command:

**exit**

### Example

```
ruckus(config-prece)# exit
The Precedence Policy entry has saved successfully.
Your changes have been saved.
ruckus(config)#
```

## quit

To exit the config-prece context without saving changes, use the following command:

**quit**

### Example

```
ruckus(config-prece)# quit
No changes have been saved.
ruckus(config)#
```

## name

Sets the Precedence Policy entry name.

## description

Sets the Precedence Policy entry description.

## show

To display the precedence settings, use the show command from within the config-prece context.

**show**

### Example

```
ruckus(config-prece)# show
Precedence Policy:
  ID:
  2:
    Name= precedencel
    Description=
    Rules:
      1:
        Description=
        Attribute = vlan
        Order = AAA,Device Policy,WLAN
      2:
        Description=
        Attribute = rate-limit
        Order = AAA,Device Policy,WLAN

ruckus(config-prece)#
```



# Configure Precedence Policy Rule Commands

Use the following commands to configure precedence policy rules.

## rule

Creates a new Precedence Policy rule or modifies an existing entry rule. Enters the config-prece-rule context.

**rule** *NUMBER*

## Syntax Description

### rule

Create a rule and enter the rule creation context.

### *NUMBER*

Enter the rule number (1-2). Each precedence policy can have up to two rules.

### description

Sets the Precedence Policy rule description.

### order *WORD*

Sets the order of a Precedence Policy rule. The default order is AAA, Device Policy, WLAN.

### show

Displays precedence policy settings.

## Example

```
ruckus(config)# prece precedencel
The Precedence Policy entry 'precedencel' has been created.
ruckus(config-prece)# rule 1
ruckus(config-prece-rule)# order "Device Policy" "WLAN" "AAA"
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-prece-rule)# end
ruckus(config-prece)# show
Precedence Policy:
  ID:
  :
  Name= precedencel
  Description=
  Rules:
    1:
      Description=
      Attribute = vlan
      Order = Device Policy,WLAN,AAA
    2:
      Description=
      Attribute = rate-limit
      Order = AAA,Device Policy,WLAN

ruckus(config-prece)#
ruckus(config-prece)# end
The Precedence Policy entry has saved successfully.
Your changes have been saved.
```

## description

To set the Precedence Policy rule description, use the following command:

**description**

### Example

```
ruckus(config-prece-rule)# description "Default precedence policy"  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-prece-rule)#
```

## order

To set the order of the precedence policy, use the following command from within the config-prece-rule context.

**order <WORD>**

### Syntax Description

<WORD>: Enter the order of Precedence Policy (for example, "AAA" "Device Policy" "WLAN").

### Example

```
ruckus(config-prece-rule)# order "AAA" "Device Policy" "WLAN"  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-prece-rule)#
```

# Configure Device Policy Commands

Use the device policy commands to configure access control and rate limiting policies based on client type. To run these commands, you must first enter the **config-dvc-pcy** context.

## dvcpcy

To create a device policy or edit an existing device policy, enter the following command:

**dvcpcy** *WORD*

### Syntax Description

**show**

Display device policy settings.

**name** *WORD*

Set the device policy entry name.

**description** *WORD*

Sets the device policy entry description.

**mode** *WORD*

Sets the device policy entry default mode (allow or deny).

**no** *NUMBER*

Delete a rule.

**rule** *NUMBER*

Create or modify a rule. Enter the config-dvc-pcy-rule context. You can create up to nine rules per access policy (one for each OS/Type).

### Defaults

None.

### Example

```
ruckus(config)# dvcpcy devpcy1
The Device Policy entry 'devpcy1' has been loaded. To save the Device Policy entry, type end or exit.
ruckus(config-dvc-pcy)# name device_policy_1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-dvc-pcy)# description "deny iOS"
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-dvc-pcy)# rule 1
ruckus(config-dvc-pcy-rule)# type deny
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-dvc-pcy-rule)# devinfo "Apple IOS"
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-dvc-pcy-rule)# vlan none
The command was executed successfully. To save the changes, type 'end' or 'exit'.

ruckus(config-dvc-pcy-rule)# rate-limit uplink 10 downlink 10
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-dvc-pcy-rule)# end
ruckus(config-dvc-pcy)# show
Device Policy:
  ID:
```

## Configuring Master Settings

### Configure Device Policy Commands

```
1:
  Name= device_policy_1
  Description= deny iOS
  Default Mode= deny
  Rules:
    1:
      Description=
      OS/Type = Apple iOS
      Type= deny
      VLAN = Any
      Rate Limiting Uplink = 10.00Mbps
      Rate Limiting Downlink = 10.00Mbps

ruckus(config-dvc-pcy)# end
The Device Policy entry has saved successfully.
Your changes have been saved.
ruckus(config)# show dvcpcy
Device Policy:
  ID:
    2:
      Name= device_policy_1
      Description= deny iOS
      Default Mode= deny
      Rules:
        1:
          Description=
          OS/Type = Apple iOS
          Type= deny
          VLAN = Any
          Rate Limiting Uplink = 10.00Mbps
          Rate Limiting Downlink = 10.00Mbps

ruckus(config)#
```

## no dvcpcy

To delete a device policy, use the following command:

```
no dvcpcy WORD
```

## rule

Use the rule command from within the config-dvc-pcy context to create or edit a device policy rule and enter the config-dvc-pcy-rule context. Up to 9 rules can be created per device policy.

### Syntax Description

#### **rule**

Create or edit a device policy rule. Enter the config-dvc-pcy-rule context.

#### **description** *WORD*

Set the Device Policy rule description.

#### **devinfo** *WORD*

Set the operating system type of a device policy rule.

#### **type** *WORD*

Set the device policy rule type (allow or deny).

#### **vlan** *NUMBER*

Set the VLAN ID to the number specified or "none."

**rate-limit uplink** *NUMBER* downlink *NUMBER*

Set the rate limiting uplink and downlink speeds in mbps.

**no rate-limit**

Set rate limiting to disabled.

**Example**

```
ruckus(config-dvc-pcy)# rule 2
ruckus(config-dvc-pcy-rule)# description "rate limit gaming devices"
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-dvc-pcy-rule)# devinfo "Gaming"
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-dvc-pcy-rule)# type allow
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-dvc-pcy-rule)# vlan none
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-dvc-pcy-rule)# rate-limit uplink 0.1 downlink 0.1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-dvc-pcy-rule)# end
ruckus(config-dvc-pcy)# show
Device Policy:
  ID:
    2:
      Name= device_policy_1
      Description= deny iOS
      Default Mode= deny
      Rules:
        1:
          Description=
          OS/Type = Apple iOS
          Type= deny
          VLAN = Any
          Rate Limiting Uplink = 10.00Mbps
          Rate Limiting Downlink = 10.00Mbps
        2:
          Description= rate limit gaming devices
          OS/Type = Gaming
          Type= allow
          VLAN = Any
          Rate Limiting Uplink = 0.10Mbps
          Rate Limiting Downlink = 0.10Mbps

ruckus(config-dvc-pcy)#
```

# Configure Application Policy Commands

Use the following commands to create or modify application policies.

## app-policy

To create a new application policy or modify an existing policy, use the following command:

**app-policy** *WORD*

### Syntax Description

app-policy: Creates a new Application Policy entry or modifies an existing entry.

<WORD>: Enter a name for the application policy.

### Example

```
ruckus(config)# app-policy policy1  
The Application Policy entry 'policy1' has been created.  
ruckus(config-app-policy)#
```

## no app-policy

To delete an Application Policy entry, use the following command:

**no app-policy** *WORD*

### Example

```
ruckus(config)# no app-policy policy1  
The Application Policy 'policy1' has been deleted.  
ruckus(config)#
```

## description

To set the description for the application policy, use the following command:

**description**

### Example

```
ruckus(config-app-policy)# description "Block Facebook"  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-app-policy)#
```

## show

To display the application policy settings, use the show command from within the config-app-policy context.

**show**

### Example

```
ruckus(config-app-policy)# show  
Application Policy:  
  ID:  
  :  
  Name= policy1  
  Description=  
  Rules:  
    1:  
      Rule Type= Denial Rules  
      Application Type= System Defined  
      Category= Social networks  
      Application= Facebook  
  
ruckus(config-app-policy)#
```

# Configure Application Policy Rules

Use the following commands to configure application policy rules.

## rule

Creates a new application policy rule or modifies an existing entry. Enters the *config-app-policy-rule* context.

**rule** *NUMBER*

### Syntax Description

**rule**: Create or modify an application policy rule.

<NUMBER>: Enter a rule ID.

### Example

```
ruckus(config-app-policy)# rule 1  
ruckus(config-app-policy-rule)#
```

## no rule

To delete a rule, use the following command:

**no rule** *NUMBER*

## rule-type

To set the application policy rule type, use the following command:

**rule-type**<WORD>

### Syntax Description

**rule-type**: Sets Application Policy rule type.

<WORD>: Enter rule type(Denial Rules | QoS | Rate Limiting).

### Example

```
ruckus(config-app-policy-rule)# rule-type Denial Rules  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-app-denial-rule)#
```

## application-type

To set the application type, use the following command:

**application-type**<WORD>



## Syntax Description

`application-type`: Sets Application Policy rule application type.

`<WORD>`: Enter application type ("System Defined" or "Port base User Defined Application" or "IP base User Defined Application" or "Application name").

## Example

```
ruckus(config-app-denial-rule)# application-type System Defined
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-app-denial-rule)#
```

## category

To set the application category, use the following command:

**category**`<WORD>`

## Syntax Description

`category`: Sets Application Policy rule application category.

`<LIST>`: Enter application name: [Instant messengers | Peer-to-peer networks | File sharing services and tools | Media streaming services | Email messaging services | VoIP services | Database tools | Online games | Management tools and protocols | Remote access terminals | Tunneling and proxy services | Investment platforms | Web services | Security update tools | Web instant messengers | Business tools | Network protocols (18) | Network protocols (19) | Network protocols (20) | Private protocols | Social networks]

## Example

```
ruckus(config-app-denial-rule)# category Social networks
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-app-denial-rule)#
```

## application

To set the application, use the following command:

**application**`<WORD>`

## Syntax Description

`category`: Sets Application Policy rule application name.

`<LIST>`: | Classmates | Yik Yak | Facebook | Flickr | Hi5 | LinkedIn | Livejournal | Twitter | Plurk | MySpace | Khan Academy | Pinterest | Tumblr | MeetMe | VKontakte | Odnoklassniki | Niwota | Tagged | PerfSpot | Me2day | Mekusharim | Draugiem | Badoo | Meetup | Foursquare | Ning | i-Part/iPair | Dudu | M ig33 | Hatena | eHarmony | Fotolog | Tencent QQ | Pixnet | Nk.PI | Twoo | Plaxo | Cyworld | Jivesoftware | WordPress | FMYLife | Dcinside | Cl ass Chinaren | Bai Sohu | Yammer | Douban | Gamer | Xuite | ChatMe | Clien.net | AdultFriendFinder | Fling.com | D elicious | Mei.fm | Streetlife | Daum-blog | Naver-blog | Panoramio | Blogger | FC2 | Yahoo Blog | Friendster | Ameba | Bebo social network | Kaixin | Orkut | AOL-Answers | CoolTalk social network | RenRen.com | TweetDeck | Hootsuite | Xing | Lokalisten | meinVZ/studiVZ | Viadeo | Tuenti | Hyves | Mixi.jp | Yahoo-mbga.jp | GREE | Netlog | 2ch | LoveTheseCurves | Weibo | Goog le+ | Skyrock | 51.com | Jackd | Touch | Skout | Instagram | Jiayuan | Zoosk | DatingDNA | 500px | iAround | pairs | Path | WeHeartit | Fancy | Vine | SnappyTV | Miliao | After School | Weico |

### **Example**

```
ruckus(config-app-denial-rule)# application Facebook  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-app-denial-rule)#
```

# Configuring User-Defined Applications

Use the following commands to configure user-defined IP-based applications. Once created, user-defined applications can be controlled using the application policy commands.

## user-app-ip

To configure IP-based user-defined application settings, and enter the config-user-app-ip context, use the following command:

**user-app-ip**

### Example

```
ruckus(config)# user-app-ip Application1
The User Defined Application entry Application1 has been created.
ruckus(config-user-app-ip)#
```

## no user-app-ip

To delete a user-defined application entry, use the following command:

**no user-app-ip***WORD*

### Example

```
ruckus(config)# no user-app-ip Application1
The policy 'Application1' has been removed .
ruckus(config)#
```

## abort

Exits the config-user-app-ip context without saving changes.

## end

Saves changes, and then exits the config-user-app-ip context.

## exit

Saves changes, and then exits the config-user-app-ip context.

## destination-IP

To set the destination address of a user-defined application entry, use the following command:

**destination-IP** *IP-ADDR*

### Example

```
ruckus(config-user-app-ip)# destination-IP 192.168.40.3  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-user-app-ip)#
```

## netmask

To set the netmask of a user-defined application, use the following command:

**netmask** *IP-ADDR*

### Example

```
ruckus(config-user-app-ip)# netmask 255.255.255.0  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-user-app-ip)#
```

## destination-port

To set the destination port of a user-defined Application, use the following command:

**destination-port** *NUMBER*

### Example

```
ruckus(config-user-app-ip)# destination-port 883  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-user-app-ip)#
```

## protocol

To set the protocol of a user-defined application, use the following command:

**protocol** *WORD*

### Example

```
ruckus(config-user-app-ip)# protocol tcp  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-user-app-ip)#
```

## application-name

To set the name the application, use the following command:

**application** *WORD*

### Example

```
ruckus(config-user-app-ip)# application-name Blocked-Application-1  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-user-app-ip)#
```

# Configuring User-Defined Applications Based on Port Mapping

Use the following commands to configure user-defined applications based on port mapping. Once configured, these user-defined applications can be controlled using the application policy commands.

## user-app-port

Configures port-based user-defined application settings. Enters config-user-app-port context.

### Example

```
ruckus(config)# user-app-port Application2
The Application Port Mapping entry Application2 has been created.
ruckus(config-user-app-port) #
```

## abort

Exits the config-user-app-port context without saving changes.

## end

Saves changes, and then exits the config-user-app-port context.

## exit

Saves changes, and then exits the config-user-app-port context.

## port

To set the Port of the port-based application, use the following command:

```
port NUMBER
```

### Example

```
ruckus(config-user-app-port)# port 443
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-user-app-port) #
```

## protocol

To set the Protocol for the port-based user-defined Application, use the following command:

```
protocol WORD
```

## Configuring Master Settings

### Configuring User-Defined Applications Based on Port Mapping

#### Example

```
ruckus(config-user-app-port)# protocol tcp
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-user-app-port)#
```

## application-name

To set the application name, use the following command:

```
application-name<WORD>
```

#### Example

```
ruckus(config-user-app-port)# application-name Application2
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-user-app-port)#
```

# Configure Whitelist Commands

Use the whitelist command to create a new client isolation whitelist or modify an existing whitelist, and enter the **config-whitelist** context.

## whitelist

To create a new white list entry or modify an existing entry, use the following command:

**whitelist** *WORD*

## no whitelist

To delete a whitelist entry, use the following command:

**no whitelist** *WORD*

## name

To set the White List entry name, use the following command:

**name** *WORD*

## description

To set the description of the whitelist entry, use the following command:

**description** *WORD*

# Configuring Whitelist Rules

Use the `rule` command from within the `config-whitelist` context to create a new rule or modify an existing rule, and enter the **config-whitelist-rule** context.

## rule

To create a new whitelist rule or modify an existing rule, use the following command:

**rule** *NUMBER*

## no rule

To delete a whitelist rule, use the following command:

**no rule** *NUMBER*

## description

To set the White List rule description, use the following command:

**description** *WORD*

## mac

To set the MAC address, use the following command (format: XX:XX:XX:XX:XX:XX):

**mac** *MAC*

## ip

To set the IP address, use the following command (format: 172.18.110.12).

**ip** *IP*



# Configure Band Balancing Commands

Client Band Balancing attempts to balance the number of clients across AP radios, allowing configurable thresholds for ratio of clients on the 2.4 vs. 5 GHz radio bands. Use the band-balancing commands to configure the controller's band balancing settings. To run these commands, you must first enter the **config-band-balancing** context.

## band-balancing

To enable load-balancing and enter the config-band-balancing context, use the following command:

**band-balancing**

## abort

Exits the band balancing context without saving changes.

## end

Saves changes, and then exits the band balancing context.

## exit

Saves changes, and then exits the band balancing context.

## quit

Exits the band balancing context without saving changes.

## enable

To enable band balancing, use the following command:

**enable**

## Example

```
ruckus(config-band-balancing)# enable
The band balancing settings have been updated.
ruckus(config-band-balancing)#
```

## disable

To disable band balancing, use the following command:

**disable**

## Configuring Master Settings

### Configure Band Balancing Commands

#### **Example**

```
ruckus(config-band-balancing)# disable  
The band balancing settings have been updated.  
ruckus(config-band-balancing)#
```

## Proactive

To enable or disable Proactive Band Balancing, use the following command:

**Proactive <NUMBER>**

### Syntax

<NUMBER>: 0 for disable, 1 for enable

### Example

```
ruckus(config-band-balancing)# proactive 0
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-band-balancing)#
```

## percent-2.4G <NUMBER>

To configure the percentage of clients on the 2.4 GHz band, use the following command:

**percent-2.4G <NUMBER>**

### Defaults

25

### Example

```
ruckus(config-band-balancing)# percent-2.4G 25
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-band-balancing)#
```

## show

Displays information about Band balancing.

### Example

```
ruckus(config-band-balancing)# show
Band Balancing:
  Enable= 1
  Percent of clients on 2.4G band: 25%
  Proactive Status= 1

ruckus(config-band-balancing)#
```

# Configure Load Balancing Commands

Client Load Balancing attempts to balance the number of clients across APs, per radio band. Use the **load-balancing** commands to configure the controller's load balancing settings. To run these commands, you must first enter the **config-load-balancing** context.

## load-balancing

To enable load-balancing and enter the config-load-balancing context, use the following command:

**load-balancing**

### Example

```
ruckus(config)# load-balancing
ruckus(config-load-balancing)#
```

## adj-threshold

To configure the adjacent threshold for load balancing, use the following command:

**adj-threshold [ wifi0 | wifi1 ] NUMBER**

### Syntax Description

#### **adj-threshold**

Configure the adjacent threshold for load balancing

#### **wifi0, wifi1**

Configure this interface

#### **NUMBER**

Set the adjacent threshold value (1~100)

### Defaults

Wifi0: 50

Wifi1: 43

### Example

```
ruckus(config-load-balancing)# enable wifi0
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-load-balancing)# adj-threshold wifi0 25
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-load-balancing)# show
Load Balancing:
  Radio 0:
    Status= Enabled
    AdjacentThreshold= 25
    WeakBypass= 33
    StrongBypass= 55
    ActivationThreshold= 10
    NewTrigger= 3
```

```
Headroom= 3

Radio 1:
  Status= Disabled
  AdjacentThreshold= 43
  WeakBypass= 35
  StrongBypass= 55
  ActivationThreshold= 10
  NewTrigger= 3
  Headroom= 3

ruckus(config-load-balancing)#
```

## weak-bypass

To configure the weak bypass for load balancing, use the following command:

```
weak-bypass [ wifi0 | wifi1 ] NUMBER
```

### Syntax Description

#### **weak-bypass**

Configure the weak bypass for load balancing

#### **wifi0, wifi1**

Configure this interface

#### *NUMBER*

Set the weak-bypass value (1~100)

### Defaults

wifi0: 33

wifi1: 35

### Example

```
ruckus(config-load-balancing)# weak-bypass wifi0 33
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-load-balancing)#
```

## strong-bypass

To configure the strong bypass for load balancing, use the following command:

```
strong-bypass [ wifi0 | wifi1 ] NUMBER
```

### Syntax Description

#### **strong-bypass**

Configure the strong bypass for load balancing

#### **wifi0, wifi1**

Configure this interface

*NUMBER*

Set the strong-bypass value (1~100)

## Defaults

55

## Example

```
ruckus(config-load-balancing)# strong-bypass wifi0 55  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-load-balancing)#
```

## act-threshold

To configure the activation threshold for load balancing, use the following command:

**act-threshold** [ **wifi0** | **wifi1** ] *NUMBER*

## Syntax Description

### **act-threshold**

Configure the activation threshold for load balancing.

### **wifi0, wifi1**

Configure this interface.

*NUMBER*

Set the activation threshold value (1~100).

## Defaults

10

## Example

```
ruckus(config-load-balancing)# act-threshold wifi0 50  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-load-balancing)#
```

## new-trigger

To configure new trigger threshold (1-100), use the following command:

**new-trigger** [ **wifi0** | **wifi1** ] *NUMBER*

## Syntax Description

### **new-trigger**

Configure a new trigger threshold for the specified interface.

### **wifi0, wifi1**

Configure this interface.

*NUMBER*

Set the new trigger threshold value (1~100).

## Defaults

3

## Example

```
ruckus(config-load-balancing)# new-trigger wifi0 3  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-load-balancing)#
```

## headroom

To configure headroom settings for the specified interface, use the following command:

**headroom** [ **wifi0** | **wifi1** ] *NUMBER*

## Syntax Description

### **headroom**

Configure headroom for the specified interface.

### **wifi0, wifi1**

Configure this interface.

### *NUMBER*

Set the headroom value (1~100).

## Defaults

3

## Example

```
ruckus(config-load-balancing)# headroom wifi0 3  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-load-balancing)#
```

## disable wifi0

Disable wifi0 load balancing.

## disable wifi1

Disable wifi1 load balancing.

## enable wifi0

Enable wifi0 load balancing.

## enable wifi1

Enable wifi1 load balancing.

## show

To display the current service settings, use the following command:

**show**

### *Syntax Description*

**show**

Display the current service settings

### *Defaults*

None.

### *Example*

```
ruckus(config-load-balancing)# show
Load Balancing:
  Radio 0:
    Status= Enabled
    AdjacentThreshold= 50
    WeakBypass= 33
    StrongBypass= 55
    ActivationThreshold= 10
    NewTrigger= 3
    Headroom= 3

  Radio 1:
    Status= Disabled
    AdjacentThreshold= 43
    WeakBypass= 35
    StrongBypass= 55
    ActivationThreshold= 10
    NewTrigger= 3
    Headroom= 3

ruckus(config-load-balancing)#
```



# Configure STP Commands

Both Ethernet ports are one logical interface. They are designed to provide high availability connections to separate switches and do not provide dual-port ISL channel bonding. Switches should use STP to block one path. The default is “no stp”.

## stp

To enable Spanning Tree Protocol, use the following command:

```
stp
```

## no stp

To disable Spanning Tree Protocol, use the following:

```
no stp
```

# Configure System Commands

Use the `sys` or `system` command to configure the controller's system settings, including its host name, FlexMaster server, NTP server, SNMP, and QoS settings. To run these commands, you must first enter the **config-sys** context.

## system

To enter the `config-sys` context and configure system settings, use the following command:

**system**

### Example

```
ruckus(config)# system
ruckus(config-sys)#
```

## dot11-country-code

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

**dot11-country-code** *COUNTRY-CODE* {arguments}

### Syntax Description

#### **dot11-country-code**

Configure the controller's country code setting

*COUNTRY-CODE*

Set the country code to this value

#### **channel-mode**

Contains commands that can be executed from within the context

#### **allow-indoor**

Allows ZoneFlex Outdoor APs to use channels regulated as indoor use-only

#### **not-allow-indoor**

Disallows ZoneFlex Outdoor APs to use channels regulated as indoor use-only

#### **channel-optimization**

Set channel optimization type (compatibility, interoperability, performance)

### Defaults

None.

### Example

To set the country code to US, enter the following command:

```
ruckus# configruckus(config)# system
ruckus(config-sys)# dot11-country-code US
The country code settings have been updated.
ruckus(config-sys)#
```

## hostname

To set the system hostname, use the following command:

**hostname**

### *Syntax Description*

**hostname**

Set the controller's system hostname

### *Defaults*

None

### *Example*

```
ruckus(config-sys)# hostname ruckus-xjoe  
The system identity/hostname settings have been updated.
```

## Interface Commands

Use the interface commands to configure the controller's IP address and VLAN settings. To run these commands, you must first enter the **config-sys-if** context.

### *interface*

To enter the config-sys-if context and configure IP address and VLAN settings, use the following command:

**interface**

### Example

```
ruckus(config-sys)# interface  
ruckus(config-sys-if)#
```

### *ip enable*

To enable IPv4 addressing, use the following command:

**ip enable**

### *ip route gateway*

To set the controller's gateway IP address, use the following command:

**ip route gateway** *GATEWAY-ADDR*

### Syntax Description

#### **ip route gateway**

Configure the controller's gateway IP address

*GATEWAY-ADDR*

Set the controller's gateway IP address to this value

### Defaults

None.

### Example

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

### *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-server** *DNS-ADDR* [ *DNS-ADDR* ]

## Syntax Description

### **ip name-server**

Configure the controller's DNS server address or addresses

### *DNS-ADDR*

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

192.168.0.1

## Example

```
ruckus# config
ruckus(config)# system
ruckus(config-sys)# interface
ruckus(config-sys-if)# ip name-server 192.168.0.1
The command was executed successfully.
```

## *ip addr*

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

**ip addr** *IP-ADDR NET-MASK*

Use a space to separate the IP address and netmask.

## Syntax Description

### **ip addr**

Configure the controller's IP address and netmask

### *IP-ADDR*

Set the controller's IP address to this value

### *NET-MASK*

Set the controller's netmask to this value

## Defaults

IP address: 192.168.0.2

Subnet mask: 255.255.255.0

## Example

```
ruckus# config
ruckus(config)# system
ruckus(config-sys)# interface
ruckus(config-sys-if)# ip addr 192.168.0.2 255.255.255.0
The command was executed successfully.
```

## **ip mode**

To set the controller's IP address mode, use the following command:

```
ip mode [ dhcp | static ]
```

### **Syntax Description**

**ip mode**

Configure the controller's IP address mode

**dhcp**

Set the controller's IP address mode to DHCP

**static**

Set the controller's IP address mode to static

### **Defaults**

None.

### **Example**

To set the controller's IP address mode to DHCP, enter the following command:

```
ruckus# config
ruckus(config)# system
ruckus(config-sys)# interface
ruckus(config-sys-if)# ip mode dhcp
The command was executed successfully.
```

## **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# config
ruckus(config)# system
ruckus(config-sys)# interface
ruckus(config-sys-if)# show
Protocol Mode= IPv4-Only
Device IP Address:
Mode= Manual
IP Address= 192.168.11.100
Netmask= 255.255.255.0
```

```
Gateway Address= 192.168.11.1  
Primary DNS= 192.168.11.1  
Secondary DNS= 168.95.1.1
```

```
Management VLAN:  
Status= Disabled  
VLAN ID=
```

```
ruckus(config-sys-if)#
```

## **vlan**

If the ZoneDirector is on a tagged Access VLAN, to set the VLAN ID, use the following command:

```
vlan NUMBER
```

## **no ip**

To disable IPv4 addressing, use the following command:

```
no ip
```

## **timezone**

To configure time zone settings, use the following command:

```
timezone TIMEZONE
```

## **Defaults**

```
GMT+0
```

## **Example**

```
ruckus(config-sys)# timezone +8  
The timezone settings have been updated.  
ruckus(config-sys)#
```

## **ftp-anon**

To enable FTP anonymous access, use the following command:

```
ftp-anon
```

## **no ftp-anon**

To disable FTP anonymous access, use the following command:

```
no ftp-anon
```

## **ftp**

Enable FTP server.

## no ftp

Disable FTP server.

## mgmt-if

To enable the management interface, use the following command:

**mgmt-if**

### Defaults

Disabled.

### Example

```
ruckus(config-sys)# mgmt-if
ruckus(config-sys-mgmt-if)#
  help                Shows available commands.
  history              Shows a list of previously run commands.
  abort                Exits the config-sys-mgmt-if context without saving changes.
  end                  Saves changes, and then exits config-sys-mgmt-if context.
  exit                 Saves changes, and then exits config-sys-mgmt-if context.
  quit                Exits the config-sys-mgmt-if context without saving changes.
  ip                   Contains commands that can be executed from within the context.
  show                 Displays current management interface settings.
ruckus(config-sys-mgmt-if)#
```

## ip addr

To configure the IP address of the management interface, use the following command:

**ip addr** *IP-ADDR NET-MASK*

### Syntax Description

#### IP-ADDR

Enter the IP address.

#### NET-MASK

Set the Netmask for the address.

### Defaults

None.

### Example

```
ruckus(config-sys-mgmt-if)# ip addr 192.168.40.4 255.255.255.0
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-sys-mgmt-if)#
```



## Unleashed-Multi-Site-Manager

To configure UMM settings, use the following command:

**Unleashed-Multi-Site-Manager**IP-ADDR NET-MASK interval <NUMBER>

### *Syntax Description*

**interval**

Configure UMM interval (1~60 minutes).

**IP-ADDR**

Configure UMM IP address.

**NET-MASK**

Configure UMM IP address Netmask.

### *Example*

```
ruckus(config-sys)# unleashed-multi-site-manager 172.17.16.1 interval 60
The Unleashed Multi-Site Manager settings have been updated.
ruckus(config-sys)#
```

## northbound

To enable northbound portal interface and set the northbound portal interface password, use the following command:

### Syntax

```
northbound password [WORD]
```

### Parameters

**password**

Set the northbound portal interface password

### Examples

```
ruckus(config-sys)# northbound password password1234  
The northbound portal interface settings have been updated.  
ruckus(config-sys)#
```

## no northbound

To disable northbound portal authentication, use the following command:

### Syntax

**no northbound**

### Command Default

Disabled.

### Examples

```
ruckus(config-sys)# no northbound
Northbound portal interface has been disabled.
ruckus(config-sys)#
```

## ntp

To enable the NTP client, use the following command:

**ntp** *IP-ADDR/DOMAIN-NAME*

### Syntax Description

**ntp**

Enable the NTP client

*IP-ADDR/DOMAIN-NAME*

Set the NTP server address to this IP address/domain name

### Defaults

None.

### Example

```
ruckus(config-sys)# ntp 192.168.2.21
The NTP settings have been updated.
ruckus(config-sys)# ntp sohu.com
The NTP settings have been updated.
```

## 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 addresss is ntp.ruckuswireless.com.

### **Example**

```
ruckus(config-sys)# no ntp  
The NTP settings have been updated.
```

## SNMPv2 Commands

Use the following commands to configure SNMPv2 settings. To use these commands, you must first enter the **config-sys-snmpv2** context.

### *snmpv2*

To configure the SNMPv2 settings, use the following command:

**snmpv2**

Executing this command enters the config-sys-snmpv2 context.

### Syntax Description

**snmpv2**

Configure the SNMPv2 settings

**abort**

Exits the config-sys-snmpv2 context without saving changes.

**end**

Saves changes, and then exits the config-sys-snmpv2 context.

**exit**

Saves changes, and then exits the config-sys-snmpv2 context.

**quit**

Exits the config-sys-snmpv2 context without saving changes.

**no access-v3**

Disables special MIB node for customer's kt.

**access-v3**

Enables special MIB node for customer's kt.

**contact** *WORD*

Enables SNMPV2 agent and sets the system contact.

**location** *WORD*

Enables SNMPV2 agent and sets the system location.

**ro-community** *WORD*

Enables SNMPV2 agent and sets the RO community name.

**rw-community** *WORD*

Enables SNMPV2 agent and sets the RW community name.

**show**

Displays SNMPV2 agent and SNMP trap settings.

### Defaults

SNMP Agent:

Status= Enabled

Contact= [https://support.ruckuswireless.com/contact\\_us](https://support.ruckuswireless.com/contact_us)

Location= 350 West Java Dr. Sunnyvale, CA 94089 US  
RO Community= public  
RW Community= private  
SNMP Trap:  
Format= Version2  
Status= Disabled  
Support-access-V3:  
Status= Disabled

### Example

```
ruckus(config-sys)# snmpv2
ruckus(config-sys-snmpv2)#
```

### contact

To enable SNMPv2 agent and set the system contact, use the following command:

**contact** *WORD*

### location

To enable SNMPv2 agent and set the system location, use the following command:

**location** *WORD*

### ro-community

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

**ro-community** *WORD*

### Syntax Description

#### **ro-community**

Configure the read-only community name

*WORD*

Set the read-only community name to this value

### Defaults

public

### Example

```
ruckus(config-sys-snmpv2)# ro-community private-123
The command was executed successfully
```

## ***rw-community***

To set the read-write (RW) community name, use the following command:

**rw-community** *WORD*

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

### **Syntax Description**

#### **rw-community**

Configure the read-write community name

*WORD*

Set the read-write community name to this value

### **Defaults**

private

### **Example**

```
ruckus(config-sys-snmpv2)# rw-community private-123
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

### **show**

To display SNMPv2 agent and SNMP trap settings, use the show command.

### **Example**

```
ruckus(config-sys-snmpv2)# show
SNMP Agent:
  Status= Enabled
  Contact= https://support.ruckuswireless.com/contact_us
  Location= 350 West Java Dr. Sunnyvale, CA 94089 US
  RO Community= public
  RW Community= private

SNMP Trap:
  Format= Version2
  Status= Disabled

Support-access-V3:
  Status= Disabled
```

## ***snmpv2-ap***

To enable SNMP AP notification, use the following command:

**snmpv2-ap**

### **Example**

```
ruckus(config-sys)# snmpv2-ap
The SNMP v2 agent settings have been updated.
ruckus(config-sys)#
```

### ***no snmpv2-ap***

To disable SNMP AP notification, use the following command:

**no snmpv2-ap**

### **Example**

```
ruckus(config-sys)# no snmpv2-ap  
The SNMP v2 agent settings have been updated.  
ruckus(config-sys)#
```



## SNMPv3 Commands

Use the following commands to configure SNMPv3 settings. To use these commands, you must first enter the **config-sys-snmpv3** context.

### *snmpv3*

To configure the SNMPv3 settings, use the following command:

**snmpv3**

Executing this command enters the config-sys-snmpv3 context.

### Syntax Description

**snmpv3**

Configure the SNMPv3 settings

**abort**

Exits the config-sys-snmpv3 context without saving changes.

**end**

Saves changes, and then exits the config-sys-snmpv3 context.

**exit**

Saves changes, and then exits the config-sys-snmpv3 context.

**quit**

Exits the config-sys-snmpv3 context without saving changes.

**ro-user** *WORD*

Contains commands that can be executed from within the context.

**ro-user** *WORD MD5 WORD*

Contains commands that can be executed from within the context.

**ro-user** *WORD MD5 WORD DES WORD*

Sets the privacy phrase of DES for SNMPV3.

**ro-user** *WORD MD5 WORD AES WORD*

Sets the privacy phrase of AES for SNMPV3.

**ro-user** *WORD MD5 WORD None*

Sets the privacy to None for SNMPV3.

**ro-user** *WORD SHA WORD*

Contains commands that can be executed from within the context.

**ro-user** *WORD SHA WORD DES WORD*

Sets the privacy phrase of DES for SNMPV3.

**ro-user** *WORD SHA WORD AES WORD*

Sets the privacy phrase of AES for SNMPV3.

**ro-user** *WORD SHA WORD; None*

Sets the privacy to None for SNMPV3.

**rw-user** *WORD*

Contains commands that can be executed from within the context.

- rw-user** *WORD MD5 WORD*  
Contains commands that can be executed from within the context.
- rw-user** *WORD MD5 WORD DES WORD*  
Sets the privacy phrase of DES for SNMPV3.
- rw-user** *WORD MD5 WORD AES WORD*  
Sets the privacy phrase of AES for SNMPV3.
- rw-user** *WORD MD5 WORD None*  
Sets the privacy to None for SNMPV3.
- rw-user** *WORD SHA WORD*  
Contains commands that can be executed from within the context.
- rw-user** *WORD SHA WORD DES WORD*  
Sets the privacy phrase of DES for SNMPV3.
- rw-user** *WORD SHA WORD AES WORD*  
Sets the privacy phrase of AES for SNMPV3.
- rw-user** *WORD SHA WORD None*  
Sets the privacy to None for SNMPV3.
- show**  
Displays SNMPV3 agent and SNMP trap settings.

## Defaults

SNMPV3 Agent:  
Status= Disabled  
Ro:  
User=  
Authentication Type= MD5  
Authentication Pass Phrase=  
Privacy Type= DES  
Privacy Phrase=  
Rw:  
User=  
Authentication Type= MD5  
Authentication Pass Phrase=  
Privacy Type= DES  
Privacy Phrase=  
SNMP Trap:  
Format= Version3  
Status= Disabled

## **snmp-trap-format**

To set the SNMP trap format to SNMPV2 or SNMPV3, use the following command:

```
snmp-trap-format [ SNMPv2 | SNMPv3 ]
```

### **Syntax Description**

#### **snmp-trap-format**

Set the SNMP trap format

[ **SNMPv2** | **SNMPv3** ]

Set to either SNMPv2 or SNMPv3

### **Defaults**

SNMPv2

### **Example**

```
ruckus(config-sys)# snmp-trap-format SNMPV2  
The SNMP trap settings have been updated.
```

## **snmpv2-trap**

To enable the SNMPv2 trap and set the IP address of the trap server, use the following command:

```
snmpv2-trap NUMBER IP/IPv6-ADDR
```

### **Syntax Description**

#### **snmpv2-trap**

Enable the SNMPv2 trap and set the trap server's IP address

*NUMBER*

Assign the trap receiver ID (1-4)

*IP/IPv6-ADDR*

Set the trap receiver IP address

### **Defaults**

None

### **Example**

```
ruckus(config-sys)# snmpv2-trap 1 192.168.10.22  
The SNMP trap settings have been updated.
```

## **snmpv3-trap**

To enable and configure the SNMPv3 trap parameters, use the following command:

```
snmpv3-trap user_name snmp_trap_server_ip [ MD5 | SHA ] auth_pass_phrase [ DES privacy_phrase | AES privacy_phrase | None ]
```

### Syntax Description

#### **snmpv3-trap**

Enable the SNMPv3 trap and configure the trap parameters

*user\_name*

Trap user name

*snmp\_trap\_server\_ip*

Trap server IP address

[ **MD5** | **SHA** ]

Authentication method

*auth\_pass\_phrase*

Authentication passphrase

[ **DES** *privacy\_phrase* | **AES** *privacy\_phrase* | **None** ]

Privacy method and privacy phrase

### Defaults

None

### Example

```
ruckus(config-sys)#snmpv3-trap test1234 192.168.0.22 MD5 test1234 DES test4321  
The command was executed successfully.
```

### **no snmp-trap-ap**

To disable SNMP trap server configuration for AP, use the following command:

```
no snmp-trap-ap
```

### Example

```
ruckus(config-sys)#no snmp-trap-ap  
The SNMP AP trap settings have been updated.
```

## 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.

### **syslog**

To enable syslog notifications and enter the config-sys-syslog context, use the following command:

**syslog**

### Example

```
ruckus(config-sys)# syslog
ruckus(config-sys-syslog)#
```

### **no syslog**

To disable syslog notification, use the following command:

**no syslog**

### Syntax Description

**no syslog**

Disable syslog notification

### Defaults

Disabled.

### Example

```
ruckus(config-sys)# no syslog
The syslog settings have been updated.
ruckus(config-sys)#
```

### **server**

To set the syslog server address, use the following command:

**server** *IP-ADDR*

### Syntax Description

**server**

Set the syslog server IP address.

*IPADDR*

Send syslog notifications to this IP address.

## Defaults

Disabled.

## Example

```
ruckus(config-sys-syslog)# server 172.17.16.2  
The syslog settings have been updated.  
ruckus(config-sys-syslog)#
```

## **type**

To set the syslog server type, use the following command:

**type** <LOG TYPE>

### **Syntax Description**

all: Sets remote syslog type to all.

client: Sets remote syslog type to client info.

### **Example**

```
ruckus(config-sys-syslog)# type all
The syslog settings have been updated.
ruckus(config-sys-syslog)#
```

## **facility**

To set the facility name, use the following command:

**facility** FACILITY NAME

### **Syntax Description**

**facility** FACILITY NAME

Sets the syslog facility name (local0 - local7)

### **Defaults**

Disabled.

## **priority**

To set the syslog priority level, use the following command:

**priority** PRIORITY LEVEL

### **Syntax Description**

**priority** PRIORITY LEVEL

Sets the syslog priority level (emerg, alert, crit, err, warning, notice, info, debug).

### **Defaults**

Disabled.

## **ap-facility**

To set the AP syslog facility name, use the following command:

**ap-facility** FACILITY-NAME

### Syntax Description

**ap-facility** *FACILITY-NAME*

Sets the AP syslog facility name (local0 - local7).

### Defaults

Disabled.

### *ap-priority*

To set the AP syslog priority level, use the following command:

**ap-priority** *PRIORITY LEVEL*

### Syntax Description

**ap-priority** *PRIORITY LEVEL*

Sets the AP syslog priority level (emerg, alert, crit, err, warning, notice, info, debug).

*IPADDR*

Send syslog notifications to this IP address.

### Defaults

Disabled.

### Example

```
ruckus# config
ruckus(config)# system
ruckus(config-sys)# syslog
ruckus(config-sys-syslog)# server 192.168.3.10
The syslog settings have been updated.
ruckus(config-sys-syslog)# facility local0
The syslog settings have been updated.
ruckus(config-sys-syslog)# priority emerg
The syslog settings have been updated.
ruckus(config-sys-syslog)# ap-facility local0
The syslog settings have been updated.
ruckus(config-sys-syslog)# ap-priority emerg
The syslog settings have been updated.
ruckus(config-sys-syslog)# end
The syslog settings have been updated.
Your changes have been saved.
ruckus(config-sys)#
```

### *no syslog-ap*

To disable external syslog server configuration for AP, use the following command:

**no syslog-ap**

### Example

```
ruckus(config-sys)#no syslog-ap
The AP syslog settings have been updated.
```



## Management Access Control List Commands

Use the following commands to create or configure management ACLs and enter the **config-sys-mgmt-acl** or **config-sys-mgmt-acl-ipv6** contexts. These commands must be used from the **config-sys** context.

### *mgmt-acl*

To create or configure a management ACL, use the following command:

```
mgmt-acl WORD
```

### Syntax Description

**mgmt-acl**

Create or configure a management ACL

*WORD*

Create or configure this management ACL

### Defaults

None.

### Usage Guidelines

Executing this command enters the **config-mgmt-acl** context.

### Example

```
ruckus(config-sys)# mgmt-acl macl1
The management ACL 'macl1' has been created. To save the Management ACL, type 'end' or 'exit'.
ruckus(config-mgmt-acl)#
```

### *no mgmt-acl*

To delete a management ACL for IPv4, use the following command:

```
no mgmt-acl WORD
```

### *mgmt-acl-ipv6*

To create or configure an IPv6 management ACL, use the following command:

```
mgmt-acl-ipv6 WORD
```

Executing this command enters the **config-mgmt-acl-ipv6** context.

### Syntax Description

**mgmt-acl-ipv6**

Create or configure a management ACL

*WORD*

Create or configure this management ACL

## Defaults

None.

## Example

```
ruckus(config-sys)# mgmt-acl-ipv6 macl1  
The management ACL 'macl1' has been created. To save the Management ACL, type 'end' or 'exit'.  
ruckus(config-mgmt-acl-ipv6)#
```

## **no mgmt-acl-ipv6**

To delete a management ACL for IPv6, use the following command:

**no mgmt-acl-ipv6** *WORD*

## **exit**

Saves changes, and then exits the config-mgmt-acl context.

## **end**

Saves changes, and then exits the config-mgmt-acl context.

## **quit**

Exits the config-mgmt-acl context without saving changes.

## **abort**

Exits the config-mgmt-acl context without saving changes.

## **name**

To set the management ACL name, use the following command:

**name** *WORD*

## **restrict-type**

To set the management ACL restriction type, use the following command:

**restrict-type** [ **single ip-addr** *IP-ADDR* | **range ip-range** *IP-ADDR IP-ADDR* | **subnet ip-subnet** *IP-ADDR IP-SUBNET* ]

## Syntax Description

### **restrict-type**

Set the management ACL restriction type (single/range).

### **single ip-addr**

Set management ACL restriction type to single.

### **range**

Sets the management ACL restriction type to range.

### **ip-range**

Sets the IP address range for management ACL. Use a space ( ) to separate addresses.

### **subnet ip-subnet**

Sets the subnet for management ACL IP address. Use a space ( ) to separate IP address and Netmask (128.0.0.0 to 255.255.255.252).

## **restrict-type single ip-addr**

To set the management ACL restriction type to a single IP address, use the following command:

**restrict-type single ip-addr** *ip\_address*

### **Syntax Description**

#### **restrict-type single ip-addr**

Set the management ACL restriction type to a single IP address

*ip\_address*

Set to this IP address only

### **Example**

```
ruckus(config-mgmt-acl)# restrict-type single ip-addr 192.168.110.22
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## **restrict-type subnet ip-subnet**

To set the management ACL restriction type to certain subnets, use the following command:

**restrict-type subnet ip-subnet** *IP-SUBNET IP-SUBNET*

### **Syntax Description**

#### **restrict-type subnet ip-subnet**

Set the management ACL restriction type to a single IP address

*IP-SUBNET*

Set to this subnet

### **Example**

```
ruckus(config-mgmt-acl)#restrict-type subnet ip-subnet 172.30.110.26 255.255.254.0
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## **restrict-type range ip-range**

To set the management ACL restriction type to an IP address range, use the following command:

**restrict-type range ip-range** *ip\_address ip\_address*

### Syntax Description

#### **restrict-type range ip-range**

Set the management ACL restriction type to a single IP address

*ip\_address ip\_address*

**Set to this IP address range. The first *ip\_address* is for the startui**

### Example

```
ruckus(config-mgmt-acl)#restrict-type range ip-range 172.30.110.28 172.30.110.39  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

### show

To display management ACL settings, use the show command.

## QoS Commands

Use the following commands to configure QoS settings on the controller. These commands must be executed from the **config-sys** context.

### no qos

To disable QoS on the controller, use the following command:

**no qos**

### Syntax Description

**no qos**

Disable QoS on the controller

### Defaults

None.

### Example

```
ruckus(config-sys)# no qos  
Changes are saved!  
System QoS function has been disabled.
```

### qos

To enable and configure Quality of Service settings on the controller, use the following command:

**qos**

### Usage Guidelines

Executing this command enters the **config-sys-qos** context. The following commands can be executed from within the qos context.

## Example

```
ruckus(config-sys)# qos  
ruckus(config-sys-qos)#
```

### **heuristics video inter-packet-gap**

Use the following command to set the QoS heuristics video inter-packet gap minimum/maximum values:

```
heuristics video inter-packet-gap min NUMBER max NUMBER
```

### **heuristics video packet-length**

Use the following command to set the heuristics video packet-length values:

```
heuristics video packet-length min NUMBER max NUMBER
```

### **heuristics voice inter-packet-gap**

Use the following command to set the heuristics voice inter-packet-gap values:

```
heuristics voice inter-packet-gap min NUMBER max NUMBER
```

### **heuristics voice packet-length**

Use the following command to set the heuristics voice packet-length values:

```
heuristics voice packet-length min NUMBER max NUMBER
```

### **heuristics classification video packet-octet-count**

Use the following command to set the heuristics classification video packet-octet-count value:

```
heuristics classification video packet-octet-count NUMBER
```

### **heuristics classification voice packet-octet-count**

Use the following command to set the heuristics classification voice packet-octet-count value:

```
heuristics classification voice packet-octet-count NUMBER
```

### **heuristics no-classification video packet-octet-count**

Use the following command to set the heuristics no-classification video packet-octet-count value

```
heuristics no-classification video packet-octet-count NUMBER
```

### **heuristics no-classification voice packet-octet-count**

Use the following command to set the heuristics no-classification voice packet-octet-count value

```
heuristics no-classification voice packet-octet-count NUMBER
```

### **tos classification video**

Use the following command to set the TOS classification video value:

**tos classification video** *WORD*

### **tos classification voice**

Use the following command to set the TOS classification voice value:

**tos classification voice** *WORD*

### **tos classification data**

Use the following command to set the TOS classification data value:

**tos classification data** *WORD*

### **tos classification background**

Use the following command to set the TOS classification background value:

**tos classification background** *WORD*

### **show**

Use the following command to display the system QoS settings:

**show**

### **Example**

```
ruckus(config-sys)# qos
ruckus(config-sys-qos)# show
System QoS:
ToS DATA TUNNEL = 0xA0
ToS CTRL TUNNEL = 0xA0
ToS Classification-Voice = 0xE0 0xC0 0xB8
ToS Classification-Video = 0xA0 0x80
ToS Classification-Data = 0x0
ToS Classification-Background = 0x0
Tx fail threshold = 50
heuristics inter-packet-gap Video = 0 65
heuristics inter-packet-gap Voice = 15 275
heuristics packet-length Video = 1000 1518
heuristics packet-length Voice = 70 400
heuristics classification Video = 50000
heuristics classification Voice = 600
heuristics no classification Video = 500000
heuristics no classification Voice = 10000

ruckus(config-sys-qos)#
```

## **tunnel-mtu**

To set the tunnel MTU, use the following command:

**tunnel-mtu** *NUMBER*

## Syntax Description

### **tunnel-mtu**

Set the tunnel MTU

## Defaults

None.

## Example

```
ruckus(config-sys)# tunnel-mtu 1500
The Tunnel MTU settings have been updated.
ruckus(config-sys)#
```

## bonjour

To enable bonjour service, use the following command:

**bonjour**

## Defaults

Disabled.

## Example

```
ruckus(config-sys)# bonjour
The bonjour service settings have been updated.
ruckus(config-sys)#
```

## no bonjour

To disable bonjour service, use the following command:

**no bonjour**

## telnetd

To enable the telnet server, use the following command:

**telnetd**

## Syntax Description

### **telnetd**

Enable the telnet server

## Defaults

None.

### Example

```
ruckus(config-sys)# telnetd
The telnet server settings have been updated.
ruckus(config-sys)#
```

## no telnetd

To disable the telnet server, use the following command:

**telnetd**

### Syntax Description

**no telnetd**

Disable the telnet server

### Defaults

None.

### Example

```
ruckus(config-sys)# no telnetd
The telnet server settings have been updated.
ruckus(config-sys)#
```

## snmp-trap

To set the SNMP trap format, use the following command:

**snmp-trap** *trap 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

### Example

```
ruckus# config
ruckus(config)# system
ruckus(config-sys)# snmp-trap 192.168.0.3
```

## no snmp-trap

To disable the SNMP trap notifications, use the following command:

**no snmp-trap** *NUMBER*



### **Syntax Description**

#### **no snmp-trap**

Disables SNMP trap notification by index

### **Example**

```
ruckus(config-sys)# no snmp-trap 1  
The SNMP trap settings have been updated.
```

## **no snmpv2-trap**

To disable the SNMP trap notifications, use the following command:

**no snmp-trap** *NUMBER*

### **Syntax Description**

#### **no snmpv2-trap**

Disables SNMP trap notification by index

### **Example**

```
ruckus(config-sys)# no snmpv2-trap 1  
The SNMP trap settings have been updated.
```

## **no snmpv3-trap**

To disable the SNMPv3 trap notification, use the following command:

**no snmpv3-trap** *NUMBER*

### **Syntax Description**

#### **no snmpv3-trap**

Disables SNMP trap notification by index

### **Example**

```
ruckus(config-sys)# no snmpv3-trap 1  
The SNMP trap settings have been updated.
```

## **no snmpv2**

To disable the SNMPv2 agent, use the following command:

**no snmpv2**

### **Syntax Description**

#### **no snmpv2**

Disables the SNMPv2 agent

### **Example**

```
ruckus(config-sys)# no snmpv2  
The SNMP v2 agent settings have been updated.
```

### **no snmpv3**

To disable the SNMPv3 agent, use the following command:

#### **no snmpv3**

### **Syntax Description**

#### **no snmpv3**

Disables the SNMPv3 agent

### **Example**

```
ruckus(config-sys)# no snmpv3  
The SNMP v3 agent settings have been updated.
```

## show support-entitle

To display the content of the entitlement file, use the following command:

**show support-entitle**

### Example

```
ruckus(config-sys)# show support-entitle
Serial Number: SN1150
Services purchased: 904
Date to Start :Thu Oct 16 00:00:00 2014

Date to End: Wed Jan 14 23:59:00 2015

Number of APs: licensed
Status: active
Detailed: Support service activated
ruckus(config-sys)#
```

## login-warning

To configure the login warning message, use the following command:

**login-warning**

### Syntax Description

#### **login-warning**

Configure the login warning message.

#### **abort**

Exits the login-warning context without saving changes.

#### **end**

Saves changes, and then exits the login-warning context.

#### **exit**

Saves changes, and then exits the login-warning context.

#### **quit**

Exits the login-warning context without saving changes.

#### **content** *WORD*

Customize login warning content.

### Example

```
ruckus(config-sys)# login-warning
ruckus(config-sys-login-warning)# content "Warning, you are logging into equipment belonging to ruckus,
if you are not an authorized user please logout immediately."
The login warning settings have been updated.
ruckus(config-sys-login-warning)# end
The login warning settings have been updated.
Your changes have been saved.
ruckus(config-sys)#
```

## no login-warning

To disable the login warning message, use the following command:

**no login-warning**

## event-log-level

To configure the event log level, use the following command:

**event-log-level** *EVENT LOG LEVEL*

### Syntax Description

**event-log-level**

**Enter the syslog event log level 1-3 (1:Critical Events Only, 2:Warning and Critical Events, 3:Show More).**

### Defaults

2: Warning and Critical Events

### Example

```
ruckus# config
You have all rights in this mode.
ruckus(config)# sys
ruckus(config-sys)# syslog
ruckus(config-sys-syslog)# event-log-level 1
The syslog settings have been updated.
ruckus(config-sys-syslog)#
```

## support-entitle

Use the following command to manually download entitlement file:

**support-entitle**

### Example

```
ruckus(config-sys)# support-entitle
Your Support service has been successfully activated for this ZoneDirector. You may proceed with
firmware upgrade.
ruckus(config-sys)#
```

## session-stats-resv

To enable session statistics recording, use the following command:

**session-stats-resv**

### Defaults

Disabled

### Example

```
ruckus(config-sys)# session-stats-resv  
The session statistics function has been enabled.  
ruckus(config-sys)#
```

## no session-stats-resv

Use the following command to disable recording of session statistics:

**no session-stats-resv**

### Example

```
ruckus(config-sys)# no session-stats-resv  
The session statistics function has been disabled.  
ruckus(config-sys)#
```

## session-limit-unauth-stats

To enable recording of Layer 2 unauthorized session statistics, use the following command:

**session-limit-unauth-stats**

### Defaults

Enabled

### Example

```
ruckus(config-sys)# session-limit-unauth-stats  
The limited unauthorized session statistics function has been enabled.  
ruckus(config-sys)#
```

## no session-limit-unauth-stats

To disable recording of Layer 2 unauthorized session statistics, use the following command:

**no session-limit-unauth-stats**

## eapol-no-retry

To disable retransmission of EAPOL-key (message 3/4 and group key), use the following command:

**eapol-no-retry**

### *Example*

```
ruckus(config-sys)# eapol-no-retry
Eapol-key retry has been disabled
ruckus(config-sys)#
```

## no eapol-no-retry

To enable retransmission of EAPOL-key, use the following command:

**no eapol-no-retry**

### *Example*

```
ruckus(config-sys)# no eapol-no-retry
Eapol-key retry has been enabled
ruckus(config-sys)#
```

## arc-data-transmission

To enable ARC data transmission, use the following command:

**arc-data-transmission**

### *Example*

```
ruckus(config-sys)# arc-data-transmission  
The ARC data transmission has been enabled.  
ruckus(config-sys)#
```



## no arc-data-transmission

To disable ARC (application recognition and control) data transmission, use the following command:

**no arc-data-transmission**

### *Example*

```
ruckus(config-sys)# no arc-data-transmission  
The ARC data transmission has been disabled.  
ruckus(config-sys)#
```

## master-protect

To configure Unleashed Master AP protection settings, use the following command:

### **master-protect**

### *Example*

```
ruckus(config-sys)# master-protect
ruckus(config-sys-master-protect)#
  help                Shows available commands.
  history             Shows a list of previously run commands.
  abort              Exits the master-protect context without saving changes.
  end                Saves changes, and then exits the master-protect context.
  exit              Saves changes, and then exits the master-protect context.
  quit              Exits the master-protect context without saving changes.
  master-max-sta <NUMBER>
                    Set the max station number in master AP.
  show              Displays master protection settings.
ruckus(config-sys-master-protect)#
```

## **cpu-reject-sta**

To configure CPU reject value settings for the Master protection, use the following command:

**cpu-reject-sta***NUMBER*

### **Syntax Description**

#### **cpu-reject-sta**

Configure CPU reject value.

#### *NUMBER*

Set the headroom CPU utilization threshold value (0~100).

### **Defaults**

3

### **Example**

```
ruckus(config-sys-master-protect)# cpu-reject-sta 85
The master AP protection settings have been updated.
ruckus(config-sys-master-protect)#
```

### **master-max-sta**

To configure Master max station value for the Master protection, use the following command:

**cpu-reject-sta***NUMBER*

### **Syntax Description**

#### **cpu-reject-sta**

Configure max APs for Master protection.

#### *NUMBER*

Set the max APs (0~100).

### **Defaults**

100

### **Example**

```
ruckus(config-sys-master-protect)# master-max-sta 85  
The master AP protection settings have been updated.  
ruckus(config-sys-master-protect)#
```

## generate-token

To Re-generate unleashed-network unique token, use the following command:

**generate-token**

### *Example*

```
ruckus(config-sys)# generate-token  
new-token: un9418490011251346969169799  
ruckus(config-sys)#
```

## show

To display config-sys current settings, use the following command:

**show**

### Example

```
ruckus(config-sys)# show
Country Code:
  Code= United States

Identity:
  Name= Unleashed

Session Statistics:
  Enable= false
  Limited Unauthorized Session= true

ARC Data Transmission:
  Enable= true

NTP:
  Status= Enabled
  Address= ntp.ruckuswireless.com
  Timezone= GMT

Log:
  Status= Disabled
  Address=
  Facility=
  Priority=
  AP Facility=
  AP Priority=
  event log level= 1

Bonjour Service:
  Status= Enabled

Telnet Server:
  Status= Disabled

FTP Server:
  Status= Enabled
  Anonymous Status= Disabled

Unleashed Multi-Site Manager:
  Status= Enabled
  Address= 172.17.16.1
  Interval= 60

login warning:
  Status= Disabled
  content= "Warning, you are logging into device for authorized user only. If you are not an authorized
user, please click Quit; otherwise click Continue to login."

LWAPP:
  MGMT queue length threshold to drop AUTH frame = 100
  MGMT queue length threshold to resume processing AUTH frame = 25

EAPoL Key no Retry:
  Status= Disabled

Unleashed Network:
  Token= un9418490011251546969169799

ruckus(config-sys)#
```

# Configure UPnP Settings

Use the following commands to enable or disable Universal Plug and Play:

## upnp

**upnp**

### *Syntax Description*

**upnp**

Enable UPnP

### *Defaults*

Enabled.

### *Example*

```
ruckus(config)# upnp
UPnP Service is enabled
/bin/upnp enable
ruckus(config)#
```

## no upnp

**no upnp**

### *Syntax Description*

**no upnp**

Enable UPnP

### *Defaults*

Enabled.

### *Example*

```
ruckus(config)# no upnp
UPnP Service is disabled
/bin/upnp disable
ruckus(config)#
```

# Configure Zero-IT Settings

To configure Zero-IT settings, use the following commands.

## zero-it

To configure Zero-IT settings, use the following command:

```
zero-it [ local | name WORD ]
```

## zero-it-auth-server

To configure Zero-IT settings, use the following command:

```
zero-it-auth-server [ local | name WORD]
```

### Syntax Description

#### **zero-it-auth-server**

Set Zero-IT authentication server

#### **local**

Set the Zero-IT authentication server to local database

#### **name**

Set the Zero-IT authentication server to an external AAA server

#### *WORD*

Name of AAA server

### Defaults

None.

### Example

```
ruckus(config)# zero-it-auth-server name radius  
The Authentication Server of Zero IT Activation has been updated.  
ruckus(config)#
```



# Configure Dynamic PSK Expiration

The following section lists commands for configuring Dynamic Pre-Shared Keys.

## dynamic-psk-expiration

To set DPSK expiration, use the following command:

**dynamic-psk-expiration** *TIME*

### Syntax Description

#### **dynamic-psk-expiration**

Set DPSK expiration

#### *TIME*

Set DPSK expiration to this time limit (one-day, one-week, two-weeks, one-month, two-months, three-months, half-a-year, one-year, two-years)

#### **unlimited**

Set DPSKs to never expire

### Defaults

None.

### Example

```
ruckus(config)# dynamic-psk-expiration unlimited
The Dynamic psk expiration value has been updated.
ruckus(config)#
```

# Configure 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.

## wlan

To create a WLAN or configure an existing WLAN, use the following command:

```
wlan <WORD>/<NAME>
```

Executing this command enters the config-wlan context.

### Syntax Description

**wlan**

Configure a WLAN

<WORD>/<NAME>

Name of the WLAN service

### Defaults

None.

### Example

```
ruckus(config)# wlan ruckus2  
The WLAN service 'ruckus2' has been created. To save the WLAN service, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## abort

Exits the config-wlan context without saving changes.

## end

Saves changes, and then exits the config-wlan context.

## exit

Saves changes, and then exits the config-wlan context.

## quit

Exits the config-wlan context without saving changes.

## description

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

**description** *WORD*

### Syntax Description

#### **description**

Configure the WLAN description

#### *WORD*

Set the WLAN description this value

### Defaults

None.

### Example

```
ruckus(config-wlan)# description ruckustestwlan2
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

## called-station-id-type

To set the called station ID type to, use the following command:

**called-station-id-type** [ **wlan-bssid** | **ap-mac** ]

### Syntax Description

#### **wlan-bssid**

Set the called station ID type to 'BSSID:SSID'

#### **ap-mac**

Set the called station ID type to 'APMAC:SSID'

### Defaults

wlan-bssid

### Example

```
ruckus(config-wlan)# called-station-id-type wlan-bssid
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## 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(config-wlan)# ssid ruckus2  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## beacon-interval

To set the beacon interval for mesh links, use the following command:

**beacon-interval** *NUMBER*

## Syntax Description

**beacon-interval**  
Set the beacon interval for the WLAN

*NUMBER*  
Enter the beacon interval (100~1000 TUs)

## Defaults

100

## Example

```
ruckus(config-wlan)# beacon-interval 100  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## wlan-bind

To set the radio for WLAN bind, use the following command:

**wlan-bind** <RADIO>

### Syntax

<RADIO>: [all | 2.g | 5g]

### Defaults

all

### Example

```
ruckus(config-wlan)# wlan-bind all
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

## mgmt-tx-rate

To set the transmit rate for management frames, use the following command:

**mgmt-tx-rate** *RATE*

### Syntax Description

**mgmt-tx-rate**

Set the max transmit rate for management frames

*RATE*

Set the transmit rate (in Mbps).

### Defaults

2

### Example

```
ruckus(config-wlan)# mgmt-tx-rate 2
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

## name

To set the name of the WLAN, use the following command:

**name** *NAME*

## Syntax Description

**name**  
Set the WLAN name

*NAME*  
Set to this name

## Defaults

None.

## Example

```
ruckus(config-wlan)# name ruckus2  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## type

To configure the WLAN type, use the following command:

**type [ standard-usage | guest-access | hotspot *WORD* | hs20 *WORD* | autonomous ]**

## Syntax Description

**type**  
Set the WLAN type

**standard-usage**  
Set the WLAN type to standard usage

**guest-access**  
Set the WLAN type to guest access

**hotspot *WORD***  
Set the WLAN type to Hotspot using the hotspot service specified

**hs20 *WORD***  
Set the WLAN type to Hotspot 2.0 using the HS2.0 operator specified

**autonomous**  
Set the WLAN type to Autonomous.

## Defaults

Standard usage

## Example

```
ruckus(config-wlan)# type standard-usage  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## type standard-usage

To set the WLAN type to “Standard Usage”, use the following command:

```
type standard-usage  
type standard
```

## type guest-access

To set the WLAN type to “Guest Access”, use the following command:

```
type guest-access WORD
```

### Example

```
ruckus(config-wlan)# type guest-access guestpolicy1  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## type hotspot

To set the WLAN type to “Hotspot”, use the following command:

```
type hotspot
```

## type hs20

To set the WLAN type to “Hotspot 2.0”, use the following command:

```
type hs20
```

## type autonomous

To set the WLAN type to “Autonomous”, use the following command:

```
type autonomous
```

## open

To set the authentication method to 'open', use the following command:

```
open [none | wpa2 | wpa-mixed | wep-64 | wep-128]
```

### Syntax Description

- none: Sets the authentication method to 'open' and encryption method to 'none'.
- wpa2: Sets the authentication method to 'open' and encryption method to 'WPA2'.
- AES: Sets the algorithm to AES.
- auto: Sets the algorithm to auto.
- key: Sets the WEP-64 or WEP-128 key.

## Defaults

None.

## Example

```
ruckus(config)# wlan wlan2
The WLAN service 'wlan2' has been created. To save the WLAN service, type 'end' or 'exit'.
ruckus(config-wlan)# open none
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)# end
The WLAN service 'wlan2' has been updated and saved.
Your changes have been saved.
ruckus(config)#
```

## 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** *WORD*

## Syntax Description

**mac**

Set the authentication method to 'MAC Address'

**none**

Set the encryption method to 'none'

**auth-server** *WORD*

Set the authorization server address to *WORD*

## Defaults

None.

## Example

```
ruckus(config-wlan)# mac none auth-server Ruckus-Auth-01
The command was executed successfully.
ruckus(config-wlan)#
```

## mac wpa2 passphrase algorithm AES auth-server

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** *WORD*

## 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** *WORD*

Set the authorization server address to *WORD*

## Defaults

None.

## Example

```
ruckus(config-wlan)# mac wpa2 passphrase 12345678 algorithm AES auth-server Ruckus-Auth-01
The command was executed successfully.
ruckus(config-wlan)#
```

## mac wpa-mixed passphrase algorithm AES auth-server

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

**mac wpa-mixed passphrase** *PASSPHRASE* **algorithm** *AES* **auth-server** *WORD*

## 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** *WORD*

Set the authorization server to this auth server

## Defaults

None.

## Example

```
ruckus(config-wlan)# mac wpa-mixed passphrase pass1234 algorithm AES auth-server radius
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

## mac wep-64 key key-id auth-server

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 {KEY} key-id {} KEY key-id KEY-ID auth-server WORD
```

### Syntax Description

<b>mac</b>	Set the authentication method to MAC address
<b>wep-64</b>	Set the encryption method to WEP 64-bit
<b>key KEY</b>	Set the WEP key to <i>KEY</i>
<b>key-id KEY-ID</b>	Set the WEP key ID to <i>KEY-ID</i>
<b>auth-server WORD</b>	Set the authorization server address to <i>WORD</i>

### Defaults

None.

### Example

```
ruckus(config-wlan)# mac wep-64 key 15791BD8F2 key-id 2 auth-server Ruckus-Auth-01  
The command was executed successfully.  
ruckus(config-wlan)#
```

## mac wep-128 key key-id auth-server

To set the authentication method to 'MAC Address', encryption method to 'WEP-128', key index, and WEP key, use the following command:

```
mac wep-128 KEY key-id KEY-ID auth-server WORD
```

### Syntax Description

<b>mac</b>	Set the authentication method to MAC address
<b>wep-128</b>	Set the encryption method to WEP 128-bit
<b>key KEY</b>	Set the WEP key to <i>KEY</i>
<b>key-id KEY-ID</b>	Set the WEP key ID to <i>KEY-ID</i>

**auth-server** *WORD*

Set the authorization server address to *WORD*

**Defaults**

None.

**Example**

```
ruckus(config-wlan)# mac wep-128 key 15715791BD8F212345691BD8F2 key-id 2 auth-server Ruckus-Auth-01  
The command was executed successfully.  
ruckus(config-wlan)#
```

## auth-server

To set the authentication server, use the following command:

```
auth-server <WORD>
```

### Syntax Description

**auth-server** *WORD*

Set the authorization server address to *WORD*

**local**

Set the authorization server address to *local database*

### Defaults

None.

### Example

```
ruckus(config-wlan)# mac wpa2 passphrase passphrase algorithm aes auth-server radius2  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## dot1x eap-type EAP-SIM auth-server

To set the authentication method to 'EAP-SIM', use the following command:

```
dot1x eap-type EAP-SIM auth-server [ local | name WORD ]
```

### Syntax Description

**dot1x**

Set the authentication method to '802.11x'

**eap-type**

Set the EAP type

**EAP-SIM**

Set the authentication method to EAP-SIM

**auth-server**

Set authentication server

**local**

Set the authentication server to 'local database'

**name**

Set the auth server

*WORD*

Name of the auth server

## Defaults

None.

## Example

```
ruckus(config-wlan)# dot1x eap-type EAP-SIM auth-server local  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## dot1x eap-type PEAP auth-server

To set the authentication method to 'PEAP', use the following command:

```
dot1x eap-type PEAP auth-server [ local | name WORD ]
```

## Syntax Description

### dot1x

Set the authentication method to '802.11x'

### eap-type

Set the EAP type

### PEAP

Set the authentication method to PEAP

### auth-server

Set authentication server

### local

Set the authentication server to 'local database'

### name

Set the auth server

### WORD

Name of the auth server

## Defaults

None.

## Example

```
ruckus(config-wlan)# dot1x eap-type PEAP auth-server local  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## dot1x wpa2 algorithm AES auth-server

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 [ local | name WORD ]
```

## Syntax Description

<b>dot1x</b>	Set the authentication method to '802.11x'
<b>wpa2</b>	Set the encryption method to WPA2
<b>algorithm AES</b>	Set the algorithm to AES
<b>auth-server</b>	Set authentication server
<b>local</b>	Set the authentication server to 'local database'
<b>name</b>	Set the auth server
<i>WORD</i>	Name of the auth server

## Defaults

None.

## Example

```
ruckus(config-wlan)# dot1x wpa2 algorithm AES auth-server Ruckus-RADIUS  
The command was executed successfully.  
ruckus(config-wlan)#
```

## dot1x wpa2 algorithm auto auth-server

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

```
dot1x wpa2 algorithm auto auth-server [ local | name WORD ]
```

## Syntax Description

<b>dot1x</b>	Set the authentication method to '802.11x'
<b>wpa2</b>	Set the encryption method to WPA2
<b>algorithm auto</b>	Set the algorithm to auto
<b>auth-server</b>	Set authentication server
<b>local</b>	Set the authentication server to 'local database'

**name**  
Set the auth server

*WORD*  
Name of the auth server

### Defaults

None.

### Example

```
ruckus(config-wlan)# dot1x wpa2 algorithm auto auth-server Ruckus-Auth-01  
The command was executed successfully.  
ruckus(config-wlan)#
```

## dot1x wpa-mixed algorithm AES auth-server

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

**dot1x wpa-mixed algorithm AES auth-server [ local | name *WORD* ]**

### 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**  
Set authentication server

**local**  
Set the authentication server to 'local database'

**name**  
Set the auth server

*WORD*  
Name of the auth server

### Defaults

None.

### Example

```
ruckus(config-wlan)# dot1x wpa-mixed algorithm AES auth-server local  
The command was executed successfully.  
ruckus(config-wlan)#
```

## dot1x wpa-mixed algorithm auto auth-server

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

```
dot1x wpa-mixed algorithm auto auth-server [ local | name WORD ]
```

### Syntax Description

**dot1x**

Set the authentication method to '802.11x'

**wpa-mixed**

Set the encryption method to WPA-Mixed

**algorithm auto**

Set the algorithm to Auto

**local**

Set the authentication server to 'local database'

**name**

Set the auth server

*WORD*

Name of the auth server

### Defaults

None.

### Example

```
ruckus(config-wlan)# dot1x wpa-mixed algorithm AES auth-server local  
The command was executed successfully.  
ruckus(config-wlan)#
```

## dot1x authentication encryption wep-64 auth-server

To set the authentication method to '802.1x EAP', encryption method to 'WEP-64', key index, and WEP key, use the following command:

```
dot1x authentication encryption wep-64 auth-server auth server
```

### Syntax Description

**dot1x authentication**

Set the authentication method to '802.11x'

**encryption wep-64**

Set the encryption method to WEP 64-bit

**auth-server** *auth server*

Set the auth server to *auth server*



## Defaults

None.

## Example

```
ruckus(config-wlan)# dot1x authentication encryption wep-64 auth-server Ruckus-Auth-01  
The command was executed successfully.  
ruckus(config-wlan)#
```

## dot1x wep-128 auth-server

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 [ local | name WORD ]
```

## Syntax Description

### dot1x

Set the authentication method to '802.11x'

### wep-128

Set the encryption method to WEP 128-bit

### auth-server[ local | name WORD ]

Set the auth server to local or to the named server

## Defaults

None.

## Example

```
ruckus(config-wlan)# dot1x authentication encryption wep-128 auth-server Ruckus-Auth-01  
The command was executed successfully.  
ruckus(config-wlan)#
```

## dot1x none

To set the encryption as none and authentication server to 'Local Database' or the named server, use the following command:

```
dot1x none auth-server [ local | name WORD ]
```

## Syntax Description

### dot1x none

Set the authentication method to '802.1x' and encryption to none

### [ auth-server local | name WORD ]

Set the auth server to local or to the named server

## Defaults

None.

## Example

```
ruckus(config-wlan)# dot1x none auth-server Ruckus-Auth-01  
The command was executed successfully.  
ruckus(config-wlan)#
```

## dot1x-mac none

To set the encryption as none and authentication method to 802.1x-MAC, use the following command:

```
dot1x-mac none auth-server name WORD
```

## Syntax Description

### **dot1x-mac none**

Set the authentication method to '802.1x-MAC' and encryption to none

### **auth-server name** *WORD*

Set the auth server to the named server

## Defaults

None.

## Example

```
ruckus(config-wlan)# dot1x-mac none auth-server Ruckus-Auth-01  
The command was executed successfully.  
ruckus(config-wlan)#
```

## bgscan

To enable background scanning on the WLAN, use the following command:

```
bgscan
```

## Example

```
ruckus(config-wlan)# bgscan  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## no bgscan

To disable background scanning on the WLAN, use the following command:

```
no bgscan
```

### Example

```
ruckus(config-wlan)# no bgscan  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## ft-roaming

To enable FT Roaming, use the following command:

**ft-roaming**

### Example

```
ruckus(config-wlan)# ft-roaming  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## no ft-roaming

To disable FT Roaming, use the following command:

**no ft-roaming**

## rrm-neigh-report

To enable 802.11k Neighbor-list report, use the following command:

**rrm-neigh-report**

### Example

```
ruckus(config-wlan)# rrm-neigh-report  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## no rrm-neigh-report

To disable 802.11k Neighbor-list report, use the following command:

**no rrm-neigh-report**

## https-redirection

To enable HTTPS redirection, use the following command:

**https-redirection**

## no https-redirection

To disable HTTPS redirection, use the following command:

**no https-redirection**

## client-flow-log

To enable logging of client flow data to external syslog, use the following command:

**client-flow-log**

### Example

```
ruckus(config-wlan)# client-flow-log
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

## no client-flow-log

To disable logging of client flow data to external syslog, use the following command:

**no client-flow-log**

### Example

```
ruckus(config-wlan)# no client-flow-log
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

## client-connect-log

To enable logging of client connect data, use the following command:

**client-connect-log**

### Defaults

Disabled

### Example

```
ruckus(config-wlan)# client-connect-log
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

## no client-connect-log

To disable logging of client connection data, use the following command:

**client-connect-log**

### Defaults

Disabled

## Example

```
ruckus(config-wlan)# no client-connect-log  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## bypasscna

Use the following command to bypass Apple Captive Network Assistance (CNA) on iOS and OS X devices.

### bypasscna

## Example

```
ruckus(config-wlan)# bypasscna  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## no bypasscna

To disable the bypass Apple CNA feature, use the following command:

### no bypasscna

## Example

```
ruckus(config-wlan)# no bypasscna  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## client-isolation

To enable client isolation (per-AP or across APs), use the following command:

```
client-isolation [ isolation-on-ap | isolation-on-subnet ] [ enable | disable ]
```

## Syntax Description

### client-isolation

Enable client isolation for this WLAN.

### isolation-on-ap

Enable client isolation per AP.

### isolation-on-subnet

Enable client isolation across APs.

## Example

```
ruckus(config-wlan)# client-isolation isolation-on-ap enable  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## whitelist

To apply a client isolation whitelist to this WLAN, use the following command:

```
whitelist name WORD
```

## no whitelist

To disable the whitelist for this WLAN, use the following command:

```
no whitelist
```

## load-balancing

To enable load balancing for this WLAN, use the following command:

```
load-balancing
```

### Defaults

Disabled

### Example

```
ruckus(config-wlan)# load-balancing  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## no load-balancing

To disable load balancing for this WLAN, use the following command:

```
no load-balancing
```

### Example

```
ruckus(config-wlan)# no load-balancing  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## band-balancing

To enable band balancing for this WLAN, use the following command:

```
band-balancing
```

### Defaults

Enabled.

### Example

```
ruckus(config-wlan)# band-balancing
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

## no band-balancing

To disable band balancing for this WLAN, use the following command:

**no band-balancing**

## send-eap-failure

To enable send EAP failure messages, use the following command:

**send-eap-failure**

### Defaults

Disabled

### Example

```
ruckus(config-wlan)# send-eap-failure
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

## no send-eap-failure

To disable send EAP failure messages, use the following command:

**no send-eap-failure**

### Example

```
ruckus(config-wlan)# no send-eap-failure
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

## pap-authenticator

To enable RADIUS message authenticator in PAP requests, use the following command:

**pap-authenticator**

### Example

```
ruckus(config-wlan)# pap-authenticator
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

## no pap-authenticator

To disable RADIUS message authenticator in PAP requests, use the following command:

```
no pap-authenticator
```

### Example

```
ruckus(config-wlan)# no pap-authenticator  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## nasid-type

To set the NAS ID type, use the following command:

```
nasid-type [ wlan-bssid | mac-addr | user-define WORD]
```

### Syntax Description

#### **nasid-type**

Set the NAS ID type

#### **wlan-bssid**

Set NAS ID type WLAN-BSSID (default)

#### **mac-addr**

Set NAS ID type to Controller MAC Address

#### **user-define** *WORD*

Set NAS ID type to a user-defined string

### Defaults

WLAN-BSSID

### Example

```
ruckus(config-wlan)# nasid-type wlan-bssid  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## priority low

To set the WLAN priority to low, use the following command:

```
priority low
```

## priority high

To set the WLAN priority to high, use the following command:

```
priority high
```



## web-auth

To enable Web authentication, use the following command:

```
web-auth [ local | name WORD ]
```

### Syntax Description

**web-auth**

Enable Web authentication

**local**

Use local database as auth server

**name**

Specify an external auth server

*WORD*

The AAA server to use for Web authentication

### Defaults

None

### Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan)# web-auth Ruckus-RADIUS
The command was executed successfully.
ruckus(config-wlan)#
```

## 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
ruckus(config-wlan)# no web-auth
The command was executed successfully.
```

## grace-period

To enable and set a maximum time (in minutes) for which users must re-authenticate after disconnecting, use the following command:

**grace-period** *NUMBER*

### Syntax Description

**grace-period**

Enables and Sets a maximum time (in minutes) for which users must re-authenticate after disconnecting.

### Defaults

Disabled.

### Example

```
ruckus(config-wlan)# grace-period 20  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## no grace-period

To disable the grace period, use the following command:

**no grace-period** *NUMBER*

### Syntax Description

**no grace-period**

Disables the grace period timeout.

### Defaults

Disabled.

### Example

```
ruckus(config-wlan)# no grace-period  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## acct-server

To set the accounting server, use the following command:

**acct-server** *WORD*

### Syntax Description

**acct-server**

Configure the AAA server

*WORD*

Set the AAA server to this address

## Defaults

None.

## Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan)# acct-server Ruckus-Acct-01
The command was executed successfully.
```

## acct-server interim-update

To configure the interim update frequency (in minutes) of the AAA server, use the following command:

**acct-server** *WORD* **interim-update** *NUMBER*

## Syntax Description

### **acct-server**

Configure the interim update frequency of the AAA server

### **interim-update{minutes}**

Set the update frequency to this value (in minutes)

## Defaults

5 (minutes)

## Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan)# acct-server Ruckus-Acct-01 interim-update 5
The command was executed successfully.
```

## no acct-server

To disable the AAA server, use the following command:

**no acct-server**

## Syntax Description

### **no acct-server**

Disable AAA server authentication

## Defaults

None.

## Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan)# no acct-server
The command was executed successfully.
```

## inactivity-timeout

To set the inactivity timeout to the specified number in minutes, use the following command:

**inactivity-timeout** *NUMBER*

### Syntax Description

#### **inactivity-timeout**

Enable and set the inactivity timeout

*NUMBER*

Set the inactivity timeout in minutes (1-500 min.)

## Defaults

5

## Example

```
ruckus(config-wlan)# inactivity-timeout 15
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

## web-auth-timeout

To enable and set the web authentication timeout time to the specified number in minutes, use the following command:

**web-auth-timeout** *NUMBER*

### Syntax Description

#### **web-auth-timeout**

Enable and set the web authentication timeout

*NUMBER*

Set the inactivity timeout in minutes

## Defaults

5

## Example

```
ruckus(config-wlan)# web-auth-timeout 15
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

## vlan

To set the VLAN ID for the WLAN, use the following command:

**vlan** *NUMBER*

### Syntax Description

**vlan**

Enable VLAN

*NUMBER*

Set the VLAN ID to this value

### Defaults

1

## Example

```
ruckus(config-wlan)# vlan 123
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

## dynamic-vlan

To enable dynamic VLAN, use the following command:

**dynamic-vlan**

### Syntax Description

**dynamic-vlan**

Enable dynamic VLAN

### Usage Guidelines

Dynamic VLAN can be enabled or disabled in the following two conditions: 1) The authentication method is '802.1X/EAP' or 'MAC Address', Encryption method is WPA, WPA2, WPA mixed, or none. 2) Authentication method is 'Open', Encryption method is WPA, WPA2 (Algorithm may not be Auto), enable Zero-IT Activation, enable Dynamic PSK.

## Example

```
ruckus(config-wlan)# dynamic-vlan
The command was executed successfully. To save the changes, type 'end' or 'exit'
```

## no dynamic-vlan

To disable dynamic VLAN, use the following command:

**no dynamic-vlan**

### *Syntax Description*

**no dynamic-vlan**

Disable dynamic VLAN

### *Defaults*

Disabled.

### *Example*

```
ruckus(config-wlan)# no dynamic-vlan  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## mcast-filter

To enable multicast filter for the WLAN, use the following command:

**mcast-filter**

## no mcast-filter

To disable multicast filter for the WLAN, use the following command:

**no mcast-filter**

## 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*

Disabled

## Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan)# hide-ssid
The command was executed successfully.
```

## 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

Disabled

## Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan)# no hide-ssid
The command was executed successfully
```

## ofdm-only

To enable support of OFDM rates only, use the following command:

**ofdm-only**

## no ofdm-only

To disable OFDM only rates, use the following command:

**no ofdm-only**

## admission-control

To enable Call Admission Control, use the following command:

**admission-control**

## no admission-control

To disable Call Admissino Control, use the following command:

**no admission-control**

## bss-minrate

To set the minimum BSS transmission rate of the WLAN (in Mbps), use the following command:

```
bss-minrate NUMBER
```

### Syntax Description

#### **bss-minrate**

Set the minimum BSS transmission rate in Mbps.

*NUMBER*

Minimum BSS transmission rate

### Defaults

None.

### Example

```
ruckus(config-wlan)# bss-minrate 2  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## no bss-minrate

To disable the minimum BSS transmission rate for the WLAN, use the following command:

```
no bss-minrate
```



## dtim-period

To set the DTIM period of the WLAN, use the following command:

```
dtim-period NUMBER
```

### Syntax Description

#### **dtim-period**

Sets the DTIM period of the WLAN (1-255).

*NUMBER*

DTIM period.

### Defaults

1

### Example

```
ruckus(config-wlan)# dtim-period 5  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## no dtim-period

To set the DTIM period of the WLAN to 1 (default), use the following command:

**no dtim-period**

### *Syntax Description*

**no dtim-period**

Set the DTIM period to 1.

### *Defaults*

1

### *Example*

```
ruckus(config-wlan)# no dtim-period  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## directed-threshold

To set the Directed MC/BC threshold of the WLAN (0-128), use the following command:

**directed-threshold** *NUMBER*

### Syntax Description

#### **directed-threshold**

Set the Directed MC/BC threshold of the WLAN.

*NUMBER*

Directed threshold (0-128)

### Defaults

5

### Example

```
ruckus(config-wlan)# directed-threshold 5
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

## no directed-threshold

To set the Directed MC/BC threshold of the WLAN to 5 (default), use the following command:

**no directed-threshold**

### Syntax Description

**no directed-threshold**

Sets the Directed Multicast/Broadcast threshold to 5.

### Defaults

5

### Example

```
ruckus(config-wlan)# no directed-threshold
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

## tunnel-mode

To enable tunnel mode, use the following command:

**tunnel-mode**

### Syntax Description

**tunnel-mode**

Enable tunnel mode

### Defaults

Disabled.

### Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan)# tunnel-mode
The command was executed successfully.
```

## no tunnel-mode

To disable the tunnel mode, use the following command:

**no tunnel-mode**

## Syntax Description

### **no tunnel-mode**

Disable the tunnel mode

## Defaults

Disabled.

## Example

```
ruckus# config
ruckus(config)# wlan wlan-123
ruckus(config-wlan-wlan-123)# no tunnel-mode
The command was executed successfully.
```

## dhcp-relay

To set the DHCP relay server to the specified address (tunneled WLANs only), use the following command:

**dhcp-relay** *WORD*

## no dhcp-relay

To disable DHCP relay, use the following command:

**no dhcp-relay**

## smart-roam

To enable and set SmartRoam with the specified roam factor (1-10), use the following command:

**smart-roam** *NUMBER/EMPTY*

## no smart-roam

To disable the SmartRoam feature, use the following command:

**no smart-roam**

## force-dhcp

To enable the Force DHCP option, use the following command:

**force-dhcp**

## Defaults

Disabled

### Example

```
ruckus(config-wlan)# force-dhcp
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

## force-dhcp-timeout

To disconnect the client if it does not obtain valid IP address within the specified timeout period (in seconds), use the following command:

**force-dhcp-timeout** *NUMBER*

### Defaults

10 seconds

### Example

```
ruckus(config-wlan)# force-dhcp-timeout 10
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

## no force-dhcp

To disable the Force DHCP option, use the following command:

**no force-dhcp**

## Configuring DHCP Option 82 Sub-Option Settings

Use the following commands to enable DHCP Option 82 and configure sub-option settings for a WLAN.

Execute this command from within the *config-wlan* context to enter the *config-wlan-option82* context and configure option 82 sub-option settings.

### Example

```
ruckus(config-wlan)# option82
Sets the DHCP option82 with default value.
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan-option82)#
```

### option82

To enable DHCP option 82 and enter the config-wlan-option82 context, use the following command:

**option82**

### Defaults

Disabled

### Syntax Description

#### **subopt1**

Enables and sets the DHCP option 82 sub-option1.

#### **subopt1 disable**

Disables the DHCP option 82 sub-option1.

#### **subopt1 rks-circuitid**

sets the DHCP option 82 sub-option1 is RKS\_CircuitID.

#### **subopt1 ap-mac-hex**

sets the DHCP option 82 sub-option1 is AP-MAC.

#### **subopt1 ap-mac-hex-ssid**

sets the DHCP option 82 sub-option1 is AP-MAC and ESSID.

#### **subopt2**

Enables and sets the DHCP option 82 sub-option2.

#### **subopt2 disable**

Disables the DHCP option 82 sub-option2.

#### **subopt2 client-mac-hex**

sets the DHCP option 82 sub-option2 is Client-Mac.

#### **subopt2 client-mac-hex-ssid**

sets the DHCP option 82 sub-option2 is Client-Mac and Essid.

#### **subopt2 ap-mac-hex**

sets the DHCP option 82 sub-option2 is AP-MAC.

**subopt2 ap-mac-hex-ssid**

sets the DHCP option 82 sub-option2 is AP-MAC and ESSID.

**subopt2 cuid**

Sets the DHCP option 82 sub-option2 is CUID.

**subopt150**

Enables and sets the DHCP option 82 sub-option150.

**subopt150 disable**

Disables the DHCP option 82 sub-option150.

**subopt150 vlan-id**

sets the DHCP option 82 sub-option150 is Vlan ID.

**subopt151**

Enables and sets the DHCP option 82 sub-option151.

**subopt151 disable**

Disables the DHCP option 82 sub-option151.

**subopt151 area-name** *WORD/NAME*

Sets the DHCP option 82 sub-option151's Area Name.

**subopt151 ssid**

Sets the DHCP option 82 sub-option151 is Essid.

## **no option82**

To disable DHCP option 82, use the following command:

**no option82**

## **sta-info-extraction**

To enable station information extraction (client fingerprinting), use the following command:

**sta-info-extraction**

## **Defaults**

Enabled

## **no sta-info-extraction**

To disable station information extraction (client fingerprinting), use the following command:

**no sta-info-extraction**

## **zero-it-activation**

To enable Zero-IT activation, use the following command:

**zero-it-activation**

**zero-it**



### Syntax Description

- zero-it-activation**  
Enable Zero-IT activation
- zero-it**  
Enable Zero-IT activation

### Defaults

Disabled.

### Example

```
ruckus(config-wlan)# zero-it-activation  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## no zero-it-activation

To disable Zero-IT activation, use the following command:

- no zero-it-activation**
- no zero-it**

### Syntax Description

- no zero-it-activation**  
Disable Zero-IT activation
- no zero-it**  
Disable Zero-IT activation

### Defaults

Disabled.

### Example

```
ruckus(config-wlan)# no zero-it  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## max-clients

To set the maximum number of clients for a specific WLAN, use the following command:

- max-clients** *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

100

### Example

```
ruckus(config-wlan)# max-clients 100
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

## 802dot11d

To enable 802.11d for the WLAN, use the following command:

**802dot11d**

### Defaults

Enabled

## no 802dot11d

To disable 802.11d for the WLAN, use the following command:

**no 802dot11d**

## arc

Use the following command to enable Application Recognition & Control:

**arc**

### Defaults

Disabled

### Example

```
ruckus(config-wlan)# arc
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

## no arc

Use the following command to disable Application Recognition and Control:

**no arc**

## apply-policy-group

Use the following command to apply an application denial policy to the WLAN:

**apply-policy-group** *WORD*

### Defaults

None

### Example

```
ruckus(config-wlan)# apply-policy-group facebook
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

## auto-proxy

To enable auto-proxy and set the location of the wpad.dat file, use the following command:

**auto-proxy** [**wpad-saved-on-zd** | **wpad-saved-on-external-server**] **url** *WORD*

### Syntax Description

#### **auto-proxy**

Enable auto-proxy and specify the location of the wpad.dat file

#### **wpad-saved-on-ZD**

WPAD.DAT file is saved on ZoneDirector

#### **wpad-saved-on-external-server**

WPAD.DAT file is saved on an external server

#### **url**

Specify the WPAD URL configured on DHCP/DNS server

#### *WORD*

Auto-proxy path and file name

### Defaults

None.

### Example

```
ruckus(config-wlan)# auto-proxy wpad-saved-on-zd url 192.168.0.2/wpad.dat
The file has been loaded into ZoneDirector successfully,Please use 'import' to apply it
ruckus(config-wlan)#
```

## no auto-proxy

To disable auto-proxy, use the following command:

```
no auto-proxy
```

## pmk-cache

To set the PMK cache time to the specified number in minutes (1~720 minutes), use the following command:

```
pmk-cache timeout NUMBER
```

### Defaults

720 minutes

## no pmk-cache

To disable PMK cache, use the following command:

```
no pmk-cache
```

## pmk-cache-for-reconnect

To apply PMK cache when client reconnects (default), use the following command:

```
pmk-cache-for-reconnect
```

## no pmk-cache-for-reconnect

To disable application of PMK caching when client reconnects, use the following command:

```
no pmk-cache-for-reconnect
```

### Defaults

Enabled

### Usage Guidelines

When “no pmk-cache-for-reconnect” is set, the controller attempts to look up PMK cache for roaming clients only, so every client reconnection requires a full reauthentication. A graceful roaming (disconnect before connecting to the roam-to AP) is not regarded as roaming from the controller’s perspective.

## roaming-acct-interim-update

To enable accounting interim-updates when a client roams, use the following command:

```
roaming-acct-interim-update
```

## Defaults

Disabled.

## Usage Guidelines

When “roaming-acct-interim-update” is set, all traffic and session-id data from the original session is carried over to the new session.

## no roaming-acct-interim-update

To disable accounting interim updates when a client roams (default: disabled), use the following command:

**no roaming-acct-interim-update**

# Configuring Dynamic PSKs

Use the following commands to enable and configure Ruckus Dynamic Pre-Shared Key functionality for the WLAN.

## dynamic-psk enable

To enable Dynamic Pre-Shared Keys, use the following command:

**dynamic-psk enable**

### Syntax Description

**dynamic-psk enable**

Enable Dynamic PSK

### Defaults

None.

### Example

```
ruckus(config-wlan)# dynamic-psk enable
The DPSK can't be enabled or disabled when the wlan type is not Standard Usage and Encryption method is
not WPA or WPA2 and Authentication method is not open and Zero-IT is not enabled.
ruckus(config-wlan)# zero-it
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)# dynamic-psk enable
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

## dynamic-psk passphrase-len

To set the Dynamic Pre-Shared Key passphrase length, use the following command:

**dynamic-psk passphrase-len** *NUMBER*

## dynamic-psk type

To sets the type of dynamic PSK (secure or mobile-friendly), use the following command:

**dynamic-psk type** [mobile-friendly | secure]

### Syntax Description

**dynamic-psk type**

Set the DPSK type

**mobile-friendly**

Set the DPSK type to mobile-friendly

**secure**

Set the DPSK type to secure

## Defaults

Secure

## Example

```
ruckus(config-wlan)# dynamic-psk type mobile-friendly
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

## no dynamic-psk

To disable Dynamic Pre-Shared Keys on the WLAN, use the following command:

**no dynamic-psk**

## limit-dpsk

To enable Dynamic PSK limits and set the max number of devices per user, use the following command:

**limit-dpsk** *NUMBER*

## no limit-dpsk

To disable Dynamic PSK limits, use the following command:

**no limit-dpsk**

## dynamic-psk-expiration

To set the WLAN Dynamic PSK expiration, use the following command:

**dynamic-psk-expiration** [ **length** | **start-point** ] *WORD*

## Syntax Description

### **dynamic-psk-expiration**

Sets the DPSK expiration.

### **length**

Sets the DPSK expiration length.

### **unlimited**

Sets wlan dynamic psk expiration to unlimited.

### **one-day**

Sets wlan dynamic psk expiration to one day.

### **one-week**

Sets wlan dynamic psk expiration to one week.

### **two-weeks**

Sets wlan dynamic psk expiration to two weeks.

**one-month**

Sets wlan dynamic psk expiration to one month.

**two-months**

Sets wlan dynamic psk expiration to two months.

**three-months**

Sets wlan dynamic psk expiration to three months.

**half-a-year**

Sets wlan dynamic psk expiration to half a year.

**one-year**

Sets wlan dynamic psk expiration to one year.

**two-years**

Sets wlan dynamic psk expiration to two years.

**start-point**

Sets the DPSK validity start-point.

**first-use**

The D-PSK expiration will be calculated from when it is first used.

**creation-time**

The D-PSK expiration will be calculated from when it is created.

**Example**

```
ruckus(config-wlan)# dynamic-psk-expiration start-point first-use
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)# dynamic-psk-expiration length one-week
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)#
```

**no l2acl**

To disable Layer 2 Access Control Lists, use the following command:

**no l2acl**

**no role-based-access-ctrl**

To disable role based access control policy service, use the following command:

**no role-based-access-ctrl**

**no l3acl**

To disable Layer 3/4 ACLs, use the following command:

**no l3acl**



## no l3acl-ipv6

To disable Layer 3/4 IPv6 ACLs, use the following command:

```
no l3acl-ipv6
```

## no dvcpcy

To disable device policy for this WLAN, use the following command:

```
no dvcpcy
```

## rate-limit

To set the rate limiting for the WLAN, use the following command:

```
rate-limit uplink NUMBER downlink NUMBER
```

### Syntax Description

#### **rate-limit**

Set the rate limit

#### **uplink**

Set the uplink rate limit

#### **downlink**

Set the downlink rate limit

#### *NUMBER*

Set the rate limiting to the value specified.

### Defaults

None.

### Example

```
ruckus(config-wlan)# rate-limit uplink 20 downlink 20  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## no rate-limit

To disable the rate limit, use the following command:

```
no rate-limit
```

### Syntax Description

#### **no rate-limit**

Disable rate limiting for the WLAN

## Defaults

Disabled.

## Example

```
ruckus(config-wlan)# no rate-limit  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## no mac-addr-format

Sets MAC auth username and password to format aabbccddeeff.

## mac-addr-format

Sets MAC auth username and password to one of the following formats:

### **mac-addr-format aa-bb-cc-dd-ee-ff**

Sets MAC auth username and password to format aa-bb-cc-dd-ee-ff.

### **mac-addr-format aa:bb:cc:dd:ee:ff**

Sets MAC auth username and password to format aa:bb:cc:dd:ee:ff.

### **mac-addr-format AABCCDDEEFF**

Sets MAC auth username and password to format AABCCDDEEFF.

### **mac-addr-format AA-BB-CC-DD-EE-FF**

Sets MAC auth username and password to format AA-BB-CC-DD-EE-FF.

### **mac-addr-format AA:BB:CC:DD:EE:FF**

Sets MAC auth username and password to format AA:BB:CC:DD:EE:FF.

## acl dvpcpy

To apply a Device Policy to the WLAN, use the following command:

```
acl dvpcpy WORD
```

## acl prece

To apply a Precedence Policy to the WLAN, use the following command:

```
acl prece WORD
```

## acl role-based-access-ctrl

To enable Role based Access Control Policy on the WLAN, use the following command:

```
acl role-based-access-ctrl
```

## Defaults

Disabled

## Example

```
ruckus(config-wlan)# acl role-based-access-ctrl  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlan)#
```

## qos classification

To enable Quality of Service classification, use the following command:

```
qos classification
```

## no qos classification

To disable Quality of Service classification, use the following command:

```
no qos classification
```

## qos heuristics-udp

To enable QoS heuristics for UDP traffic, use the following command:

```
qos heuristics-udp
```

## no qos heuristics-udp

To disable QoS heuristics for UDP traffic, use the following command:

```
no qos heuristics-udp
```

## qos directed-multicast

To enable QoS directed multicast, use the following command:

```
qos directed-multicast
```

## no qos directed-multicast

To disable QoS directed multicast, use the following command:

```
no qos directed-multicast
```

## qos igmp-snooping

To disable QoS directed multicast, use the following command:

```
qos igmp-snooping
```

## no qos igmp-snooping

To disable QoS IGMP snooping, use the following command:

**no qos igmp-snooping**

## qos mld-snooping

To enable QoS MLD snooping, use the following command:

**no qos mld-snooping**

## no qos mld-snooping

To disable QoS MLD snooping, use the following command:

**no qos mld-snooping**

## qos tos-classification

To enable QoS TOS classification, use the following command:

**qos tos-classification**

## no qos tos-classification

To disable QoS TOS classification, use the following command:

**no qos tos-classification**

## qos priority high

To set QoS priority to 'high', use the following command:

**qos priority high**

## qos priority low

To set QoS priority to 'low', use the following command:

**qos priority low**

## qos directed-threshold

To set the QoS directed threshold, use the following command:

**qos directed-threshold** *NUMBER*

## disable-dgaf

To disable Downstream Group-Address Frame Forwarding, use the following command (Hotspot 2.0 WLAN only):

**disable-dgaf**

## no disable-dgaf

To enable Downstream Group-Address Frame Forwarding, use the following command (Hotspot 2.0 WLAN only):

```
no disable-dgaf
```

## proxy-arp

To enable Proxy ARP service for the WLAN, use the following command:

```
proxy-arp
```

## no proxy-arp

To disable Proxy ARP service for the WLAN, use the following command:

```
no proxy-arp
```

## 80211w-pmf

To enable 802.11w PM, use the following command:

```
80211w-pmf
```

## no 80211w-pmf

To disable 802.11w PMF, use the following command:

```
no 80211w-pmf
```

## ignor-unauth-stats

To enable ignoring unauthorized client statistics, use the following command:

```
ignor-unauth-stats
```

## no ignor-unauth-stats

To disable ignoring unauthorized client statistics, use the following command:

```
no ignor-unauth-stats
```

## show

To display the WLAN settings, use the following command:

```
show
```

### *Syntax Description*

```
show
```

Display WLAN settings

## Defaults

None.

## Example

```
ruckus(config)# wlan ruckus1
The WLAN service 'ruckus1' has been loaded. To save the WLAN service, type 'end' or 'exit'.
ruckus(config-wlan)# show
WLAN Service:
ID:
  1:
    NAME = Ruckus-Wireless-1
    Tx. Rate of Management Frame(2.4GHz) = 2.0Mbps
    Tx. Rate of Management Frame(5GHz)   = 6.0Mbps
    Beacon Interval = 100ms
    SSID = Ruckus-Wireless-1
    Description = Ruckus-Wireless-1
    Type = Standard Usage
    Authentication = open
    Encryption = wpa
    Algorithm = aes
    Passphrase = password
    FT Roaming = Disabled
    802.11k Neighbor report = Disabled
    Web Authentication = Disabled
    Authentication Server = Disabled
    Accounting Server = Disabled
    Called-Station-Id type = wlan-bssid
    Tunnel Mode = Disabled
    DHCP relay = Disabled
    Max. Clients = 100
    Isolation per AP = Disabled
    Isolation across AP = Disabled
    Zero-IT Activation = Enabled
    Load Balancing = Disabled
    Band Balancing = Disabled
    Dynamic PSK = Enabled
    Dynamic PSK Passphrase Length =
    Limit Dynamic PSK = Disabled
    Auto-Proxy configuration:
      Status = Disabled
    Inactivity Timeout:
      Status = Disabled
    VLAN-ID = 1
    Dynamic VLAN = Disabled
    Closed System = Disabled
    OFDM-Only State = Disabled
    Multicast Filter State = Disabled
    802.11d State = Disabled
    Force DHCP State = Disabled
    Force DHCP Timeout = 0
    DHCP Option82:
      Status = Disabled
      Option82 sub-Option1 = Disabled
      Option82 sub-Option2 = Disabled
      Option82 sub-Option150 = Disabled
      Option82 sub-Option151 = Disabled
    Ignore unauthorized client statistic = Disabled
    STA Info Extraction State = Enabled
    BSS Minrate = Disabled
    Call Admission Control State = Disabled
    PMK Cache Timeout= 720 minutes
    PMK Cache for Reconnect= Enabled
    NAS-ID Type= wlan-bssid
    Roaming Acct-Interim-Update= Disabled
    PAP Message Authenticator = Enabled
    Send EAP-Failure = Disabled
    L2/MAC = No ACLS
```

```
L3/L4/IP Address = No ACLS  
L3/L4/IPv6 Address = No ACLS  
Precedence = No ACLS  
Proxy ARP = Disabled  
Device Policy = No ACLS  
Role based Access Control Policy = Disabled  
SmartRoam = Disabled Roam-factor = 1  
White List = No ACLS  
Application Visibility = disabled  
Apply Policy Group = No_Denys
```

```
ruckus(config)#
```

# 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** *WORD*

### Syntax Description

**wlan-group**

Configure the WLAN group

*WORD*

Name of the WLAN group

### Defaults

Default.

### Example

```
ruckus# config
ruckus(config)# wlan-group wlangroup2
The WLAN group 'wlangroup2' has been created. To save the WLAN group, type 'end' or 'exit'.
ruckus(config-wlangrp)#
```

## no wlan-group

To delete a WLAN group from the list, use the following command:

**no wlan-group** *WORD*

### Syntax Description

**no wlan-group**

Delete the WLAN group

*WORD*

Name of the WLAN group

### Defaults

None.

### Example

```
ruckus(config)# no wlan-group wlan-grp-01
The WLAN group 'wlan-grp-01' has been removed.
ruckus(config)#
```



## abort

To exit the wlan-group context without saving changes, use the abort command. Enter this command from within the context of the WLAN group that you are configuring.

**abort**

### Syntax Description

**abort**

Exit the WLAN group without saving changes

### Defaults

None.

### Example

```
ruckus# config
ruckus(config)# wlan-group wlangroup2
The WLAN group 'wlangroup2' has been created. To save the WLAN group, type 'end' or 'exit'.
ruckus(config-wlangrp)# abort
No changes have been saved.
ruckus(config)#
```

## 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 wlangroup2
The WLAN group 'wlangroup2' has been created. To save the WLAN group, type 'end' or 'exit'.
ruckus(config-wlangrp)# end
The WLAN group 'wlangroup2' has been updated.
Your changes have been saved.
ruckus(config)#
```

## 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# config
ruckus(config)# wlan-group wlangroup2
The WLAN group entry 'wlangroup2' has been loaded. To save the WLAN group, type 'end' or 'exit'.
ruckus(config-wlangrp)# exit
The WLAN group 'wlangroup2' has been updated.
Your changes have been saved.
ruckus(config)#
```

## quit

To exit the wlan-group context without saving changes, use the following command. Enter this command from within the context of the WLAN group that you are configuring.

**quit**

### Syntax Description

**quit**

Exit the WLAN group without saving changes

### Defaults

None.

### Example

```
ruckus# config
ruckus(config)# wlan-group wlangroup2
The WLAN group entry 'wlangroup2' has been loaded. To save the WLAN group, type 'end' or 'exit'.
ruckus(config-wlangrp)# quit
No changes have been saved.
ruckus(config)#
```

## 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** *WORD*

### Syntax Description

#### **name**

Configure the WLAN group name

#### *WORD*

Set the WLAN group name to this value

### Defaults

None.

### Example

```
ruckus# config
ruckus(config)# wlan-group wlangroup2
The WLAN group entry 'wlangroup2' has been loaded. To save the WLAN group, type 'end' or 'exit'.
ruckus(config-wlangrp)# name wlangroup2
ruckus(config-wlangrp)# show
WLAN Group:
  ID:
    2:
      Name= wlangroup2
      Description=
      WLAN Service=

ruckus(config-wlangrp)#
```

## 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. Multiple word text must be enclosed in quotes.

**description** *WORD*

### Syntax Description

#### **description**

Configure the WLAN group description

#### *WORD*

Set the WLAN group description to this value

### Defaults

None.

## Example

```
ruckus# config
ruckus(config)# wlan-group wlangroup2
ruckus(config-wlangrp)# description "WLAN Group 2"
ruckus(config-wlangrp)# show
WLAN Group:
  ID:
    2:
      Name= wlangroup2
      Description= WLAN Group 2
      WLAN Service:

ruckus(config-wlangrp)#
```

## wlan

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

**wlan** *WORD*

## Syntax Description

### **wlan**

Add a WLAN to the WLAN group

### *WORD*

Name of the WLAN to be added

## Defaults

None.

## Example

```
ruckus(config-wlangrp)# wlan ruckus1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlangrp)# show
WLAN Group:
  ID:
    :
      Name= wlangroup1
      Description=
      WLAN Service:
        WLAN1:
          NAME= ruckus1
          VLAN=

ruckus(config-wlangrp)#
```

## no wlan

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

**no wlan** *WORD*

## Syntax Description

### **no wlan**

Delete an existing WLAN service from the WLAN group

### *WORD*

Name of the WLAN to be removed

## Defaults

None.

## Example

```
ruckus(config-wlangrp)# no wlan ruckus1  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlangrp)#
```

## 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 *WORD* vlan override none**

## Syntax Description

### **wlan *WORD***

Add the WLAN to the WLAN group

### **vlan override none**

Set the VLAN tag to No Change

## Defaults

None.

## Example

```
ruckus(config-wlangrp)# wlan ruckus1 vlan override none  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-wlangrp)#
```

## wlan vlan override tag

To add a WLAN service to the WLAN group and set the VLAN tag to the specified VLAN ID, use the following command:

**wlan *NAME* vlan override tag *NUMBER***

## Syntax Description

### **wlan *NAME***

**Add the *NAME* to the WLAN group**

**vlan override tag** *NUMBER*

Set the VLAN tag of *NAME* to the specified *NUMBER*

**Defaults**

None.

**Example**

```
ruckus(config-wlangrp)# wlan ruckus1 vlan override tag 12
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlangrp)#
```

**show**

To display WLAN group settings, use the following command:

**show**

**Defaults**

**ruckus(config-wlangrp)# show**

```
WLAN Group:
ID:
1:
Name= Default
Description= Default WLANs for Access Points
WLAN Service:
WLAN1:
NAME= Ruckus1
VLAN=
```

**ruckus(config-wlangrp)#**

# Configure Role Commands

Use the role commands to configure user roles on the controller. To run these commands, you must first enter the **config-role** context.

## role

To create a new role or modify an existing role, use the following command:

**role** *WORD*

### Syntax Description

**role**

Create or modify a user role

*WORD*

Name of role

### Defaults

None.

### Example

```
ruckus(config)# role role1
The role entry 'role1' has been created
ruckus(config-role)#
```

## no role

To delete a role entry from the list, use the following command:

**no role** *WORD*

### Syntax Description

**no role**

Delete a user role

*WORD*

Name of role

### Defaults

None.

### Example

```
ruckus(config)# no role role1
The Role 'role1' has been deleted.
ruckus(config)#
```

## abort

To exit the config-role context without saving changes, use the abort command. Enter this command from within the context of the role that you are configuring.

**abort**

### Syntax Description

**abort**

Exit the role without saving changes

### Defaults

None.

### Example

```
ruckus(config-role)# abort
No changes have been saved.
ruckus(config)#
```

## end

To save changes, and then exit the config-role context, use the following command:

**end**

### Syntax Description

**end**

Save changes, and then exit the context

### Defaults

None.

### Example

```
ruckus(config-role)# end
The Role entry has saved successfully.
Your changes have been saved.
ruckus(config)#
```

## exit

To save changes, and then exit the config-role context, use the following command:

**exit**



## Syntax Description

### **exit**

Save changes, and then exit the context

## Defaults

None.

## Example

```
ruckus(config-role)# exit
The Role entry has saved successfully.
Your changes have been saved.
ruckus(config)#
```

## quit

To exit the config-role context without saving changes, use the quit command. Enter this command from within the context of the role that you are configuring.

### **quit**

## Syntax Description

### **quit**

Exit the role without saving changes

## Defaults

None.

## Example

```
ruckus(config-role)# quit
No changes have been saved.
ruckus(config)#
```

## name

To set the name of a user role, use the following command:

**name** *WORD*

## Syntax Description

### **name**

Set the name of a user role

### *WORD*

Set to this role

## Defaults

None.

## Example

```
ruckus(config-role)# name guest33  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## description

To set the description for a user role, use the following command:

**description** *WORD*

### Syntax Description

#### **description**

Set the description of a user role

*WORD*

Set to this description

## Defaults

None.

## Example

```
ruckus(config-role)# description testforCLI  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## group-attributes

To set the group attributes of a user role, use the following command:

**group-attributes** *WORD*

### Syntax Description

#### **group-attributes**

Set the attributes of a user role

*WORD*

Set to this attribute

## Defaults

None.

## Example

```
ruckus(config-role)# group-attributes ruckus1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## wlan-allowed

To set the WLANs to which a user role will have access, use the following command:

```
wlan-allowed [ all | specify-wlan ]
```

### Syntax Description

#### **wlan-allowed**

Set the WLANs to which a role will have access

#### **all**

Grant access to all WLANs

#### **specify-wlan**

Grant access to a specific WLAN

### Defaults

None.

## Example

```
ruckus(config-role)# wlan-allowed all
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-role)# wlan-allowed specify-wlan
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## specify-wlan-access

To add a particular WLAN to the list of WLANs that a user role can access, use the following command:

```
specify-wlan-access wlan_ssid
```

### Syntax Description

#### **specify-wlan-access**

Add access to a WLAN by a user role

#### *wlan\_ssid*

Add access to this WLAN

### Defaults

None.

### Example

```
ruckus(config-role)# specify-wlan-access joejoe98  
The wlan 'joejoe98' has been added to the Role.
```

## no specify-wlan-access

To remove a particular WLAN from the list of WLANs that a user role can access, use the following command:

```
no specify-wlan-access WORD/SSID
```

### Syntax Description

#### **no specify-wlan-access**

Remove access to a WLAN by a user role

*WORD/SSID*

Remove access to this WLAN

### Defaults

None.

### Example

```
ruckus(config-role)# no specify-wlan-access joejoe98  
The wlan 'joejoe98' has been removed from the Role.
```

## guest-pass-generation

To add guest pass generation privileges to a user role, use the following command:

```
guest-pass-generation
```

### Syntax Description

#### **guest-pass-generation**

Add guest pass generation privileges to a user role

### Defaults

None.

### Example

```
ruckus(config-role)# guest-pass-generation  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## no guest-pass-generation

To remove guest pass generation privileges from a user role, use the following command:

**no guest-pass-generation**

### **Syntax Description**

**no guest-pass-generation**

Remove guest pass generation privileges from a user role

### **Defaults**

None.

### **Example**

```
ruckus(config-role)# no guest-pass-generation  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## **admin**

To add ZoneDirector administration privileges to a user role, use the following command:

**admin [ super | operator | monitoring ]**

### **Syntax Description**

**admin**

Add ZoneDirector administration privileges to a user role

**super**

Sets to Super (Perform all configuration and management tasks)

**operator**

Sets to Operator (Change settings affecting single AP's only)

**monitoring**

Sets to Monitoring (Monitoring and viewing operation status only)

### **Defaults**

None.

### **Example**

```
ruckus(config-role)# admin super  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## **no admin**

To remove ZoneDirector administration privileges from a user role, use the following command:

**no admin**

## Syntax Description

### **no admin**

Remove ZoneDirector administration privileges from a user role

## Defaults

None.

## Example

```
ruckus(config-role)# no admin
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## access-ctrl

Enables access control policy.

## Defaults

Disabled

## Example

```
ruckus(config)# role role1
The Role entry 'role1' has been created.
ruckus(config-role)# access-ctrl
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-role)# show
Role:
  ID:
  :
  Name= role1
  Description=
  Group Attributes=
  Guest Pass Generation= Disallowed
  ZoneDirector Administration:
    Status= Disallowed
  Allow All WLANs:
    Mode= Allow Specify WLAN access
  Access Control Policy= Allowed
  Allow All OS Types:
    Mode= Allow all OS types to access
  VLAN = Any
  Rate Limiting Uplink = Disabled
  Rate Limiting Downlink = Disabled

ruckus(config-role)#
```

## no access-ctrl

Disables access control policy.

### **no access-ctrl**

## os-type-allowed all

Allows all OS types to access.

**os-type-allowed all**

## os-type-allowed specify

Specifies OS types access.

**os-type-allowed specify**

## specify-os-type-access

Adds the specify OS type into the role entry.

**specify-os-type-access** *WORD*

### Defaults

None

### Example

```
ruckus(config)# role role1
The Role entry 'role1' has been created.
ruckus(config-role)# access-ctrl
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-role)# os-type-allowed specify
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-role)# specify-os-type-access Windows
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-role)#
```

## no specify-os-type-access

Deletes the specify OS type from the role entry.

**no specify-os-type-access** *WORD*

## vlan

Sets the VLAN ID to the specified ID number or "none"

**vlan** *NUMBER*

## rate-limit uplink

Sets the rate limiting of uplink.

**rate-limit uplink** *NUMBER*

## rate-limit uplink downlink

Sets the rate limiting of downlink.

**rate-limit uplink** *NUMBER* **downlink** *NUMBER*

## no rate-limit

Sets rate limiting to Disable.

**no rate-limit**



## apply-arc-policy

To configure an ARC policy with the specified name, use the following command:

```
apply-arc-policy<WORD>
```

### Syntax Description

#### **apply-arc-policy**

Configures an Application Recognition and Control policy with the specified name.

*WORD*

Name of the ARC policy.

### Defaults

None.

### Example

```
ruckus(config-role)# apply-arc-policy Facebook  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-role)#
```

## no apply-arc-policy

To disable ARC policy, use the following command:

**no apply-arc-policy**

### Example

```
ruckus(config-role)# no apply-arc-policy
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-role)#
```

## show

To display the settings of a role, use the following command:

**show**

### Syntax Description

**show**

Display the settings of a role

### Defaults

None.

### Example

```
ruckus(config-role)# show
Role:
  ID:
  :
  Name= role1
  Description=
  Group Attributes=
  Guest Pass Generation= Disallowed
  ZoneDirector Administration:
    Status= Disallowed
  Allow All WLANs:
    Mode= Allow Specify WLAN access
  Access Control Policy= Disallowed

ruckus(config-role)#
```

# Configure User Commands

Use the user commands to configure a user's name, password, and role. To run these commands, you must first enter the **config-user** context.

## user

To create a user or modify an existing user and enter the config-user context, use the following command:

**user** *WORD*

### Syntax Description

<b>user</b>	Create or modify a user entry
<i>WORD</i>	Name of the user

### Defaults

None.

### Example

```
ruckus(config)# user johndoe1
The User entry 'johndoe1' has been created.
ruckus(config-user)#
```

## no user

To delete a user record, use the following command:

**no user** *WORD*

### Syntax Description

<b>user</b>	Create or modify a user entry
<i>WORD</i>	Name of the user

### Defaults

None.

### Example

```
ruckus(config)# no user johndoe1
The User 'johndoe1' has been deleted.
ruckus(config)#
```

## abort

To exit the config-user context without saving changes, use the abort command. Enter this command from within the context of the user that you are configuring.

**abort**

### *Syntax Description*

**abort**

Exit the user settings without saving changes

### *Defaults*

None.

### *Example*

```
ruckus(config-user)# abort
No changes have been saved.
ruckus(config)#
```

## end

To save changes, and then exit the config-user context, use the following command (you must first set a password before exiting):

**end**

### *Syntax Description*

**end**

Save changes, and then exit the context

### *Defaults*

None.

### *Example*

```
ruckus(config-user)# end
The User entry has saved successfully.
Your changes have been saved.
ruckus(config)#
```

## exit

To save changes, and then exit the config-user context, use the following command (you must first set a password before exiting):

**exit**

## Syntax Description

### **exit**

Save changes, and then exit the context

## Defaults

None.

## Example

```
ruckus(config-user)# exit
The User entry has saved successfully.
Your changes have been saved.
ruckus(config)#
```

## quit

To exit the config-user context without saving changes, use the quit command. Enter this command from within the context of the user that you are configuring.

### **quit**

## Syntax Description

### **quit**

Exit the user settings without saving changes

## Defaults

None.

## Example

```
ruckus(config-role)# quit
No changes have been saved.
ruckus(config)#
```

## user-name

To set the name of a user, use the following command:

**user-name** *WORD*

## Syntax Description

### **user-name**

Set the name of a user

### *WORD*

Set to this user name

## Defaults

None.

## Example

```
ruckus(config-user)# user-name joel  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## full-name

To set the full name of a user, use the following command:

**full-name** *WORD*

## Syntax Description

### **full-name**

Set the full name of a user

### *WORD*

Set to this full name

## Defaults

None.

## Example

```
ruckus(config-user)# full-name joeblow  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## password

To set the password of a user, use the following command:

**password** *WORD*

## Syntax Description

### **password**

Set the password of a user

### *WORD*

Set to this password

## Defaults

None.

## Example

```
ruckus(config-user)# password 12345678  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## role

To assign a role to a user, use the following command:

```
role WORD
```

## Syntax Description

### **role**

Assign a role to a user.

### WORD

The name of the role to be assigned to the user.

## Defaults

Default

## Example

```
ruckus(config-user)# role guest  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## show

To display the settings of a user, use the following command:

```
show
```

## Syntax Description

### **show**

Show user settings

## Defaults

None.

## Example

```
ruckus(config-user)# show  
User:  
  ID:  
  :  
  User Name= Joe  
  Full Name= Joe Blow  
  Password= *****  
  Role= Default
```

## Configuring Master Settings

### Configure User Commands

```
ruckus(config-user)#
```



# Configure Guest Access Commands

Use the guest-access commands to configure guest access services. To run these commands, you must first enter the **config-guest-access** context.

## guest-access

To create/configure a Guest Access service and enter the config-guest-access context, use the following command:

**guest-access** *WORD*

### Example

```
ruckus(config)# guest-access guestpolicy1
The Guest Access entry 'guestpolicy1' has been created.
ruckus(config-guest-access)#
```

## no guest-access

To delete a Guest Access service, use the following command:

**no guest-access**

### Example

```
ruckus(config)# no guest-access guest1
The Guest Access 'guest1' has been deleted.
ruckus(config)#
```

## abort

To exit the config-guest-access context without saving changes, use the abort command.

**abort**

## end

To save changes, and then exit the config-guest-access context, use the following command:

**end**

## exit

To save changes, and then exit the config-guest-access context, use the following command:

**exit**

## quit

To exit the config-guest-access context without saving changes, use the quit command.

**quit**

## guest-access-force-https-redirection

Enables guest access force HTTPS redirection.

### *Syntax*

**guest-access-force-https-redirection**

### *Command Default*

Disabled

### *Examples*

```
ruckus(config)# guest-access-force-https-redirection  
The command was executed successfully.  
ruckus(config)#
```

## no guest-access-force-https-redirection

Disables guest access force HTTPS redirection.

### *Syntax*

**no guest-access-force-https-redirection**

### *Command Default*

Disabled.

### *Examples*

```
ruckus(config)# no guest-access-force-https-redirection
The command was executed successfully.
ruckus(config)#
```

## guest-access-guestpass-effective

To set the guest pass effective date to begin from the creation time or from first use, use the following command:

```
guest-access-guestpass-effective [now | first-use-expired <NUMBER>]
```

### Syntax Description

**now**

Sets Effective from the creation time.

**first-use-expired** <NUMBER>

Effective from first use, Expire new guest passes if not used within xx days.

### Example

```
ruckus(config-guest-access)# guest-access-guestpass-effective first-use-expired 10  
The command was executed successfully.  
ruckus(config-guest-access)#
```

## name

To set the name of the guest access policy, use the following command:

```
name WORD
```

## self-service

To enable guest pass self-registration, use the following command:

```
self-service
```

## no self-service

To disable guest pass self-registration, use the following command:

```
no self-service
```

## guestpass-duration

To set the guest pass duration, use the following command:

```
guestpass-duration [ hour | day | week ] NUMBER
```

## guestpass-reauth

To set the guest pass reauthorization timeout, use the following command:

```
guestpass-reauth [ hour | day | week ] NUMBER
```

## no guestpass-reauth

To disable guest pass reauthorization timeout, use the following command:

```
no guestpass-reauth
```

## guestpass-share-number

To set the limit on how many devices can share one guest pass, use the following command (valid values: [0, 10] and 0 means unlimited):

```
guestpass-share-number NUMBER
```

## guestpass-sponsor

To enable guest pass sponsor approval, use the following command:

```
guestpass-sponsor
```

## no guestpass-sponsor

To disable guest pass sponsor approval, use the following command:

```
no guestpass-sponsor
```

## guestpass-sponsor-auth-server

Sets the authentication server to 'Local Database' or to a specified AAA server name, use the following command:

```
guestpass-sponsor-auth-server [ local | name WORD ]
```

## guestpass-sponsor-number

To set the number of sponsors that can be used for this guest pass service (valid values: [1,5]), use the following command:

```
guestpass-sponsor-number NUMBER
```

## guestpass-notification

To set the notification method for delivering guest passes, use the following command:

```
guestpass-notification NUMBER
```

### Syntax Description

- 1 Device Screen
- 2 Mobile

- 3           Emai
- 4           Mobile and Email

## guestpass-terms-and-conditions

To enable and set the terms and conditions, use the following command:

**guestpass-terms-and-conditions** *WORD*

## no guestpass-terms-and-conditions

To disable the terms and conditions, use the following command:

**no guestpass-terms-and-conditions**

## onboarding

To configure onboarding portal options, use the following command:

**onboarding** [**key-and-zeroit** | **zeroit**]

### Syntax Description

**onboarding**

Enable onboarding portal.

**key-and-zeroit**

Enables guest pass and zero-it activation.

**zeroit**

Enables zero-it activation only.

### Defaults

Enabled, Guest Pass and Zero-IT.

### Example

```
ruckus(config-guest-access)# onboarding key-and-zeroit
The command was executed successfully.
ruckus(config-guest-access)#
```

## no onboarding

To disable the onboarding portal, use the following command:

**no onboarding**

## no authentication

To disable guest access authentication, use the following command:

**no authentication**

### *Syntax Description*

**no authentication**

Disable guest access authentication

### *Defaults*

Enabled.

### *Example*

```
ruckus(config-guest-access)# no authentication  
The command was executed successfully.
```

## authentication guest-pass-and-social-login

To enable guest pass and social media login authentication for this guest access service, use the following command:

**authentication guest-pass-and-social-login**

### *Syntax Description*

**authentication guest-pass-and-social-login**

Enable guest pass and social media authentication.

### *Example*

```
ruckus(config-guest-access)# authentication guest-pass-and-social-login  
The command was executed successfully.  
ruckus(config-guest-access)#
```

## authentication only-social-login

To enable social media login only for this guest access service, use the following command:

**authentication only-social-login**

### Syntax Description

**authentication only-social-login**

Enable social media authentication only.

### Example

```
ruckus(config-guest-access)# authentication only-social-login  
The command was executed successfully.  
ruckus(config-guest-access)#
```

## no term-of-use

To hide the Terms of Use text on the guest pass access page, use the following command:

**no term-of-use**

### Syntax Description

**no term-of-use**

Hide Terms of Use

### Defaults

Disabled.

### Example

```
ruckus(config-guest-access)# no term-of-use  
The command was executed successfully.
```

## term-of-use

To display and specify the Terms of Use text on the guest pass access page, use the following command:

**term-of-use WORD**

### Syntax Description

**term-of-use**

Display Terms of Use

*WORD*

Display this text as content of Terms of Use on Guest Pass access page



## Defaults

Disabled.

## Example

```
ruckus(config-guest-access)# term-of-use test.guest  
The command was executed successfully.
```

## redirect

To set the URL to which to redirect a guest user after passing authentication, use the following command:

```
redirect [ original | url WORD ]
```

## Syntax Description

### **redirect**

Set the URL to which the guest user will be redirected

### **original**

Redirect user to the original page that he intended to visit

### **url** *WORD*

**Redirect user to a different URL. Specify the URL in *WORD*.**

## Defaults

original

## Example

```
ruckus(config-guest-access)# redirect url http://www.ruckuswireless.com  
The command was executed successfully.
```

## welcome-text

To configure the text to display on the guest access user login page, use the following command:

```
welcome-text WORD
```

## Syntax Description

### **welcome-text**

Configure the welcome message

### *WORD*

Use this as the welcome message

## Defaults

Welcome to the Guest Access login page.

## Example

```
ruckus(config-guest-access)# welcome-text "Welcome to the Guest Access Login Page."  
The command was executed successfully.  
ruckus(config-guest-access)#
```

## show

To display the guest access policy settings, use the following command:

**show**

## Syntax Description

**show**

Display the guest access settings

## Example

```
ruckus(config)# guest-access guestpolicy1  
The Guest Access entry 'guestpolicy1' has been loaded. To save the Guest Access entry, type end or exit.  
ruckus(config-guest-access)# show  
Guest Access:  
  Name = guestpolicy1  
  Onboarding Portal:  
    Aspect = Guest pass and ZeroIT  
  Authentication:  
    Mode = Use guest pass and Social login authentication  
  Effective time:  
    Countdown-by-issued = false  
    Effective Period    = 7 Days  
  Title = Welcome to the Guest Access login page.  
  Terms of Use:  
    Status = Disabled  
  Redirection:  
    Mode = To the URL that the user intends to visit  
  Self Service Registration:  
    Status = Disabled  
  Restricted Subnet Access:  
    Rules:  
    1:  
      Description=  
      Type= Deny  
      Source Address= Any  
      Destination Address= local  
      Source Port= Any  
      Destination Port= Any  
      Protocol= Any  
    2:  
      Description=  
      Type= Deny  
      Source Address= Any  
      Destination Address= 10.0.0.0/8  
      Source Port= Any  
      Destination Port= Any  
      Protocol= Any  
    3:  
      Description=  
      Type= Deny  
      Source Address= Any  
      Destination Address= 172.16.0.0/12  
      Source Port= Any  
      Destination Port= Any  
      Protocol= Any  
    4:
```

```
Description=  
Type= Deny  
Source Address= Any  
Destination Address= 192.168.0.0/16  
Source Port= Any  
Destination Port= Any  
Protocol= Any  
  
Restricted IPv6 Access:  
Rules:  
  1:  
    Description=  
    Type= Deny  
    Source Address= Any  
    Destination Address= local  
    Source Port= Any  
    Destination Port= Any  
    Protocol= Any  
    ICMPv6 Type= Any  
  
ruckus(config-guest-access) #
```

## social-media-login

To set the social media login, use the following command:

**social-media-login** *WORD*

### Syntax

<WORD>: Specify the social media login type:

- google <WORD> <WORD>: Sets the social media login to Google/Google+
- linkedin <WORD> <WORD>: Sets the social media login to LinkedIn
- microsoft <NUMBER> <WORD> <WORD>: Sets the social media login to Microsoft
- wechat <WORD> <WORD> <WORD> <WORD>: Sets the social media logging to WeChat.

### Example

```
ruckus(config-guest-access)# social-media-login linkedin 1234456 test1  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-guest-access) #
```

### ***social-media-login delete-social-media***

To delete the social media, use the following command:

**social-media-login delete-social-media <NUMBER>**

### **Syntax Description**

**<NUMBER>**

Delete the social media, google:3 linkdin:4 microsoft:5 wechat:6

### **Example**

```
ruckus(config-guest-access)# social-media-login delete-social-media 3  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-guest-access)#
```

### ***social-media-login google***

To set the social media login to Google/Google+, use the following command:

**social-media-login google WORD WORD**

### ***social-media-login linkedin***

To set the social media login to LinkedIn, use the following command

**social-media-login linkedin WORD WORD**

### ***social-media-login microsoft***

To sets the social media login to Microsoft, use the following command:

**social-media-login microsoft NUMBERWORD WORD**

### ***social-media-login wechat***

To sets the social media login to WeChat, use the following command:

**social-media-login wechat WORDWORD WORDWORD**

### ***social-media-login wechat force-follow***

To set the WeChat social media WLAN to force follow , use the following command:

**social-media-login wechat WORDWORD WORDWORD force-follow WORD**

# web-portal-force-https-redirection

Enables web portal force HTTPS redirection.

## Syntax

**web-portal-force-https-redirection**

## Command Default

Disabled.

## Examples

```
ruckus(config)# web-portal-force-https-redirection
The command was executed successfully.
ruckus(config)#
```

# no web-portal-force-https-redirection

Disables web portal force HTTPS redirection.

## Syntax

**no web-portal-force-https-redirection**

## Command Default

Disabled.

## Examples

```
ruckus(config)# no web-portal-force-https-redirection  
The command was executed successfully.  
ruckus(config)#
```

# portal-auth-force-dns-server

Enables portal authentication WLAN (Hotspot Service, Guest Access and Web Authentication) force DNS server.

## Syntax

**portal-auth-force-dns-server <IP/IPv6-ADDR1 [IP/IPv6-ADDR2]>**

## Command Default

Disabled

## Examples

```
ruckus(config)# portal-auth-force-dns-server 192.168.40.10  
The command was executed successfully.  
ruckus(config)#
```

## no portal\_auth-force-dns-server

Disable portal authentication WLAN (Hotspot Service, Guest Access and Web Authentication) force DNS server.

### Syntax

**no portal\_auth-force-dns-server**

### Command Default

Disabled

### Examples

```
ruckus(config)# no portal_auth-force-dns-server  
The command was executed successfully.  
ruckus(config)#
```



# guest-access-auth-server

Sets the authentication server to 'Local Database' or to a specified AAA server.

## Syntax

```
guest-access-auth-server { local | name <WORD> }
```

## Command Default

None

## Parameters

### local

Sets the authentication server to 'Local Database'.

### name <WORD>

Sets the authentication server to specified AAA server name.

## Examples

```
ruckus(config)# guest-access-auth-server name radius1  
The command was executed successfully.  
ruckus(config)#
```

## Configuring Guest Access Restriction Rules

Use the following commands to configure restricted access rules for a guest policy. To use these commands, you must enter the **config-guest-restrict-access** context from within the **config-guest-access** context.

### no restrict-access-order

To delete a restrict access order, use the following command:

**no restrict-access-order** *NUMBER*

#### *Syntax Description*

**no restrict-access-order**

Delete a restrict access order

*NUMBER*

Delete this order ID

#### *Example*

```
ruckus(config-guest-access)# no restrict-access-order 4
The Restricted Subnet Access entry has been removed from the Guest Access.
ruckus(config-guest-access)#
```

## restrict-access-order

To create a new restrict access order or modify an existing restrict access order, use the following command:

**restrict-access-order** *NUMBER*

This command enters the config-guest-restrict-access context. The following commands are available from within this context:

### Syntax Description

**help**

Shows available commands

**history**

Shows a list of previously run commands.

**abort**

Exits the config-guest-restrict-access context without saving changes.

**end**

Saves changes, and then exits the config-guest-restrict-access context.

**exit**

Saves changes, and then exits the config-guest-restrict-access context.

**quit**

Exits the config-guest-restrict-access context without saving changes.

**order** *NUMBER*

Sets the guest access rule order.

**description** *WORD*

Sets the guest access rule description.

**type** [ **allow** | **deny** ]

Sets the guest access rule type to allow or deny.

**destination** [ **address** *ADDR* | **port** *NUMBER/WORD* ]

Sets the destination address/port of a guest access rule.

**protocol** *NUMBER/WORD*

Sets the protocol of a guest access rule.

**show**

Displays restricted subnet access settings.

## show

To display guest access restriction settings, use the following command:

**show**

### Syntax Description

**show**

Display guest access restriction settings

## Defaults

None.

## order

To configure the guest access rule order, use the following command:

**order** *NUMBER*

## Syntax Description

### **order**

Set the order of a guest access rule

### *NUMBER*

Assign the rule this order

## Example

```
ruckus(config-guest-restrict-access)# order 3  
The command was executed successfully.
```

## description

To set the description of a guest access rule, use the following command:

**description** *WORD*

## Syntax Description

### **description**

Set the description of a guest access rule

### *WORD*

Set this as description

## Defaults

None.

## Example

```
ruckus(config-guest-restrict-access)# description guestd3  
The command was executed successfully.
```

## type allow

To set the guest access rule type to 'allow', use the following command:

**type allow**

## Syntax Description

- type**  
Set the guest access rule type
- allow**  
Set the rule type to 'allow'

## Defaults

Deny.

## Example

```
ruckus(config-guest-restrict-access)# type allow  
The command was executed successfully.
```

## type deny

To set the guest access rule type to 'deny', use the following command:

**type deny**

## Syntax Description

- type**  
Set the guest access rule type
- deny**  
Set the rule type to 'deny'

## Defaults

Deny.

## Example

```
ruckus(config-guest-restrict-access)# type deny  
The command was executed successfully.
```

## destination address

To set the destination address of the rule, use the following command:

**destination address** *IP-ADDR/WORD*

## Syntax Description

- destination address**  
Set the destination address of the rule
- IP-ADDR/WORD**  
Set the destination to this IP address

## Defaults

Any.

## Example

```
ruckus(config-guest-restrict-access)# destination address 192.168.0.20/24  
The command was executed successfully.
```

## destination port

To set the destination port of the rule, use the following command:

**destination port** *NUMBER/WORD*

## Syntax Description

### **destination port**

Set the destination port of the rule

*NUMBER/WORD*

Set the destination to this port number

## Defaults

Any.

## Example

```
ruckus(config-guest-restrict-access)# destination port 562  
The command was executed successfully.
```

## protocol

To set the protocol for the rule, use the following command:

**protocol** *NUMBER/WORD*

## Syntax Description

### **protocol**

Set the protocol for the rule

*NUMBER/WORD*

Set to this protocol

## Defaults

Any.

### **Example**

```
ruckus(config-guest-restrict-access)# protocol 69  
The command was executed successfully.
```

# IPv6 Guest Restrict Access Commands

Use the IPv6 guest restrict access commands to configure IPv6 restrict access rules. To run these commands, you must first enter the **config-ipv6-guest-restrict-access** context.

## no restrict-access-order-ipv6

To delete a restrict access order, use the following command:

```
no restrict-access-order-ipv6 NUMBER
```

### Syntax Description

**no restrict-access-order-ipv6**

Delete a restrict access order

*NUMBER*

Delete this order ID

### Defaults

None.

### Example

```
ruckus(config-guest-access)# no restrict-access-order-ipv6 2  
The IPv6 Restricted Subnet Access entry has been removed from the Guest Access.  
ruckus(config-guest-access)#
```

## restrict-access-order-ipv6

To create a new restrict access order or modify an existing restrict access order, use the following command:

```
restrict-access-order-ipv6 NUMBER
```

This command enters the **config-ipv6-guest-restrict-access** context. The following commands are available from within this context:

### Syntax Description

**help**

Shows available commands

**history**

Shows a list of previously run commands.

**abort**

Exits the config-guest-restrict-access context without saving changes.

**end**

Saves changes, and then exits the config-guest-restrict-access context.



- exit**  
Saves changes, and then exits the config-guest-restrict-access context.
- quit**  
Exits the config-guest-restrict-access context without saving changes.
- order** *NUMBER*  
Sets the guest access rule order.
- description** *WORD*  
Sets the guest access rule description.
- type** [ **allow** | **deny** ]  
Sets the guest access rule type to allow or deny.
- destination** [**address** *IPv6-ADDR* | **port** *NUMBER/WORD*]  
Sets the destination address/port of a guest access rule.
- protocol** *NUMBER/WORD*  
Sets the protocol of a guest access rule.
- icmpv6-type**  
Sets the ICMPv6 type of a Guest Access rule.
- show**  
Displays restricted subnet access settings.

## Example

```
ruckus(config-guest-access)# restrict-access-order-ipv6 2
ruckus(config-ipv6-guest-restrict-access)# type allow
The command was executed successfully.
ruckus(config-ipv6-guest-restrict-access)# show
  Description=
  Type= Allow
  Destination Address= Any
  Destination Port= Any
  Protocol= Any
  ICMPv6 Type= Any
ruckus(config-ipv6-guest-restrict-access)# end
The IPv6 Restricted Subnet Access entry has been added to the Guest Access.
Your changes have been saved.
ruckus(config-guest-access)#
```

## show

To display guest access restriction settings, use the following command:

**show**

## Syntax Description

**show**

Display guest access restriction settings

## Example

```
ruckus(config-ipv6-guest-restrict-access)# show
  Description=
  Type= Allow
  Destination Address= Any
  Destination Port= Any
  Protocol= Any
  ICMPv6 Type= Any
ruckus(config-ipv6-guest-restrict-access)#
```

## order

To configure the guest access rule order, use the following command:

**order** *NUMBER*

### Syntax Description

**order**

Set the order of a guest access rule

*NUMBER*

Assign the rule this order

### Defaults

None.

## Example

```
ruckus(config-ipv6-guest-restrict-access)# order 3
The command was executed successfully.
```

## description

To set the description of a guest access rule, use the following command:

**description** *WORD*

### Syntax Description

**description**

Set the description of a guest access rule

*WORD*

Set this as description

### Defaults

None.

## Example

```
ruckus(config-ipv6-guest-restrict-access)# description guestd3  
The command was executed successfully.
```

## type allow

To set the guest access rule type to 'allow', use the following command:

```
type allow
```

## Syntax Description

**type** Set the guest access rule type

**allow** Set the rule type to 'allow'

## Defaults

Deny.

## Example

```
ruckus(config-ipv6-guest-restrict-access)# type allow  
The command was executed successfully.
```

## type deny

To set the guest access rule type to 'deny', use the following command:

```
type deny
```

## Syntax Description

**type** Set the guest access rule type

**deny** Set the rule type to 'deny'

## Defaults

Deny.

## Example

```
ruckus(config-ipv6-guest-restrict-access)# type deny  
The command was executed successfully.
```

## destination address

To set the destination address of the rule, use the following command:

**destination address** *IP-ADDR/WORD*

### Syntax Description

**destination address**

Set the destination address of the rule

**IP-ADDR/WORD**

Set the destination to this IP address

### Defaults

None.

### Example

```
ruckus(config-ipv6-guest-restrict-access)# destination address fe80::/64
The command was executed successfully.
ruckus(config-ipv6-guest-restrict-access)#
```

## destination port

To set the destination port of the rule, use the following command:

**destination port** *NUMBER/WORD*

### Syntax Description

**destination port**

Set the destination port of the rule

*NUMBER/WORD*

Set the destination to this port number

### Defaults

None.

### Example

```
ruckus(config-ipv6-guest-restrict-access)# destination port 562
The command was executed successfully.
```

## protocol

To set the protocol for the rule, use the following command:

**protocol** *NUMBER/WORD*

## Syntax Description

### **protocol**

Set the protocol for the rule

### *NUMBER/WORD*

Set to this protocol

## Defaults

None.

## Example

```
ruckus(config-ipv6-guest-restrict-access)# protocol 69  
The command was executed successfully.
```

## icmpv6-type

To set the ICMPv6 type of a Guest Access rule, use the following command:

```
icmpv6-type [ any | number NUMBER ]
```

## Defaults

Any.

## Example

```
ruckus(config-ipv6-guest-restrict-access)# icmpv6-type any  
The command was executed successfully.  
ruckus(config-ipv6-guest-restrict-access)#
```

# Configure Hotspot Commands

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

## hotspot

To create a new hotspot or edit an existing entry and enter the config-hotspot context, use the following command:

**hotspot** *WORD*

### Syntax Description

**hotspot**

Create or edit a hotspot service

*WORD*

Name of hotspot service

### Defaults

None.

### Example

```
ruckus(config)# hotspot hotspot1
The Hotspot entry 'hotspot1' has been loaded. To save the Hotspot entry, type end or exit.
ruckus(config-hotspot)#
```

## no hotspot

To delete a hotspot record from the list, use the following command:

**no hotspot** *WORD*

### Syntax Description

**hotspot**

Create or edit a hotspot service

*WORD*

Name of hotspot service

### Defaults

None.

### Example

```
ruckus(config)# hotspot hotspot1
The Hotspot entry 'hotspot1' has been loaded. To save the Hotspot entry, type end or exit.
ruckus(config-hotspot)#
```

## abort

To exit the config-hotspot context without saving changes, use the abort command.

**abort**

### Syntax Description

**abort**

Exit the hotspot settings without saving changes

### Defaults

None.

### Example

```
ruckus(config-hotspot)# abort
No changes have been saved.
ruckus(config)#
```

## end

To save changes, and then exit the config-hotspot context, use the following command:

**end**

### Syntax Description

**end**

Save changes, and then exit the context

### Defaults

None.

### Example

```
ruckus(config-hotspot)# end
The login page url can't be empty.
ruckus(config-hotspot)# end
The Hotspot entry has saved successfully.
Your changes have been saved.
ruckus(config)#
```

## exit

To save changes, and then exit the config-hotspot context, use the following command:

**exit**

## Syntax Description

### **exit**

Save changes, and then exit the context

## Defaults

None.

## Example

```
ruckus(config-hotspot)# exit
The login page url can't be empty
ruckus(config-hotspot)# exit
The Hotspot entry has saved successfully.
Your changes have been saved.
```

## quit

To exit the config-hotspot context without saving changes, use the quit command.

### **quit**

## Syntax Description

### **quit**

Exit the hotspot settings without saving changes

## Defaults

None.

## Example

```
ruckus(config-hotspot)# quit
No changes have been saved.
ruckus(config)#
```

## show

To display the current hotspot settings, use the following command:

### **show**

## Syntax Description

### **show**

Display the current hotspot settings

## Defaults

None.



## Example

```
ruckus(config-hotspot)# show
Hotspot:
ID:
1:
Name= h1
Login Page Url= http://172.18.110.122
Start Page= redirect to the URL that the user intends to visit.
Session Timeout= Disabled
Idle Timeout= Enabled
Timeout= 60 Minutes
Authentication Server= Local Database
Accounting Server= Disabled
Location ID=
Location Name=
Walled Garden 1=
Walled Garden 2=
Walled Garden 3=
Walled Garden 4=
Walled Garden 5=
Rules:
Order= 1
Description= h1_order1
Type= Deny
Destination Address= 192.168.20.20/24
Destination Port= 920
Protocol= 58
```

## name

To set the hotspot name, use the following command

```
name WORD
```

## Syntax Description

### **name**

Set the hotspot name

### *WORD*

Set to this name

## Defaults

None.

## Example

```
ruckus(config-hotspot)# name ruckus1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## smartclient

Use the following command to enable WISPr smart client support

```
smartclient [ secure https ] [ secure http ] [ wispr-only secure https ] [ wispr-only secure-http ] [ info ]
```

## Syntax Description

### **smartclient**

Enable WISPr smartclient support.

### **secure https**

Enables WISPr smart client support with HTTPS security.

### **secure http**

Enables WISPr smart client support with no security.

### **wispr-only secure https**

Enables only WISPr smart client support with HTTPS security.

### **wispr-only secure http**

Enables only WISPr smart client support with no security.

### **info**

Sets the instruction to guide user to login by Smart Client application.

## Defaults

None.

## Example

```
ruckus(config-hotspot)# smartclient secure https
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-hotspot)#
```

## no smartclient

To disable WISPr Smart Client support, use the following command:

**no smartclient**

## login-page

To set the URL of the hotspot login, use the following command:

**login-page** [ **original** | *WORD* ]

## Syntax Description

### **login-page**

Set the URL of the hotspot login

*WORD*

Set to this URL

### **original**

Redirect to the URL that the user intends to visit

## Defaults

None.

## Example

```
ruckus(config-hotspot)# login-page http://ruckuswireless.com  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## start-page

To set the URL or page to which the user will be redirected after logging into the hotspot, use the following command:

```
start-page [ original | url WORD ]
```

## Syntax Description

### start-page

Set the URL or page to which the user will be redirected after logging into the hotspot

### original

Redirect user to the original page he or she intended to visit

### url WORD

**Redirect use to another page. Set the URL of the page in WORD.**

## Defaults

original

## Example

```
ruckus(config-hotspot)# start-page url http://www.ruckuswireless.com  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## no session-timeout

To disable the session timeout for hotspot usage, use the following command:

```
no session-timeout
```

## Syntax Description

### no session-timeout

Disable the session timeout for hotspot usage

## Defaults

None.

## Example

```
ruckus(config-hotspot)# no session-timeout  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## session-timeout

To enable and set the session timeout for hotspot usage, use the following command:

**session-timeout** *minutes*

### Syntax Description

**session-timeout**

Disable the session timeout for hotspot usage

*minutes*

Set the session timeout to this value (in minutes)

### Defaults

1440 minutes

## Example

```
ruckus(config-hotspot)# session-timeout 20  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## no grace-period

To disable the grace period (idle timeout) for hotspot users, use the following command:

**no grace-period**

### Syntax Description

**no grace-period**

Disable the idle timeout for hotspot users

### Defaults

None.

## Example

```
ruckus(config-hotspot)# no grace-period  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## grace-period

To enable and set the grace period (idle timeout) for hotspot users, use the following command:

**grace-period** *minutes*

### Syntax Description

**grace-period**

Set the idle timeout for hotspot users

*minutes*

Set the idle timeout to this value (in minutes)

### Defaults

60 minutes

### Example

```
ruckus(config-hotspot)# grace-period 20  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## auth-server local

To use ZoneDirector as the authentication server for hotspot users, use the following command:

**auth-server local**

### Syntax Description

**auth-server**

Set an authentication server for hotspot users

**local**

Use ZoneDirector as the authentication server

### Defaults

local

### Example

```
ruckus(config-hotspot)# auth-server local  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## auth-server name

To use an external server for authenticating hotspot users, use the following command:

**auth-server name** *WORD*

## Syntax Description

### **auth-server name**

Set an external authentication server for hotspot users

*WORD*

Use this server as the authentication server

## Defaults

None.

## Example

```
ruckus(config-hotspot)# auth-server name radius1  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-hotspot)#
```

## auth-server name no-mac-bypass

To disable MAC authentication bypass (no redirection), use the following command:

**auth-server name** *WORD* **no-mac-bypass**

## auth-server name mac-bypass

To enable MAC authentication bypass (no redirection) and use password as authentication password, use the following command:

**auth-server name** *WORD* **mac-bypass** [ **mac** | **password** *WORD* ]

## Syntax Description

### **auth-server name**

Set an external authentication server for hotspot users

*WORD*

Authentication server name

### **mac-bypass**

Enable MAC auth bypass

### **mac**

Enables MAC authentication bypass (no redirection) and use device MAC address as authentication password.

### **password** *WORD*

Enables MAC authentication bypass (no redirection) and use password as authentication password.

### **mac-in-dot1x**

Use device MAC address as authentication password and enable to send username and password in 802.1X format of 00-10-A4-23-19-C0 (by default 0010a42319c0).

### **password-in-dot1x** *WORD*

Use password as authentication password and enable to send username and password in 802.1X format of 00-10-A4-23-19-C0 (by default 0010a42319c0).

## Defaults

None.

## Example

```
ruckus(config-hotspot)# auth-server name radius1 mac-bypass mac
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-hotspot)#
```

## auth-server name mac-bypass mac-addr-format

To set MAC auth username and password to one of the following formats, use the following command:

```
auth-server name WORD mac-bypass mac-addr-format [ FORMAT ]
```

## Syntax Description

### **auth-server name**

Set an external authentication server for hotspot users

*WORD*

Authentication server name

### **mac-bypass**

Enable MAC auth bypass

### **mac-addr-format**

Enable MAC authentication bypass (no redirection) and use device MAC address as authentication password.

[**FORMAT** ]

Set the MAC address format.

### **aabbccddeeff**

Set the MAC address format to aabbccddeeff.

### **aa-bb-cc-dd-ee-ff**

Set the MAC address format to aa-bb-cc-dd-ee-ff.

### **aa:bb:cc:dd:ee:ff**

Set the MAC address format to aa:bb:cc:dd:ee:ff.

### **AABBCCDDEEFF**

Set the MAC address format to AABBCCDDEEFF.

### **AA-BB-CC-DD-EE-FF**

Set the MAC address format to AA-BB-CC-DD-EE-FF.

### **AA:BB:CC:DD:EE:FF**

Set the MAC address format to AA:BB:CC:DD:EE:FF.

## acct-server

To enable the accounting server for hotspot usage, use the following command:

```
acct-server WORD
```

## Syntax Description

### **acct-server**

Enable the accounting server for hotspot usage

*WORD*

Name of the AAA server

## Defaults

None.

## Example

```
ruckus(config-hotspot)# acct-server "RADIUS Accounting"  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-hotspot)#
```

## no acct-server

To disable the accounting server for hotspot usage, use the following command:

**no acct-server**

## Syntax Description

### **no acct-server**

Disable the accounting server for hotspot usage

## Defaults

None.

## Example

```
ruckus(config-hotspot)# no acct-server  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## acct-server interim-update

To enable and set the accounting server for hotspot usage, use the following command:

**acct-server** *WORD* **interim-update** *NUMBER*

## Syntax Description

### **no acct-server**

Enable and set the accounting server for hotspot usage

*WORD*

Set to this accounting server



### **interim-update**

Set the interim update interval

*NUMBER*

Set to this interval (in minutes)

### **Defaults**

5 minutes

### **Example**

```
ruckus(config-hotspot)# acct-server asd interim-update 10
The AAA server 'asd' could not be found. Please check the spelling, and then try again.
ruckus(config-hotspot)# acct-server acct1 interim-update 20
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## **client-isolation**

To enable wireless client isolation (on AP or across APs), use the following command:

**client-isolation [ isolation-on-ap | isolation-across-ap ] [ enable | disable ]**

### **Syntax Description**

#### **client-isolation**

Enable client isolation.

#### **isolation-on-ap**

Enable client isolation per AP.

#### **isolation-on-subnet**

Enable spoof guarding and across AP client isolation using whitelist.

### **Defaults**

Disabled

### **Example**

```
ruckus(config-hotspot)# client-isolation isolation-on-ap enable
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-hotspot)# client-isolation isolation-on-subnet enable
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-hotspot)#
```

## **whitelist**

To apply a client isolation whitelist to this Hotspot, use the following command:

**whitelist name** *WORD*

## location-id

To set the location ID of the hotspot, use the following command:

**location-id** *location-id*

### Syntax Description

**location-id**

Set the location ID of the hotspot

*location-id*

Set to this location ID

### Defaults

None.

### Example

```
ruckus(config-hotspot)# location-id us
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## location-name

To set the location name of the hotspot, use the following command:

**location-name** *location-name*

### Syntax Description

**location-name**

Set the location name of the hotspot

*location-name*

Set to this location name

### Defaults

None.

### Example

```
ruckus(config-hotspot)# location-name shenzhen
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## walled-garden

To set a hotspot “walled garden” URL, use the following command:

**walled-garden** *INDEX WORD*

## Syntax Description

### walled-garden

Create a walled garden rule

### INDEX

Enter walled garden URL index. (1~35)

### WORD

Destination URL

## Defaults

None.

## Example

```
ruckus(config-hotspot)# walled-garden 1 www.ruckuswireless.com
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-hotspot)#
```

## no walled-garden

To delete a walled garden URL, use the following command

**no walled-garden** INDEX

## Syntax Description

### walled-garden

Delete a walled garden rule

### INDEX

Enter walled garden URL index. (1~35)

## Defaults

None.

## Example

```
ruckus(config-hotspot)# no walled-garden 1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-hotspot)#
```

# Configuring Hotspot Restricted Access Rules

The following commands are used to create and modify Hotspot restricted access rules. Use the `restrict-access-order` command from the **config-hotspot** context to enter the **config-hotspot-restrict-access** context.

## restrict-access-order

To create a new restrict access order or modify an existing restrict access order, use the following command:

**restrict-access-order** *NUMBER*

### Syntax Description

**restrict-access-order**

Add a restrict access order

*NUMBER*

Add this order ID

**order** *NUMBER*

Sets the hotspot rule order.

**description** *WORD*

Sets the hotspot rule description.

**type allow**

Sets the hotspot rule type to 'allow'.

**type deny**

Sets the hotspot rule type to 'deny'.

**destination address** *IP-ADDR/WORD*

Sets the destination address of a hotspot rule.

**destination port** *NUMBER/WORD*

Sets the destination port of a hotspot rule.

**protocol** *NUMBER/WORD*

Sets the protocol of a hotspot rule.

**show**

Displays the policy rule.

### Defaults

None.

### Example

```
ruckus(config-hotspot)# restrict-access-order 1
ruckus(config-hotspot-restrict-access)#
ruckus(config-hotspot-restrict-access)# show
  Description=
  Type= Deny
  Destination Address= Any
  Destination Port= Any
```

```
Protocol= Any  
ruckus(config-hotspot-restrict-access)#
```

## no restrict-access-order

To delete a restrict access order, use the following command:

```
no restrict-access-order NUMBER
```

### Syntax Description

**no restrict-access-order**

Delete a restrict access order

NUMBER

Delete this order ID

### Defaults

None.

### Example

```
ruckus(config-hotspot)# no restrict-access-order 1  
The rule '1' has been removed from the Hotspot.
```

## restrict-access-order-ipv6

To create a new IPv6 restrict access order or modify an existing restrict access order, use the following command:

```
restrict-access-order-ipv6 NUMBER
```

### Syntax Description

**restrict-access-order-ipv6**

Add a restrict access order

NUMBER

Add this order ID

**order** NUMBER

Sets the hotspot rule order.

**description** WORD

Sets the hotspot rule description.

**type allow**

Sets the hotspot rule type to 'allow'.

**type deny**

Sets the hotspot rule type to 'deny'.

**destination address** IP-ADDR/WORD

Sets the destination address of a hotspot rule.

**destination port** *NUMBER/WORD*

Sets the destination port of a hotspot rule.

**protocol** *NUMBER/WORD*

Sets the protocol of a hotspot rule.

**icmpv6 type** [*any*] **number** *NUMBER*

Sets the icmpv6 type of a hotspot rule.

**show**

Displays the policy rule.

## Defaults

None.

## Example

```
ruckus(config-hotspot)# restrict-access-order-ipv6 1
ruckus(config-hotspot-restrict-access)#
ruckus(config-hotspot-restrict-access-ipv6)# show
  Description=
  Type= Deny
  Destination Address= Any
  Destination Port= Any
  Protocol= Any
  ICMPv6 Type= Any
ruckus(config-hotspot-restrict-access-ipv6)#
```

## no restrict-access-order-ipv6

To delete a restrict access order, use the following command:

**no restrict-access-order-ipv6** *order\_id*

## Syntax Description

**no restrict-access-order**

Delete a restrict access order

*order\_id*

Delete this order ID

## Defaults

None.

## Example

```
ruckus(config-hotspot)# no restrict-access-order-ipv6 1
The rule '1' has been removed from the Hotspot.
```

## icmpv6-type

To set the ICMPv6 type, use the following command:

```
icmpv6-type [any | number NUMBER]
```

### Defaults

Any.

### Example

```
ruckus(config-hotspot-restrict-access-ipv6)# icmpv6-type any  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-hotspot-restrict-access-ipv6)#
```

## Hotspot Access Restriction Commands

Use the hotspot-restrict-access commands to configure network segments to which hotspot access will be blocked. To run these commands, you must first enter the **config-hotspot-restrict-access** context.

The same commands are available for IPv6 networks from the **config-hotspot-restrict-access-ipv6** context.

### end

To save changes, and then exit the config-hotspot-restrict-access context, use the following command:

**end**

#### Syntax Description

**end**  
Save changes, and then exit the context

#### Defaults

None.

#### Example

```
ruckus(config-hotspot-restrict-access)# end  
ruckus(config-hotspot)#
```

### exit

To save changes, and then exit the config-hotspot-restrict-access context, use the following command:

**exit**

#### Syntax Description

**exit**  
Save changes, and then exit the context

#### Defaults

None.

#### Example

```
ruckus(config-hotspot-restrict-access)# exit  
ruckus(config-hotspot)#
```

### show

To display hotspot access restriction settings, use the following command:



**show**

### **Syntax Description**

**show**

Display the hotspot access restriction settings

### **Defaults**

None.

## **order**

To configure the hotspot access rule order, use the following command:

**order** *NUMBER*

### **Syntax Description**

**order**

Set the order of a hotspot access rule

*NUMBER*

Assign the rule this order

### **Defaults**

None.

### **Example**

```
ruckus(config-hotspot-restrict-access)# order 1  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## **description**

To set the description of a hotspot access rule, use the following command:

**description** *WORD*

### **Syntax Description**

**description**

Set the description of a hotspot access rule

*WORD*

Set this as description

### **Defaults**

None.

## Example

```
ruckus(config-hotspot-restrict-access)# description h1_order1  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## type allow

To set the hotspot access rule type to 'allow', use the following command:

```
type allow
```

## Syntax Description

**type**  
Set the hotspot access rule type

**allow**  
Set the rule type to 'allow'

## Defaults

None.

## Example

```
ruckus(config-hotspot-restrict-access)# type allow  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## type deny

To set the hotspot access rule type to 'deny', use the following command:

```
type deny
```

## Syntax Description

**type**  
Set the hotspot access rule type

**deny**  
Set the rule type to 'deny'

## Defaults

None.

## Example

```
ruckus(config-hotspot-restrict-access)# type deny  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## destination address

To set the destination address of the rule, use the following command:

**destination address** *IP-ADDR/WORD*

### Syntax Description

**destination address**

Set the destination address of the rule

**IP-ADDR/WORD**

Set the destination to this IP address

### Defaults

None.

### Example

```
ruckus(config-hotspot-restrict-access)# destination address 192.168.20.20/24  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## destination port

To set the destination port of the rule, use the following command:

**destination port** *NUMBER/WORD*

### Syntax Description

**destination port**

Set the destination port of the rule

*NUMBER/WORD*

Set the destination to this port number

### Defaults

None.

### Example

```
ruckus(config-hotspot-restrict-access)# destination port 920  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## protocol

To set the protocol for the rule, use the following command:

**protocol** *NUMBER/WORD*

## Syntax Description

### **protocol**

Set the protocol for the rule

### *NUMBER/WORD*

Set to this protocol

## Defaults

None.

## Example

```
ruckus(config-hotspot-restrict-access)# protocol 58  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## intrusion-prevention

To enable temporary blocking of Hotspot clients with repeated authentication attempts, use the following command:

**intrusion-prevention**

## Defaults

Disabled.

## Example

```
ruckus(config-hotspot)# intrusion-prevention  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-hotspot)#
```

## no intrusion-prevention

To disable temporary blocking of Hotspot clients with repeated authentication failure, use the following command:

**no intrusion-prevention**

## Example

```
ruckus(config-hotspot)# no intrusion-prevention  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-hotspot)#
```

# Configure Hotspot 2.0 Commands

Use the `hs20op` and `hs20sp` commands to configure the controller's Hotspot 2.0 operator and service provider settings. To run these commands, you must first enter the **config-hs20op** or **config-hs20sp** context.

To deploy a Hotspot 2.0 service, you must configure the following:

- A Hotspot 2.0 Operator entry
- A Hotspot 2.0 Service Provider entry
- A WLAN with Hotspot 2.0 service enabled

## hs20op

Use the following command to configure a Hotspot 2.0 Operator entry:

```
hs20op WORD
```

### Syntax Description

**hs20op**

Create or configure a Hotspot 2.0 Operator entry

*WORD*

The name of the Hotspot 2.0 Operator entry.

### Example

```
ruckus(config)# hs20op operator1
The Hotspot (2.0) operator entry 'operator1' has been created.
ruckus(config-hs20op)# end
The Hotspot (2.0) operator entry has saved successfully.
Your changes have been saved.
ruckus(config)#
```

## no hs20op

Use the following command to delete a Hotspot 2.0 Operator entry:

```
no hs20op WORD
```

### Example

```
ruckus(config)# no hs20op operator1
The Hotspot (2.0) operator 'operator1' has been deleted.
ruckus(config)#
```

## Configure Hotspot 2.0 Operator Settings

The following commands can be used to configure Hotspot 2.0 Operator entry settings. To execute these commands, you must first create or edit a Hotspot 2.0 Operator entry using the `hs20op` command and entering the **config-hs20op** context.

### Syntax Description

**help**

Shows available commands.

**history**

Shows a list of previously run commands.

**abort**

Exits the config-hs20op context without saving changes.

**end**

Saves changes, and then exits the config-hs20op context.

**exit**

Saves changes, and then exits the config-hs20op context.

**quit**

Exits the config-hs20op context without saving changes.

**no internet-option**

Disables with connectivity to internet.

**no hessid**

Sets the HESSID to empty.

**no service-provider** *WORD NUMBER*

Deletes a service provider from the Hotspot (2.0) operator.

**no venue-group-type**

Sets both venue group and venue type to unspecified.

**no friendly-name** *LANGUAGE*

Disable the friendly name for the specified language.

**no asra**

Disables additional step required for access.

**no asra terms**

Disables ASRA Type: Acceptance of terms and conditions.

**no asra enrollment**

Disables ASRA Type: On-line enrollment supported.

**no asra http-https**

Disables ASRA Type: http/https redirection.

**no asra dns**

Disables ASRA Type: DNS redirection.

**no asra http-https-url**

Sets the redirect URL of http/https redirection to empty.

**no wan-metrics sym**

Disables Symmetric Link.

**no custm-conn-cap** *NUMBER*

Deletes a Connection Capability entry.

**no adv-gas dos-detect**

Disables the GAS DOS detection.

**no hs-caps operating-class-indication**

Disables the operating class indication.

**name** *WORD*

Sets the hotspot(2.0) operator entry name.

**description** *WORD*

Sets the hotspot(2.0) operator entry description.

**internet-option**

Enables with connectivity to internet.

**hessid** *MAC*

Sets the HESSID.

**hessid-use-bssid**

Sets the HESSID to use BSSID.

**service-provider** *WORD*

Adds a service provider to the Hotspot (2.0) operator.

**venue-group-type unspecified**

Sets the venue group to unspecified

**venue-group-type assembly**

Sets the venue group to assembly

**venue-group-type assembly unspecified**

Sets the venue type to unspecified

**venue-group-type assembly arena**

Sets the venue type to arena

**venue-group-type assembly stadium**

Sets the venue type to stadium

**venue-group-type assembly passenger-terminal**

Sets the venue type to passenger terminal

**venue-group-type assembly amphitheater**

Sets the venue type to amphitheater

**venue-group-type assembly amusement-park**

Sets the venue type to amusement park

**venue-group-type assembly place-worship**

Sets the venue type to place of worship

**venue-group-type assembly convention-center**

Sets the venue type to convention center

**venue-group-type assembly library**

Sets the venue type to library

**venue-group-type assembly museum**

Sets the venue type to museum

**venue-group-type assembly restaurant**

Sets the venue type to restaurant

**venue-group-type assembly theater**

Sets the venue type to theater

**venue-group-type assembly bar**

Sets the venue type to bar

**venue-group-type assembly coffee-shop**

Sets the venue type to coffee shop

**venue-group-type assembly zoo-or-aquarium**

Sets the venue type to zoo or aquarium

**venue-group-type assembly emergency-coordination-center**

Sets the venue type to emergency coordination center

**venue-group-type business**

Sets the venue group to business

**venue-group-type business unspecified**

Sets the venue type to unspecified

**venue-group-type business doctor-or-dentist-office**

Sets the venue type to doctor or dentist office

**venue-group-type business bank**

Sets the venue type to bank

**venue-group-type business fire-station**

Sets the venue type to fire station

**venue-group-type business police-station**

Sets the venue type to police station

**venue-group-type business post-office**

Sets the venue type to post office

**venue-group-type business professional-office**

Sets the venue type to professional office

**venue-group-type business research-and-development-facility**

Sets the venue type to research and development facility

**venue-group-type business attorney-office**

Sets the venue type to attorney office

**venue-group-type educational**

Sets the venue group to educational

**venue-group-type educational unspecified**

Sets the venue type to unspecified



**venue-group-type educational school-primary**

Sets the venue type to school primary

**venue-group-type educational school-secondary**

Sets the venue type to school secondary

**venue-group-type educational university-or-college**

Sets the venue type to university or college

**venue-group-type factory-industrial**

Sets the venue group to factory industrial

**venue-group-type factory-industrial unspecified**

Sets the venue type to unspecified

**venue-group-type factory-industrial factory**

Sets the venue type to factory

**venue-group-type institutional**

Sets the venue group to institutional

**venue-group-type institutional unspecified**

Sets the venue type to unspecified

**venue-group-type institutional hospital**

Sets the venue type to hospital

**venue-group-type institutional long-term-care-facility**

Sets the venue type to long term care facility

**venue-group-type institutional alcohol-and-drug-reHabilitation-center**

Sets the venue type to alcohol and drug reHabilitation center

**venue-group-type institutional group-home**

Sets the venue type to group home

**venue-group-type institutional prison-or-jail**

Sets the venue type to prison or jail

**venue-group-type mercantile**

Sets the venue group to mercantile

**venue-group-type mercantile unspecified**

Sets the venue type to unspecified

**venue-group-type mercantile retail-store**

Sets the venue type to retail store

**venue-group-type mercantile grocery-market**

Sets the venue type to grocery market

**venue-group-type mercantile automotive-service-station**

Sets the venue type to automotive service station

**venue-group-type mercantile shopping-mall**

Sets the venue type to shopping mall

**venue-group-type mercantile gas-station**

Sets the venue type to gas station

**venue-group-type residential**

Sets the venue group to residential

**venue-group-type residential unspecified**

Sets the venue type to unspecified

**venue-group-type residential private-residence**

Sets the venue type to private residence

**venue-group-type residential hotel-or-motel**

Sets the venue type to hotel or motel

**venue-group-type residential dormitory**

Sets the venue type to dormitory

**venue-group-type residential boarding-house**

Sets the venue type to boarding house

**venue-group-type storage**

Sets the venue group to storage

**venue-group-type storage unspecified**

Sets the venue type to unspecified

**venue-group-type utility-miscellaneous**

Sets the venue group to utility miscellaneous

**venue-group-type utility-miscellaneous unspecified**

Sets the venue type to unspecified

**venue-group-type vehicular**

Sets the venue group to vehicular

**venue-group-type vehicular unspecified**

Sets the venue type to unspecified

**venue-group-type vehicular automobile-or-truck**

Sets the venue type to automobile or truck

**venue-group-type vehicular airplane**

Sets the venue type to airplane

**venue-group-type vehicular bus**

Sets the venue type to bus

**venue-group-type vehicular ferry**

Sets the venue type to ferry

**venue-group-type vehicular ship-or-boat**

Sets the venue type to ship or boat

**venue-group-type vehicular train**

Sets the venue type to train

**venue-group-type vehicular motor-bike**

Sets the venue type to motor bike

**venue-group-type outdoor**

Sets the venue group to outdoor

**venue-group-type outdoor unspecified**

Sets the venue type to unspecified

**venue-group-type outdoor muni-mesh-network**

Sets the venue type to muni mesh network

**venue-group-type outdoor city-park**

Sets the venue type to city park

**venue-group-type outdoor rest-area**

Sets the venue type to rest area

**venue-group-type outdoor traffic-control**

Sets the venue type to traffic control

**venue-group-type outdoor bus-stop**

Sets the venue type to bus stop

**venue-group-type outdoor kiosk**

Sets the venue type to kiosk

**friendly-name** *LANGUAGE WORD*

Sets the friendly name for the specified language.

**asra**

Enables additional step required for access.

**asra terms**

Enables ASRA Type: Acceptance of terms and conditions.

**asra enrollment**

Enables ASRA Type: On-line enrollment supported.

**asra http-https**

Enables ASRA Type: http/https redirection.

**asra http-https url***WORD*

Sets the redirect URL of http/https redirection.

**asra dns**

Enables ASRA Type: DNS redirection.

**accs-net-type private**

Sets the access network type to Private network.

**accs-net-type private-with-guest**

Sets the access network type to Private network with guest access.

**accs-net-type chargeable-public**

Sets the access network type to Chargeable public network.

**accs-net-type free-public**

Sets the access network type to Free public network.

**accs-net-type personal-device**

Sets the access network type to Personal device network.

**accs-net-type test-or-experimental**

Sets the access network type to Test or experimental.

**accs-net-type wildcard**

Sets the access network type to Wildcard.

**ip-addr-type ipv4 not-avail**

Sets the IPv4 Address Type to not available.

**ip-addr-type ipv4 public**

Sets the IPv4 Address Type to public address.

**ip-addr-type ipv4 port-restricted**

Sets the IPv4 Address Type to port-restricted address.

**ip-addr-type ipv4 single-nated**

Sets the IPv4 Address Type to single NATed private address.

**ip-addr-type ipv4 double-nated**

Sets the IPv4 Address Type to double NATed private address.

**ip-addr-type ipv4 port-single**

Sets the IPv4 Address Type to port-restricted address and single NATed private address.

**ip-addr-type ipv4 port-double**

Sets the IPv4 Address Type to port-restricted address and double NATed private address.

**ip-addr-type ipv4 unknown**

Sets the IPv4 Address Type to unknown.

**ip-addr-type ipv6 not-avail**

Sets the IPv6 Address Type to not available.

**ip-addr-type ipv6 avail**

Sets the IPv6 Address Type to available.

**ip-addr-type ipv6 unknown**

Sets the IPv6 Address Type to unknown.

**wan-metrics sym**

Enables Symmetric Link.

**wan-metrics link-stat up**

Sets Link Status to Link UP.

**wan-metrics link-stat down**

Sets Link Status to Link Down.

**wan-metrics link-stat test**

Sets Link Status to Link in Test State.

**wan-metrics downlink-load *NUMBER***

Sets WAN downlink load.

**wan-metrics downlink-speed *NUMBER***

Sets WAN downlink speed.

**wan-metrics uplink-load *NUMBER***

Sets WAN uplink load.

**wan-metrics uplink-speed *NUMBER***

Sets WAN uplink speed.

**wan-metrics lmd** *NUMBER*

Sets Load Measurement Duration.

**conn-cap icmp closed**

Sets the ICMP Connection Capability Status to closed

**conn-cap icmp open**

Sets the ICMP Connection Capability Status to open

**conn-cap icmp unknown**

Sets the ICMP Connection Capability Status to unknown

**conn-cap ftp closed**

Sets the FTP Connection Capability Status to closed

**conn-cap ftp open**

Sets the FTP Connection Capability Status to open

**conn-cap ftp unknown**

Sets the FTP Connection Capability Status to unknown

**conn-cap ssh closed**

Sets the SSH Connection Capability Status to closed

**conn-cap ssh open**

Sets the SSH Connection Capability Status to open

**conn-cap ssh unknown**

Sets the SSH Connection Capability Status to unknown

**conn-cap http closed**

Sets the HTTP Connection Capability Status to closed

**conn-cap http open**

Sets the HTTP Connection Capability Status to open

**conn-cap http unknown**

Sets the HTTP Connection Capability Status to unknown

**conn-cap tls-vpn closed**

Sets the TLS VPN Connection Capability Status to closed

**conn-cap tls-vpn open**

Sets the TLS VPN Connection Capability Status to open

**conn-cap tls-vpn unknown**

Sets the TLS VPN Connection Capability Status to unknown

**conn-cap pptp-vpn closed**

Sets the PPTP VPN Connection Capability Status to closed

**conn-cap pptp-vpn open**

Sets the PPTP VPN Connection Capability Status to open

**conn-cap pptp-vpn unknown**

Sets the PPTP VPN Connection Capability Status to unknown

**conn-cap voip-tcp closed**

Sets the VoIP(TCP) Connection Capability Status to closed

**conn-cap voip-tcp open**

Sets the VoIP(TCP) Connection Capability Status to open

**conn-cap voip-tcp unknown**

Sets the VoIP(TCP) Connection Capability Status to unknown

**conn-cap ikev2 closed**

Sets the IKEv2 Connection Capability Status to closed

**conn-cap ikev2 open**

Sets the IKEv2 Connection Capability Status to open

**conn-cap ikev2 unknown**

Sets the IKEv2 Connection Capability Status to unknown

**conn-cap voip-udp closed**

Sets the VoIP(UDP) Connection Capability Status to closed

**conn-cap voip-udp open**

Sets the VoIP(UDP) Connection Capability Status to open

**conn-cap voip-udp unknown**

Sets the VoIP(UDP) Connection Capability Status to unknown

**conn-cap ipsec-vpn closed**

Sets the IPsec VPN Connection Capability Status to closed

**conn-cap ipsec-vpn open**

Sets the IPsec VPN Connection Capability Status to open

**conn-cap ipsec-vpn unknown**

Sets the IPsec VPN Connection Capability Status to unknown

**conn-cap esp closed**

Sets the ESP Connection Capability Status to closed

**conn-cap esp open**

Sets the ESP Connection Capability Status to open

**conn-cap esp unknown**

Sets the ESP Connection Capability Status to unknown

**custm-conn-cap NUMBER ip-proto NUMBER port NUMBERstatus closed**

Sets Status to closed.

**custm-conn-cap NUMBER ip-proto NUMBER port NUMBERstatus closed description WORD**

Sets the description of Connection Capability entry.

**custm-conn-cap NUMBER ip-proto NUMBER port NUMBERstatus open**

Sets Status to open.

**custm-conn-cap NUMBER ip-proto NUMBER port NUMBERstatus open description WORD**

Sets the description of Connection Capability entry.

**custm-conn-cap NUMBER ip-proto NUMBER port NUMBERstatus unknown**

Sets Status to unknown.

**custm-conn-cap NUMBER ip-proto NUMBER port NUMBERstatus unknown description WORD**

Sets the description of Connection Capability entry.

**adv-gas cb-delay** *NUMBER*

Sets the GAS Comeback Delay.

**adv-gas rsp-limit** *NUMBER*

Sets the GAS query response length limit.

**adv-gas rsp-buf-time** *NUMBER*

Sets the GAS query response buffering time.

**adv-gas dos-detect**

Enables the GAS DOS detection.

**adv-gas dos-maxreq** *NUMBER*

Set the GAS DOS detection maximum request number.

**hs-caps operating-class-indication 2.4**

Sets the operating class indication to 2.4 GHz.

**hs-caps operating-class-indication 5**

Sets the operating class indication to 5 GHz.

**hs-caps operating-class-indication dual-band**

Sets the operating class indication to 2.4/5 GHz.

**show**

Displays hotspot 2.0 operator settings.

## hs20sp

Use the following command to configure a Hotspot 2.0 Service Provider entry:

**hs20sp** *WORD*

### Example

```
ruckus(config)# hs20sp serviceprovider1
```

The Hotspot (2.0) service provider entry 'serviceprovider1' has been created.

```
ruckus(config-hs20sp)# end
```

The Hotspot (2.0) service provider entry has saved successfully.

Your changes have been saved.

```
ruckus(config)#
```

## no hs20sp

Use the following command to delete a Hotspot 2.0 Service Provider entry:

**no hs20sp** *WORD*

### Example

```
ruckus(config)# no hs20sp provider1
```

The Hotspot (2.0) service provider 'provider1' has been deleted.

```
ruckus(config)#
```

## Configure Hotspot 2.0 Service Provider Settings

The following commands can be used to configure Hotspot 2.0 Service Provider entry settings. To execute these commands, you must first create or edit a Hotspot 2.0 Service Provider entry using the **hs20sp** command and entering the **config-hs20sp** context.

### Syntax Description

**help**

Shows available commands.

**history**

Shows a list of previously run commands.

**abort**

Exits the config-hs20sp context without saving changes.

**end**

Saves changes, and then exits the config-hs20sp context.

**exit**

Saves changes, and then exits the config-hs20sp context.

**quit**

Exits the config-hs20sp context without saving changes.

**no nai-realm** *NUMBER*

Deletes a NAI Realm entry.

**no domain-name** *NUMBER*

Deletes a domain name entry.

**no roam-consortium** *NUMBER*

Deletes a roaming consortium entry.

**no anqp-3gpp-info** *NUMBER*

Deletes a 3GPP cellular network information entry.

**name** *WORD*

Sets the hotspot(2.0) service provider entry name.

**description** *WORD*

Sets the hotspot(2.0) service provider entry description.

**nai-realm** *NUMBER*

Creates a new NAI Realm entry or modifies an existing entry.

**domain-name** *NUMBER*

Creates a new domain name entry or modifies an existing entry.

**domain-name***NUMBER* **name** *WORD*

Sets the domain name of a domain name entry.

**roam-consortium** *NUMBER*

Creates a new roaming consortium entry or modifies an existing entry.

**roam-consortium***NUMBER* **org-id** *HEX*

Sets the organization ID of a roaming consortium entry.



**roam-consortium** *NUMBER org-id HEX name WORD*

Sets the name of a roaming consortium entry.

**anqp-3gpp-info** *NUMBER*

Creates a 3GPP cellular network information entry or modifies an existing entry list.

**anqp-3gpp-info** *NUMBER mcc NUMBER*

Sets the MCC of 3GPP cellular network information entry.

**anqp-3gpp-info** *NUMBER mcc NUMBER mnc NUMBER*

Sets the MNC of 3GPP cellular network information entry.

**anqp-3gpp-info** *NUMBER mcc NUMBER mnc NUMBER name WORD*

Sets the name of 3GPP cellular network information entry.

**show**

Displays hotspot 2.0 service provider settings.

## nai-realm

To create, a new NAI Realm entry or modifies an existing entry, use the following command:

**nai-realm** *NUMBER*

This command enters the config-hs20sp-nai-realm context. The following commands can be executed from within this context.

### Syntax Description

**name**

Sets the name of the NAI Realm entry.

**encoding**

Sets the encoding of the NAI Realm entry.

**eap-method** *NUMBER*

Sets the EAP method #X of the NAI Realm entry. (X:1~4)

**no**

Contains commands that can be executed from within the context.

**show**

Displays NAI Realm settings.

### Example

```
ruckus(config-hs20sp)# nai-realm 1
ruckus(config-hs20sp-nai-realm)# name realm1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-hs20sp-nai-realm)# show
  Name= realm1
  Encoding= RFC-4282
  EAP Method #1= N/A
  EAP Method #2= N/A
  EAP Method #3= N/A
  EAP Method #4= N/A
ruckus(config-hs20sp-nai-realm)# end
To save the changes, type 'end' or 'exit'.
ruckus(config-hs20sp)# end
```

```
The Hotspot (2.0) service provider entry has saved successfully.  
Your changes have been saved.  
ruckus(config)#
```

## name

Use the following command to set the name of the NAI Realm entry:

```
name WORD
```

## encoding

Use the following command to set the encoding of the NAI Realm entry:

```
encoding [ rfc-4282 | utf-8 ]
```

## eap-method

Use the following command to set the EAP method of the NAI Realm entry:

```
eap-method NUMBER
```

## eap-method eap-mthd

Use the following command to set the EAP method of the NAI Realm entry:

```
eap-method NUMBER eap-mthd [N/A | NAME ]
```

## Syntax Description

### **N/A**

Sets the EAP method of the NAI Realm entry to N/A.

### **MD5-Challenge**

Sets the EAP method of the NAI Realm entry to MD5-Challenge.

### **EAP-TLS**

Sets the EAP method of the NAI Realm entry to EAP-TLS.

### **EAP-CISCO**

Sets the EAP method of the NAI Realm entry to EAP-Cisco.

### **EAP-SIM**

Sets the EAP method of the NAI Realm entry to EAP-SIM.

### **EAP-TTLS**

Sets the EAP method of the NAI Realm entry to EAP-SIM.

### **PEAP**

Sets the EAP method of the NAI Realm entry to PEAP.

### **MSCHAP-V2**

Sets the EAP method of the NAI Realm entry to EAP-MSCHAP-V2.

### **EAP-AKA**

Sets the EAP method of the NAI Realm entry to EAP-AKA.

### **EAP-AKA-Prime**

Sets the EAP method of the NAI Realm entry to EAP-AKA'.

### **Reserved**

Sets the EAP method of the NAI Realm entry to Reserved.

## **Example**

```
ruckus(config-hs20sp-nai-realm)# eap-method 1 eap-mthd EAP-TLS
The command was executed successfully. To save the changes, type 'end' or 'exit'
ruckus(config-hs20sp-nai-realm)#
```

## **eap-method auth-info**

To set the Auth Info of the EAP method, use the following command:

**eap-method** *NUMBER* **auth-info** *NUMBER*

## **Syntax Description**

### **auth-id**

Sets the auth info ID of the auth info.

### **auth-id expanded-EAP-method**

Sets the Auth Info of the EAP method to expanded-EAP-method.

### **auth-id expanded-EAP-method vndr-id** *NUMBER*

Sets the vendor ID of the auth info.

### **auth-id expanded-EAP-method vndr-id** *NUMBER NUMBER*

Sets the vendor type of the auth info.

### **auth-id nonEAP-inner-auth**

Sets the Auth Info of the EAP method to Non-EAP Inner Authentication Type.

### **auth-id nonEAP-inner-auth auth-type**

Sets the auth info type of the auth info.

### **nonEAP-inner-auth auth-type Reserved**

Sets the Non-EAP Inner Authentication Type to Reserved.

### **auth-id nonEAP-inner-auth auth-type PAP**

Sets the Non-EAP Inner Authentication Type to PAP.

### **auth-id nonEAP-inner-auth auth-type CHAP**

Sets the Non-EAP Inner Authentication Type to CHAP.

### **auth-id nonEAP-inner-auth auth-type MSCHAP**

Sets the Non-EAP Inner Authentication Type to MSCHAP.

### **auth-id nonEAP-inner-auth auth-type MSCHAPV2**

Sets the Non-EAP Inner Authentication Type to MSCHAPV2.

### **auth-id inner-auth-EAP-mthd**

Sets the Auth Info of the EAP method to Inner Authentication EAP Method Type.

- auth-id inner-auth-EAP-mthd auth-type**  
Sets the auth info type of the auth info.
- auth-id inner-auth-EAP-mthd auth-type EAP-TLS**  
Sets the Inner Authentication EAP Method Type to EAP-TLS.
- auth-id inner-auth-EAP-mthd auth-type EAP-SIM**  
Sets the Inner Authentication EAP Method Type to EAP-SIM.
- auth-id inner-auth-EAP-mthd auth-type EAP-TTLS**  
Sets the Inner Authentication EAP Method Type to EAP-TTLS.
- auth-id inner-auth-EAP-mthd auth-type EAP-AKA**  
Sets the Inner Authentication EAP Method Type to EAP-AKA.
- auth-id inner-auth-EAP-mthd auth-type EAP-AKA-Prime**  
Sets the Inner Authentication EAP Method Type to EAP-AKA'.
- auth-id exp-inner-EAP-mthd**  
Sets the Auth Info of the EAP method to expanded-inner-EAP-method.
- auth-id inner-EAP-mthd vndr-id** *NUMBER*  
Sets the vendor ID of the auth info.
- auth-id exep-inner-EAP-mthd vndr-id** *NUMBER* **vndr-type** *NUMBER*  
Sets the vendor type of the auth info.
- auth-id credential-type**  
Sets the Auth Info of the EAP method to Credential Type.
- auth-id credential-type auth-type**  
Sets the auth info type of the auth info.
- auth-id credential-type auth-type SIM**  
Sets the Credential Type to SIM.
- auth-id credential-type auth-type USIM**  
Sets the Credential Type to USIM.
- auth-id credential-type auth-type NFC-secure-elem**  
Sets the Credential Type to NFC Secure Element.
- auth-id credential-type auth-type hardware-token**  
Sets the Credential Type to Hardware Token.
- auth-id credential-type auth-type softoken**  
Sets the Credential Type to Softoken.
- auth-id credential-type auth-type certificate**  
Sets the Credential Type to Certificate.
- auth-id credential-type auth-type**  
**auth-id credential-type auth-type username-password**  
Sets the Credential Type to username/password.
- auth-id credential-type auth-type none**  
Sets the Credential Type to none.
- auth-id credential-type auth-type reserved**  
Sets the Credential Type to Reserved.

**auth-id tunnel-EAP-mthd-crdn-type**

Sets the Auth Info of the EAP method to Tunneled EAP Method Credential Type.

**auth-id tunnel-EAP-mthd-crdn-type auth-type**

Sets the auth info type of the auth info.

**auth-id tunnel-EAP-mthd-crdn-type auth-type SIM**

Sets the Tunneled EAP Method Credential Type to SIM.

**auth-id tunnel-EAP-mthd-crdn-type auth-type USIM**

Sets the Tunneled EAP Method Credential Type to USIM.

**auth-id tunnel-EAP-mthd-crdn-type auth-type NFC-secure-elem**

Sets the Tunneled EAP Method Credential Type to NFC Secure Element.

**auth-id tunnel-EAP-mthd-crdn-type auth-type hardware-token**

Sets the Tunneled EAP Method Credential Type to Hardware Token.

**auth-id tunnel-EAP-mthd-crdn-type auth-type softoken**

Sets the Tunneled EAP Method Credential Type to Softoken.

**auth-id tunnel-EAP-mthd-crdn-type auth-type certificate**

Sets the Tunneled EAP Method Credential Type to Certificate.

**auth-id tunnel-EAP-mthd-crdn-type auth-type username-password**

Sets the Tunneled EAP Method Credential Type to username/password.

**auth-id tunnel-EAP-mthd-crdn-type auth-type reserved**

Sets the Tunneled EAP Method Credential Type to Reserved.

**auth-id tunnel-EAP-mthd-crdn-type auth-type anonymous**

Sets the Tunneled EAP Method Credential Type to Anonymous.

**no eap-method *NUMBER***

Sets the EAP method #X of the NAI Realm entry. (X:1~4)

**no eap-method *NUMBER* auth-info *NUMBER***

Disable the Auth Info of the EAP method

**show**

Displays NAI Realm settings.

# Configure Mesh Commands

Use the mesh commands to configure the controller's mesh networking settings. To run these commands, you must first enter the **config-mesh** context.

## mesh

Use the mesh command to enter the config-mesh context and configure the mesh-related settings.

**mesh**

### Syntax Description

**mesh**

Configure mesh settings

### Defaults

none

### Example

```
ruckus(config)# mesh
ruckus(config-mesh)#
```

## abort

To exit the config-mesh context without saving changes, use the abort command.

## end

To save changes, and then exit the config-mesh context, use the end command.

## exit

To save changes, and then exit the config-mesh context, use the exit command.

## quit

To exit the config-mesh context without saving changes, use the quit command.

## show

To display the current mesh settings, use the following command from within the *config-mesh* context:

**show**

## Syntax Description

### show

Display the current mesh settings

## Example

```
ruckus(config-mesh)# show
Mesh Settings:
  Mesh Status= Enabled
  Mesh Name (ESSID)= Mesh-951608000220
  Mesh Passphrase= bzj9Y0kEpKxOPzPXyKqLrJHZSAAntfaTm7Ebh6qps24PFPcc5MtCiiJGGwFZBG
  Mesh Radio Option= 5G
  Mesh Uplink Selection Algorithm = default(static)
  Mesh Hop Detection:
    Status= Disabled
  Mesh Downlinks Detection:
    Status= Disabled
  Tx. Rate of Management Frame= 2Mbps
  Beacon Interval= 200ms
  Zero-Touch-Mesh status= Enabled
Zero Touch Mesh Pre-Approved Serial Number List:
serial number = 921802014959, approved = 0, time = 0, id = 1
serial number = 441e981cf0d0, approved = 0, time = 0, id = 2
serial number = 4f1e681cf3f0, approved = 0, time = 0, id = 3
serial number = c41e781bd7c0, approved = 0, time = 0, id = 4
ruckus(config-mesh)#
```

## ssid

To set the SSID of the mesh network, use the following command:

**ssid** *WORD/SSID*

## Syntax Description

### ssid

Set the SSID of the mesh network

*WORD/SSID*

Set to this SSID

## Defaults

None.

## Example

```
ruckus(config-mesh)# ssid rks_mesh
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## passphrase

To set the passphrase that allows access to the mesh network, use the following command:

**passphrase** *WORD*

## Syntax Description

### **passphrase**

Set the passphrase that allows access to the mesh network

*WORD*

Set to this passphrase

## Defaults

None.

## Example

```
ruckus(config-mesh)# passphrase test123456  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## hops-warn-threshold

To enable and configure the mesh hop threshold, use the following command:

**hops-warn-threshold** *NUMBER*

## Syntax Description

### **hops-warn-threshold**

Set the mesh hop threshold (max hops)

*NUMBER*

Set to this threshold value

## Defaults

5

## Example

```
ruckus(config-mesh)# hops-warn-threshold 6  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## no detect-hops

To disable the mesh hop threshold, use the following command:

**no detect-hops**

## Syntax Description

### **no detect-hops**

Disable the mesh hop threshold



## Defaults

None.

## Example

```
ruckus(config-mesh)# no detect-hops  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## fan-out-threshold

To enable and configure the mesh downlink threshold, use the following command:

```
fan-out-threshold NUMBER
```

## Syntax Description

### **fan-out-threshold**

Set the mesh downlink threshold (max downlinks)

*NUMBER*

Set to this threshold value

## Defaults

5

## Example

```
ruckus(config-mesh)# fan-out-threshold 8  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## no detect-fanout

To disable the mesh downlink threshold, use the following command:

```
no detect-fanout
```

## Syntax Description

### **no detect-fanout**

Disable the mesh downlink threshold

## Example

```
ruckus(config-mesh)# no detect-fanout  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## beacon-interval

To set the beacon interval for mesh links, use the following command:

**beacon-interval** *NUMBER*

### Syntax Description

**beacon-interval**

Set the beacon interval for mesh links

*NUMBER*

Enter the beacon interval (100~1000 TUs)

### Defaults

200

### Example

```
ruckus(config-mesh)# beacon-interval 200
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-mesh)#
```

## mgmt-tx-rate

To set the transmit rate for management frames, use the following command:

**mgmt-tx-rate** *RATE*

### Syntax Description

**mgmt-tx-rate**

Set the max transmit rate for management frames

*RATE*

Set the transmit rate (in Mbps).

### Defaults

2

### Example

```
ruckus(config-mesh)# mgmt-tx-rate 2
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-mesh)#
```

## mesh-uplink-selection static

Sets static on mesh uplinks, the default is static.

**mesh-uplink selection static**

## Syntax Description

### **mesh-uplink-selection**

Set the mesh uplink selection method.

### **static**

Set mesh uplink selection to static.

## Defaults

Static

## Example

```
ruckus(config-mesh)# mesh-uplink-selection static
Nothing changed
ruckus(config-mesh)#
```

## mesh-uplink-selection dynamic

Sets dynamic on mesh uplinks.

### **mesh-uplink selection dynamic**

## Syntax Description

### **mesh-uplink-selection**

Set the mesh uplink selection method.

### **dynamic**

Set mesh uplink selection to dynamic.

## Defaults

Static

## Example

```
ruckus(config-mesh)# mesh-uplink-selection dynamic
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-mesh)#
```

## mesh-radio-option

To set the mesh radio, use the following command:

**mesh-radio-option <2.4G | 5G>**

### Options

2.4G: Sets mesh radio type to 2.4 GHz.

5G: Sets mesh radio type to 5 GHz.

### Defaults

5G

### Example

```
ruckus(config-mesh)# mesh-radio-option 5G  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-mesh)#
```

## zero-touch-mesh

To enable zero touch mesh, use the following command:

**zero-touch-mesh**

### *Defaults*

Disabled

### *Example*

```
ruckus(config-mesh)# zero-touch-mesh  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-mesh)#
```

## no zero-touch-mesh

To disable zero touch mesh, use the following command:

**no zero-touch-mesh**

### *Defaults*

Disabled

### *Example*

```
ruckus(config-mesh)# no zero-touch-mesh  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-mesh)#
```

## zt-mesh-serial

To add one or more zero-touch mesh pre-approved serial numbers, use the following command:

```
zt-mesh-serial[<SERIAL_1> <SERIAL_2> <...> <SERIAL_n>]
```

### Syntax Description

zt-mesh-serial: Add zero-touch mesh pre-approved serial number.

<SERIAL\_1>... : Serial number to be added to Zero Touch Mesh pre-approved list.

#### NOTE

The `zt-mesh-serial` command only submits these serial numbers to a system memory buffer. It does not save them to the pre-approved AP list. If you enter the `exit` or `end` command, these serial numbers will be saved to the pre-approved serial list and deleted from the system memory buffer. If you enter the `quit` or `abort` command, these serial numbers will be discarded and deleted from the system memory buffer.

### Example

```
ruckus(config-mesh)# zt-mesh-serial 111122223333 222233334444 333344445555 444455556666
Add all serial numbers to zt-mesh pre-approved list submit ok!
ruckus(config-mesh)# end
Add 111122223333 to zt-mesh pre-approved list execute success!
Add 222233334444 to zt-mesh pre-approved list execute success!
Add 333344445555 to zt-mesh pre-approved list execute success!
Add 444455556666 to zt-mesh pre-approved list execute success!
Your changes have been saved.
ruckus(config)#
```

## no zt-mesh-serial

To delete a zero-touch mesh pre-approved serial number, use the following command:

```
no zt-mesh-serial [<SERIAL_1> <SERIAL_2> <...> <SERIAL_n>]
```

### Syntax Description

no zt-mesh-serial: Delete zero-touch mesh pre-approved serial number.

<SERIAL\_1>... : Serial number to be removed from Zero Touch Mesh pre-approved list.

#### NOTE

The `no zt-mesh-serial` command only submits these serial numbers to a system memory buffer. It does not remove them from the pre-approved AP list. If you enter the `exit` or `end` command, these serial numbers will be removed from the pre-approved serial list and deleted from the system memory buffer. If you enter the `quit` or `abort` command, these serial numbers will be discarded and deleted from the system memory buffer.

### Example

```
ruckus(config-mesh)# no zt-mesh-serial 111122223333 222233334444 333344445555 444455556666
Delete all serial numbers from zt-mesh pre-approved list submit ok!
ruckus(config-mesh)# end
Delete 111122223333 from zt-mesh pre-approved list execute success!
Delete 222233334444 from zt-mesh pre-approved list execute success!
Delete 333344445555 from zt-mesh pre-approved list execute success!
Delete 444455556666 from zt-mesh pre-approved list execute success!
Your changes have been saved.
ruckus(config)#
```



# Configure Alarm Commands

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

## alarm

To enter the config-alarm context, use the following command.

```
alarm
```

## Defaults

Disabled

## Example

```
ruckus(config)# alarm  
ruckus(config-alarm)#
```

## no alarm

To disable alarm settings, use the following command:

```
no alarm
```

## Example

```
ruckus(config)# no alarm  
The Alarm settings have been updated.  
ruckus(config)#
```

## abort

To exit the config-alarm context without saving changes, use the abort command.

```
abort
```

## end

To save changes, and then exit the config-alarm context, use the following command:

```
end
```

## Example

```
ruckus(config-alarm)# end  
The Alarm settings have been updated.  
Your changes have been saved.  
ruckus(config)#
```

## exit

To save changes, and then exit the config-alarm context, use the following command:

**exit**

### Example

```
ruckus(config-alarm)# exit
The Alarm settings have been updated.
Your changes have been saved.
```

## quit

To exit the config-alarm context without saving changes, use the quit command.

**quit**

### Example

```
ruckus(config-alarm)# quit
No changes have been saved.
ruckus(config)#
```

## e-mail

To set the email address to which alarm notifications will be sent, use the following command:

**e-mail** *WORD*

### Syntax Description

**e-mail**

Set the email address to which alarm notifications will be sent

*WORD*

Send alarm notifications to this email address

### Defaults

None.

### Example

```
ruckus(config-alarm)# e-mail joe@163.com
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## show

To display the current alarm settings, use the following command:

**show**

### **Example**

```
ruckus(config-alarm)# show
Alarm:
  Status= Enabled
  Email Address= test@hotmail.com

ruckus(config-alarm)#
```

# Configure Alarm-Event Settings

Use the alarm-event commands to configure which events will trigger ZoneDirector email alerts. Entering this command enters the **config-alarm-event** context.

## alarm-event

To enter the config-alarm-event context and configure email alarm notifications for specific event types, use the following command:

**alarm-event**

## event

To enable email alarm notifications for a specific alarm event, use the following command:

**event** *WORD*

## Syntax Description

### **event all**

Enable email alarms for all event types

### **rogue-ap-detected**

Enable email notification when Rogue AP detected

### **rogue-device-detected**

Enable email notification when Ad hoc network detected

### **ap-lost-contacted**

AP lost contact

### **ssid-spoofing-ap-detected**

SSID spoofing AP detected

### **mac-spoofing-ap-detected**

MAC spoofing AP detected

### **user-blocked-ap-detected**

User blocked AP detected

### **rogue-dhcp-server-detected**

Rogue DHCP server detected

### **temporary-license-expired**

Temporary license has expired

### **temporary-license-will-expire**

Temporary license will expire

### **lan-rogue-ap-detected**

LAN Rogue AP detected

### **radius-server-unreachable**

RADIUS server unreachable

**ap-has-hardware-problem**

AP hardware problem detected

**uplink-ap-lost**

Mesh AP uplink connection lost

**incomplete-primary/secondary-ip-settings**

AP fails to maintain primary/secondary ZD IP address settings

**smart-redundancy-state-changed**

Smart Redundancy device status change detected

**smart-redundancy-active-connected**

Smart Redundancy device active device connected

**smart-redundancy-standby-connected**

Smart Redundancy standby device connected

**smart-redundancy-active-disconnected**

Smart Redundancy active device disconnected

**smart-redundancy-standby-disconnected**

Smart Redundancy standby device disconnected

**entitlement-download-fail**

Failure to download the Support Entitlement file from the Ruckus Entitlement server

**test-alarm ap-lose-connection**

Test AP connection lost alarm event

**show**

Show alarm settings

**Defaults**

All enabled

**Example**

```
ruckus(config)# alarm-event
ruckus(config-alarm-event)# event all
ruckus(config-alarm-event)# show
Alarm Events Notify By Email:
MSG_rogue_AP_detected=                enabled
MSG_ad_hoc_network_detected=          enabled
MSG_AP_lost=                          enabled
MSG_SSID_spoofing_AP_detected=        enabled
MSG_MAC_spoofing_AP_detected=         enabled
MSG_admin_rogue_dhcp_server=          enabled
MSG_admin_templic_expired=            enabled
MSG_admin_templic_oneday=             enabled
MSG_same_network_spoofing_AP_detected= enabled
MSG_RADIUS_service_outage=            enabled
MSG_AP_hardware_problem=              enabled
MSG_AP_no_mesh_uplink=                enabled
MSG_AP_keep_no_AC_cfg=                enabled
MSG_cltr_change_to_active=            enabled
MSG_cltr_active_connected=            enabled
MSG_cltr_standby_connected=           enabled
MSG_cltr_active_disconnected=         enabled
MSG_cltr_standby_disconnected=        enabled
MSG_user_blocked_AP_detected=         enabled
```

```
MSG_Entitlement_file_download_fail=          enabled  
ruckus(config-alarm-event)#
```

## no event

To disable email alarm notifications for specific event types, use the following command:

```
no event event_name
```

### Syntax Description

**no event**

Disable email alarms for this event type

**all**

Disable email alarms for all event types

**rogue-ap-detected**

Rogue AP detected

**rogue-device-detected**

Ad hoc network detected

**ap-lost-contacted**

AP lost contact

**ssid-spoofing-ap-detected**

SSID spoofing AP detected

**mac-spoofing-ap-detected**

MAC spoofing AP detected

**user-blocked-ap-detected**

User blocked AP detected

**rogue-dhcp-server-detected**

Rogue DHCP server detected

**temporary-license-expired**

Temporary license has expired

**temporary-license-will-expire**

Temporary license will expire

**lan-rogue-ap-detected**

LAN Rogue AP detected

**radius-server-unreachable**

RADIUS server unreachable

**ap-has-hardware-problem**

AP hardware problem detected

**uplink-ap-lost**

Mesh AP uplink connection lost

**incomplete-primary/secondary-ip-settings**

AP fails to maintain primary/secondary ZD IP address settings

**smart-redundancy-state-changed**

Smart Redundancy device status change detected

**smart-redundancy-active-connected**

Smart Redundancy device active device connected

**smart-redundancy-standby-connected**

Smart Redundancy standby device connected

**smart-redundancy-active-disconnected**

Smart Redundancy active device disconnected

**smart-redundancy-standby-disconnected**

Smart Redundancy standby device disconnected

**entitlement-download-fail**

Failure to download the Support Entitlement file from the Ruckus Entitlement server

**Example**

```
ruckus(config-alarm-event)# no event aaa-server-unreachable
ruckus(config-alarm-event)# show
Alarm Events Notify By Email:
MSG_rogue_AP_detected=                enabled
MSG_ad_hoc_network_detected=          enabled
MSG_AP_lost=                           enabled
MSG_SSID_spoofing_AP_detected=        enabled
MSG_MAC_spoofing_AP_detected=         enabled
MSG_admin_rogue_dhcp_server=           enabled
MSG_admin_templc_expired=              enabled
MSG_admin_templc_oneday=                enabled
MSG_same_network_spoofing_AP_detected= enabled
MSG_RADIUS_service_outage=             disabled
MSG_AP_hardware_problem=                enabled
MSG_AP_no_mesh_uplink=                  enabled
MSG_AP_keep_no_AC_cfg=                  enabled
MSG_cltr_change_to_active=              enabled
MSG_cltr_active_connected=              enabled
MSG_cltr_standby_connected=             enabled
MSG_cltr_active_disconnected=           enabled
MSG_cltr_standby_disconnected=          enabled
MSG_user_blocked_AP_detected=           enabled
MSG_Entitlement_file_download_fail=     enabled

ruckus(config-alarm-event)#
```

# Configure Services Commands

Use the services commands to configure miscellaneous service settings, such as automatic power and channel selection settings, ChannelFly, background scanning, rogue AP and rogue DHCP server detection, etc. To run these commands, you must first enter the **config-services** context.

## abort

To exit the config-services context without saving changes, use the abort command.

**abort**

### Syntax Description

**abort**

Exit the service settings without saving changes

### Example

```
ruckus(config-services)# abort
No changes have been saved.
ruckus(config)#
```

## end

To save changes, and then exit the config-services context, use the following command:

**end**

### Syntax Description

**end**

Save changes, and then exit the context

### Example

```
ruckus(config-services)# end
Your changes have been saved.
ruckus(config)#
```

## exit

To save changes, and then exit the config-services context, use the following command:

**exit**

### Syntax Description

**exit**

Save changes, and then exit the context



## Example

```
ruckus(config-services)# exit  
Your changes have been saved.  
ruckus(config)#
```

## quit

To exit the config-services context without saving changes, use the quit command.

**quit**

## Syntax Description

**quit**

Exit the service settings without saving changes

## Example

```
ruckus(config-services)# quit  
No changes have been saved.  
ruckus(config)#
```

## auto-adjust-ap-power

To enable the auto adjustment of theAP radio power, which helps optimize radio coverage when radio interference is present, use the following command:

**auto-adjust-ap-power**

## Syntax Description

**auto-adjust-ap-power**

Enable the auto adjustment of theAP radio power

## Defaults

Disabled.

## Example

```
ruckus(config-services)# auto-adjust-ap-power  
The command was executed successfully.
```

## no auto-adjust-ap-power

To disable the auto adjustment of theAP radio power, which helps optimize radio coverage when radio interference is present, use the following command:

**no auto-adjust-ap-power**

### **Syntax Description**

#### **no auto-adjust-ap-power**

Disable the auto adjustment of the AP radio power

### **Defaults**

Disabled.

### **Example**

```
ruckus(config-services)# no auto-adjust-ap-power  
The command was executed successfully.
```

## **auto-adjust-ap-channel**

To enable the auto adjustment of the AP radio channel when radio interference is present, use the following command:

#### **auto-adjust-ap-channel**

### **Syntax Description**

#### **auto-adjust-ap-channel**

Enable the auto adjustment of the AP radio channel

### **Defaults**

None.

### **Example**

```
ruckus(config-services)# auto-adjust-ap-channel  
The command was executed successfully.
```

## **no auto-adjust-ap-channel**

To disable the auto adjustment of the AP radio channel when radio interference is present, use the following command:

#### **no auto-adjust-ap-channel**

### **Syntax Description**

#### **no auto-adjust-ap-channel**

Disable the auto adjustment of the AP radio channel

### **Defaults**

None.

## Example

```
ruckus(config-services)# no auto-adjust-ap-channel  
The command was executed successfully.
```

## raps

To enable the Radar Avoidance Pre-Scanning (RAPS) feature on supported access points (SC-8800-S, 7782, 7781, etc.), use the following command:

```
raps
```

## no raps

To disable the Radar Avoidance Pre-Scanning (RAPS) feature on supported access points (SC-8800-S, 7782, 7781, etc.), use the following command:

```
no raps
```

## channelfly

To enable ChannelFly channel management, use the following command:

```
channelfly [ radio-2.4-mtbc | radio-5-mtbc ] NUMBER
```

## Syntax Description

### **channelfly**

Enable ChannelFly automatic adjustment of the AP radio channel

### **radio-2.4**

Enable ChannelFly on the 2.4 GHz radio

### **radio-5**

Enable ChannelFly on the 5 GHz radio

### **mtbc**

Set the mean time between channel changes

### *NUMBER*

Number in minutes (1~1440) to set as mean time between channel change

## Defaults

Enabled for both 2.4 and 5 GHz radios

MTBC: 100

## Example

Enable ChannelFly channel management for 2.4G radios

```
ruckus(config-services)# channelfly radio-2.4 100  
The command was executed successfully.  
ruckus(config-services)#
```

Enable ChannelFly channel management for 5 G radios

```
ruckus(config-services)# channelfly radio-2.4-mtbc 100
The command was executed successfully.
ruckus(config-services)#
```

## no channelfly

To disable ChannelFly channel management, use the following command:

**no channelfly [ radio-2.4 | radio-5 ]**

### Syntax Description

**no channelfly**

Disable ChannelFly automatic adjustment of theAP radio channel

**radio-2.4**

Disable ChannelFly on the 2.4 GHz radio

**radio-5**

Disable ChannelFly on the 5 GHz radio

### Defaults

None.

### Example

```
ruckus(config-services)# no channelfly radio-2.4
The command was executed successfully.
ruckus(config-services)# no channelfly radio-5
The command was executed successfully.
ruckus(config-services)#
```

## background-scan

To enable background scanning and configure the scan interval, use the following command:

**background-scan [ radio-2.4-interval | radio-5-interval ] NUMBER**

### Syntax Description

**background-scan**

Enable background scanning and configure the scan interval

**radio-2.4-interval**

Configure background scanning interval for the 2.4 GHz radio

**radio-5-interval**

Configure background scanning interval for theGHz radio

**NUMBER**

Perform background scan at this interval (in seconds)

## Defaults

20 seconds

## Example

```
ruckus(config-services)# background-scan radio-2.4-interval 6  
The command was executed successfully.
```

## no background-scan

To disable background scanning on the 2.4GHz radio, use the following command:

```
no background-scan [ radio-2.4-interval | radio-5 ]
```

## Syntax Description

### **no background-scan**

Disable background scanning

### **radio-2.4**

Disable background scanning on the 2.4GHz radio

### **radio-5**

Disable background scanning on the 5GHz radio

## Defaults

None

## Example

```
ruckus(config-services)# no background-scan radio-2.4  
The command was executed successfully.  
ruckus(config-services)# no background-scan radio-5  
The command was executed successfully.
```

## background-scan low-threshold

To set the min threshold to switch channels for the 2.4 GHz radio, use the following command:

```
background-scan low-threshold <NUMBER>
```

## Syntax Description

### **background-scan low-threshold**

Configure the low threshold for the radio.

### *NUMBER*

Set the minimum threshold value (0~2000).

## **Defaults**

Disabled

## **Example**

```
ruckus(config-services)# background-scan low-threshold 20  
The command was executed successfully.  
ruckus(config-services)#
```

## aeroscout-detection

To enable detection of AeroScout RFID Tags by APs that are managed by ZoneDirector, use the following command:

**aeroscout-detection**

### Syntax Description

**aeroscout-detection**

Enable detection of AeroScout RFID Tags by APs

### Defaults

Disabled

### Example

```
ruckus(config-services)# aeroscout-detection  
The command was executed successfully.
```

## no aeroscout-detection

To disable detection of AeroScout RFID Tags by APs that are managed by ZoneDirector, use the following command:

**no aeroscout-detection**

### Syntax Description

**no aeroscout-detection**

Disable detection of AeroScout RFID Tags by APs

### Defaults

Disabled

### Example

```
ruckus(config-services)# no aeroscout-detection  
The command was executed successfully.
```

## ekahau

To enable and set Ekahau Blink support with ERC IP and port, use the following command:

**ekahau** *ERC IP ERC Port*

### Defaults

Disabled

## Example

```
ruckus(config-services)# ekahau 10.10.10.1 500
The command was executed successfully.
ruckus(config-services)# show
Services:
  Automatically adjust ap radio power= Disabled
  Automatically adjust ap channel= Enabled
  Channelfly works on 2.4GHz radio:
    Status= Disabled
  Channelfly works on 5GHz radio:
    Status= Disabled
  Run a background scan on 2.4GHz radio:
    Status= Enabled
    Time= 2000 seconds
  Run a background scan on 5GHz radio:
    Status= Enabled
    Time= 2000 seconds
  AeroScout RFID tag detection= Disabled
  Tunnel encryption for tunneled traffic= Disabled
  Block multicast traffic from network to tunnel= Block non well-known
  Block broadcast traffic from network to tunnel except ARP and DHCP= Disabled
  Tunnel Proxy ARP of tunnel WLAN:
    status= Disabled
    ageing time= 0
  Packet Inspection Filter(PIF) uplink process= Disabled
  Packet Inspection Filter(PIF) rate limit:
    status= Disabled
  RAPS= Enabled
  EKHAU settings:
    status= Enabled
    ERC IP= 10.10.10.1
    ERC port= 500
ruckus(config-services)#
```

## no ekahau

To disable Ekahau Blink support, use the following command:

**no ekahau**

## Defaults

Disabled

## Example

```
ruckus(config-services)# no ekahau
The command was executed successfully.
ruckus(config-services)#
```

## pif

To enable Packet Inspection Filter and set rate limiting threshold, use the following command:

**pif [uplink-proc | rate-limit NUMBER ]**

## Syntax Description

**pif**

Enable Packet Inspection Filter



### **uplink-proc**

Enable uplink process of Packet Inspection Filter

### **rate-limit**

Enable and set Broadcast Neighbor Discovery Packets (ARP and ICMPv6 Neighbor Solicit) rate limit threshold.

### **NUMBER**

Rate limiting threshold for PIF feature.

## **Example**

```
ruckus(config-services)# pif uplink-proc
The command was executed successfully.
ruckus(config-services)# pif rate-limit 1000
The command was executed successfully.
ruckus(config-services)# show
Services:
  Automatically adjust ap radio power= Disabled
  Automatically adjust ap channel= Enabled
  Channelfly works on 2.4GHz radio:
    Status= Disabled
  Channelfly works on 5GHz radio:
    Status= Disabled
  Run a background scan on 2.4GHz radio:
    Status= Enabled
    Time= 20 seconds
  Run a background scan on 5GHz radio:
    Status= Enabled
    Time= 20 seconds
  AeroScout RFID tag detection= Disabled
  Tunnel encryption for tunneled traffic= Enabled
  Block multicast traffic from network to tunnel= Disabled
  Block broadcast traffic from network to tunnel except ARP and DHCP= Disabled
  Tunnel Proxy ARP of tunnel WLAN:
    status= Disabled
  Packet Inspection Filter(PIF) uplink process= Enabled
  Packet Inspection Filter(PIF) rate limit:
    status= Enabled
    rate limit= 1000
ruckus(config-services)#
```

## **no pif**

To disable uplink process of packet inspection filter or disables Broadcast Neighbor Discovery Packets (ARP and ICMPv6 Neighbor Solicit), use the following command:

**no pif [uplink-proc | rate-limit ]**

## **Example**

```
ruckus(config-services)# no pif uplink-proc
The command was executed successfully.
ruckus(config-services)# no pif rate-limit
The command was executed successfully.
ruckus(config-services)#
```

## **show**

To display the current service settings, use the following command:

**show**

## Syntax Description

### show

Display the current service settings

## Defaults

None.

## Example

```
ruckus(config-services)# show
Services:
  Automatically adjust ap radio power= Disabled
  Automatically adjust ap channel= Enabled
  Channelfly works on 2.4GHz radio:
    Status= Disabled
  Channelfly works on 5GHz radio:
    Status= Disabled
  Run a background scan on 2.4GHz radio:
    Status= Enabled
    Time= 2000 seconds
  Run a background scan on 5GHz radio:
    Status= Enabled
    Time= 2000 seconds
  AeroScout RFID tag detection= Disabled
  Tunnel encryption for tunneled traffic= Disabled
  Block multicast traffic from network to tunnel= Block non well-known
  Block broadcast traffic from network to tunnel except ARP and DHCP= Disabled
  Tunnel Proxy ARP of tunnel WLAN:
    status= Disabled
    ageing time= 0
  Packet Inspection Filter(PIF) uplink process= Disabled
  Packet Inspection Filter(PIF) rate limit:
    status= Disabled
ruckus(config-services)#
```

# Configure WIPS Commands

Use the wips commands to configure Wireless Intrusion Prevention settings. To run these commands, you must first enter the **config-wips** context.

## wips

Use the following command to enter the config-wips context and configure WIPS settings:

**wips**

### Syntax Description

**help**

Shows available commands

**history**

Shows a list of previously run commands

**end**

Saves changes, and the exits the config-wips context

**exit**

Saves changes, and the exits the config-wips context

**no** *WORD*

Disable WIPS services

**protect-excessive-wireless-request**

Enables protecting the wireless network against excessive wireless requests

**temp-block-auth-failed-client time** *NUMBER*

Temporarily block wireless clients with repeated authentication failures for the specified time (in seconds)

**rogue-report** [ **all** ] | [ **malicious** *ssid-spoofing* | **same-network** | **user-blocked** | **mac-spoofing** ]

Enables report rogue devices in ZD event log.

**all**

Report all rogue devices.

**malicious** [ *ssid-spoofing* | **same-network** | **user-blocked** | **mac-spoofing** ]

Report particular malicious type.

**malicious-report**

Enables protecting the network from malicious rogue access points

**rogue-dhcp-detection**

Enables rogue DHCP server detection

**show**

Displays the WIPS settings

### Example

```
ruckus(config)# wips
ruckus(config-wips)# show
Protect my wireless network against excessive wireless requests= Disabled
```

## Configuring Master Settings

### Configure WIPS Commands

```
Temporarily block wireless clients with repeated authentication failures:
  Status= Enabled
  Time= 30 seconds
Report rogue devices in ZD event log= Enabled
Protect the network from malicious rogue access points= Disabled
Rogue DHCP server detection= Enabled
ruckus(config-wips)# temp-block-auth-failed-client time 30
The command was executed successfully.
ruckus(config-wips)# rogue-report all
The command was executed successfully.
ruckus(config-wips)# rogue-report malicious same-network
The command was executed successfully.
ruckus(config-wips)# rogue-dhcp-detection
The command was executed successfully.
ruckus(config-wips)# no rogue-dhcp-detection
The command was executed successfully.
ruckus(config-wips)# no rogue-report
The command was executed successfully.
ruckus(config-wips)# show
  Protect my wireless network against excessive wireless requests= Disabled
  Temporarily block wireless clients with repeated authentication failures:
    Status= Enabled
    Time= 30 seconds
  Report rogue devices in ZD event log= Disabled
  Protect the network from malicious rogue access points= Disabled
  Rogue DHCP server detection= Disabled
ruckus(config-wips)#
```

# Configure Email Server Commands

Use the email-server commands to configure email server settings. To run these commands, you must first enter the **config-email-server** context.

## email-server

Use the following command to enter the **config-email-server** context and configure email server settings:

**email-server**

### Syntax Description

**help**

Shows available commands.

**history**

Shows a list of previously run commands.

**abort**

Exits the config-email-server context without saving changes.

**end**

Saves changes, and the exits the config-email-server context.

**exit**

Saves changes, and the exits the config-email-server context.

**quit**

Exits the config-email-server context without saving changes.

**enable**

Enables the E-Mail server.

**from** *WORD*

Sets the E-Mail from for email server.

**smtp-server-name** *WORD*

Sets the smtp server name for email server.

**smtp-server-port** *NUMBER*

Sets the smtp server port for email server.

**smtp-auth-name** *WORD*

Sets the smtp authentication user name for email server.

**smtp-auth-password** *WORD*

Sets the smtp authentication password for email server.

**smtp-wait-time**

Sets the smtp server wait time (in seconds).

**tls-smtp-encryption** *tls*

Enables TLS of smtp encryption for email server.

**tls-smtp-encryption starttls**

Enables starttls in the TLS of smtp encryption for email server.

**no enable**

Disables the email server setting.

**no tls-smtp-encryption tls**

Disables TLS of smtp encryption for email server.

**no tls-smtp-encryption starttls**

Disables starttls in the TLS of smtp encryption for email server.

**show**

Shows email server settings.

## Example

```
ruckus(config)# email-server
ruckus(config-email-server)# enable
ruckus(config-email-server)# from example@example.com
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-email-server)# smtp-server-name smtp.example.com
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-email-server)# smtp-server-port 587
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-email-server)# smtp-auth-name johndoe
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-email-server)# smtp-auth-password password
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-email-server)# tls-smtp-encryption tls
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-email-server)# tls-smtp-encryption starttls
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-email-server)# show
Email Server:
  Status= Enabled
  E-mail From = example@example.com
  SMTP Server Name= smtp.example.com
  SMTP Server Port= 587
  SMTP Authentication Username= johndoe
  SMTP Authentication Password= *****
  SMTP Encryption Options:
    TLS= Enabled
    STARTTLS= Enabled

ruckus(config-email-server)# end
The Email server settings have been updated.
Your changes have been saved.
ruckus(config)#
```

## from

To set the sender from address for email alarms, use the following command:

**from** *WORD*

## Syntax Description

**from**

Set the email address from which alarm notifications will be sent

*WORD*

Send alarm notifications from this email address

## Defaults

None.

## Example

```
ruckus(config-email-server)# from test1@gmail.com
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-email-server)#
```

## enable

To enable the email server, use the following command:

**enable**

## Example

```
ruckus(config-email-server)# enable
ruckus(config-email-server)#
```

## no enable

To disable the email server, use the following command:

**no enable**

## Example

```
ruckus(config-email-server)# no enable
ruckus(config-email-server)# show
Email Server:
  Status= Disabled

ruckus(config-email-server)#
```

## smtp-server-name

To set the SMTP server that ZoneDirector uses to send alarm notifications, use the following command:

**smtp-server-name** *WORD*

## Syntax Description

### **smtp-server-name**

Set the SMTP server that ZoneDirector uses to send alarm notifications

*WORD*

Set to this SMTP server name

## Defaults

None.

### Example

```
ruckus(config-email-server)# smtp-server-name smtp.163.com  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## smtp-server-port

To set the SMTP server port that ZoneDirector uses to send alarm notifications, use the following command:

```
smtp-server-port NUMBER
```

### Syntax Description

#### **smtp-server-port**

Set the SMTP server port that ZoneDirector uses to send alarm notifications

*NUMBER*

Set to this SMTP server port

### Defaults

587

### Example

```
ruckus(config-email-server)# smtp-server-port 25  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## smtp-auth-name

To set the user name that ZoneDirector uses to authenticate with the SMTP server, use the following command:

```
smtp_auth_name WORD
```

### Syntax Description

#### **smtp\_auth\_name**

Set the user name that ZoneDirector uses to authenticate with the SMTP server

*WORD*

Set to this user name

### Defaults

None.

### Example

```
ruckus(config-email-server)# smtp-auth-name joe  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```



## smtp-auth-password

To set the password that ZoneDirector uses to authenticate with the SMTP server, use the following command:

**smtp-auth-password** *WORD*

### Syntax Description

**smtp-auth-password**

Set the password that ZoneDirector uses to authenticate with the SMTP server

*WORD*

Set to this password

### Defaults

None.

### Example

```
ruckus(config-email-server)# smtp-auth-password 123456  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## smtp-wait-time

To set the SMTP server wait time (in seconds), use following command:

**smtp-wait-time** *NUMBER*

### Example

```
ruckus(config-email-server)# smtp-wait-time 10  
The command was executed successfully. To save the changes, type 'end' or 'exit'.  
ruckus(config-alarm)#
```

## tls-smtp-encryption

To enable TLS for SMTP encryption of email notifications, use the following command:

**tls-smtp-encryption** [ **tls** | **starttls** ]

### Syntax Description

**tls-smtp-encryption**

Enable SMTP encryption of email notifications

**tls**

Enable TLS encryption for email notifications

**starttls**

Enable STARTTLS encryption for email notifications

## Defaults

None.

## Example

```
ruckus(config-email-server)# tls-smtp-encryption tls  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

## no tls-smtp-encryption

To disable TLS for SMTP encryption of alarm notifications, use the following command:

**no tls-smtp-encryption [ tls | starttls ]**

## Syntax Description

### no tls-smtp-encryption

Disable SMTP encryption of alarm notifications

### tls

Disable TLS encryption

### starttls

Disable STARTTLS encryption

## Defaults

None.

## Example

```
ruckus(config-email-server)# no tls-smtp-encryption tls  
The command was executed successfully. To save the changes, type 'end' or 'exit'.
```

# Configure SMS Server Commands

Use the `sms-server` commands to configure SMS server settings. To run these commands, you must first enter the **config-sms-server** context.

## sms-server

Use the following command to enter the **config-sms-server** context and configure SMS server settings:

**sms-server**

### Syntax Description

**help**

Shows available commands.

**history**

Shows a list of previously run commands.

**abort**

Exits the `config-sms-server` context without saving changes.

**end**

Saves changes, and the exits the `config-sms-server` context.

**exit**

Saves changes, and the exits the `config-sms-server` context.

**quit**

Exits the `config-sms-server` context without saving changes.

**twilio**

Configures SMS server settings for twilio. Enters `ruckus(config-sms-server-twilio)#`

**clickatell**

Configures SMS server settings for clickatell. Enters `ruckus(config-sms-server-clickatell)#`

**account-sid** *WORD*

Sets the account sid for twilio of sms server

**auth-token** *WORD*

Sets the auth token for twilio of sms server

**from-phonenummer** *WORD*

Sets the from phonenummer for twilio of sms server

**user-name** *WORD*

Sets the user name for clickatell of sms server

**password** *WORD*

Sets the password for clickatell of sms server

**api-id** *WORD*

Sets the api id for clickatell of sms server

**show**

Displays the SMS server settings.

## Configuring Master Settings

sns

customized

Configures SMS server settings for customized server. Enters `ruckus(config-sms-server-customized)#`

url <WORD> <WORD>

Sets the URL for customized sms server

post <WORD>

Sets the post for customized sms server

### Example

```
ruckus(config)# sms-server
ruckus(config-sms-server)# twilio
ruckus(config-sms-server-twilio)# account-sid example1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-sms-server-twilio)# auth-token token1
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-sms-server-twilio)# from-phonenum 111222333444555
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-sms-server-twilio)# end
The SMS server settings have been updated.
Your changes have been saved.
ruckus(config-sms-server)# show
SMS Server:
  Server Type= twilio
  Account SID= example1
  Auth Token= token1
  From PhoneNumber= 111222333444555

ruckus(config-sms-server)# end
The SMS server settings have been updated.
Your changes have been saved.
ruckus(config)#
```

### no sms-server

To disable SMS server settings, use the following command:

**no sms-server**

### Example

```
ruckus(config)# no sms-server
The SMS server settings have been updated.
ruckus(config)#
```

## sns

To configure Short Notification Service settings and enter the *config-sns* context, use the following command:

**sns**

### Syntax Description

abort	Exits the config-sns context without saving changes.
end	Saves changes, and then exits the config-sns context.

exit	Saves changes, and then exits the config-sns context.
quit	Exits the config-sns context without saving changes.
enable	Enables Short Notification Service.
no enable	Disables Short Notification Service.
show	Shows Short Notification Service settings.

## Defaults

Enabled.

## Example

```
ruckus(config)# sns
ruckus(config-sns)# enable
ruckus(config-sns)# show
Short Notification Service:
  Status= Enabled

ruckus(config-sns)# end
The Short Notification Service settings have been updated.
Your changes have been saved.
ruckus(config)#
```

## Configure Station Rename Commands

Use the following commands to configure the renamed station list.

## sta-rename

To create or modify the renamed station list, use the following commands:

### Syntax Description

help	Shows available commands
history	Shows a list of previously run commands
no sta	Delete a renamed station
end	Save the current rule and quit
exit	Save the current rule and quit
abort	Discard the current rule and quit
quit	Discard the current rule and quit

### Example

```
ruckus(config)# sta-rename
ruckus(config- sta-rename)# sta 6C:AA:B3:00:00:A0 my-iphone
ruckus(config- sta-rename)# end
Your changes have been saved. ruckus(config)# show sta-name Displays sta rename list:
MAC Address= 6C:AA:B3:00:00:A0
rename= my-iphone
```

```
All sta rename number: 1.
ruckus(config)#
```

## Configure Favorite Station Commands

Use the following commands to configure the favorite station list.

## sta-favorite

To create or modify the favorite station list, use the following commands:

### Syntax Description

help	Shows available commands
history	Shows a list of previously run commands
no sta	Delete a favorite station
sta <MAC>	Enable station favorite
end	Save the current rule and quit
exit	Save the current rule and quit
abort	Discard the current rule and quit
quit	Discard the current rule and quit

### Example

```
ruckus(config)# sta-favorite
ruckus(config-sta-favorite)# sta aa:aa:aa:aa:aa:aa
ruckus(config-sta-favorite)# end
Your changes have been saved. ruckus(config)# show sta-favorite Displays sta favorite list:
MAC Address= aa:aa:aa:aa:aa:aa
```

```
All sta favorite number: 1.
ruckus(config)#
```

## Configure mDNS (Bonjour) Commands

Use the following commands to configure mDNS (Bonjour Gateway) service.

### mdnsproxy

Use the following command to enable mDNS proxy (Bonjour Gateway) service:

```
mdnsproxy [ zd | ap ]
```

### no mdnsproxy

Use the following command to disable mDNS proxy (Bonjour Gateway) service:

```
no mdnsproxy [ zd | ap ]
```

### mdnsproxyrule

Use the following command to create a new Bonjour Gateway rule or modify an existing rule, and enter the config-mdnsproxyrule context:

```
mdnsproxyrule ID
```

### no mdnsproxyrule

Use the following command to delete a Bonjour Gateway rule:

```
no mdnsproxyrule ID
```



## Configuring a Bonjour Policy

The following commands can be used from within the **config-bonjourpolicy** context to configure the Bonjour policy.

### *bonjour-policy*

To create or edit a Bonjour policy, use the following command:

**bonjour-policy** *WORD*

### Syntax Description

**help**

Shows available commands

**history**

Shows a list of previously run commands

**no mdnsproxyrule**

Delete mDNSproxy rule

**mdnsproxyrule** *ID*

Add/update mDNSproxy rules

**note** *NOTE*

Rule comments

**end**

Save the current rule and quit

**exit**

Save the current rule and quit

**abort**

Discard the current rule and quit

**quit**

Discard the current rule and quit

### Example

```
ruckus(config)# bonjour-policy bonjour1
ruckus(config-bonjourpolicy)# note bonjourpolicy1
ruckus(config-bonjourpolicy)# end
Your changes have been saved.
ruckus(config)# show bonjour-policy
bonjour-policy:
  ID: 1
  Name: bonjour1
  Description: bonjourpolicy1
  rule:
ruckus(config)#
```

### *no bonjour-policy*

To delete a Bonjour policy, use the following command:

**no bonjour-policy** *WORD*

## Configuring mDNS Proxy Rules

The following commands can be used from within the **config-mdnsproxyrule** context to configure the Bonjour Gateway bridge service rule.

### Syntax Description

**help**

Shows available commands

**history**

Shows a list of previously run commands

**service** *Service-Name*

Service name in ? list, or new bonjour rule

**from-vlan** *VLAN-From*

VLAN from

**to-vlan** *VLAN-to*

VLAN to

**note** *NOTE*

Rule comments

**show**

Show the current edited rule

**end**

Save the current rule and quit

**abort**

Discard the current rule and quit

**quit**

Discard the current rule and quit

### Example

```
ruckus(config-bonjourpolicy)# mdnsproxyrule 1
ruckus(config-policyrule)# service AirDisk
ruckus(config-policyrule)# from-vlan 220
ruckus(config-policyrule)# to-vlan 1
ruckus(config-policyrule)# note "share printer to vlan1"
ruckus(config-policyrule)# end
ruckus(config-bonjourpolicy)# end
ruckus(config)# show bonjour-policy
bonjour-policy:
  ID: 1
  Name: bonjour1
  Description: bonjourpolicy1
  rule:
  1:
    mdnsservice: AirDisk
    from_vlan: br0.220
    to_vlan: br0
  Notes: share printer to vlan1
ruckus(config)#
```

## Configuring a Bonjour Fencing Policy

To create a Bonjour Fencing policy and enter the **config-bonjourfencing** context, use the following command:

**bonjour-fencing** <NAME>

### Syntax Description

#### **bonjour-fencing**

Configure a Bonjour Fencing policy.

NAME

Set the name of the fencing policy.

no <ID>	Delete fencing rules
show	Show the current edited bonjour fence
description	Sets the bonjour fence description.
fencerule <ID>	Add/Update fence rules
end	Save current rule and quit
exit	Save current rule and quit
abort	Discard current rule and quit
quit	Discard current rule and quit

### Defaults

None.

### Example

```
ruckus(config)# bonjour-fencing fencel
ruckus(config-bonjourfencing)#
  help           Shows available commands.
  history        Shows a list of previously run commands.
  no <ID>        Delete fencing rules
  show           Show the current edited bonjour fence
  description <WORD> Sets the bonjour fence description.
  fencerule <ID> Add/Update fence rules
  end            Save current rule and quit
  exit           Save current rule and quit
  abort          Discard current rule and quit
  quit          Discard current rule and quit
ruckus(config-bonjourfencing)#
```

### fencerule

To add or update fence rules, and enter the *config-fencerule* context, use the following command:

**fencerule** <ID >

### Syntax Description

show	Show the current edited rule
source-type <TYPE>	Wired or wireless.
device-mac <MAC>	Device MAC.

## Configuring Master Settings

### Configure mDNS (Bonjour) Commands

anchor-ap <MAC>	Anchor AP MAC.
service <Service-Name>	List service names.
fencing-range <RANGE>	Fencing Range: Same AP or 1-Hop AP Neighbors.
description <WORD>	Fencing rule description.
end	Save current rule and quit
quit	Save current rule and quit

### Example

```
ruckus(config-bonjourfencing)# fencerule 1
ruckus(config-fencerule)#
  help                Shows available commands.
  history             Shows a list of previously run commands.
  show               Show the current edited rule
  source-type <TYPE> Wireless or Wired.
  device-mac <MAC>   Device MAC.
  anchor-ap <MAC>    Anchor AP MAC.
  service <Service-Name>
                    List service names.
  fencing-range <RANGE>
                    Fenceing Range: Same AP or 1-Hop AP Neighbors.
  description <WORD> Fencing rule description.
  end                Save current rule and quit
  exit               Save current rule and quit
ruckus(config-fencerule)#
```

# upload-debug

To configure upload debug file settings, use the following command:

**upload-debug***NUMBER*

## Syntax Description

abort	Exits the config-upload-debug context without saving changes.
end	Saves changes, and then exits the config-upload-debug context.
exit	Saves changes, and then exits the config-upload-debug context.
quit	Exits the config-upload-debug context without saving changes.
show	Shows upload debug file settings.
enable	Enables the upload debug file.
proto <tftp or ftp>	Sets the protocol for upload debug file.
host <WORD>	Sets the host for upload debug file.
port <NUMBER>	Sets the port for upload debug file.
ftp-user <WORD>	Sets the FTP username for upload debug file.
ftp-pass <WORD>	Sets the FTP password for upload debug file.

## Defaults

Disabled.

## Example

```
ruckus(config-upload-debug)#
  help                Shows available commands.
  history             Shows a list of previously run commands.
  abort              Exits the config-upload-debug context without saving changes.
  end                Saves changes, and then exits the config-upload-debug context.
  exit               Saves changes, and then exits the config-upload-debug context.
  quit              Exits the config-upload-debug context without saving changes.
  show               Shows upload debug file settings.
  enable             Enables the upload debug file.
  proto <tftp or ftp> Sets the protocol for upload debug file.
  host <WORD>        Sets the host for upload debug file.
  port <NUMBER>     Sets the port for upload debug file.
  ftp-user <WORD>   Sets the FTP username for upload debug file.
  ftp-pass <WORD>   Sets the FTP password for upload debug file.
ruckus(config-upload-debug)# enable
ruckus(config-upload-debug)# proto tftp
ruckus(config-upload-debug)# host 192.168.40.11
ruckus(config-upload-debug)# port 443
ruckus(config-upload-debug)# ftp-user user1
ruckus(config-upload-debug)# ftp-pass password1234
ruckus(config-upload-debug)# show
Upload Debug:
  Status= Enabled
  Protocol= TFTP
  Host = 192.168.40.11

ruckus(config-upload-debug)# end
The upload debug file settings have been updated.
Your changes have been saved.
ruckus(config)#
```

# no upload-debug

## Syntax

**no upload-debug**

## Command Default

Disabled.

## Examples

```
ruckus(config)# no upload-debug  
The upload debug file settings have been updated.  
ruckus(config)#
```

# Using Debug Commands

---

- Debug Commands Overview..... 447
- General Debug Commands.....447
- Show Commands..... 454
- Accessing a Remote AP CLI..... 460
- Working with Debug Logs and Log Settings.....462
- Remote Troubleshooting.....469
- AP Core Dump Collection..... 471
- Script Execution.....473

## Debug Commands Overview

This section describes the commands that you can use to debug Unleashed and connected APs, and to configure debug log settings.

From the privileged commands context, type **debug** to enter the debug context. To show a list of commands available from within the debug context, type **help** or **?**.

## General Debug Commands

The following section describes general debug commands can be executed from within the debug context.

### help

Shows available commands.

### list-all

List all available commands.

### history

Shows a list of previously run commands.

### quit

Exits the debug context.

### apfw\_upgrade

To upgrade the controller's firmware, use the following command:

```
apfw_upgrade <protocol>://server ip|server name/path/image name [ -f ]
```

## apfw\_upgrade OPTIONS

### Syntax Description

#### apfw\_upgrade

Upgrade the AP's firmware

#### protocol

Protocol for image transfer (FTP, TFTP, HTTP, KERMIT)

#### OPTIONS

- p** protocol
- s** server IP address or name
- n** image name with path on the server
- f** non-verbose mode
- h** fw\_upgrade help message

### Defaults

None.

### Example

```
ruckus(debug) # apfw_upgrade
-----
Name: apfw_upgrade - AP Firmware Upgrade Tool (Ver.1.2)
Synopsis : apfw_upgrade tftp://<server ip|server name>/<path/image name>
-----
apfw_upgrade
ruckus(debug) #
```

## delete-station

To deauthorize the station with the specified MAC address, use the following command.

**delete-station** MAC

### Syntax Description

#### delete-station

Delete the station with the specified MAC address

#### MAC

The MAC address of the station that will be deleted



## Defaults

None.

## Example

```
ruckus# debug
ruckus(debug)# delete-station 00:10:77:01:00:01
The command was executed successfully.
```

## restart-ap

To restart the device with the specified MAC address, use the restart ap command.

**restart-ap** *MAC*

## Syntax Description

### **restart-ap**

Restart the device with the specified MAC address

### *MAC*

The MAC address of the device to be restarted

## Defaults

None.

## Example

```
ruckus# debug
ruckus(debug)# restart-ap 00:13:92:EA:43:01
The command was executed successfully.
```

## restore

To restore the controller's configuration, use the following command:

**restore** [ **all** | **failover** | **policy** ]

## wlaninfo

Configures and enables debugging of WLAN service settings. Enter wlaninfo without arguments to see all options.

**wlaninfo** *OPTIONS*

## Syntax Description

### **wlaninfo**

Enable logging of WLAN info

### *OPTIONS*

Configure WLAN debug information options

## Defaults

None.

## Example

```
ruckus(debug)# wlaninfo -W -x
WLAN svc "Rhastah1" (id=1):
  WLAN ID = 0, ref_cnt = 7
  SSID = "Rhastah1" enabled
  Apply to 11a and 11g/b radios
  Closed system = No, Privacy = Enabled, ACL enabled Guest-WLAN = No
  WISPr-WLAN = No
  Access Policy = 0/0, Web Auth = No, grace period = 0 (0 means disable), max clients = 100
  WMM = enabled priority = 0 uplink = DISABLE downlink = DISABLE
  Cipher = Clear Text Local bridging = Enabled, DHCP relay = Disabled, vlan = 1, dvlan = Disabled,
  bgscan = Enabled
  Proxy ARP = Disabled (IE:Disabled)
  wep key index = 0, wep key len = 0
  PAP message authenticator = Enabled, EAP-Failure = Disabled
  Device Policy = 0, Precedence = 1
  Smart Roam = Disabled Roam-factor = 1
  Hotspot2.0--WLAN = No (id=0)
  Num of VAP deployed: 6
    VAP: 04:4f:aa:0c:b1:0c, number of stations = 0
    VAP: 04:4f:aa:0c:b1:08, number of stations = 0
    VAP: c0:c5:20:3b:91:fc, number of stations = 1
    VAP: c0:c5:20:3b:91:f8, number of stations = 0
    VAP: c4:10:8a:1f:d1:fc, number of stations = 1
    VAP: c4:10:8a:1f:d1:f8, number of stations = 0
  ACL 1 (System): default=Allowed system-wide=yes
  Auth Policy:
    Auth Algorithms:RSN/PSK RSN/Dynamic PSK
    Auth Server Type: None
    WPA Verson: WPA2
    WPA Auth and Key Managment: WPA PSK
    WPA PSK Pass Phrase:password
    WPA PSK Prev Pass Phrase:
    WPA PSK Pass Phrase (Hex):
      31306173 68613130
    WPA PSK:
      6aa94bac df5346ac ecc7d38f a14a6dbf
      7ba6f6f8 df2a4943 b23c9655 ac4f33de
    WPA Prev PSK:
      00000000 00000000 00000000 00000000
      00000000 00000000 00000000 00000000
    GTK life time = 28800 seconds, GTK Life size = 2000 Kpkts
    GMK life time = 86400 seconds, Strict Rekey = No
    WPA Group Cipher Suites:0x00000010
      CCMP
    WPA Pairwise Cipher Suites:0x00000010
      CCMP
  NASID Type: = wlan-bssid
  PMK Cache Time: = 43200
  PMK Cache for Reconnect: = enabled
  Roaming Acct-Inerim-Update: = disabled
  Called-Station-Id-type: 0
  Classification: enabled
  UDP Heuristic Classification: enabled
  Directed Multicast: enabled
  IGMP Snooping: enabled
  MLD Snooping: disabled
  ToS Classification: enabled
  Dot1p Classification: disabled
  Multicast Filter: disabled
  Directed Threshold: 5
  Priority: Voice:0 Video:2 Data:4 Background:6
  Force DHCP: disabled Timeout:10
```

```
*** Total WLAN Entries: 1 ***  
ruckus(debug)#
```

## save\_debug\_info

Saves debug information.

**save\_debug\_info** *IP-ADDR FILE-NAME*

### Syntax Description

#### **save\_debug\_info**

Save debug log file

*IP-ADDR*

The destination IP address

*FILE-NAME*

The destination file name

### Defaults

None.

### Example

```
ruckus(debug)# save_debug_info 192.168.11.26 log.log  
Creating debug info file ...  
Done  
Sending debug info file to "log.log@192.168.11.26" ...  
...  
ruckus(debug)#
```

## remote\_ap\_cli

Use the **remote\_ap\_cli** command to access an AP remotely and execute AP CLI commands.

**remote\_ap\_cli** [ **-q** ] { **-a** *ap\_mac* | **-A** } "*cmd arg1 arg2 ..*"

### Syntax Description

#### **remote\_ap\_cli**

Execute CLI commands in a remote AP

**-q**

Do not display results

**-a**

Specify AP by MAC address

**ap\_mac**

The AP's MAC address

**-A**

All connected APs

## Using Debug Commands

### General Debug Commands

*cmd*

AP CLI command

*arg*

AP CLI command argument

### Example

```
ruckus(debug)# remote_ap_cli -A "get director"
---- Command 'rkscli -c "get director "' executed at c0:c5:20:3b:91:f0
----- ZoneDirector Info -----
Primary Controller   : n/a
Secondary Controller : n/a
DHCP Opt43 Code     : 3

The information of the most recent Zone Director:
[1] 192.168.40.100

AP is under management of ZoneDirector: 192.168.40.100 / c0:c5:20:18:97:c1,
Currently AP is in state: RUN
OK
---- Command 'rkscli -c "get director "' executed at c4:10:8a:1f:d1:f0
----- ZoneDirector Info -----
Primary Controller   : n/a
Secondary Controller : n/a
DHCP Opt43 Code     : 3

The information of the most recent Zone Director:
[1] 192.168.40.100

AP is under management of ZoneDirector: 192.168.40.100 / c0:c5:20:18:97:c1,
Currently AP is in state: RUN
OK
---- Command Execution Summary:
      success: 2
      failure: 0
      total: 2
ruckus(debug)#
```

## save-config

Upload the configuration file to the designated TFTP site.

**save-config** *IP-ADDR FILE-NAME*

### Syntax Description

#### **save-config**

Upload the configuration file

*IP-ADDR*

The destination IP address

*FILE-NAME*

The destination file name

### Defaults

None.

## Example

```
ruckus(debug)# save-config 192.168.11.26 config.log
Creating backup config file
Done
Uploading backup config file
...
ruckus(debug)#
```

## emfd-malloc-stats

Show uclibc malloc statistics.

## Example

```
ruckus(debug)# emfd-malloc-stats
===== [pid=350] Sat Feb 15 15:58:42 2014
total bytes allocated          = 2691072
total bytes in use             = 2471920
total bytes freed              = 219152
total allocated mmap space    = 311296
number of free chunks         = 18
number of fastbin blocks      = 0
space in freed fastbin blocks = 0
bin[ 1]: chunk_num= 1, list_len= 1, alloc_bytes= 4152, min_chunk[1]= 4152,
max_chunk[1]= 4152
bin[ 3]: chunk_num= 3, list_len= 3, alloc_bytes= 72, min_chunk[1]= 24,
max_chunk[1]= 24
bin[ 4]: chunk_num= 1, list_len= 1, alloc_bytes= 32, min_chunk[1]= 32,
max_chunk[1]= 32
bin[ 5]: chunk_num= 4, list_len= 4, alloc_bytes= 160, min_chunk[1]= 40,
max_chunk[1]= 40
bin[ 6]: chunk_num= 1, list_len= 1, alloc_bytes= 48, min_chunk[1]= 48,
max_chunk[1]= 48
bin[10]: chunk_num= 1, list_len= 1, alloc_bytes= 80, min_chunk[1]= 80,
max_chunk[1]= 80
bin[14]: chunk_num= 1, list_len= 1, alloc_bytes= 112, min_chunk[1]= 112,
max_chunk[1]= 112
bin[45]: chunk_num= 1, list_len= 1, alloc_bytes= 2928, min_chunk[1]= 2928,
max_chunk[1]= 2928
bin[49]: chunk_num= 1, list_len= 1, alloc_bytes= 5168, min_chunk[1]= 5168,
max_chunk[1]= 5168
bin[51]: chunk_num= 2, list_len= 2, alloc_bytes= 14952, min_chunk[1]= 7248,
max_chunk[2]= 7704
bin[52]: chunk_num= 1, list_len= 1, alloc_bytes= 8208, min_chunk[1]= 8208,
max_chunk[1]= 8208
ruckus(debug)#
```

## Show Commands

This section describes the show commands available within the debug context.

### show ap

To display AP information for all APs, use the following command:

```
show ap
```

#### Syntax Description

```
show ap
```

Display a list of all approved APs.

#### Example

```
ruckus(debug)# show ap
AP:
  ID:
    1:
      MAC Address= 44:1e:94:1b:f0:d0
      Model= r510
      Approved= Yes
      Device Name= RuckusAP
      Description=
      Location=
      GPS=
      CERT = Normal
      Bonjour-policy=
      Bonjour-fencing=
      Group Name= System Default
      Channel Range:
        A/N= 36,40,44,48,149,153,157,161 (Disallowed= )
        B/G/N= 1,2,3,4,5,6,7,8,9,10,11 (Disallowed= )
      Radio a/n:
        Channelization= Auto
        Channel= Auto
        WLAN Services enabled= Yes
        Tx. Power= Auto
        WLAN Group Name= Default
        Call Admission Control= OFF
        Protection Mode= Auto
      Radio b/g/n:
        Channelization= Auto
        Channel= Auto
        WLAN Services enabled= Yes
        Tx. Power= Auto
        WLAN Group Name= Default
        Call Admission Control= OFF
        Protection Mode= 2
      Override global ap-model port configuration= No
      Network Setting:
        Protocol mode= Use Parent Setting
        Device IP Settings= Keep AP's Setting
        IP Type= DHCP
        IP Address= 192.168.0.10
        Netmask= 255.255.255.0
        Gateway= 192.168.0.1
        Primary DNS Server=
        Secondary DNS Server=

      Device IPv6 Settings= Keep AP's Setting
```

```
IPv6 Type= Auto Configuration
IPv6 Address= ::461e:98ff:fe1b:f0d0
IPv6 Prefix Length= 64
IPv6 Gateway=
IPv6 Primary DNS Server=
IPv6 Secondary DNS Server=
Mesh:
  Mode= Use Parent Setting
  max hops= Use Parent Setting
LLDP:
  Status = Use Parent Setting
LAN Port:
  0:
    Interface= eth0
    Dot1x= None
    LogicalLink= Up
    PhysicalLink= Up 10Mbps full
    Label= 10/100/1000 PoE LAN1
  1:
    Interface= eth1
    Dot1x= None
    LogicalLink= Down
    PhysicalLink= Down
    Label= 10/100/1000 LAN2
2:
  MAC Address= d4:c2:9e:35:c9:50
  Model= r610
  Approved= Yes
  Device Name= RuckusAP
  Description=
  Location=
  GPS=
  CERT = Normal
  Bonjour-policy=
  Bonjour-fencing=
  Group Name= System Default
  Channel Range:
    A/N= 36,40,44,48,149,153,157,161 (Disallowed= )
    B/G/N= 1,2,3,4,5,6,7,8,9,10,11 (Disallowed= )
  Radio a/n:
    Channelization= Auto
    Channel= Auto
    WLAN Services enabled= Yes
    Tx. Power= Auto
    WLAN Group Name= Default
    Call Admission Control= OFF
    Protection Mode= Auto
  Radio b/g/n:
    Channelization= Auto
    Channel= Auto
    WLAN Services enabled= Yes
    Tx. Power= Auto
    WLAN Group Name= Default
    Call Admission Control= OFF
    Protection Mode= 2
  Override global ap-model port configuration= No
  Network Setting:
    Protocol mode= Use Parent Setting
    Device IP Settings= Keep AP's Setting
    IP Type= DHCP
    IP Address= 192.168.0.3
    Netmask= 255.255.255.0
    Gateway= 192.168.0.1
    Primary DNS Server=
    Secondary DNS Server=

    Device IPv6 Settings= Keep AP's Setting
    IPv6 Type= Auto Configuration
    IPv6 Address= ::d6c1:9eff:fe35:c950
    IPv6 Prefix Length= 64
    IPv6 Gateway=
```

## Using Debug Commands

### Show Commands

```
IPv6 Primary DNS Server=  
IPv6 Secondary DNS Server=  
Mesh:  
Mode= Use Parent Setting  
max hops= Use Parent Setting  
LLDP:  
Status = Use Parent Setting  
LAN Port:  
0:  
  Interface= eth0  
  Dot1x= None  
  LogicalLink= Up  
  PhysicalLink= Up 1000Mbps full  
  Label= 10/100/1000 PoE LAN1  
1:  
  Interface= eth1  
  Dot1x= None  
  LogicalLink= Down  
  PhysicalLink= Down  
  Label= 10/100/1000 LAN2  
PoE Mode= Auto  
802.3af PoE Tx. chain= 2
```

```
ruckus(debug) #
```

## show station

Displays a list of all connected stations (or clients).

### show station

### Syntax Description

#### show station

Show all connected stations

### Defaults

None.

### Example

```
ruckus(debug) # show station  
Clients List:  
Client:  
MAC Address= 6c:62:6d:1b:e3:00  
User Name=  
IP Address= 192.168.11.11  
IPv6 Address=  
Access Point= 04:4f:aa:0c:b1:00  
WLAN= Ruckus1  
Channel= 1  
Signal (dB)= 53  
  
Client:  
MAC Address= 00:22:fb:ad:1b:2e  
User Name=  
IP Address= 192.168.11.7  
IPv6 Address=  
Access Point= 04:4f:aa:0c:b1:00  
WLAN= Ruckus1  
Channel= 165
```



```
Signal (dB)= 42  
ruckus(debug) #
```

## show logs

Displays a list of debug log components.

**show logs**

### Syntax Description

**show logs**

Display debug log components

### Defaults

None.

### Example

```
ruckus(debug) # show logs  
Debug Logs:  
All= Enabled  
Sys-mgmt= Enabled  
Mesh= Enabled  
Web-auth= Enabled  
Rf-mgmt= Enabled  
Radius= Enabled  
Hotspot-srv= Enabled  
Aps= Enabled  
Net-mgmt= Enabled  
802.1x= Enabled  
Web-svr= Enabled  
802.11= Enabled  
Dvlan= Enabled  
Smart-redundancy= Enabled  
Debug logs of specified MAC address:  
Status= Disabled  
ruckus(debug) #
```

## show remote-troubleshooting

Shows remote-troubleshooting status.

**show remote-troubleshooting**

### Syntax Description

**show remote-troubleshooting**

Display remote troubleshooting status

### Defaults

None.

## Example

```
ruckus(debug)# show remote-troubleshooting
Ruckus CA troubleshooting is stopped!
The server addr is: None

ruckus(debug)#
```

## ps

Displays information about all processes that are running (ps -aux).

**ps**

## Syntax Description

**ps**

Display a list of all running processes

## Defaults

None.

## Example

```
ruckus(debug)# ps
PID  PPID  USER      VSZ  STAT  COMMAND
  1     0  ruckus    1200  S     init
  2     1  ruckus     0  SWN   [ksoftirqd/0]
  3     1  ruckus     0  SW    [watchdog/0]
  4     1  ruckus     0  SW<   [events/0]
  5     1  ruckus     0  SW<   [khelper]
  6     1  ruckus     0  SW<   [kthread]
  7     6  ruckus     0  SW<   [kblockd/0]
  8     6  ruckus     0  SW<   [khubd]
  9     6  ruckus     0  SW    [pdflush]
 10    6  ruckus     0  SW    [pdflush]
 12    6  ruckus     0  SW<   [aio/0]
 11    1  ruckus     0  SW    [kswapd0]
 13    1  ruckus     0  SW    [mtdblockd]
 14    6  ruckus     0  SW<   [scsi_eh_0]
 15    6  ruckus     0  SW<   [usb-storage]
 17    6  ruckus     0  SW<   [V54_bodygard/0]
 18    1  ruckus     0  SW    [pktgen/0]
 29    6  ruckus     0  SW<   [reiserfs/0]
104    1  ruckus    956  S     /usr/sbin/in.tftpd -l -s /etc/airespider-images
110    1  ruckus    660  S     /bin/wd_feeder
242    1  ruckus   2572  S     /bin/emf_repo_flashsync monitor 15
243    1  ruckus    944  S     ttylogd
246    1  ruckus     0  SW<   [uif-246]
260    1  ruckus  14492  S     stamgr -d3 -t0
266   260  ruckus  14492  S     stamgr -d3 -t0
267   266  ruckus  14492  S <    stamgr -d3 -t0
268   266  ruckus  14492  S     stamgr -d3 -t0
269    1  ruckus   2268  S     apmgr
277   269  ruckus   2268  S     apmgr
278   277  ruckus   2268  S <    apmgr
299    1  ruckus  19564  S     emfd
316   299  ruckus  19564  S     emfd
317   316  ruckus  19564  S     emfd
318   316  ruckus  19564  S     emfd
```

```

322      1 ruckus      1108 S    /usr/sbin/dropbear -e /bin/login.sh -r /etc/air
328      1 ruckus      1188 S    /bin/sh /bin/login.sh
329      1 ruckus      1188 S    /bin/sh /bin/tacmon.sh
331      1 ruckus        676 S    /bin/rhttpd
332      1 ruckus      1140 S <  /bin/zapd
333      1 ruckus      1100 S <  /bin/clusterD
334     328 ruckus        856 S    /bin/login
335     329 ruckus        680 S    /bin/tacmon -i 30 -r 15
347      1 ruckus        808 S    /bin/tsyslogd -r -h -n --rotate=7
368     277 ruckus      2268 S <  apmgr
369     277 ruckus      2268 S <  apmgr
572      1 ruckus      1184 S    /sbin/udhcpd -i br0 --pidfile=/var/run/udhcpd.p
580     316 ruckus     19564 S    emfd
612     316 ruckus     19564 S    emfd
616     316 ruckus     19564 S    emfd
622     316 ruckus     19564 S    emfd
624     299 ruckus      6132 S <  webs &
625     316 ruckus     19564 S    emfd
637     624 ruckus      6132 S    webs &
638     637 ruckus      6132 S <  webs &
639     637 ruckus      6132 S <  webs &
640     637 ruckus      6132 S <  webs &
641     637 ruckus      6132 S <  webs &
642     637 ruckus      6132 S    webs &
655     637 ruckus      6132 S <  webs &
656     637 ruckus      6132 S <  webs &
20503   316 ruckus     19564 S    emfd
30679    1 ruckus      2672 S    /usr/sbin/vsftpd /etc/vsftpd2.conf
10220   322 ruckus      1184 S    /usr/sbin/dropbear -e /bin/login.sh -r /etc/air
10221  10220 ruckus      1188 S    /bin/sh /bin/login.sh
10222  10221 ruckus        856 S    /bin/login
10223  10222 ruckus      7972 S    ruckus_cli2
10426  10223 ruckus      1188 S    sh -c /bin/ps -aux
10427  10426 ruckus      1188 R    /bin/ps -aux
ruckus (debug) #

```

## Accessing a Remote AP CLI

The following command is used to access the command line interface of a connected AP and execute AP CLI commands from the controller CLI. Configuration changes made through the AP CLI may be overwritten by controller settings if the AP is restarted or reconnects to the controller.

### remote\_ap\_cli

Use the **remote\_ap\_cli** command to access an AP remotely and execute AP CLI commands.

```
remote_ap_cli [ -q ] { -a ap_mac | -A } "cmd arg1 arg2 .."
```

### Syntax Description

#### **remote\_ap\_cli**

Execute CLI commands in a remote AP

#### **-q**

Do not display results

#### **-a**

Specify AP by MAC address

#### **ap\_mac**

The AP's MAC address

#### **-A**

All connected APs

#### *cmd*

AP CLI command

#### *arg*

AP CLI command argument

### Example

```
ruckus(debug)# remote_ap_cli -A "get director"
---- Command 'rkscli -c "get director "' executed at c0:c5:20:3b:91:f0
----- ZoneDirector Info -----
Primary Controller   : n/a
Secondary Controller : n/a
DHCP Opt43 Code     : 3

The information of the most recent Zone Director:
[1] 192.168.40.100

AP is under management of ZoneDirector: 192.168.40.100 / c0:c5:20:18:97:c1,
Currently AP is in state: RUN
OK
---- Command 'rkscli -c "get director "' executed at c4:10:8a:1f:d1:f0
----- ZoneDirector Info -----
Primary Controller   : n/a
Secondary Controller : n/a
DHCP Opt43 Code     : 3

The information of the most recent Zone Director:
[1] 192.168.40.100
```

```
AP is under management of ZoneDirector: 192.168.40.100 / c0:c5:20:18:97:c1,  
Currently AP is in state: RUN  
OK  
---- Command Execution Summary:  
      success: 2  
      failure: 0  
      total: 2  
ruckus(debug) #
```

# Working with Debug Logs and Log Settings

This section describes the commands that you can use to configure and review ZoneDirector debug logs.

## logs all

Enables debug logs of all debug components.

### Syntax Description

#### logs all

Enable logging of all debug components

### Usage Guidelines

Running this command can place considerable load on the system. If your ZoneDirector is already under load, running this command could potentially cause errors resulting in a reboot. In general, only use this command when working with Ruckus support to troubleshoot an issue.

### Example

```
ruckus(debug)# logs all
The command was executed successfully.
ruckus(debug)# show logs
Debug Logs:
  All= Enabled
  Sys-mgmt= Enabled
  Mesh= Enabled
  Web-auth= Enabled
  Rf-mgmt= Enabled
  Radius= Enabled
  Hotspot-srv= Enabled
  Aps= Enabled
  Net-mgmt= Enabled
  802.1x= Enabled
  Web-svr= Enabled
  802.11= Enabled
  Dvlan= Enabled
  Smart-redundancy= Enabled
  Client-association= Enabled
  Debug logs of specified MAC address:
    Status= Disabled
ruckus(debug)#
```

## no logs all

Disables debug logs of all debug components.

### Syntax Description

#### no logs

Disable debug logs

#### all

Disable all log components

## Example

```
ruckus(debug)# no logs all
The command was executed successfully.
ruckus(debug)#
```

## logs comp sys-mgmt

Enables debug logs of system management components.

## Syntax Description

### logs

Enable debug logs

### comp sys-mgmt

Component system management

## Example

```
ruckus(debug)# logs comp sys-mgmt
The command was executed successfully.
ruckus(debug)# show logs
Debug Logs:
  All= Disabled
  Sys-mgmt= Enabled
  Mesh= Disabled
  Web-auth= Disabled
  Rf-mgmt= Disabled
  Radius= Disabled
  Hotspot-srv= Disabled
  Aps= Disabled
  Net-mgmt= Disabled
  802.1x= Disabled
  Web-svr= Disabled
  802.11= Disabled
  Dvlan= Disabled
  Smart-redundancy= Disabled
  Client-association= Disabled
  Debug logs of specified MAC address:
    Status= Disabled
ruckus(debug)#
```

## no logs comp sys-mgmt

Disables debug logs of system management components.

## logs comp mesh

Enables debug logs of mesh components.

## no logs comp mesh

Disables debug logs of mesh components.

## logs comp web-auth

Enables debug logs of web authentication components.

## no logs comp web-auth

Disables debug logs of web authentication components.

## logs comp rf-mgmt

Enables debug logs of RF management components.

## no logs comp rf-mgmt

Disables debug logs of RF management components.

## logs comp radius

Enables debug logs of radius components.

## no logs comp radius

Disables debug logs of radius components.

## logs comp hotspot-srv

Enables debug logs of hotspot services components.

## no logs comp hotspot-srv

Disables debug logs of hotspot services components.

## logs comp aps

Enables debug logs of AP components.

## no logs comp aps

Disables debug logs of access points components.

## logs comp net-mgmt

Enables debug logs of network management components.



## **no logs comp net-mgmt**

Disables debug logs of network management components.

## **logs comp 802.1x**

Enables debug logs of 802.1x components.

## **no logs comp 802.1x**

Disables debug logs of 802.1x components.

## **logs comp web-svr**

Enables debug logs of web server components.

## **no logs comp web-svr**

Disables debug logs of web server components.

## **logs comp 802.11**

Enables debug logs of 802.11 components.

## **no logs comp 802.11**

Disables debug logs of 802.11 components.

## **logs comp dvlan**

Enables debug logs of dynamic VLAN components.

## **no logs comp dvlan**

Disables debug logs of dynamic vlan components.

## **logs comp smart-redundancy**

Enable Smart Redundancy component debug logs.

## **no logs comp smart-redundancy**

Disable Smart Redundancy component debug logs.

## logs comp bonjour-gateway

Enable Bonjour Gateway debug logs.

## no logs comp bonjour-gateway

Disable Bonjour Gateway debug logs.

## logs comp mDNSd

Enable Bonjour mDNSd debug logs.

## no logs comp mDNSd

Disable Bonjour mDNSd debug logs.

## logs comp client-association

Enable client association debug logs.

## no logs comp client-association

Disable client association debug logs.

## logs mac

Enables and sets filter running logs based on specified mac address.

**logs mac** *MAC*

### *Syntax Description*

<b>logs</b>	Enable debug logs
<b>mac</b>	Filter logs by specific MAC address
<i>MAC</i>	The MAC address of the device to be filtered

### *Example*

```
ruckus(debug)# logs mac 04:4f:aa:0c:b1:00
The command was executed successfully.
ruckus(debug)#
```

## no logs mac

Disables MAC address filtering on running logs.

### Syntax Description

#### no logs

Disable debug logs

#### mac

Filter by MAC address

### Example

```
ruckus(debug)# no logs mac
The command was executed successfully.
ruckus(debug)#
```

## logs play

Starts displaying logs on console.

### Syntax Description

#### logs

Enable debug logs

#### play

Start log play

### Usage Guidelines



#### CAUTION

Running this command can place considerable load on the system. If your ZoneDirector is already under load, running this command could potentially cause errors resulting in a reboot. In general, only use this command when working with Ruckus support to troubleshoot an issue.

### Example

```
ruckus(debug)# logs play
ruckus(debug)# [Feb 15 05:53:30][EMFD][debug]jobServiceFunc():Executing job[user auth
attempt_hash_autoexpire] at 1329285210...
[Feb 15 05:53:30][EMFD][debug]jobServiceFunc():Executing job at 1329285210...Done
[Feb 15 05:53:30][EMFD][debug]jobServiceFunc():Executing job[station auth attempt_hash_autoexpire] at
1329285210...
[Feb 15 05:53:30][EMFD][debug]jobServiceFunc():Executing job at 1329285210...Done
[Feb 15 05:53:33][STAMgr][debug]acsrvc_thread():ACSRVC rcv AP 04:4f:aa:0c:b1:00, IP= 192.168.11.6,
IPv6=fc00::1
...
...
ruckus(debug)# no logs play
ruckus(debug)#
```

## no logs play

Stops displaying logs on console.

### Syntax Description

#### no logs

Disable debug logs

#### play

Stop log play

### Example

```
ruckus(debug)# logs play
ruckus(debug)# [Feb 15 05:53:30][EMFD][debug]jobServiceFunc():Executing job[user auth
attempt_hash_autoexpire] at 1329285210...
[Feb 15 05:53:30][EMFD][debug]jobServiceFunc():Executing job at 1329285210...Done
[Feb 15 05:53:30][EMFD][debug]jobServiceFunc():Executing job[station auth attempt_hash_autoexpire] at
1329285210...
[Feb 15 05:53:30][EMFD][debug]jobServiceFunc():Executing job at 1329285210...Done
[Feb 15 05:53:33][STAMgr][debug]acsrvc_thread():ACSRVC rcv AP 04:4f:aa:0c:b1:00, IP= 192.168.11.6,
IPv6=fc00::1
...
...
ruckus(debug)# no logs play
ruckus(debug)#
```

## support\_tls1.0

To upgrade the controller's firmware, use the following command:

**support\_tls1.0**

## no support\_tls1.0

To disable AP core dump collection, use the following command:

**no support\_tls1.0**

# Remote Troubleshooting

This section describes remote troubleshooting commands.

## remote-troubleshooting server

To set the remote troubleshooting server IP address, use the following command:

```
remote-troubleshooting server IP-ADDR
```

## remote-troubleshooting start

Enables remote troubleshooting.

### Syntax Description

<b>remote-troubleshooting</b>	Remote troubleshooting
<b>start</b>	Start remote troubleshooting

### Defaults

None.

### Example

```
ruckus(debug)# remote-troubleshooting start  
ruckus(debug)#
```

## remote-troubleshooting stop

Disables remote troubleshooting.

### Syntax Description

<b>remote-troubleshooting</b>	Remote troubleshooting
<b>stop</b>	Stop remote troubleshooting

### Defaults

None.

### **Example**

```
ruckus(debug) # remote-troubleshooting stop  
ruckus(debug) #
```

### **radius-stats-wlan**

Show web-auth WLAN radius statistics bins.

### **radius-stats-authsvr**

Show web-auth WLAN radius statistics bins.

# AP Core Dump Collection

This section lists the AP core dump commands.

## collect\_ap\_coredump

Enable AP core dump collection.

**collect\_ap\_coredump** [ all | MAC ]

### Syntax Description

**collect\_ap\_coredump**

Collect AP core dump

**all**

Collect core dump from all connected APs

**MAC**

Specific AP MAC address

### Defaults

None.

### Example

```
ruckus(debug)# collect_ap_coredump all
---- Command 'apmgrinfo --coredump y ' executed at 04:4f:aa:0c:b1:00
start reporting coredump to ZD!
---- Command 'apmgrinfo --coredump y ' executed at 00:24:82:3f:14:60
start reporting coredump to ZD!
---- Command Execution Summary:
      success: 2
      failure: 0
      total: 2
rm: cannot remove '/etc/airespider-images/firmwares/ap-dump/*': No such file or directory
sh: codump_server: not found
start collecting AP's coredump !
ok
ruckus(debug) #
```

## no collect\_ap\_coredump

Disable AP core dump collection.

### Syntax Description

**no collect\_ap\_coredump**

Stop collecting AP core dump

### Defaults

None.

## Example

```
ruckus(debug)# no collect_ap_coredump all
---- Command 'apmgrinfo --coredump n ' executed at 04:4f:aa:0c:b1:00
stop reporting coredump to ZD!
---- Command 'apmgrinfo --coredump n ' executed at 00:24:82:3f:14:60
stop reporting coredump to ZD!
---- Command Execution Summary:
      success: 2
      failure: 0
      total: 2
rm: cannot remove '/etc/airespider-images/firmwares/ap-dump/*': No such file or directory
stop collecting AP's coredump !
ok
ruckus(debug)#
```



# Script Execution

This section lists the commands that can be executed from the **script** context. The script context must be entered from the debug context.

## script

Enters the script context from the debug context. You must first enter the script context before executing a script.

**script**

### Syntax Description

**script**

Enter the script context

### Defaults

None.

### Example

```
ruckus(debug)# script
ruckus(script)#
```

## quit

Exit the script context.

**quit**

### Syntax Description

**quit**

Exit the script context

### Defaults

None.

### Example

```
ruckus(script)# quit
ruckus(debug)#
```

## list

List all available scripts.

**list**

## Syntax Description

### list

List all available scripts

## Defaults

None.

## Example

```
ruckus(script)# list -a
Index                Scripts
1                    .version.sh
ruckus(script)#
```

## del

Deletes a script.

## info

Display script help file

### info

## Syntax Description

### info

Display script information

## Defaults

None.

## Example

```
ruckus(script)# info
info <file>
ruckus(script)#
```

## exec

Execute script.

**exec** *file* {parameter}

## Syntax Description

### exec

Execute the script

## **Defaults**

None.

## **Example**

```
ruckus(script)# exec  
exec <file> {parameter}  
ruckus(script)#
```



# Accessing the AP-Mode CLI

- [Accessing the AP Mode CLI from the Unleashed CLI.....477](#)

## Accessing the AP Mode CLI from the Unleashed CLI

To access the AP CLI from the Unleashed Master (controller) CLI, use the following command:

### ap-mode

```
ruckus# ap-mode
You have all rights in this mode.
ruckus(ap-mode)#
```

## Configure LTE Commands

The following CLI commands are provided to GET/SET the 3G/4G/LTE mobile configuration options for Unleashed LTE+Wi-Fi Access Points (Unleashed M510).

To use these CLI commands, you must enter the ap-mode CLI.

### *get lte*

Use the following commands to display current LTE settings:

```
ruckus> en
ruckus# ap-mode
You have all rights in this mode.
ruckus(ap-mode)#
The following CLI commands are supported.
get lte-airplane-mode-state : get lte-airplane-mode-state
    Display LTE airplane mode state
get lte-default-eth-for-wan : get lte-default-eth-for-wan
    Display LTE default ethernet port for wan
get lte-failover-selection : get lte-failover-selection
    Display LTE failover selection info
get lte-gps-probe-interval : get lte-gps-probe-interval
    Display configured GPS probe interval time
get lte-imei : get lte-imei
    Display LTE IMEI info
get lte-internet-host : get lte-internet-host
    Display the remote host details configured for internet availability check
get lte-primary-wan-recovery-time : get lte-primary-wan-recovery-time
    Display primary wan recovery time
get lte-sim-apn : get lte-sim-apn {all|primary|secondary}
    Display LTE sim-apn info
get lte-sim-network-selection : get lte-sim-network-selection {all|primary|secondary}
    Display LTE sim-network-selection status
get lte-sim-password : get lte-sim-password {all|primary|secondary}
    Display LTE sim-password info
get lte-sim-pincode : get lte-sim-pincode {all|primary|secondary}
    Display LTE sim-pincode info
get lte-sim-roaming : get lte-sim-roaming {all|primary|secondary}
    Display LTE sim-roaming status

get lte-sim-selection : get lte-sim-selection
    Display LTE sim-selection info
```

## Accessing the AP-Mode CLI

### Accessing the AP Mode CLI from the Unleashed CLI

```
get lte-sim-username : get lte-sim-username {all|primary|secondary}
    Display LTE sim-user-name info
get lte-state : get lte-state
    Display LTE state
get lte-statistics : get lte-statistics {all|primary|secondary}
    Display LTE status info
get lte-status : get lte-status
    Display LTE status
```

## set lte

Use the following commands to configure LTE settings:

```
set lte-airplane-mode-state : set lte-airplane-mode-state {enable|disable}
    Set LTE airplane mode state
set lte-default-eth-for-wan : set lte-default-eth-for-wan {eth0|eth1}
    Set LTE default ethernet port for wan (It will be overwritten by WEB UI configuration)
set lte-failover-selection : set lte-failover-selection {ethernet-lte|lte-ethernet|ethernet|lte}
    Set LTE failover selection info (It will be overwritten by WEB UI configuration)
    -----
    ethernet-lte - primary ethernet, failover LTE
    lte-ethernet - primary LTE, failover ethernet
    ethernet - ethernet only
    lte - LTE only
    -----
set lte-gps-probe-interval : set lte-gps-probe-interval {seconds}
    Set how frequently to probe GPS coordinates
    min - 1 sec, max - 500000 sec
set lte-internet-host : set lte-internet-host {host_index} {status|addr|port} {value}
    Set the host address and TCP port number to confirm the internet availability
    {host_index} = numeric number, valid range = 0 to 4
    {status|addr|port} = specifies the purpose of {value}.
    {value} = {enable|disable} specific host if the previous attribute is 'status' (or)
    URL or IP address of remote host if the previous attribute is 'addr', max. allowed URL address
    length = 255 (or)
    TCP port number if the previous attribute is 'port', valid port range = 0 to 65535.
```

#### Examples:

```
-> set lte-internet-host 0 addr www.google.com
    (Set www.google.com in 0'th index)
-> set lte-internet-host 0 port 443
    (Set port number 443 in 0'th index)
-> set lte-internet-host 0 status enable
    (Allow 0'th indexed host to be considered for internet reachability check)
-> set lte-internet-host 0 status disable
    (Don't use 0'th indexed host for internet reachability check)
```

#### Note:

The user must ensure the correctness and reliability of host URL/IP before the configuration.

```
set lte-primary-wan-recovery-time : set lte-primary-wan-recovery-time {seconds}
    Set primary wan recovery time (It will be overwritten by WEB UI configuration)
    min - 10 sec    max - 300 sec
set lte-reset : set lte-reset
    Reset LTE chip
    Note : Issue "set lte-state disable" before executing lte-reset
set lte-sim-apn : set lte-sim-apn {primary|secondary} {APN name} (It will be overwritten by WEB UI
configuration)
    max. allowed characters - 100
    allowed characters - A-Z, a-z, 0-9, (-)
set lte-sim-network-selection : set lte-sim-network-selection {primary|secondary} {lte|3g|auto}
set lte-sim-password : set lte-sim-password {primary|secondary} {Password}
    Omit the {Password} to disable/set to default
set lte-sim-pincode : set lte-sim-pincode {primary|secondary} {pincode}
    Omit the {pincode} to disable/set to default
set lte-sim-roaming : set lte-sim-roaming {primary|secondary} {enable|disable}

set lte-sim-selection : set lte-sim-selection {auto|primary|secondary}
    primary - SIM 0
    secondary - SIM 1
set lte-sim-username : set lte-sim-username {primary|secondary} {User name}
    Omit the {User name} to disable/set to default
```

```
set lte-state : set lte-state {enable|disable}  
Set LTE state
```



© 2020 CommScope, Inc. All rights reserved.  
Ruckus Wireless, Inc., a wholly owned subsidiary of CommScope, Inc.  
350 West Java Dr., Sunnyvale, CA 94089 USA  
[www.ruckuswireless.com](http://www.ruckuswireless.com)