

RUCKUS SmartZone (LT-GD) Command Reference Guide, 6.1.2

Supporting SmartZone 6.1.2

© 2023 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

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see <https://www.commscope.com/trademarks>. All product names, trademarks, and registered trademarks are the property of their respective owners.

Patent marking notice

For applicable patents, see www.cs-pat.com.

Contents

Contact Information, Resources, and Conventions.....	11
Contacting RUCKUS Customer Services and Support.....	11
What Support Do I Need?.....	11
Open a Case.....	11
Self-Service Resources.....	12
Document Feedback.....	12
RUCKUS Product Documentation Resources.....	12
Online Training Resources.....	12
Document Conventions.....	13
Notes, Cautions, and Safety Warnings.....	13
Command Syntax Conventions.....	13
About This Guide.....	15
Introduction.....	15
New In This Document.....	15
Using the Controller Command Line Interface.....	17
Overview of the Controller Command Line Interface.....	17
Accessing the Command Line Interface.....	17
What you will Need.....	17
Connect the Administrative Computer to the Controller.....	17
Start and Configure the SSH Client.....	18
Using SSH Connection.....	19
Using Serial Connection.....	20
Log onto CLI.....	23
Command Help.....	26
Generic Command Options.....	27
Commands A through C.....	29
acct-profile.....	29
admin.....	31
admin (DP).....	33
admin-radius.....	35
adv-forwarding-profile.....	37
ad-service.....	39
allow-ap-certificate-replacement.....	41
ap.....	42
ap-auto-approve.....	50
ap-auto-tagging.....	51
ap-cert-check.....	53
ap-cert-expired-check.....	54
ap-certificate-reset.....	55
ap-cli.....	56
apcli.....	57
ap-control-mgmt-tos.....	58
ap-group.....	59
ap-heartbeat.....	60
ap-internal-subnet.....	61

ap-model.....	62
ap-routine-config-interval.....	64
ap-routine-status-interval.....	65
ap-subnet-discovery.....	66
ap-zone-aggregate.....	67
auth-method.....	68
auth-profile.....	69
auth-type.....	71
backup.....	73
backup (Dataplane).....	74
backup config.....	76
backup network.....	77
backup schedule.....	78
backup-upgrade.....	80
bonjour-policy.....	81
bridge-profile.....	82
calea.....	84
calea-mac.....	86
calea-server-ip.....	88
cert-store.....	89
changepassword.....	92
clock.....	93
clone.....	94
cluster in-service.....	96
cluster-ip-list.....	97
cluster-redundancy.....	98
controller.....	99
controller-description.....	100
copy.....	101
copy ap-certificate-request.....	102
copy backup.....	103
copy backup-config.....	104
copy backup-network.....	105
copy report-result.....	106
Commands D through F.....	107
data-plane.....	107
data-plane.....	108
debug.....	110
debug-tools.....	111
delete backup.....	112
delete backup-config.....	113
delete backup-network.....	114
delete client.....	115
dhcp.....	116
dhcp-relay.....	118
diag.....	120
diagnostic.....	122
diagnostic.....	125
diameter-system-wide.....	127
dns-server-service.....	128

domain.....	130
dp-customized-config.....	155
dp-group.....	156
dp-packet-capture.....	160
eap-aka.....	161
eap-sim.....	163
enable (new password).....	165
enc-method.....	166
encrypt-mac-ip.....	167
encrypt-zone-name.....	168
eth-port-validate-one-trunk.....	169
event.....	170
event-email.....	173
event-threshold.....	174
export log.....	175
fips.....	176
fips.....	177
force-recover-escluster.....	179
fresh upgrade.....	180
ftp-server.....	181
ftp-test.....	183
firmware-download-limit.....	184
Commands G through I.....	187
gateway-advance.....	187
gdpr-pii.....	188
ggsn-service.....	189
hlr-mnc-ndc.....	191
hlr-service.....	192
hlr-system-wide.....	195
hostname.....	196
hotspot.....	197
identity-provider.....	199
hotspot-profile.....	201
interface.....	203
internal-dp-group.....	205
ip.....	206
ip control-nat.....	208
ip data-nat.....	209
ip default-gateway.....	210
ip default-gateway-ipv6.....	211
ip internal-subnet.....	212
ip ipv6-route.....	213
ip name-server.....	214
ip name-server-ipv6.....	215
ip route.....	216
ip separate-access-core.....	217
ip-support.....	218
ipsec-profile.....	219
Commands J through N.....	223

kdump.....	223
l2-acl.....	225
l2ogre-profile.....	227
lbs-service.....	230
ldap-service.....	231
legacy-ssh-algorithm.....	233
license cloud.....	234
license export.....	235
license import.....	236
license local.....	237
license sync-now.....	238
lineman.....	239
localdb-service.....	240
logging.....	241
lwapp2scg.....	242
manage-alias-ssh-port.....	244
mgmt-acl.....	246
mvno.....	248
nat.....	250
no cls-sess msisdn.....	252
no control-plane.....	253
no data-plane.....	254
no domain.....	255
no oauth-service.....	257
no osu-portal-profile.....	258
no zone.....	259
node-affinity-config.....	261
non-tpm-switch-cert-validate.....	263
northbound-authtype.....	264
northbound-portal.....	265
ntp-server.....	266
Commands O through Sh.....	267
operator-profile.....	267
outbound-firewall.....	269
output-format.....	271
patches.....	272
ping.....	274
ping6.....	275
profile-based-nat.....	276
proxy-aaa.....	277
radius-service.....	278
rbddump.....	281
rebalance-aps.....	283
reboot.....	284
reindex-elasticsearch-all.....	285
reload.....	286
reload ap.....	287
reload data-plane.....	288
remote ap-cli.....	289
remote-syslogd.....	290

report.....	291
reset.....	295
restore.....	296
restore.....	297
restore config.....	298
restore network.....	299
rks-gre.....	300
route.....	302
save-log.....	304
scan-jmxport.....	306
sci-profile.....	307
screen-pagination.....	309
service.....	310
session-timeout.....	312
set-factory.....	313
setup.....	314
sha1.....	321
shutdown.....	323
Show Commands.....	325
show (DP debug).....	325
show admin-activity.....	326
show alarm.....	328
show ap.....	329
show ap-certificate-status.....	331
show ap-stats.....	332
show ap-subnet-discovery-status.....	335
show backup.....	336
show backup-config.....	337
show backup-config-state.....	338
show backup-network.....	339
show backup-schedule.....	340
show backup-state.....	341
show backup-upgrade-state.....	342
show client.....	343
show clock.....	344
show cls-sess.....	345
show cluster.....	346
show cluster-node.....	347
show cluster-state.....	350
show controller.....	351
show control-plane.....	352
show control-plane-stats.....	355
show counter.....	357
show cpuinfo.....	358
show data-plane.....	359
show data-plane-stats.....	361
show dhcp binding.....	363
show dhcp-relay-stats.....	364
show diskinfo.....	365
show dp-customized-config.....	366

show event.....	367
show ggsn-cnxn-stats.....	369
show ggsn-gtpc-stats.....	370
show history.....	371
show interface.....	372
show internal-subnet.....	374
show ip.....	375
show ip (DP).....	376
show license.....	377
show logs-filter.....	379
show md-stats.....	380
show meminfo.....	382
show nat.....	383
show radius-proxy-stats.....	384
show radshm-stats.....	385
show report-result.....	386
show rogue-aps.....	387
show running-config.....	388
show service.....	389
show sha1-state.....	391
show snapshot-disk-state.....	392
show ssh-rekey-limit-state.....	393
show stats.....	394
show status.....	395
show strict-wfa-compliance-state.....	397
show system-capacity.....	398
show tlsv1-state.....	399
show ttg-client.....	400
show ue-nat-session.....	401
show upgrade.....	402
show upgrade-history.....	403
show upgrade-state.....	404
show version.....	405
show wired- client.....	406
show zone.....	407
Commands Si - Z.....	409
sms-server.....	409
smtp-server.....	411
snmp-notification.....	413
snmp-v2-community.....	414
snmp-v3-user.....	416
soft-gre.....	419
ssh-rekey-limit.....	421
stats-upload.....	422
strict-wfa-compliance.....	424
subpackages.....	425
support-admin.....	427
syslog.....	428
syslog-server.....	430
tlsv1.....	432

tlsversion.....	434
traceroute.....	435
traceroute6.....	438
ttg-pdg-profile.....	440
upload ap-certificate-status.....	443
use sz.....	444
user-agent-blacklist.....	445
user-group.....	446
user-role.....	448
user-traffic-profile.....	450
usgv6.....	452
vlan-pooling.....	454
vpn.....	456
weak-cipher-allowed.....	459
web-authentication.....	460
wechat.....	462
with-public-key-change.....	464
wlan.....	465
wlan-group.....	470
wlan-scheduler.....	472
zone.....	474
zone-template.....	507

Contact Information, Resources, and Conventions

- [Contacting RUCKUS Customer Services and Support](#)..... 11
- [Document Feedback](#)..... 12
- [RUCKUS Product Documentation Resources](#)..... 12
- [Online Training Resources](#)..... 12
- [Document Conventions](#)..... 13
- [Command Syntax Conventions](#)..... 13

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.ruckusnetworks.com> and select **Support**.

What Support Do I Need?

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

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

Open a Case

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

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

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

Self-Service Resources

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

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

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

Document Feedback

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

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

When contacting us, include the following information:

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

For example:

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

RUCKUS Product Documentation Resources

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

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

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

Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at <https://commscopeuniversity.myabsorb.com/>. The registration is a two-step process described in this [video](#). You create a CommScope account and then register for, and request access for, CommScope University.

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>
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the Start menu, click All Programs .
<i>italics</i>	Publication titles	Refer to the <i>RUCKUS Small Cell Release Notes</i> for more information.

Notes, Cautions, and Safety Warnings

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

NOTE

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

ATTENTION

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



CAUTION

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



DANGER

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

Command Syntax Conventions

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

Convention	Description
bold text	Identifies command names, keywords, and command options.
<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.
{x y z}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <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.

About This Guide

- Introduction..... 15
- New In This Document..... 15

Introduction

This *Command Reference Guide* contains the syntaxes and commands for configuring and managing SZ100/300/vSZ-H/vSZ-D (collectively referred to as “the controller” throughout this guide) from the 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 networks, 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 support site at <https://support.ruckuswireless.com/contact-us>

New In This Document

TABLE 2 New/updated/deprecated commands in SmartZone 6.1.2 Rev A (November 2023)

Feature	Description	Reference
legacy-ssh-algorithm	New: Disables/Enables legacy algorithm from SmartZone SSH.	legacy-ssh-algorithm on page 233
diagnostic	Updated: remote-packet-capture disable and remote-packet-capture enable keywords to disable and enable the remote packet capture with IP of the capture tool server.	diagnostic on page 122
firmware-download-limit	Updated: The default bandwidth per AP firmware download limit from 1k to 256k bytes.	firmware-download-limit on page 184

Using the Controller Command Line Interface

- Overview of the Controller Command Line Interface..... 17
- Accessing the Command Line Interface..... 17
- What you will Need..... 17
- Connect the Administrative Computer to the Controller..... 17
- Start and Configure the SSH Client..... 18
- Using SSH Connection..... 19
- Using Serial Connection..... 20
- Command Help..... 26
- Generic Command Options..... 27

Overview of the Controller Command Line Interface

The Controller command line interface (CLI) is a software tool that enables you to configure and manage SmartCell Gateway 200 and Virtual SmartZone High-Scale. Using the command line interface, you can issue commands from an operating system prompt, such as the Microsoft Windows command prompt or a Linux operating system terminal. Each command performs a specific action for configuring device settings or returning information about the status of a specific device feature.

Accessing the Command Line Interface

The controller has a built-in command line interface (CLI) that you can use to configure controller settings and manage access points. This section describes the requirements and the procedure for accessing the controller CLI.

What you will Need

To access controller CLI, you need the following:

- A computer that you want to designate as administrative computer.
- A network connection to the controller (if you want to use an SSH connection) or an RS-232 serial to RJ45 cable (if you want to use a serial connection) .
- An SSH (secure shell) client.

Connect the Administrative Computer to the Controller

Connect the administrative computer to controller either through the network or directly using an RS-232 serial to RJ45 cable.

1. If you want to use an SSH connection, connect the administrative computer to the same subnet or broadcast domain as the Management (Web) interface of the controller.

Using the Controller Command Line Interface

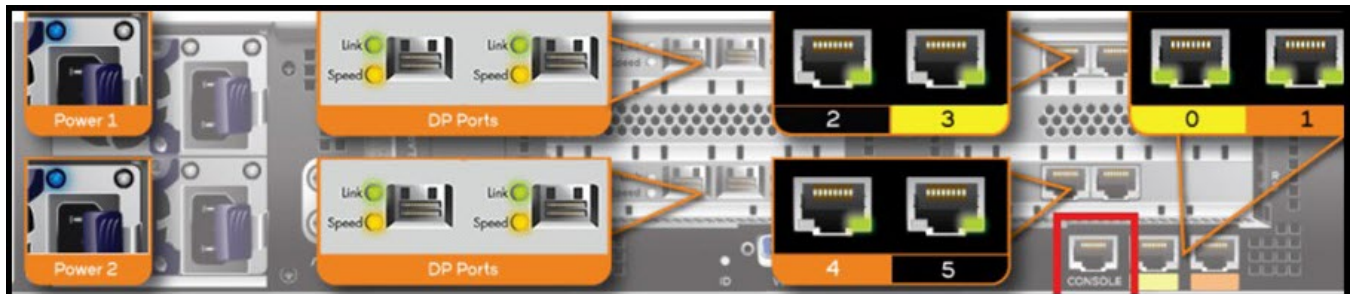
Start and Configure the SSH Client

2. If you want to use a serial connection, make sure that both the administrative computer and the controller are both powered on. And then, do the following:
 - Connect the RJ45 end of the cable to the port labeled |O|O| (console port) on the controller. See [Figure 1](#) for the location of the console port.
 - Connect the RS-232 end of the cable to a COM port on the administrative computer.

FIGURE 1 SCG200 Location of console port



FIGURE 2 SZ300 Location of console port



Start and Configure the SSH Client

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

NOTE

The following procedure describes how to use PuTTY, a free and open source telnet/SSH client, to access the controller CLI. If you are using a different 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.

See the following sections depending on your connection method:

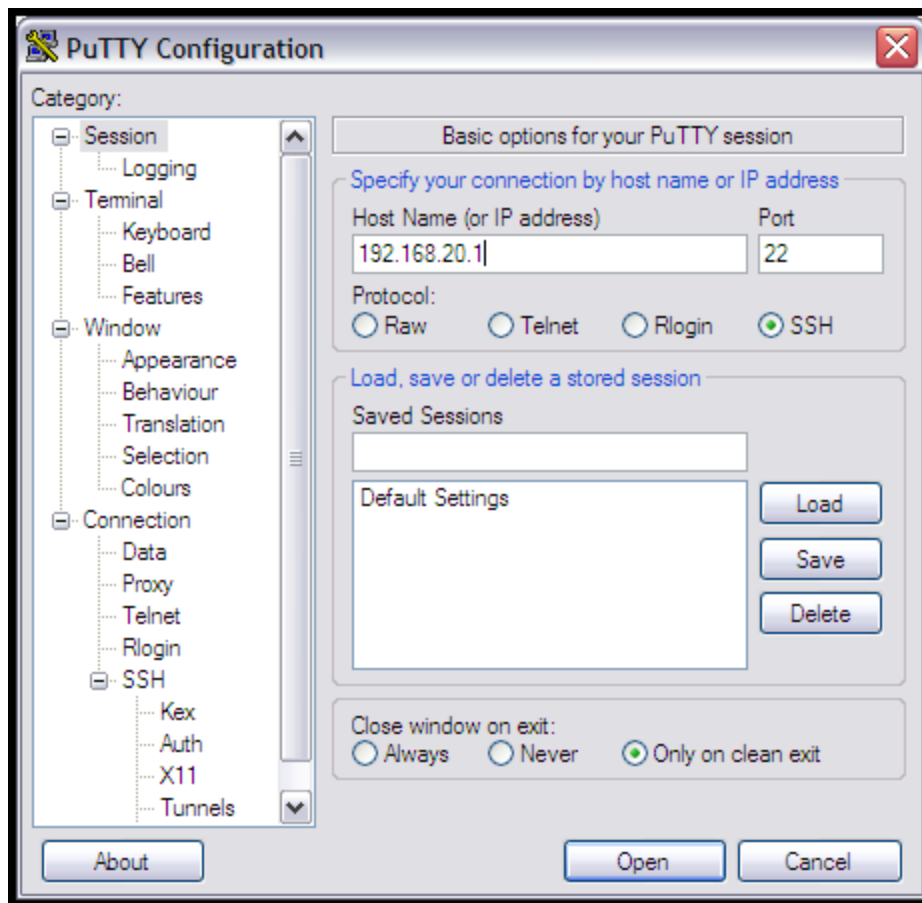
- [Using SSH Connection](#) on page 19
- [Using Serial Connection](#) on page 20

Using SSH Connection

If you have connected the administrative computer to the same subnet or broadcast domain as the Management (Web) interface of the controller, follow these steps to start and configure the SSH client.

1. Start PuTTY. The PuTTY configuration dialog box appears, showing the **Session** screen as seen in [Figure 3](#).
2. In **Connection type**, select SSH.

FIGURE 3 Selecting SSH as a connection type



3. Enter the IP address of the Management (Web) interface of the controller in the **Host Name** (or IP address) field as seen in [Figure 3](#).

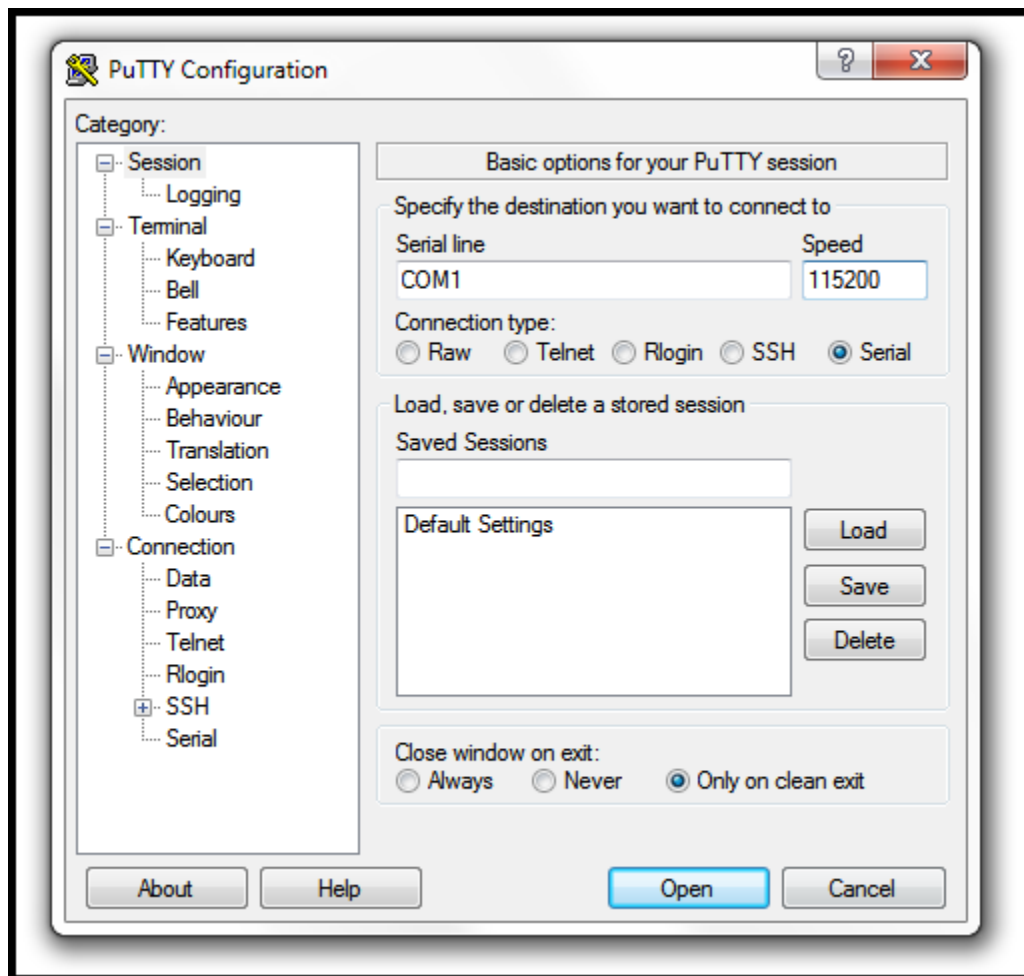
4. Click **Open**. The **PuTTY console** appears and displays the login prompt. See [Figure 7](#) on page 23.

Using Serial Connection

If you have connected the administrative computer to the console port on the controller using an RS-232 serial to RJ45 cable, follow these steps to start and configure the SSH client.

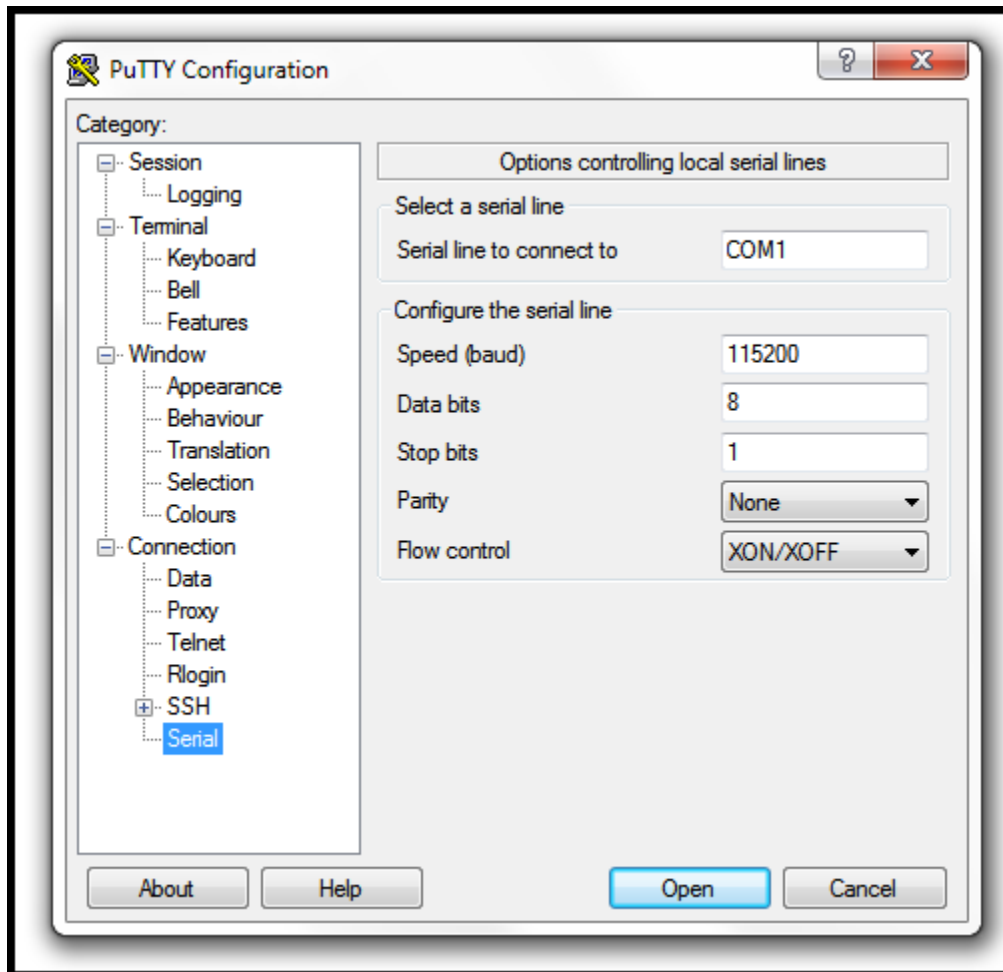
1. Start **PuTTY**. The **PuTTY Configuration** dialog box appears, showing the **Session** screen as seen in [Figure 4](#).
2. In **Connection** type, select **Serial** if you are connecting via serial cable.

FIGURE 4 Selecting serial as a connection type



3. Under Category, click **Connection** > **Serial**. The serial connection options appear on the right side of the dialog box, displaying PuTTY's default serial connection settings. See [Figure 5](#).

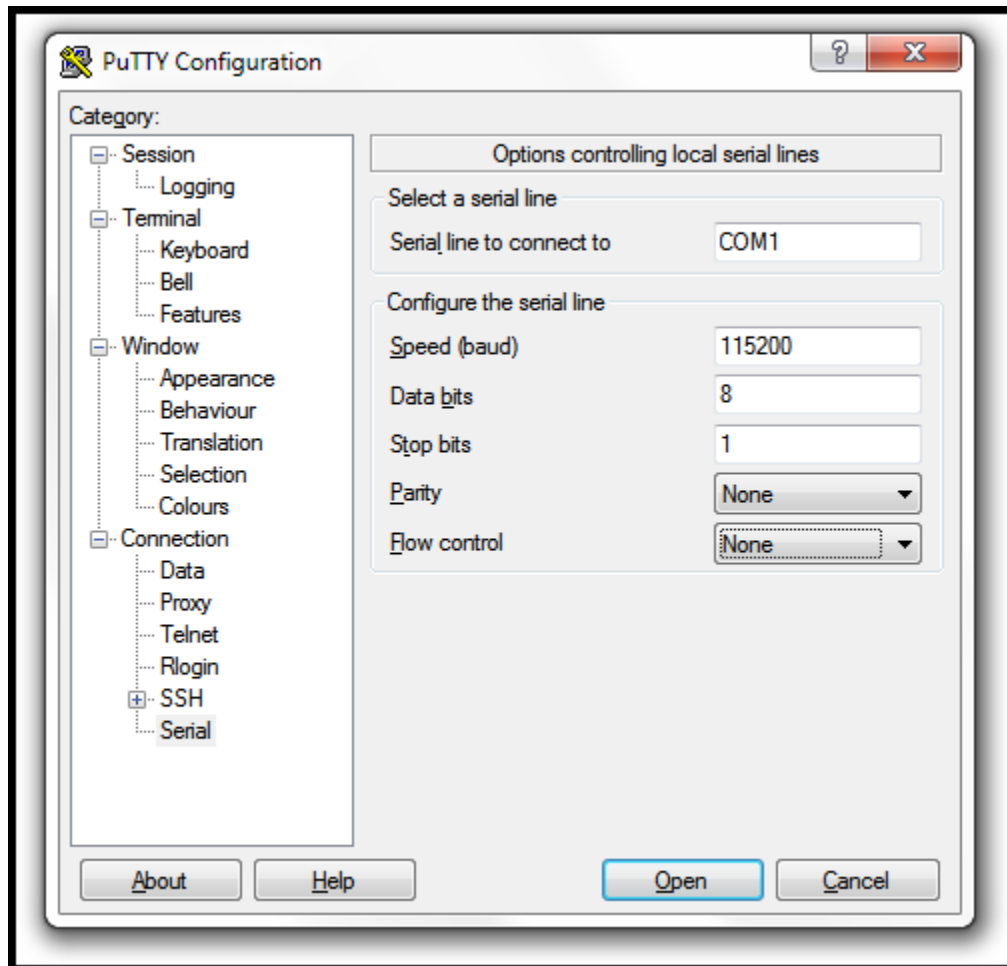
FIGURE 5 PuTTY's default serial connection setting



Using the Controller Command Line Interface Using Serial Connection

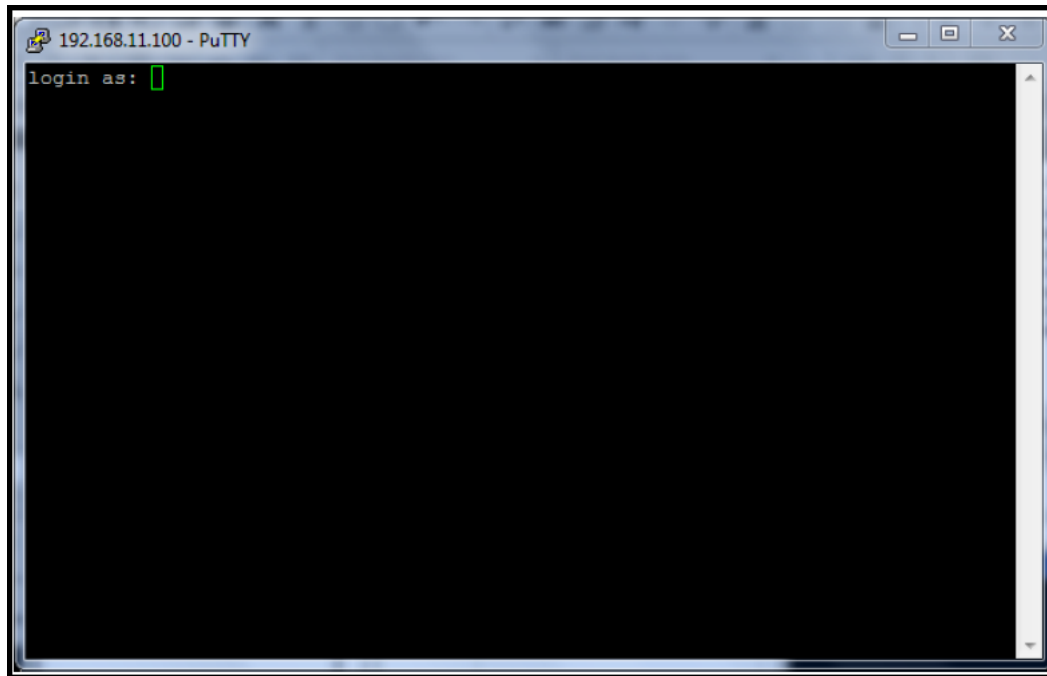
4. Configure the serial connection settings as follows. See [Figure 6](#).
 - Serial line to connect to: Type the COM port name to which you connected the RS-232 cable.
 - Bits per second: 115200
 - Data bits: 8
 - Stop bits: 1
 - Parity: None
 - Flow control: None

FIGURE 6 PuTTY's serial connection settings for connecting to controller



5. Click **Open**. The PuTTY console appears and displays the login prompt as seen in [Figure 7](#).

FIGURE 7 PuTTY console displaying the login prompt



You have completed configuring the SSH client to connect to the controller CLI.

Log onto CLI

The following describes the process for logging onto the CLI.

- Log onto the controller using putty/Xssh (any other application) using the user credentials of login name and password as given.

NOTE

You cannot use 'admin' as a password, which is used during the controller installation procedure.

- The controller CLI welcome message appears with the CLI prompt as seen below.

FIGURE 8 Login Screen

```
login as: admin
Pre-authentication banner message from server:
| #####
| #       Welcome to vSZ       #
| #####
End of banner message from server
admin@10.206.84.138's password:
Last successful login: 2023-09-06 14:22:04
Last successful login from: 10.45.179.243
Failed login attempts since last successful login: 0
Account privilege changes: No
Please wait. CLI initializing...

Welcome to the Ruckus Virtual SmartZone - High Scale Command Line Interface
Version:
```

- You are now logged into the controller CLI as a user with limited privileges by looking at the CLI prompt. If you are in limited mode, the prompt appears as ruckus> (with a greater than sign). To view a list of commands that are available at the root level or user mode, enter **help** or **?**.

NOTE

To change the CLI prompt to a privileged mode, see step 5.

FIGURE 9 Using show commands

```
NODE63# show meminfo
Total Memory: 127.9 GB
Used Memory: 19.4 GB
Free Memory: 108.6 GB

NODE63# show diskinfo
Total Disk: 1.01504 TB
Used Disk: 111.7 GB
Free Disk: 927.7 GB
```

- To view login and password details for AP SmartZone, enter **show running-config** zone name. Refer the CLI details below.

FIGURE 10 View AP Login and Password

```

dhcp-10-206-84-163# show running-config zone zone01
General Options
-----
Zone Name           : zone01
Description         :
Timezone            : UTC
AP IP Mode          : IPv4
AP Firmware Version : 6.1.2.0.408
Country Code        : US
Location            :
Location Additional Information :
GPS Coordinates     :
GPS Altitude        :
AP Admin Logon      : Logon ID   : admin
                   : Password   : *****
DP Group           : Default DP Group
  
```

- As a user with limited privileges, you can view a history of commands that were previously executed and ping a device as seen in [Figure 11](#).

FIGURE 11 Using system commands

```

set-1> show
clock      Show current GMT date time
cpuinfo    Show CPU usage status
diskinfo   Show Disk usage status
meminfo    Show Memory usage status
version    Show system version

set-1> ping 172.19.13.60
PING 172.19.13.60 (172.19.13.60) 56(84) bytes of data.
64 bytes from 172.19.13.60: icmp_seq=1 ttl=64 time=0.015 ms
64 bytes from 172.19.13.60: icmp_seq=2 ttl=64 time=0.019 ms
64 bytes from 172.19.13.60: icmp_seq=3 ttl=64 time=0.021 ms
64 bytes from 172.19.13.60: icmp_seq=4 ttl=64 time=0.020 ms
64 bytes from 172.19.13.60: icmp_seq=5 ttl=64 time=0.018 ms

--- 172.19.13.60 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.015/0.018/0.021/0.005 ms
  
```

- If you want to run more commands, you need to switch to privileged mode by entering enable and the password at the root prompt as seen in [Figure 12](#). The prompt changes from ruckus> to ruckus# (with a pound sign) as seen in [Figure 12](#). Refer to **enable** command for details.

FIGURE 12 Changing to privileged mode

```
INDUS4> en → User mode
Password: *****

INDUS4# config → Privileged mode

INDUS4 (config) # █
```

Command Help

You can display commands and syntax information in any mode and from any point in the command hierarchy.

Enter a question mark (?) or a tab in any command mode to display the list of commands available in that mode.

```
device (config) #?
acct-profile          Create/Update Accounting Service Profile configuration
ad-service            Create/Update Active Directory Service configuration
admin                 Create/Update Administrator account configuration
admin-radius          Create/Update RADIUS server for Administrators
adv-forwarding-profile Create/Update Advanced (Mixed Mode) profile configuration
ap                    Update AP configuration
ap-auto-tagging       Create/Update/Enable Critical AP Auto Tagging rules
ap-cert-check         Enable AP certificate check
ap-cert-expired-check Enable AP expired certificate check
ap-certificate-reset  Reset AP certificate request which failed to updating certificate
ap-control-mgmt-tos   Enable AP control and management traffic TOS and set TOS value
ap-heartbeat          Update AP Heartbeat interval
ap-internal-subnet    Tunnel Internal Subnet
ap-zone-aggregate     Enable AP Zone data aggregation task
auth-profile          Create/Update Authentication Service Profile configuration
bridge-profile        Create/Update Bridge profile
(output truncated)
```

To display a list of commands that start with a specified character, type the character followed by a question mark (?) or a tab.

```
device (config) #g?
gateway-advance       Set gateway advance options
get                   command.description
ggsn-service           Update GGSN / PGW GTP configuration
```

To display keywords and arguments associated with a command, enter the command followed by a question mark (?) or a tab.

```
device (config) #qos ?
egress-buffer-profile User defined QoS egress profile
mechanism              Change mechanism
name                   Change name
profile                 Change bandwidth allocation
scheduler-profile       User defined QoS profile
tagged-priority         Change tagged frame priority to profile mapping
```

Generic Command Options

Across the SmartZone controllers there are some command options that have the same or similar functionality.

To avoid repetition and to keep the command syntax looking less complex, generic command options are being introduced here. These options will appear under the ? on the controllers for many commands in various modes. Consult this page for an explanation of the functionality.

The following table describes the generic command options.

TABLE 3 Generic Command Options

Command Option	Description	Configuration Mode
config	Enters Global configuration mode.	Privileged EXEC User EXEC
do	Allows show and other EXEC commands to be executed in configuration mode.	Global configuration mode
description	Text description of the command.	Global configuration mode
end	Ends the current configuration session and returns to privileged EXEC mode.	Global configuration mode
exit	Exits the current configuration mode and returns to the previous mode. If in User EXEC mode, exits the session.	Global configuration mode Privileged EXEC User EXEC
help	Displays the help text for the current command.	Global configuration mode
history	Displays a list of previously entered commands.	Global configuration mode Privileged EXEC User EXEC
logout	Exit from EXEC mode. The command is only available in Debug configuration mode for the SmartZone Data Plane controllers only.	Debug configuration mode Privileged EXEC User EXEC
name <i>name</i>	Usually a variable entered after a command to define the initial name. After initial configuration, the name <i>name</i> allows name changes.	Global configuration mode
quit	Exits the configuration session. This option is only supported on the SZ Data Plane controllers.	Privileged EXEC User EXEC
Quotation Marks	Using quotation marks (" ") around strings that contain white spaces but only double quotation. We do not support single quotation.	Privileged EXEC User EXEC Config EXEC

Commands A through C

acct-profile

Enables accounting service profile configurations.

Syntax

acct-profile*name*

no acct-profile[*name*]

After the **acct-profile** command is entered to enable the Account Profile configuration mode, the following configuration syntax is available:

[**default**{**no-match-realm**|**no-realm**}**acct**{**na**|*name*}|**description***text*|**name***name*|**realm***realm*]

After the **realm** command is entered to enable the Account Profile Realm configuration mode, the following additional configuration syntax is available:

[**acct-service***name*|**name***name*]

Command Default

No accounting service profiles are created.

Parameters

name

Specifies the accounting service profile.

default

Sets the default services.

no-match-realm

Sets the default service for when no matching realm is found.

no-realm

Sets the default service for when no realm is specified.

acct

Sets the default accounting service.

na

Specifies that NA is disabled.

name

Specifies the accounting service name.

description*text*

Sets the description of the account profile.

name*name*

Sets the accounting service profile name.

Commands A through C

acct-profile

realm*realm*

Sets the accounting service realm and enters Account Profile Realm configuration mode.

acct-service*name*

Sets the accounting service.

name*name*

Sets the accounting service realm name.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only.

The **no** form of the command removes configured accounting service profiles. If no account service profile is specified, all accounting service profile configurations are removed.

Examples

The following example creates an accounting service profile and enters Account Profile configuration mode.

```
device# config
device(config)# acct-profile rad-profile
device(config-acct-profile)#
```

The following example creates an accounting service profile, enters Account Profile configuration mode and specifies an accounting service profile name.

```
device# config
device(config)# acct-profile rad-profile
device(config-acct-profile)# name myaccountsp
```

The following example removes all accounting service profile configurations.

```
device# config
device(config)# no acct-profile
device(config)# no acct-profile
Do you want to continue to delete (or input 'no' to cancel)? [yes/no] yes
```

admin

Creates or update the profile for an administrator.

Syntax

admin*name*

no admin[*username*]

After the **admin** command is entered to enable the Admin configuration mode, the following configuration syntax is available:

[**email***email-address* | **name***name* | **password** | **phone***number* | **real-name***name* | **title***job-title*]

Command Default

The default Administrator Profile is used.

Parameters

name

Specifies an account name.

email*email-address*

Sets the email address for the user.

name*name*

Sets the account name.

password

Sets the password for the account

phone*number*

Sets the phone number of the user.

real-name*name*

Sets the real name of the user.

title*job-title*

Sets the job title of the user.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes configured administrator profiles.

Examples

The following example creates an administrator profile, and sets an email address, password, phone number, real name, and title for the profile.

```
device# admin joe
device(config-admin)# email joe@company.com
device(config-admin)# password
  Password: *****
  Retype: *****
device(config-admin)# phone 22870001
device(config-admin)# real-name "Joe Admin"
device(config-admin)# title CTO
```

The following example removes a previous configured administrator profile.

```
device# config
device(config)# no admin joe
Do you want to continue to delete (or input 'no' to cancel)? [yes/no]
```


admin (DP)

Creates or update the profile for an administrator.

Syntax

admin

After the **admin** command is entered to enable the Admin configuration mode, the following configuration syntax is available:

[history|logout|name *name*|passwd *password* |session-idle *minutes*|show]

Command Default

The default Administrator Profile is used.

Parameters

history

Displays the list of previously run commands.

logout

Logs the user out.

name *name*

Specifies the account name.

passwd *password*

Sets the password for the account

session-idle *minutes*

Sets the CLI idle timeout value in minutes.

show

Displays the account settings.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.

Examples

The following example creates an administrator profile, and sets a name for that profile.

```
device# admin
device(config-admin)# admin1
device(config-admin)#
```

Commands A through C

admin (DP)

The following examples shows a list of previously run commands.

```
device(config-admin)# history
```

```
Command history:
```

```
0. enable  
1. config  
2. admin  
3. name admin1
```

The following examples displays the administrative settings.

```
device(config-admin)# show
```

```
ADMIN Settings:
```

```
vSZ-D HostName: admin1
```

```
vSZ-D Session Idle: 600 (seconds)
```

admin-radius

Configures the RADIUS server and enters Admin Radius configuration mode.

Syntax

admin-radius*name*

no admin-radius[*name*]

After the **admin-radius** command is entered to enable the Admin Radius configuration mode, the following configuration syntax is available:

[**ip***ip-address* | **name***name* | **port***port-number* | **shared-secret** | **test***username**password* [**chap** | **pap**] | **type**{**radius** | **tacacs**}]

Command Default

The RADIUS server is not configured.

Parameters

name

Specifies the RADIUS server name.

ip-address*ip-address*

Sets the IP address for the primary RADIUS server.

name*name*

Sets the RADIUS server name.

port*number*

Sets the port number for the primary RADIUS server.

shared-secret

Sets the shared secret for the primary RADIUS server. Valid values range from 1 through 255 characters.

test

Tests the RADIUS server based on the user credentials and protocol settings.

username

Specifies the user name.

password

Specifies the password.

chap

Specifies the CHAP protocol.

pap

Specifies the PAP protocol.

type

Sets the authentication type.

radius

Specifies RADIUS authentication.

Commands A through C

admin-radius

tacacs

Specifies TACACS authentication.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes RADIUS server configurations. If no RADIUS server is specified, all RADIUS server configurations are removed.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example enters Admin Radius configuration mode and configures the RADIUS server.

```
device# config
device(config)# admin-radius aaa-auth
device(config-admin-radius)# ip 10.1.1.1
device(config-admin-radius)# port 1813
device(config-admin-radius)# shared-secret
Password: **
Retype: ***
```

The following example removes all RADIUS server configurations.

```
device# config
device(config)# no admin-radius
Do you want to continue to delete (or input 'no' to cancel)? [yes/no] yes
```

adv-forwarding-profile

Enters Advanced (mixed mode) Profile configuration mode to create or update advanced (mixed mode) profile configurations.

Syntax

adv-forwarding-profile*name*

no adv-forwarding-profile*name*

After the **adv-forwarding-profile** command is entered to enable the Advanced (mixed mode) Profile configuration mode, the following configuration syntax is available:

```
[ apn { ni <apn> | nioi <apn> } | default { no-match-realm | no-realm } apn value } | description text | name name | realm realm
apnvalue ]
```

After the **apn** command is entered to enable the APN Advanced Profile configuration mode, the following configuration syntax is available:
route-type { *Bridge* | *L2oGRE* }

Command Default

No advanced (mixed mode) profile configurations are created.

Parameters

name

Specifies the advanced (mixed mode) profile name.

apn

Creates or updates the forwarding policy for APN configuration commands.

ni <*apn*>

Specifies the NI forwarding policy.

nioi <*apn*>

Specifies the NIOI forwarding policy.

default

Specifies the default APN settings.

no-match-realm

Sets the default for when no matching realm is found.

no-realm

Sets the default for when no realm is specified.

apn *value*

Specifies the default APN.

description *text*

Sets the profile description. The description length must be between 1 and 128 characters.

name *name*

Sets the advanced (mixed mode) profile name.

Commands A through C

adv-forwarding-profile

realm *realm*

Sets the realm name.

route-type

Sets the route type.

Bridge

Sets the route type to either Bridge.

L2oGRE

Sets the route type to either L2oGRE.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only.

Multiple realms are supported.

The **no** form of the command deletes advanced (mixed mode) profile configurations.

Examples

The following example creates an advanced (mixed mode) profile and enters advanced (mixed mode) profile configuration mode.

```
device# config
device(config)# adv-forwarding-profile ttg-pdg
device(config-adv-forwarding-profile)#
```

The following example deletes all advanced (mixed mode) profiles.

```
device# config
device(config)# no adv-forwarding-profile
Do you want to continue to delete (or input 'no' to cancel)? [yes/no] yes
```

ad-service

Enters Active Directory Service configuration mode to enable active directory services configurations.

Syntax

ad-service*name*

no ad-service[*name*]

After the **ad-service** command is entered to enable the Active Directory Service configuration mode, the following configuration syntax is available:

[**description** *text* | **friendly-name** *friendly-name* | **global-catalog** | **group-attrs** *attr-value* { **Default** | **RATE_LIMIT_USR_ROLE** | **User-Role-GA** | **user1** | *user-role* } | **ip-address** *ip-address* | **name** *name* | **port** *port* | **windows-domain-name** *domain-name*]

Command Default

No active directory services profiles are configured.

Parameters

name

Specifies an active directory service.

description *text*

Sets the description for the active directory service.

friendly-name *friendly-name*

Sets the active directory friendly name.

global-catalog

Enables global catalog support.

group-attrs *attr-value*

Sets user traffic profile mapping.

Default

Sets the default profile.

RATE_LIMIT_USR_ROLE

Sets the accounting service.

User-Role-GA

Sets the RATE_LIMIT_USR_ROLE profile.

user1

Sets the user1.

user-role

Sets the user-role.

ip-address *ip-address*

Sets the IP address for the primary server.

Commands A through C

ad-service

name *name*

Sets the active directory service name.

port *number*

Sets the port for the primary server.

windows-domain-name *domain-name*

Sets the Windows Domain name. Valid values are **dc=domain**, **dc=ruckuswireless**, and **dc=com**.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes configured active directory services. If no active directory service is specified, all active service directories are removed.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example configures an active directory service and enters Active Directory Service configuration mode.

```
device# config
device(config)# ad-service ads
device(config-ad-service)#
```

The following example removes an active directory service called "active-orange".

```
device# config
device(config)# no ad-service active-orange
Do you want to continue to delete (or input 'no' to cancel)? [yes/no]
```

The following example removes all active directory service configurations.

```
device# config
device(config)# no ad-service
Do you want to continue to delete (or input 'no' to cancel)? [yes/no]
```

The following example sets the port for the primary server in Active Directory Service configuration mode.

```
device# config
device(config)# ad-service ads
device(config-ad-service)# port 1
```


allow-ap-certificate-replacement

Enables AP certificate replacement configuration.

Syntax

```
allow-ap-certificate-replacement  
no allow-ap-certificate-replacement
```

Command Default

AP certificate replacement configuration is enabled.

Parameters

This command has no parameters.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables AP certificate replacement configuration.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example allow the AP certificate replacement.

```
device# config  
device(config)# allow-ap-certificate-replacement  
Successful operation  
% This configuration will take effect in a few minutes.
```

The following example block the AP certificate replacement.

```
device# config  
device(config)# no allow-ap-certificate-replacement  
Successful operation  
% This configuration will take effect in a few minutes.
```

ap

Creates or updates access point (AP) configurations.

Syntax

```
ap mac-address [ approve | lock | move zone name | pre-prov | swap | trigger-prefer-node | trigger-swap]
```

```
ap { pre-prov | swap } { export | import } ftp-url
```

```
no ap mac-address [ lock ]
```

After the **acct-profile** command is entered to enable the Account Profile configuration mode, the following configuration syntax is available:

```
[ description text | name name | realm realm ]
```

After the **realm** command is entered in Account Profile Realm configuration mode, the following additional configuration syntax is available:

```
[ acct-service name | name name ]
```

Command Default

AP configurations are not created.

Parameters

mac-address

Specifies the AP MAC address.

approve

Approves the AP to proceed with the registration process.

lock

Locks the AP.

move zone

Moves the AP to a target AP zone. Valid values for the *name* variable are **5.1.2_Zone**, **5.1.1_GA**, **"Default Zone"**, **Dual**, **ER-7581**, **IPv6_ZOne**, **"SZ Dis-Shreyas"**, **zone-discovery**, and *ap-zone-name*.

pre-prov

Specifies pre-provision APs.

swap

Specifies swapping APs.

trigger-prefer-node

Specifies the trigger prefer node action.

trigger-swap

Specifies the trigger swap action.

export

Export to a CSV file using FTP.

import

Import from a CSV file using FTP.

ftp-url

Specifies the FTP directory URL.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

The **trigger-prefer-node** keyword is only available on the SmartZone 300.

Examples

The following example creates an AP and specifies an AP MAC address. It also imports pre-provision APs from a CSV file using FTP and exports swapping APs using FTP.

```
device# config
device(config)# ap A1:87:45:34:56:FE
device(config)# ap pre-prov import ftp://device:device1!@172.19.7.100/backup/AP_ad8745345
device(config)# ap swap export ftp://device:device1!@172.19.7.100
```

Related Commands

- [Table 4](#) lists the related **ap profile** configuration commands.
- [Table 5](#) lists the related **ap model** configuration commands.
- [Table 6](#) lists the related **ap model lan1** configuration commands.
- [Table 6](#) lists the related **ap pre-prov** configuration commands for the SmartZone 300.

TABLE 4 Commands related to device(config-ap)

Syntax and Type	Parameters (if any)	Description
device(config-ap)# admin	<i>logonpassword</i>	Sets the administrative logon credentials.
device(config-ap)# admin-mode	<i>lockedunlocked</i>	Sets the administrative mode to either locked or unlocked.
device(config-ap)# ap-logon	<i>logon-id</i>	Sets the access point administration login credentials.
device(config-ap)# ap-model	<i>ap-model</i>	Sets the model specification (overrides the zone configuration).
device(config-ap)# ap-password	<i>password</i>	Sets the access point administrative password.
device(config-ap)# area-code	<i>areacode</i>	Sets the user location information of LAC or TAC.
device(config-ap)# bonjour-gateway		Enables the bonjour gateway.
device(config-ap)# bonjour-policy		Enables the bonjour policy.
device(config-ap)# channel-evaluation-interval	<i>seconds</i> : The interval value (60~3600 secs)	Sets the channel evaluation interval.

TABLE 4 Commands related to device(config-ap) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-ap)# channel-select-mode	2.4g {value}: 2.4GHz radio 5g {value}: 5GHz radio	Automatically adjusts the AP channels.
device(config-ap)# channelfly-mtbc	2.4g number: 2.4GHz radio number: MTBC value range:100-1440 5g number: 5GHz radio number: MTBC value range:100-1440	Set MTBC value of Channelfly.
device(config-ap)# client-admission-control	2.4g 5g 2.4g minClientCountminClientCount Min Client Count (Default: 10) 2.4g maxRadioLoadmaxRadioLoad Max Radio Load (Default: 75%) 2.4g minClientThroughput minClientThroughput: Min Client Throughput (Default: 0.0Mbps) 5g minClientCountminClientCount Min Client Count (Default: 20) 5g maxRadioLoadmaxRadioLoad Max Radio Load (Default: 75%) 5g minClientThroughput minClientThrough put Min Client Throughput (Default: 0.0Mbps)	Enables the client admission control.
device(config-ap)# description	description	Sets the model specification (overrides the zone configuration).
device(config-ap)# device-ip-mode	[ipv6 ipv4 dual]	Sets the device IP mode.
device(config-ap)# gps	latitudelongitude	Sets the GPS coordinates to latitude and longitude values.
device(config-ap)# gps-latitude	gps-latitude	Sets the GPS coordination latitude.
device(config-ap)# gps-longitude	gps-longitude	Sets the GPS coordination longitude.

TABLE 4 Commands related to device(config-ap) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-ap)# hotspot20	<i>name</i> [swe cze spa eng chi ger fre jpn dan tur] <i>name</i> : Name swe : Swedish cze : Czech spa : Spanish eng : English chi : Chinese ger : German fre : French jpn : Japanese dan : Danish tur : Turkish	Sets the hotspot 2.0 settings.
device(config-ap)# ip	address <i>ipnetwork-maskgateway</i> name-server <i>dns-serversecondary</i>	Sets the IP address and primary and secondary DNS servers.
device(config-ap)# ip6	address <i>ipgateway</i> : address : Set IPv6 address <i>ip</i> : Static IPv6 address <i>gateway</i> : Gateway name-server <i>dns-serversecondary</i> name-server : Set primary and secondary DNS server <i>dns-server</i> : DNS server secondary : Secondary DNS server	Sets the AP IPv6 network settings.
device(config-ap)# location	<i>location</i>	Sets the location.
device(config-ap)# location-additional-info	<i>text</i>	Sets the additional information for location.
device(config-ap)# mesh	[disable mesh root auto]	Sets the mesh mode to either: disable: Disable mesh: Mesh AP root: Root AP auto: Auto
device(config-ap)# model		Sets the model specifications. It overrides the zone configuration.
device(config-ap)# name	<i>name</i>	Sets the AP name.

TABLE 4 Commands related to device(config-ap) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-ap)# no	admin bonjour-gateway channel-evaluation-interval channel-select-mode client-admission-control description gps hotspot20 <i>ipaddressname-server secondary</i> <i>ip6addressname-server secondary</i> location location-additional-info model override-client-admission-control override-smart-mon override-mgmt-ap-vlan override-channel-select-mode override-client-admission-control override-syslog-opt override-zone-location no protection-mode override-zone-location-additional-info radio recovery-ssid smart-mon swap-in-ap syslog uplink-ap venue-profile	Disables the configuration.
device(config-ap)# override-ap-mgmt-vlan	<i>vlanTag</i> : VLAN tag (1-4094) enter 'keep' to retain the APs setting.	Overrides AP Management VLAN
device(config-ap)# override-channel-select-mode	2.4g : 2.4GHz radio 5g : 5 GHz radio	Overrides Auto Channel Selection Mode and Channelfly MTBC.
device(config-ap)# override-client-admission-control	2.4g5g	Overrides the client admission control.
device(config-ap)# override-smart-mon		Overrides the smart monitor.
device(config-ap)# override-syslog-opt		Overrides the Syslog option.
device(config-ap)# override-zone-location		Overrides the zone location settings.
device(config-ap)# override-zone-location-additional-info		Overrides the zone's additional information setting on location.

TABLE 4 Commands related to device(config-ap) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-ap)# protection-mode	2.4g \${value}	Overrides the protection mode on 2.4 GHz radio
device(config-ap)# radio	2.4g channel channel 5g channel channel 2.4g channelization channelization 5g channelization channelization 2.4gtx-power tx-power 5gtx-power tx-power 2.4gwlan-service 5gwlan-service 2.4gwlan-group name 5gwlan-group name 2.4groam [enable disable] 5groam [enable disable] 2.4groam-macfilt-time seconds (0-600) Smart roam MAC filter time in seconds 5groam-macfilt-time seconds (0-600) Smart roam MAC filter time in seconds	Sets the radio channels.
device(config-ap)# recovery-ssid-enabled	disable	Overrides the enable recovery SSID broad case.
device(config-ap)# smart-mon	interval between 5-60 threshold between 1-10	Enables the smart monitor.
device(config-ap)# swap-in-ap	mac	Sets the AP Mac IP address for swap-in.
device(config-ap)# syslog	enable ipport: Enable the syslog server enable ipport [Local2 Keep Original Local1 Local5 Local6 Local0 Local7 Local3 Local4] [Error Critical Warning All Alert Notice Info Emergency] disable : Disables the syslog server	Sets the syslog server.
device(config-ap)# uplink	[smart manual]	Sets the uplink selection to either smart or manual.
device(config-ap)# uplink-ap		Sets the uplink to manual access point.
device(config-ap)# venue-profile	name	Sets the venue profile
device(config-ap)# zone	name	Move the access point to another zone.

TABLE 5 Commands related to device(config-ap-model)

Syntax and Type	Parameters (if any)	Description
device(config-ap-model)# ext-ant	2.4g number : 2.4 with DBI number 2.4gg number [3 2] : 3/2 antennas numbers: DBI number 5g number : 5g with DBI number 5gg number [2 3]: 5gg with 2/3 antennas	Enables the external antenna.

TABLE 5 Commands related to device(config-ap-model) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-ap-model)# internal-heater		Enables the internal heater.
device(config-ap-model)# lan1 device(config-ap-model)# lan2 device(config-ap-model)# lan3 device(config-ap-model)# lan4 device(config-ap-model)# lan5		Sets the LAN configurations from 1 to 5.
device(config-ap-model)# led		Enables the status of LEDs.
device(config-ap-model)# led-mode		Sets the LED mode.
device(config-ap-model)# lldp		Enables link layer discovery protocol.
device(config-ap-model)# lldp-ad-interval	<i>seconds</i>	Sets the LLDP advertise interval.
device(config-ap-model)# lldp-hold-time	<i>seconds</i>	Sets the LLDP hold time.
device(config-ap-model)# lldp-mgmt		Enables LLDP management IP TLV.
device(config-ap-model)# no	ext-ant internal-heater lan1 lan2 lan3 lan4 lan5 led lldp lldp-mgmt poe-operating-mode poe-out-port radio-band usb usb-software	Disables or deletes the settings that have been configured.
device(config-ap-model)# poe-operating-mode	<i>\$value</i>	Switches the PoE mode.
device(config-ap-model)# poe-out-port		Enables the PoE out port.
device(config-ap-model)# radio-band	<i>\$value</i>	Switches the radio band.
device(config-ap-model)# usb		Enables the USB port.
device(config-ap-model)# usb-software	<i>\$value</i>	Sets the AP USB software package.

TABLE 6 Commands related to device(config-ap-model-lan1)

Syntax and Type	Parameters (if any)	Description
device(config-ap-model-lan1)# 8021x	<i>802.1x-type</i>	Sets 802.1x.
device(config-ap-model-lan1)# acct-service	<i>acct-service</i>	Sets the authentication service configurations.
device(config-ap-model-lan1)# auth-service	<i>auth-service</i>	Sets the authentication service configurations.
device(config-ap-model-lan1)# mac-bypass		Sets the MAC bypass.

TABLE 6 Commands related to device(config-ap-model-lan1) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-ap-model-lan1)# members	<i>members</i>	Sets the AP model configurations.
device(config-ap-model-lan1)# no	acct-service mac-bypass overwrite	Disables or deletes the settings that have been configured.
device(config-ap-model-lan1)# overwrite		Enable overwriting of VLAN
device(config-ap-model-lan1)# profile	<i>profile</i> : Ethernet port profile	Sets Ethernet port profile
device(config-ap-model-lan1)# supplicant	mac <i>customusernamepassword</i>	Sets the supplicant.
device(config-ap-model-lan1)# type	[trunk-port access-port general-port]	Sets the port type.
device(config-ap-model-lan1)# vlan-untag-id	<i>untag-id</i> : VLAN untag ID	Sets the VLAN untag ID.
device(config-ap-model-lan1)# vlan-members	<i>members</i> : VLAN members	Sets the VLAN members.

TABLE 7 Commands related to device(config-ap-pre-prov)

Syntax and Type	Parameters (if any)	Description
device(config-ap-pre-prov)# ip6		Sets IPV6 network settings.
device(config-ap-pre-prov)# ip6 address	<i>ip</i> : IP address <i>gateway</i> : Gateway	Sets the IPV6 address and gateway.
device(config-ap-pre-prov)# ip6 name-server	<i>primary-dns</i> : Primary DNS. <i>secondary-dns</i> : Secondary DNS	Sets the primary or secondary DNS.

ap-auto-approve

Enables auto approve for access points (APs).

Syntax

ap-auto-approve

no ap-auto-approve

Command Default

Auto approve for APs is not enabled.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone 100 and vSZ-E controllers only.

Examples

The following example enables auto approve for APs.

```
device# config
device(config)# ap-auto-approve
Successful operation
```

The following example disables auto approve for APs.

```
device# config
device(config)# no ap-auto-approve
Do you want to continue to disable (or input 'no' to cancel)? [yes/no] yes
Successful operation
```

ap-auto-tagging

Sets up critical access point (AP) auto tagging rules and enters AP auto tagging configuration mode.

Syntax

ap-auto-tagging

no ap-auto-tagging enable

After the **ap-auto-tagging** command is entered to enable the AP auto tagging configuration mode, the following configuration syntax is available:

[**enable**]

After the **enable** command is entered in AP auto tagging configuration mode, the following configuration syntax is available:

[**rule daily-threshold** | **threshold** *value* | **unit** { **g** | **m** }]

Command Default

Auto tagging rules for APs is not set up.

Parameters

no ap-auto-taggingenable

Disables critical AP auto tagging.

enable

Enables the auto-tagging of critical APs.

ruledaily-threshold

Sets the auto tagging rule to daily traffic bytes, which exceeds the threshold rule.

threshold*value*

Sets the threshold value.

unit

Sets the unit.

g

Sets the unit to gigabytes.

m

Sets the unit to megabytes.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

The **no** form of the command disables critical AP auto tagging.

Commands A through C

ap-auto-tagging

Examples

The following example enables auto tagging for APs and enters AP auto tagging configuration mode. It also sets the auto tagging rule to daily traffic bytes.

```
device# config
device(config)# ap-auto-tagging
device(config-ap-auto-tagging)# enable
device(config-ap-auto-tagging)# rule daily-threshold
```

The following example disables auto tagging for APs.

```
device# config
device(config)# no ap-auto-tagging enable
```

ap-cert-check

Enable the access point (AP) certificate check.

Syntax

ap-cert-check
no ap-cert-check

Command Default

Certificate checking is not enabled for APs.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example enables certificate checking for APs.

```
device# config
device(config)# ap-cert-check
Successful operation
```

The following example disables certificate checking for APs.

```
device# config
device(config)# no ap-cert-check
Do you want to continue to disable (or input 'no' to cancel)? [yes/no] yes
Successful operation
```

ap-cert-expired-check

Enables the expired certificate checking for access points (APs).

Syntax

ap-cert-expired-check
no ap-cert-expired-check

Command Default

Expired certificate checking is not enabled for APs.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example enables expired certificate checking for APs.

```
device# config
device(config)# ap-cert-expired-check
Successful operation
```

The following example disables expired certificate checking for APs.

```
device# config
device(config)# no ap-cert-expired-check
Successful operation
```

History

Release version	Command history
3.6	This command was introduced.

ap-certificate-reset

Resets access point (AP) certificate requests.

Syntax

```
ap-certificate-reset { all | zone zone-name
```

Command Default

AP certificate requests are not reset.

Parameters

all

Resets all AP certificate requests.

zone zone-name

Specifies the target zone.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example resets all AP certificate requests.

```
device# config
device(config)# ap-certificate-reset all
```

ap-cli

Enters debug AP CLI configuration mode for AP CLI debug script management.

Syntax

ap-cli

After the **ap-cli** command is entered to enable the debug AP CLI configuration mode, the following configuration syntax is available:

{ execute | show } zone zone-name

upload zone zone-name ftp-url

Parameters

execute

Executes the AP CLI script.

show

Shows the script execution summary of a specified zone.

upload

Uploads an AP CLI script from a remote FTP server

zone zone-name

Sets the default service.

ftp-url

Specifies the FTP URL.

Modes

Debug configuration mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only.

Examples

The following example enters debug AP CLI configuration mode where AP CLI debug script management can be run.

```
device# debug
device(debug)# ap-cli
device(debug-ap-cli)#
```


apcli

Enters debug AP CLI configuration mode to run the AP CLI debug script management.

Syntax

apcli

After the **apcli** command is entered to enable the debug AP CLI configuration mode, the following configuration syntax is available:

[**execute** | **show** { **diagnostic-script** *script-name* | **schedule** }]

show-execution-status

upload *ftp-url*

Parameters

execute

Executes the AP CLI script.

show

Shows script summaries.

diagnostic-script *script-name*

Shows the diagnostic script.

schedule

Shows the schedule script.

show-execution-status

Shows the script execution summary.

upload

Uploads an AP CLI script from a remote FTP server

ftp-url

Specifies the FTP URL.

Modes

Debug configuration mode

Usage Guidelines

This command is supported on the SmartZone 100 and vSZ-E controllers only.

Examples

The following example enters debug AP CLI configuration mode where AP CLI debug script management can be run.

```
device# debug
device(debug)# apcli
device(debug-apcli)#
```

ap-control-mgmt-tos

Enables the access point (AP) control management traffic type of service (TOS).

Syntax

ap-control-mgmt-tos *value*
no ap-control-mgmt-tos

Command Default

The AP control management traffic TOS is not enabled.

Parameters

value
Specifies the TOS value.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.
The **no** form of the command removes configured authentication service profiles.

Examples

The following example enables the AP control management TOS and sets a TOS value of 10.

```
device# config  
device(config)# ap-control-mgmt-tos 10
```

The following example disables AP the control management TOS and removes configured TOS values.

```
device# config  
device(config)# no ap-auto-tagging enable
```

ap-group

Creates an Access Point (AP) group.

Syntax

ap-group *group-name*

no ap-group *group-name*

Command Default

AP groups are not created.

Parameters

group-name

Specifies an AP group name.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to delete an AP group.

Examples

The following example creates the AP group "myapgroup".

```
device# config
device(config)# ap-group myapgroup
device(config-ap-group)
```

The following example deletes the AP group named myapgroup.

```
device# config
device(config)# no ap-group myapgroup
```

```
Do you want to continue to delete (or input 'no' to cancel)? [yes/no] yes
```

ap-heartbeat

Configures the access point (AP) heartbeat interval.

Syntax

ap-heartbeat *seconds*

Command Default

The AP heartbeat interval is not changed.

Parameters

seconds

Specifies the TOS value. Valid values are 30, 60, 150, or 300 seconds.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example sets AP heartbeat interval to 60 seconds.

```
device# config
device(config)# ap-heartbeat 60
```

ap-internal-subnet

Configures internal subnet for a tunnel.

Syntax

ap-internal-subnet *ip-address*

Command Default

An internal subnet is not configured for a tunnel.

Parameters

ip address

Specifies the IP address in 10.x.0.0 format.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example configures an internal subnet for a tunnel with the IP address 10.1.0.0.

```
device# config
device(config)# ap-internal-subnet 10.1.0.0
```

ap-model

Specifies the AP model to be used.

Syntax

ap-model *ap-model-name*

After the ap-model command has been entered to enter AP Model configuration mode, the following configuration syntax is available (syntax in groupings for clarity):

[**ext-ant** { **2.4g** *num* | **2.4gg** *num* [**2** | **3**] | **5g** *num* | **5gg** *num* [**2** | **3**] }

[**internal-heater** | **lan** | **led** | **led-mode** | **lldp** | **lldp-ad-interval** *seconds* | **lldp-hold-time** *seconds* | **lldp-mgmt** | **poe-operating-mode** *poe-value* | **poe-out-port** | **radio-band** *radio-value* |]

[{ **usb** | **usb-software** } *ap-model* [**enable** | **disable**]

Command Default

No AP model is specified.

Parameters

ap-model-name

Specifies the AP model name.

ext-ant

Specifies the external antenna wireless frequency.

2.4g *num*

Enables the external 2.4 GHz antenna on the selected AP model and sets the gain number as a number between 0 and 90dBi.

2.4gg *num* **2** **3**

Enables the external 2.4 GHz antenna on the selected AP model, sets the gain number, and .

5g *num*

Enables the external 5 GHz antenna on the selected AP model and sets the gain number as a number between 0 and 90dBi.

5gg *num* **2** **3**

Enables the external 5 GHz antenna on the selected AP model, sets the gain number, and sets the.

internal-heater

Enables the heater that is built into the AP model.

led

Specifies Hotspot 2.0 as the authentication method.

led-mode

Specifies Hotspot 2.0 Secure Onboarding (OSEN) as the authentication method.

web-authentication

Specifies Web authentication as the authentication method.

wechat

Specifies WeChat as the authentication method.

Modes

IPSec Profile configuration mode

WLAN Zone configuration mode

Usage Guidelines

This command is available only after one of the following commands is entered:

- ipsec-profile
- wlan

Examples

The following example creates a WLAN in zone Zone10, and sets the authentication type to be guest access.

```
device# config
device(config)# zone zone10
device(config-zone)# wlan wlan20
device(config-zone-wlan)# auth-type guest-access
```

ap-routine-config-interval

Sets the AP routine configuration interval.

Syntax

ap-routine-config-interval*seconds*

Parameters

seconds

Specifies the interval period in seconds.

Modes

Debug configuration mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only.

Examples

The following example set the AP routine configuration interval to 60 seconds.

```
device# debug
device(debug)# ap-routine-config-interval 60
```


ap-routine-status-interval

Sets the AP routine status interval.

Syntax

```
ap-routine-status-interval { slowdown | speedup }
```

Parameters

slowdown

Specifies that all APs report status at 900 second intervals.

speedup

Specifies that all APs report status at 180 second intervals.

Modes

Debug configuration mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only.

Examples

The following example sets all APs to report status at 900 second intervals.

```
device# debug
device(debug)# ap-routine-status-interval speedup
```

The following example sets all APs to report status at 180 second intervals.

```
device# debug
device(debug)# ap-routine-status-interval slowdown
```

ap-subnet-discovery

Enables the AP subnet discovery service.

Syntax

ap-subnet-discovery

no ap-subnet-discovery

Modes

Debug configuration mode

Usage Guidelines

This command is supported on the SmartZone 100 and vSZ-E controllers only.

The **no** form of the command disables the AP subnet discovery service.

Examples

The following example enables the AP discovery service.

```
device# debug
device(debug)# ap-subnet-discovery
```

The following example disables the AP discovery service.

```
device# debug
device(debug)# no ap-subnet-discovery
```

ap-zone-aggregate

Enables zone aggregation for access points (APs).

Syntax

ap-zone-aggregate
no ap-zone-aggregate

Command Default

Certificate checking is not enabled for APs.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only.

Examples

The following example enables zone aggregation for APs.

```
device# config
device(config)# ap-zone-aggregate
Successful operation
```

The following example enables zone aggregation for APs.

```
device# config
device(config)# no ap-zone-aggregate
Successful operation
```

auth-method

Specifies the authentication method to be used.

Syntax

auth-method 8021x | 8021xmac | mac | open

Command Default

No authentication method is specified.

Parameters

8021x

Specifies 802.1x EAP as the authentication method.

8021xmac

Specifies 802.1x EAP and the MAC address as the authentication method.

mac

Specifies the MAC address as the authentication method.

open

Specifies no authentication method.

Modes

WLAN Zone configuration mode

Authentication Profile REALM configuration mode

Identity Provider Account Profile REALM configuration mode

Usage Guidelines

This command is available only after one of the following commands is entered:

- authentication-profile
- identity-profile
- wlan

Examples

The following example creates a WLAN in zone Zone10, and sets the authentication method to be 8021x EAP.

```
device# config
device(config)# zone zone10
device(config-zone)# wlan wlan20
device(config-zone-wlan)# auth-method 8021x
```

auth-profile

Enters Authentication Service Profile configuration mode to configure authentication services.

Syntax

auth-profile*name*

no auth-profile*name*

After the **auth-profile** command is entered to enable the Authentication Service Profile configuration mode, the following configuration syntax is available:

[**aaa-support** | **default**{**no-match-realm** | **no-realm**}**acct** | **description***text* | **gpp-support** | **name***name* | **realm***realm*]

After the **realm** command is entered to enable the Authentication Service Profile Realm configuration mode, the following additional configuration syntax is available:

[**auth-service***name* | **dynamic-vlan***vlan-id* | **name***name*]

Command Default

Authentication services profiles are not created.

Parameters

aaa-support

Enables Hosted AAA Support.

default

Sets the default services.

no-match-realm

Sets the default service for when no matching realm is found.

no-realm

Sets the default service for when no realm is specified.

acct

Sets the default authentication service.

description*text*

Sets the description of the authentication service profile.

gpp-support

Configures the PLMN identifier.

name*name*

Sets the authentication service profile name.

realm*realm*

Sets the authentication service realm.

auth-service*name*

Sets the authentication service.

Commands A through C

auth-profile

dynamic-vlan*vlan-id*

Sets the dynamic VLAN ID. Valid values range from 2 through 4094.

name*name*

Sets the authentication service realm name.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only.

The **no** form of the command removes configured authentication service profiles.

Examples

The following example creates an Authentication Service Profile and enters Authentication Service Profile configuration mode.

```
device# configure
device(config) auth-profile aaa-auth
device(config-auth-profile) #
```

The following example removes all configured Authentication Service Profiles.

```
device# configure
device(config) no auth-profile
```

auth-type

Specifies the authentication type to be used.

Syntax

auth-type **guest-access** | **hotspot** | **hotspot2** | **osen** | **standard** | **web-authentication** | **wechat**

Command Default

No authentication type is specified.

Parameters

guest-access

Specifies 802.1x EAP as the authentication type.

hotspot

Specifies Hotspot service (WISPr) as the authentication type.

hotspot2

Specifies Hotspot 2.0 as the authentication method.

osen

Specifies Hotspot 2.0 Secure Onboarding (OSEN) as the authentication method.

web-authentication

Specifies Web authentication as the authentication method.

wechat

Specifies WeChat as the authentication method.

Modes

WLAN Zone configuration mode

Usage Guidelines

This command is available only after the following command is entered:

- wlan

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example creates a WLAN in zone Zone10, and sets the authentication type to be guest access.

```
device# config
device(config)# zone zone10
device(config-zone)# wlan wlan20
device(config-zone-wlan)# auth-type guest-access
```

History

Release version	Command history
6.0	The command is not supported for IPsec configuration mode.

backup

Backs up the whole cluster system of the controller.

Syntax

backup

Command Default

The configuration is not backed up.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example backs up the whole cluster system of the controller.

```
device# backup
```

backup (Dataplane)

Backs up the controller configurations.

Syntax

```
backup{ftp|sftp}ip-address / path [filename]user-namepassword  
backup tftp ip-address / path [filename]
```

Command Default

The controller configuration is not backed up.

Parameters

ftp	Specifies an FTP server.
sftp	Specifies an SFTP server.
<i>ip-address</i>	Specifies the IP address of the server.
<i>path</i>	Specifies the path to the backup file.
<i>filename</i>	Specifies the file name.
<i>user-name</i>	Specifies the user name.
<i>password</i>	Specifies the password.
tftp	Specifies a TFTP server.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.

Enter the FTP/TFTP/SFTP URL in the following format: **ftp://tftp://sftp://ip-addresspathfilename**

A user name and password must be specified if you are using an FTP or SFTP server.

Examples

The following example backs up the controller configurations and specifies the TFTP URL, path, and file name.

```
device# backup tftp 10.0.0.10 /tmp/filename.bak
```

The following example backs up the controller configurations and specifies the TFTP URL and path. The file name will be automatically generated.

```
device# backup tftp 10.0.0.10 /tmp/
```

backup config

Backs up the controller configurations.

Syntax

backup config

Command Default

The configuration is not backed up.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example backs up the controller configuration.

```
device# backup configuration
Do you want to backup configurations (or input 'no' to cancel)? [yes/no] yes
Starting to backup configurations...
Successful operation
```

backup network

Backs up controller network configuration.

Syntax

backup network

Command Default

The network configuration is not backed up.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example backs up the controller network configuration.

```
device# backup network
Do you want to backup configurations (or input 'no' to cancel)? [yes/no] yes
Starting to backup configurations...
Successful operation
```

backup schedule

Schedules a configuration backup.

Syntax

backup schedule daily *hour minute minute*

backup schedule disable

backup schedule monthly *date-of-month hour hour minute minute*

backup schedule weekly { **friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday** } **hour** *hour minute minute*

Command Default

A configuration backup is not scheduled.

Parameters

daily

Specifies a daily configuration backup.

hour

Specifies the hour for which the back up is scheduled. Valid values range from 0 through 24. The timing is set at GMT values.

minute

Specifies the minute.

minute

Specifies the minute for which the back up is scheduled. Valid values range from 0 through 59. The timing is set at GMT values.

disable

Disables the schedule backup of the configuration.

monthly

Specifies a monthly configuration backup.

date-of-month

Specifies the date each month for which the back up is scheduled. Valid values range from 1 through 31.

weekly

Specifies a weekly configuration backup.

friday

Specifies a weekly configuration backup on a Friday.

monday

Specifies a weekly configuration backup on a Monday.

saturday

Specifies a weekly configuration backup on a Saturday.

sunday

Specifies a weekly configuration backup on a Sunday.

- thursday**
Specifies a weekly configuration backup on a Thursday.
- tuesday**
Specifies a weekly configuration backup on a Tuesday.
- wednesday**
Specifies a weekly configuration backup on a Wednesday.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example schedules a daily configuration backup at 15:20 PM GMT.

```
device# backup schedule daily 15 minute 20  
Successful operation
```

The following example disables scheduled configuration backups.

```
device# backup schedule disable
```

The following example schedules a monthly configuration backup on the 22nd day of each month at 10:30 AM GMT.

```
device# backup schedule monthly 22 hour 10 minute 30  
Successful operation
```

The following example schedules a weekly configuration backup on a Friday at 19:35 AM GMT.

```
device# backup schedule weekly friday hour 19 minute 35  
Successful operation
```

backup-upgrade

Backs up and upgrades the whole cluster system for the controller.

Syntax

```
backup-upgrade ftp-url
```

Command Default

The system is not backed up.

Parameters

ftp-url
Specifies the FTP URL.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Enter the FTP URL in the following format: `ftp://username:password@ftp-host[/dir-path]`

Examples

The following example backs up and upgrades the whole cluster system and specifies the FTP URL.

```
device# backup-upgrade ftp://mahan:ruckus1!@172.19.7.100/backup/AP_ad87453456fe.csv
```


bonjour-policy

Creates or updates the bonjour policy.

Syntax

bonjour-policy*name**rule**priority*

no bonjour-policy*name*

After the **bonjour-policy** command is entered to enter Bonjour Policy configuration mode, the following configuration syntax is available:

rule*priority*

Command Default

No bonjour policy is created.

Parameters

name

Specifies the bonjour policy name.

rule*priority*

Specifies the bonjour policy set of rules based on the rule priority.

Modes

Global configuration mode

Zone configuration mode

Usage Guidelines

This command is supported for SmartZone 100 devices. For more information on Bonjour settings, refer to the **Bonjour** section in the *RUCKUS SZ100 and vSZ-E Administrator Guide*.

Use the **no** form of this command to delete a Bonjour policy.

Examples

The following example creates the bonjour policy named `bpolicy8`.

```
device# config
device(config)# bonjour-policy bpolicy8
device(configbonjour-policy) rule
```

The following example deletes the configured bonjour policy named `bpolicy8`.

```
device# config
device(config)# no bonjour-policy bpolicy8
Do you want to continue to delete (or input 'no' to cancel)? [yes/no] yes
```

bridge-profile

Enters Bridge Profile configuration mode to configure bridge forwarding profiles.

Syntax

bridge-profile *name*

After the **bridge-profile** command is entered to enable the Bridge Profile configuration mode, the following configuration syntax is available:

[**description***text* | **dhcp-option-82** | **dhcp-relay** | **dhcp-server1***ip-address* | **dhcp-server2***ip-address* | **name***name* | **relay-both**]

After the **dhcp-option-82** command is entered to enable the Bridge Profile DHCP Option82 configuration mode, the following configuration syntax is available:

[**subopt1**{**ap-ssid** | **ap-info-default** | **ap-info-location** | **ap-mac** | *format*} | **subopt150** | **subopt151**{**area-name***name* | **ssid**} | **subopt2**{**ap-ssid** | **ap-mac** | **ue-ssid** | **ue-mac** | *format*}]

Command Default

The bridge forwarding profile is not configured.

Parameters

name

Specifies the bridge profile name

description*text*

Sets the description of the bridge profile.

dhcp-option82

Enables DHCP option 82.

dhcp-relay

Enables DHCP relay.

dhcp-server1*ip-address*

Sets the DHCP server 1.

dhcp-server2*ip-address*

Sets the DHCP server 2.

name*name*

Sets the bridge profile name.

relay-both

Enables DHCP to send requests to both servers simultaneously.

subopt1

Specifies sub-option 1.

ap-ssid

Specifies the ESSID of the AP.

ap-info-default

Specifies the default information for the AP.

ap-info-location

Specifies the AP location.

ap-mac

Specifies the MAC address of the AP.

subopt150

Specifies sub-option 150.

subopt151

Specifies sub-option 151.

area-name *name*

Specifies the area.

ssid

Specifies the ESSID.

subopt2

Specifies sub-option 2.

ue-ssid

Specifies the ESSID of the client.

ue-mac

Specifies the MAC address of the client..

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only.

The **dhcp-option82**, **dhcp-server1ip-address**, **dhcp-server2ip-address**, and **relay-both** options are only available after DHCP relay has been enabled.

The **no** form of the command deletes the configured bridge profile.

Examples

The following example creates a bridge profile “auth-prof” and enters Bridge Profile configuration mode.

```
device# config
device(config)# bridge-profile auth-prof
device(config-bridge-profile)#
```

The following example removes the bridge profile “auth-prof”.

```
device# config
device(config)# no bridge-profile auth-prof
```

calea

Configures the Communications Assistance for Law Enforcement Act (CALEA) server settings.

Syntax

calea

After the **calea** command is entered to enable the CALEA configuration mode, the following configuration syntax is available:

[history|logout|macmac-address|show]

nomacmac-address

Command Default

The CALEA server is not configured.

Parameters

history

Displays the list of previously run commands.

logout

Logs the user out.

macmac-address

Specifies the MAC address.

show

Displays the CALEA global configuration and the server details.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.

Examples

The following example enters CALEA configuration mode and sets the MAC address.

```
device# config
device(config-admin)# calea
device(config-calea)# mac A1:87:45:34:56:FE
```

The following example removes the configured MAC address for the CALEA server.

```
device# config
device(config-admin)# calea
device(config-calea)# no mac A1:87:45:34:56:FE
```

calea-mac

Configures the Communications Assistance for Law Enforcement Act (CALEA) MAC server settings.

Syntax

```
calea-mac import ftp-url  
calea-mac mac-address  
no calea-mac [mac-address]
```

Command Default

The CALEA MAC server is not configured

Parameters

import
Specifies that the MAC list is imported by FTP.

ftp-url
Specifies the FTP URL.

mac-address
Specifies the MAC address.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only.

The **no** form of the command deletes all CALEA MAC server configurations unless a MAC address is specified.

If you use the **import** keyword, enter the FTP URL in the following format: `ftp://username:password@ftp-host[/dir-path]`

Examples

The following example deletes all CALEA MAC server configuration.

```
device# config  
device(config)# no calea-mac
```

The following example specifies that the MAC list is imported by FTP

```
device# config  
device(config)# calea-mac import ftp://mahan:ruckus1!@172.19.7.100/backup/AP_ad87453456fe.csv
```

History

Release version	Command history
3.5.1	This command was introduced on the SmartZone 300.

calea-server-ip

Updates Calea server IP configurations.

Syntax

`calea-server-ip ip-address`
`no-calea-server-ip`

Command Default

Calea servers are not configured.

Parameters

ip-address
Specifies an IP address.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only.
The **no** form of the command deletes all Calea MAC server IP address configurations.

Examples

The following example configures a Calea MAC server with the IP address 10.1.1.1

```
device# config
device(config)# calea-server-ip 10.1.1.1
```

The following example deletes all Calea MAC server IP address configurations.

```
device# config
device(config)# no calea-server-ip
Do you want to continue to delete (or input 'no' to cancel)?
[yes/no]
```

History

Release version	Command history
3.5.1	This command was introduced on the SmartZone 300.

cert-store

Creates or updates certificate store configurations.

Syntax

cert-store [**ap-cert** *name* | **cert** *name* | **communicator-cert** *name* | **csr** *name* | **hotspot-cert** *name* | **web-cert** *name*]

no cert-store [**cert** *name* | **csr** *name*]

After the **cert** command is entered in global configuration mode to enable the Certification configuration mode, the following configuration syntax is available:

[**days** *text* | **inter-cert** *ftp-url* | **name** *name* | **passphrase** *passphrase* | **private-key** { **csr** *csr-name* | **upload** *ftp-url* } | **root-cert** *ftp-url* | **server-cert** *ftp-url*]

After the **csr** command is entered in global configuration mode to enable the CSR configuration mode, the following configuration syntax is available:

[**city** *city* | **common-name** *domain-name* | **country** *country* | **description** *text* | **email** *email-address* | **name** *name* | **organization** *org* | **state** *state* | **unit** *org-unit*]

Command Default

Certificate stores are not configured.

Parameters

ap-cert *name*

Specifies the AP Portal Certificate.

cert *name*

Creates or updates the Certificate configuration and enters Certification configuration mode.

communicator-cert *name*

Sets the Communicator Certificate.

csr *name*

Creates or updates the Certificates Signing Request (CSR) configuration.

hotspot-cert *name*

Sets the Set Hotspot Certificate.

days

Sets the expired days as 124-1098 or default (824). Valid only on default certificates only. Other configuration are ignored.

description *text*

Sets the certificate description.

inter-cert *ftp-url*

Uploads the Intermediate CA Certificate.

name *name*

Sets the certificate name.

passphrase *passphrase*

Sets the key passphrase.

Commands A through C

cert-store

web-cert *name*

Sets the Management Web Certificate.

private-key

Sets the Private key.

csr *csr-name*

Upload using CSR.

upload *ftp-url*

Upload a private key file using FTP.

root-cert *ftp-url*

Uploads a Root CA Certificate.

server-cert *ftp-url*

Uploads a server Certificate.

city *city*

Specifies a city.

common-name *domain-name*

Specifies the domain name.

country *country*

Specifies the country. Type a "?" for a full list of valid entries.

description *text*

Sets the description.

email *email-address*

Specifies the email address..

name *name*

Specifies the CSR name.

organization *org*

Sets the organization.

state *state*

Sets the state or province.

unit *org-unit*

Sets the organization unit.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

The **no cert-store cert** *name* command removes configured certificates.

The **no cert-store csr** *name* command removes CSR configurations.

Examples

The following example configures a certificate and enters Certification configuration mode.

```
device# config
device(config)# cert-store cert apcert
SZ100-Node1(config-cert)#
```

The following example configures a CSR and enters CSR configuration mode.

```
device# config
device(config)# cert-store csr
device(config)# cert-store csr csrpool
device(config-csr)#
```

The following example removes all configured certificates.

```
device# config
device(config)# no cert-store cert
Do you want to continue to delete (or input 'no' to cancel)? [yes/no] yes
```

The following example removes all configured CSRs.

```
device# config
device(config)# no cert-store csr
Do you want to continue to delete (or input 'no' to cancel)? [yes/no] yes
```

History

Release version	Command history
5.2.1	This command (config-cert-store) days was introduced.

changepassword

Changes the administrative password.

Syntax

changepassword

no changepassword

Command Default

The administrative password is not changed.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

The new password must contain at least eight characters with at least one number, one letter, and one special character (~ ! @ # \$ % ^ & * () - _ = + [] { } \ | ; : ' " , . < > / ?) except ` or \$(.

Examples

The following example changes the administrative password. The old password must be entered and the new password must be entered twice.

```
device# config
device(config)# changepassword
Old Password: *****
New Password: *****
Retype: *****
```

clock

Updates the system clock timezone configuration.

Syntax

clock*timezone**timezone*

Parameters

timezone*timezone*

Specifies the timezone for the system.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

For a full list of available timezones that can be entered using the *timezone*, enter the **timezone** and type a ?.

Examples

The following example sets the system timezone to that of Chicago in America.

```
device# config
device(config)# clock timezone America/Chicago
```

The following example sets the system timezone to that of Lisbon in Europe.

```
device# config
device(config)# clock timezone Europe/Lisbon
```

clone

Backs up the controller configuration and unique ID.

Syntax

Syntax

clone{**ftp** | **sftp**}*ip-address/path/[filename]**user-name**password*

clone**tftp***ip-address/path/[filename]*

Command Default

The controller configuration and unique ID is not cloned.

Parameters

ftp

Specifies an FTP server.

sftp

Specifies an SFTP server.

ip-address

Specifies the IP address of the server.

/path/

Specifies the path to the backup file.

filename

Specifies the file name.

user-name

Specifies the user name.

password

Specifies the password.

tftp

Specifies a TFTP server.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.

Enter the FTP/TFTP/SFTP URL in the following format: **ftp://tftp://sftp://ip-addresspathfilename**

A user name and password must be specified if you are using an FTP or SFTP server.

Examples

The following example backs up the controller configuration and unique ID, and specifies the TFTP URL, path, and file name.

```
device# clone tftp 10.0.0.10 /tmp/filename.bak
```

The following example backs up the controller configuration and unique ID, and specifies the TFTP URL and path. The file name will be automatically generated.

```
device# clone tftp 10.0.0.10 /tmp/
```

cluster in-service

Restores the cluster to a normal state.

Syntax

cluster in-service

Command Default

The cluster is not restored to a normal state.

Modes

Privileged EXEC mode

Examples

The following example restores the cluster to a normal state.

```
device# cluster in-service
```


cluster-ip-list

Updates the node IP address mapping list for the cluster configuration.

Syntax

cluster-ip-list *ip-mappings*

Command Default

The node IP address mapping list is not updated.

Parameters

ip-mappings

Specifies the node IP mapping list.

Modes

Global configuration mode

Usage Guidelines

A : must be entered between the old IP address and the new IP address.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example updates the node IP address mapping list for the cluster configuration. A : is entered between the old IP address and the new IP address. A space is entered between each entry.

```
device# config
device(config)# cluster-ip-list 172.19.18.96:172.19.13.56 172.19.15.67:172.19.10.07
```

cluster-redundancy

Creates or updates a cluster redundancy configuration.

Syntax

cluster-redundancy

After the **cluster redundancy** command is entered to enable the Cluster Redundancy configuration mode, the following configuration syntax is available:

[get-ap-keep-connected-timeout | get-mode | set-ap-keep-connected-timeout *timeout* | set-mode {backupname | monitor}]

Command Default

A cluster redundancy configuration is not created or updated.

Parameters

get-ap-keep-connected-timeout

Gets the AP keep connected timeout.

get-mode

Gets the redundancy mode of the standby cluster.

set-ap-keep-connected-timeout *timeout*

Sets the AP keep connected timeout in minutes. Valid values range from 10 through 720 minutes.

Modes

Global configuration mode

Usage Guidelines

The **get-mode** command gets the redundancy mode of the standby cluster. In monitor mode it indicates that the standby cluster does NOT serve any Active cluster and in backup mode it indicates that the standby cluster serves as an Active cluster. This command is supported on the SmartZone 300 and vSZ-H controllers only.

Examples

The following example enters Cluster Redundancy configuration mode.

```
device# cluster-redundancy
device(config-cluster-redundancy)
```

History

Release version	Command history
5.1	get-mode was added.

controller

Enters Controller configuration mode to configure the virtual data plane settings.

Syntax

controller

After the **controller** command is entered to enable the Controller configuration mode, the following configuration syntax is available:

[**history**|**ipip-address**|**logout**|**set_cert_chain**|**verify_cert_chain**]

no{**verify_cert_chain**}

Command Default

The virtual data plane settings are not altered.

Parameters

history

Displays the list of previously run commands.

ipip-address

Specifies an IP address.

logout

Logs the user out.

set_cert_chain

Sets the vSZ certificate chain.

verify_cert_chain

Verifies the vSZ certificate chain by the controller.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.

Examples

The following example enters Controller configuration mode and sets an IP address.

```
device# controller
device(config-controller)#
device(config-controller)# ip 10.1.1.1
The command was executed successfully. To save the changes, type 'end'.
device(config-controller)#
```

controller-description

Modifies or updates the controller description.

Syntax

controller-description *controller description*

Command Default

The controller description is not updated.

Parameters

controller description

Specifies the controller description.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example updates the controller description to "sz300.

```
device(config)# controller-description sz300
This command will restart some services. Do you want to continue (or input 'no' to cancel)? [yes/no]
```

copy

Copy files from an external FTP server.

copy *ftp-url* { **backup** | **backup-config** | **backup-network** }

Command Default

Files are not copied from external FTP servers.

Parameters

ftp-url

Specifies the FTP directory URL.

backup

Specifies the backup file.

backup-config

Specifies the backup configuration file.

backup-network

Specifies the network backup configuration file.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

When entering the FTP directory URL, use the following format: `ftp://<username>:<password>@<ftp-host>[/<dir-path>]`.

Examples

The following example copies the backup file from an external FTP server.

```
device# copy ftp://test:testpwd@172.17.22.11 backup
```

The following example copies the backup configuration file from an external FTP server.

```
device# copy ftp://test:testpwd@172.17.22.11 backup-config
```

The following example copies the network backup configuration file from an external FTP server.

```
device# copy ftp://test:testpwd@172.17.22.11 backup-network
```

copy ap-certificate-request

Copies the AP certificate request to an external FTP server.

Syntax

```
copy ap-certificate-request { all | new } ftp-url ]
```

Command Default

AP certificate requests are not copied to external FTP servers.

Parameters

- all**
Copies all AP certificate requests.
- new**
Copies specified AP certificate requests.
- ftp-url*
Specifies the FTP directory URL.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

When entering the FTP directory URL, use the following format: ftp://<username>:<password>@<ftp-host>[/<dir-path>].

Examples

The following example copies all AP certificate requests and specifies an external FTP server.

```
device# copy ap-certificate-request all ftp://test:testpwd@172.17.22.11
```

copy backup

Copies the backup file to an external TFTP or FTP server.

Syntax

```
copy backup tftp tftp-server-host
```

```
copy backup ftp-url
```

Command Default

Backup files are not copied to external TFTP or FTP servers.

Parameters

tftp *tftp-server-host*

Specifies a TFTP server.

ftp-url

Specifies the FTP directory URL.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

When entering the FTP directory URL, use the following format: `ftp://<username>:<password>@<ftp-host>[/<dir-path>]`.

Examples

The following example copies the backup file to a specified external FTP server.

```
device# copy backup ftp://test:testpwd@172.17.22.11
```

copy backup-config

Copy the backup configuration file to external TFTP or FTP server.

Syntax

```
copy backup-config tftp tftp-server-host  
copy backup-config ftp-url
```

Command Default

Backup configuration files are not copied to external TFTP or FTP servers.

Parameters

tftp *tftp-server-host*
Specifies a TFTP server.

ftp-url
Specifies the FTP directory URL.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

When entering the FTP directory URL, use the following format: ftp://<username>:<password>@<ftp-host>[/<dir-path>].

Examples

The following example copies the backup configuration file to a specified external FTP server.

```
device# copy backup-config ftp://Username:Password@<IP Address>/folder/  
device# copy backup-config ftp://test:testpwd@172.17.22.11/scg-config
```


copy backup-network

Copies the backup network configuration file to an external TFTP or FTP server

Syntax

```
copy backup-network tftp tftp-server-host
```

```
copy backup-network ftp-url
```

Command Default

Backup network configuration files are not copied to external TFTP or FTP servers.

Parameters

tftp *tftp-server-host*

Specifies a TFTP server.

ftp-url

Specifies the FTP directory URL.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

When entering the FTP directory URL, use the following format: ftp://<username>:<password>@<ftp-host>[/<dir-path>].

Examples

The following example copies the backup network configuration file to a specified external FTP server.

```
device# copy backup-network ftp://test:testpwd@172.17.22.11/scg-network
```

copy report-result

Copies a report result to an external FTP server.

Syntax

```
copy report-result name ftp-url
```

Command Default

Report results are not copied to external FTP servers.

Parameters

name

Specifies the name of the report.

ftp-url

FTP directory, FTP URL format: ftp://username:password@ftp-host[/dir-path]

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

When entering the FTP directory URL, use the following format: ftp://<username>:<password>@<ftp-host>[/<dir-path>].

Examples

The following example copies all AP certificate requests and specifies an external FTP server.

```
device# copy report-result Sytem ftp://test:testpwd@172.17.22.11
```

Commands D through F

data-plane

Updates data plane configurations.

Syntax

data-plane *name* **forward-stp**

no data-plane *name* **forward-stp**

Command Default

Data plane configurations are not updated.

Parameters

name

Specifies a data plane.

forward-stp

Enables the STP package bridge.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes a data plane and disables the STP package bridge. This command is supported on the SmartZone 300 and vSZ-H controllers only.

Examples

The following example configures the data plane settings and enables the STP package bridge.

```
device# configure
device(config)# data-plane
device(config)# data-plane KKK-SZ300-D0 forward-stp

Successful operation
```

data-plane

Retrieves data plane information and enters debug data-plane configuration mode.

Syntax

data-plane *name*

After the **data-plane** *name* command is entered to enable debug data-plane configuration mode, the following configuration syntax is available:

```
[ show summary | show detail | dp arp | dp arp summary | dp flow fid id | dp flow filter | dp flow summary | dp fpa | dp gretun tid id |  
  dp gretun summary | dp host all | dp host summary | dp macs | dp macs summary | dp misc | dp route show | dp route summary  
  | dp route summary | dp sysctl | ping | route | uptime ]
```

Command Default

Data plane information is not retrieved

Parameters

show summary

Displays dataplane summarized information.

show detail

Displays detailed dataplane information.

dp arp

Displays datacore ARP table information.

dp arp summary

Displays datacore ARP table summarized information.

dp flow fid *id*

Displays datacore flow entry.

dp flow filter

Adds datacore flow filter.

dp flow summary

Displays datacore flow table summary.

dp fpa

Displays the datacore FPA table.

dp gretun tid *id*

Displays datacore GRE tunnel entries.

dp gretun summary

Displays summarized datacore GRE tunnel table information.

dp host all

Displays datacore host table information.

dp host summary

Displays summarized datacore host table summary information.

dp macs

Displays the datacore MAC table.

dp macs summary

Displays summarized datacore MAC table information.

dp misc

Datacore misc commands.

dp route show

Displays datacore routing entries.

dp route summary

Displays summarized datacore routing table information.

dp sysctl

Datacore control commands.

route

Displays linux routing table information.

Uptime

Displays the time the system has been up.

Modes

Debug configuration mode

Usage Guidelines

This command is supported on the SmartZone 100 and SmartZone 300.

Examples

The following example enters debug data-plane configuration mode.

```
device(debug)# data-plane dp
device(debug-data-plane)#
```

Commands D through F
debug

debug

Enters debug configuration mode.

Syntax

debug

Command Default

Debug configuration mode is not configured.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all the controllers including the SmartZone Data Plane.

Examples

The following example enters debug configuration mode.

```
device# debug  
device(debug)#
```

debug-tools

Enables debug CLI framework.

Syntax

debug-tools

Command Default

Displays system and debug framework commands.

Modes

Debug configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms.

Examples

```
device# debug
device(debug)# debug-tools
[Change to system]
Welcome to Debug CLI Framework!
(debug tool-set) system $ ?
Debug Tools (system):
Command          Help
=====
collectd-start   collectd-start
collectd-status  collectd-status
collectd-stop    collectd-stop
disable-upgrade-recovery disable upgrade recovery for one time
enable-code-coverage enable code coverage
enable-upgrade-recovery enable upgrade recovery (default enabled)
system-performance system performance qualification(CPU/IO)
upload-code-coverage upload code coverage report to SONAR

Debug framework commands:
=====
exit  help  show  use
```

Commands D through F
delete backup

delete backup

Deletes backup files.

Syntax

delete backup

Command Default

Backup files are not deleted.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example deletes backup files.

```
device# delete backup
```


delete backup-config

Deletes backup configuration files.

Syntax

```
delete backup-config
```

Command Default

Backup configuration files are not deleted.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example deletes backup configuration files.

```
device# delete backup-config
```

delete backup-network

Deletes backup network configuration files.

Syntax

```
delete backup-network
```

Command Default

Backup network files are not deleted.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example deletes backup network files.

```
device# delete backup-network
```

delete client

Deletes specified AP clients.

Syntax

delete client *client-mac*

Command Default

AP clients are not deleted.

Parameters

client-mac

Specifies the Client MAC address.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example deletes and AP client with the Client MAC address "A1:87:45:34:56:FE"

```
device# delete client A1:87:45:34:56:FE
```

dhcp

Creates or sets the Dynamic Host Configuration (DHCP) server configuration settings.

Syntax

dhcp [*pool-name*]

After the **dhcp***pool-name* command is entered to enable DHCP configuration mode, the following configuration syntax is available:
[**dhcp-log-syslog level value value** | **show** [**stats** | **summary**]]

Command Default

A DHCP sever pool is not configured.

Parameters

pool-name

Specifies a DHCP file.

dhcp-log-syslog level level

Specifies that DHCP events are sent to the Syslog server. Valid values range from 1 through 7.

show stats

Displays DHCP statistical information.

show summary

Displays summarized DHCP information.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.

Examples

The following example enters DHCP configuration mode.

```
device# config
device(config)# dhcp
device(config-dhcp)#
```

The following example specifies that DHCP events are sent to the Syslog server and specifies a value of 7.

```
device# config
device(config)# dhcp
device(config-dhcp)# dhcp-log-syslog value 7
```

The following example configures a DHCP server pool.

```
device> config
device(config)# dhcp mypool
device(config-dhcp-pool mypool)#
```

dhcp-relay

Enables Dynamic Host Configuration (DHCP) relay.

Syntax

dhcp-relay

no dhcp-relay

After the **dhcp-relay** command is entered, the following configuration syntax is available:

```
{ dhcp-option82 | dhcp-server1 server-name | dhcp-server2 server-name }
```

After the **dhcp-option82** command is entered, the following configuration syntax is available:

```
{ subopt1 } { ap-ssid | ap-info-default | ap-info-location | ap-mac | format }
```

subopt150

```
subopt151 { ssid area-name area-name }
```

```
subopt2 { ap-ssid | ue-ssid | ue-mac | ap-mac }
```

Command Default

DHCP relay is not enabled.

Parameters

dhcp-option82

Enables DHCP Option82.

subopt1

Enables Subopt-1.

ap-ssid

Uses the Access Point (AP) MAC hex ESSID.

ap-info-default

Uses the default AP information in the following format: IF-Name:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC.

ap-info-location

Uses the AP location information in the following format: IF-Name:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC:Location.

ap-mac

Uses the AP MAC in the following format: AP-MAC-hex.

format

Uses the specified format.

subopt150

Enables Subopt-1.

subopt151

Enables Subopt-1.

subopt2
Enables Subopt-1.

dhcp-server1
Sets DHCP server 1

dhcp-server2
Sets DHCP server 1

Modes

TTG PDG Profile configuration mode

Domain configuration mode

Zone configuration mode

Usage Guidelines

This command is used in several different configuration modes.

This command is supported on all the controllers in zone and domain configuration mode. In TTG PDG Profile configuration mode, only the SmartZone 300 supports this command.

Examples

The following example creates a TTG PDG profile named newprofile123 and configures DHCP relay with DHCP Option82 parameters.

```
device# config
device(config)# ttg-pdg-profile newprofile123
device(config-ttg-pdg-profile)# dhcp-relay
device(config-ttg-pdg-profile)# dhcp-option82
device(config-ttg-pdg-profile-dhcp-option82)# subopt1 ap-ssid
```

The following example disables DHCP Relay when in the Zone configuration mode.

```
device(config-zone)# no dhcp-relay
Do you want to continue to disable (or input 'no' to cancel)? [yes/no] yes
Successful operation
```

diag

Enables the running of diagnostic commands.

Syntax

```
diag { cfgfwd | cfgwlan | cfg3rdwlan | dp_comm | dp_cia_client | ps | tbldump | top | tunnelmgr_cli | tunnelmgr_client_cli }
```

Command Default

Diagnostic commands are not run.

Parameters

- cfgfwd**
Specifies forwarding configuration information.
- cfgwlan**
Specifies WLAN information.
- cfg3rdwlan**
Specifies 3rd WLAN information.
- dp_comm**
Specifies that all command supported by the data plane are listed.
- dp_cia_client**
Specifies CIA client information.
- ps**
Specifies PS information.
- tbldump**
Specifies Table dump
- top**
Specifies detailed user information.
- tunnelmgr_cli**
Specifies that the tunnel manager set of commands is displayed.
- tunnelmgr_client_cli**
Specifies tunel manger client command line interface.

Modes

Debug configuration mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.

Examples

The following example displays the tunnel manager set of commands.

```
device> debug
device(debug)# diag tunnelmgr_cli
Usage: tunnelmgr_cli [-d -D] {-a | -c | {-g all|<tun_id>|global|cb} | {-s cert_check <enable/disable>}
| {-t <secs>} | {-r <secs>} | {-v <enable/disable>}}
  -a -- Add a tunnel table entry
  -c -- Clear all tunnel table information
  -g all|global|cb|<tun_id> -- Get information for all valid entries,
                             for specified tunnel entry, or for global data,
                             for tunnelmgr cb
  -s cert_check <enable/disable> > -- Set , certificate velidation on/off
  -t <secs> -- Set garbage collection timeout interval (seconds)
  -k <secs> -- Set cleanup interval based on heartbeat interval (seconds)
  -l <0~7> -- Set log level of tunnelmgr
  -r <secs> -- Calculate average RX/TX bit/pkt rates within the seconds you sepcify
  -v <enable/disable> -- Enable/Disable certificate vilidation
  -v -- verbose, show more information
  -V -- Very verbose, show all detailed information
```

diagnostic

Enters Diagnostic configuration mode.

Syntax

diagnostic

The following configuration syntax are available in the **diagnostic** configuration mode:

```
[ application-log-level | application-log-level-all { debug | error | info | warn } | copy snapshot ftp-url | delete snapshot | execute { all | all-full | case } | show { cases case | ipmi { health | sel | sensors } | snapshot | version } | trigger-ap-binary-log ap-mac | trigger-trap { all | multi-trap | remote-packet-capture-disable | remote-packet-capture-enable source ip address} ]
```

Command Default

Diagnostic commands are not executed.

Parameters

application-log-level

Sets the log level of an application.

application-log-level-all

Sets the log level for all applications.

debug

Sets the log level to debug.

error

Sets the log level to error.

info

Sets the log level to information.

warn

Sets the log level to warning.

copy snapshot *ftp-url*

Copy snapshot to an external FTP server.

delete snapshot

Delete all snapshots.

execute

Get a snapshot.

all

Gets the snapshot with the current running system and all application logs.

all-full

Gets the snapshot of the current running system and all application logs. It also includes rotated or archived logs.

case

Gets the snapshot for a specified case.

showcases *case*

Displays information for a specified case.

showipmi

Shows IPMI information.

health

Specifies BMC basic health.

sel

Specifies system event log records.

sensors

Specifies hardware sensors, fru, LEDs information.

showsnapshot

Show snapshot files.

show version

Shows version.

show version

Shows version.

trigger-ap-binary-log *ap-mac*

Shows .

trigger-trap

Specifies trigger testing traps.

all

Specifies all traps.

multi-trap

Specific traps, separated by a comma.

remote-packet-capture disable

Disables remote packet capture

remote-packet-capture enable

Enable remote packet capture with IP of the capture tool server.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

The **show ipmi health** and **show ipmi sel** parameters are supported for SmartZone 300 only.

Examples

The following example disables the **remote-packet-capture**.

```
device# diagnostic
device(diagnostic)# remote-packet-capture disable
1
0
successfully stop rpcapd
```

The following example enables the **remote-packet-capture**

```
dhcp-10-206-84-138(diagnostic)# remote-packet-capture enable
Please input the source IP address that is going to capture packet: 165.198.0.1
0
0
successfully start rpcapd
```

The following example deletes all snapshots.

```
device# diagnostic
device(diagnostic)# delete snapshot
Do you want to continue to delete (or input 'no' to cancel)? [yes/no]
```

The following example gets a snapshot with the current running system and all application logs.

```
device# diagnostic
device(diagnostic)# execute allLoading common/_DEFAULT.conf ...
```

diagnostic

Enters Debug diagnostic configuration mode to enable the running of diagnostic script management commands.

Syntax

diagnostic

After the **diagnostic** command is entered to enable Debug Diagnostic configuration mode, the following configuration syntax is available:

```
[ delete script-name | execute script-name parameters | no schedule script-name cron-time-spec | schedule script-name cron-time-spec |
show { diagnostic script script-name | schedule } | upload ftp-url ]
```

Command Default

Diagnostic script management commands are not executed.

Parameters

delete *script-name*

Deletes a diagnostic script.

execute

Executes a diagnostic script.

script-name

Specifies a script.

parameters

Specifies script parameters.

no schedule

Schedule a script to run.

cron-time-spec

Specifies the time specification.

schedule

Schedule a script to run.

cron-time-spec

Specifies the time specification.

show

Show scripts.

diagnostic-script *script-name*

Specifies diagnostic scripts.

schedule

Specifies schedule scripts.

upload *ftp-url*

Uploads a diagnostic script from remote FTP server.

Commands D through F
diagnostic

Modes

Debug configuraiton mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example enters Debug diagnostic configuraiton mode and deletes a script.

```
device> debug
device(debug)# diagnostics
device(debug-diagnostic) delete myscript

Do you want to continue to delete (or input 'no' to cancel)? [yes/no]
```

diameter-system-wide

Enters the diameter-system-wide configuration mode to set diameter system wide configurations.

Syntax

diameter-system-wide

After the **diameter-system-wide***name* command is entered to enter diameter-system-wide configuration mode, the following configuration syntax is available:

[**local-host-name** *name* | **local-realm-name** *name* | **peer-timeout** *time* | **retry-timeout** *time* | **watch-dog-timeout** *time*]

Command Default

Diameter system wide settings are not configured.

Parameters

local-host-name *name*

Sets the local host name.

local-realm-name *name*

Sets the local realm name.

peer-timeout *time*

Updates the peer expiry time in seconds.

retry-timeout *time*

Updates the connection retry time in seconds.

watch-dog-timeout *time*

Updates the device watch dog time in seconds.

Modes

Configuration mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only.

Examples

The following example enters diameter system wide configuration mode.

```
device> config
device(config)# diameter-system-wide
device(config-diameter-system-wide)#
```

dns-server-service

Enters DNS server services configuration mode to create or update DNS server services.

Syntax

dns-server-service [*name*]

no dns-server-service *name*

After the **dns-server-service***name* command is entered to enable DNS server services configuration mode, the following configuration syntax is available:

[**description** *description* | **name** *dns-server-name* | **primary-ip** *ip-address* | **secondary-ip** *ip-address*]

no [**description** *description* | **primary-ip** *ip-address* | **secondary-ip** *ip-address*]

Command Default

DNS server services are not configured.

Parameters

name

DNS server service name.

description *description*

Sets the DNS server service description.

name *dns-server-name*

Sets the DNS server service name.

primary-ip *ip-address*

Sets the primary IP.

secondary-ip *ip-address*

Sets the secondary IP.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

The **no** form of the command deletes all DNS server services or a specified DNS server service.

Examples

The following example enters DNS server service and creates a name for the DNS server service.

```
device> config
device(config)# dns-server-service
device(config-dns-server-service)# name myserver
```

The following example deletes a configured DNS server service.

```
device> config
device(config)# no dns-server-service myserver
Do you want to continue to delete (or input 'no' to cancel)? [yes/no] yes
```

The following example deletes all configured DNS server services.

```
device> config
device(config)# no dns-server-service
Do you want to continue to delete (or input 'no' to cancel)? [yes/no] yes
```

domain

Creates or updates the domain configuration.

Syntax

domain *name*

After the **domain***name* command is entered to enable the domain configuration mode, the following configuration syntax is available:

[**description** *description* | **name** *name* | **parent** *name* | **zone** *zone-name*]

Command Default

Domain configurations are not created or updated.

Parameters

name

Specifies the domain name.

description *description*

Sets a description for the domain.

name *name*

Sets the domain name.

parent *name*

Sets the parent domain name.

zone *name*

Specifies an AP zone of a domain.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only.

Examples

The following example enters domain configuration mode.

```
device# config
device(config)# domain mydomain
device(config-domain)#
```

Related Commands

- [Table 8](#) lists the related **domain** configuration commands.

- [Table 9](#) lists the related **domain-zone** configuration commands.
- [Table 10](#) lists the related **domain-zone-aaa** configuration commands.
- [Table 11](#) lists the related **domain-zone-ap-group** configuration commands.
- [Table 12](#) lists the related **domain-zone-ap-snmp** configuration commands.
- [Table 13](#) lists the related **domain-zone-ap-group-lldp** configuration commands.
- [Table 15](#) lists the related **domain-zone-ap-model** configuration commands.
- [Table 16](#) lists the related **domain-zone-ap-model-lan1** configuration commands.
- [Table 17](#) lists the related **domain-zone-ap-registration-rule** configuration commands.
- [Table 18](#) lists the related **domain-zone-block-client** configuration commands.
- [Table 19](#) lists the related **domain-zone-bonjour-fencing-policy** configuration commands.
- [Table 27](#) lists the related **domain-zone-bonjour-policy-rule** configuration commands.
- [Table 22](#) lists the related **domain-zone-client-isolation-whitelist** configuration commands.
- [Table 25](#) lists the related **domain-zone-bonjour-policy** configuration commands.
- [Table 28](#) lists the related **domain-zone-device-policy** configuration commands.
- [Table 29](#) lists the related **domain-zone-device-policy rule** configuration commands.
- [Table 19](#) lists the related **domain-zone-ethernet-port-profile** configuration commands.
- [Table 32](#) lists the related **domain zone-guest-access** configuration commands.
- [Table 33](#) lists the related **domain-zone-hotspot** configuration commands.
- [Table 37](#) lists the related **domain-zone-l2-acl** configuration commands.
- [Table 39](#) lists the related **domain-zone-web-authentication** configuration commands.
- [Table 40](#) lists the related **domain-zone-wechat** configuration commands.
- [Table 41](#) lists the related **domain-zone-wlan-group** configuration commands.
- [Table 42](#) lists the related **domain-zone-wlan-scheduler** configuration commands.

TABLE 8 Commands related to config-domain)

Syntax and Type	Parameters (if any)	Description
device(config-domain)# admin	<i>username</i> <i>rolename</i>	Adds an administrator and assign a role in the current domain.
device(config-domain)# no	<i>admin</i> < <i>username</i> > <i>zone</i> < <i>name</i> >	Disables and deletes command configuration.
device(config-domain)# parent	<i>name</i>	Sets the parent domain name.
device(config-domain)# zone	<i>name</i> : AP zone name <i>nametemplatename</i> : Create from template <i>nameclonename</i> : Clone from an existing AP zone <i>nameap-firmwareap-firmware</i> : Change AP firmware <i>namecluster-switch-overname</i> : Enable cluster switchover	Create or update an AP zone in the current domain.
device(config-domain)# zone-zd	<i>ap-firmwareimportftp-url</i>	Create AP zone from ZD backup file.

TABLE 9 Commands related to device(config-domain-zone)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone)# aaa	<i>name</i>	Creates or updates the AAA server configuration.
device(config-domain-zone)# adj-threshold	2.4g { <i>value</i> } 5g { <i>value</i> } Value is minimum = 1 and maximum = 100	Sets the adjacent radio threshold of the client load balancing.
device(config-domain-zone)# ap-firmware	<i>ap-firmware</i>	Sets the AP firmware.
device(config-domain-zone)# ap-group	<i>name</i>	Creates or updates the AP group configuration.
device(config-domain-zone)# ap-ip-mode	[ipv4 ipv6 dual]	Sets the AP IP mode to either IPv4 or IPv6.
device(config-domain-zone)# ap-logon	<i>logon-id</i>	Sets the login ID for the AP administrator.
device(config-domain-zone)# ap-mgmt-vlan	<i>lvlanTag</i> : VLAN Tag (1-4094); enter 'keep' to keep APs setting.	Sets the AP management VLAN.
device(config-domain-zone)# ap-model	<i>name</i>	Sets the AP model configuration.
device(config-domain-zone)# ap-password		Sets the password for the AP administrator.
device(config-domain-zone)# ap-ping-latency-interval	<i>enable</i> <i>disable</i>	Sets the AP latency detection by enabling or disabling the AP ping.
device(config-domain-zone)# ap-reboot-timeout	default-gateway [<i>hours and minutes</i>] : Sets the default gateway timeout in hours and minutes. control-interface <i>hours</i> : Sets the control interface timeout in hours.	Sets the AP reboot timeout.
device(config-domain-zone)# ap-registration-rule	<i>priority</i>	Creates or updates the AP registration rule configuration.
device(config-domain-zone)# ap-snmp-options		Sets the AP SNMP options.
device(config-domain-zone)# background-scan	2.4g <i>seconds</i> 5g <i>seconds</i>	Sets the background scanning.
device(config-domain-zone)# band-balancing	2.4gint2.4g 2.4G band <i>int</i> : Percentage of clients on 2.4G band	Sets the band balance.
device(config-domain-zone)# block-client	<i>mac</i> : Client MAC Address	Sets to block clients.
device(config-domain-zone)# bonjour-gateway		Enables the bonjour gateway.
device(config-domain-zone)# bonjour-policy	<i>name</i>	Creates or updates the bonjour policy.
device(config-domain-zone)# channel	2.4g <i>channel</i> 5g indoor <i>channel</i> 5g outdoor <i>channel</i>	Sets the channel.
device(config-domain-zone)# channel-evaluation-interval	<i>seconds</i> : The interval value (Range: 60~3600 sec)	Sets the channel evaluation interval.
device(config-domain-zone)# channel-range	2.4g [<i>channel</i> all] 5g indoor [<i>channel</i> all] 5g outdoor [<i>channel</i> all]	Sets the channel range.
device(config-domain-zone)# channel-select-mode	2.4g { <i>value</i> } 5g { <i>value</i> }	Set a mode to automatically adjust AP channels.

TABLE 9 Commands related to device(config-domain-zone) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone)# channelfly-mtbc	2.4g number: MTBC value (Range: 100~1440) 5g number	Sets the MTBC value of ChannelFly.
device(config-domain-zone)# channelization	2.4g [20 40] 5g [40 20]	Sets the channelization.
device(config-domain-zone)# client-admission-control	2.4g 5g 2.4g minClientCountminClientCount 2.4g maxRadioLoadmaxRadioLoad 2.4g minClientThroughputminClientThroughput 5g minClientCountminClientCount 5g maxRadioLoadmaxRadioLoad 5g minClientThroughputminClientThroughput	Enables the client admission control.
device(config-domain-zone)# client-isolation-whitelist	name: Client isolation whitelist name	Creates or updates the client isolation whitelist.
device(config-domain-zone)# country-code	country-code	Sets the country code.
device(config-domain-zone)# description	text	Sets the description,
device(config-domain-zone)# device-policy	name	Sets the device policy.
device(config-domain-zone)# dfs-channel		Enable DFS channels for the US country code.
device(config-domain-zone)# diffserv	name	Creates or updates the diff server profile.
device(config-domain-zone)# dos-protection	dosBarringPeriod : DoS protection period dosBarringThreshold : DoS protection threshold dosBarringCheckPeriod : DoS protection checkperiod	Enables DoS (Denial-of-service) protection.
device(config-domain-zone)# ethernet-port-profile	name:Ethernet Port Profile name.	Sets the Ethernet Port profile.
device(config-domain-zone)# gps	latitudelongitude	Displays the help.
device(config-domain-zone)# gps-altitude	altitude[floor meters] altitude value floor meters	Sets the GPS altitude.
device(config-domain-zone)# guest-access	name	Sets the guest access.
device(config-domain-zone)# headroom	2.4g client 5g : 5 GHz radio	Sets the headroom (# of clients) of client load balancing.
device(config-domain-zone)# hotspot	name	Creates or updates the WISPr hotspot configuration.
device(config-domain-zone)# hotspot20-venue-profile	name	Creates or updates the venue profile for hotspot release 2 configuration.
device(config-domain-zone)# hotspot20-wlan-profile	name	Creates or updates the WLAN profile for hotspot release 2 configuration.
device(config-domain-zone)# indoor-channel		Enables the indoor channels.
device(config-domain-zone)# ipsec-profile	profile-name	Sets the IPsec profile.

TABLE 9 Commands related to device(config-domain-zone) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone)# ipsec-tunnel-profile	<i>value</i>	Sets the IPsec Tunnel Profile.
device(config-domain-zone)# l2-acl	<i>name</i>	Sets the layer 2 access control list.
device(config-domain-zone)# lbs		Enables the location based service.
device(config-domain-zone)# lbs-service		Sets the location based service.
device(config-domain-zone)# load-balancing	2.4g 5g	Sets the client load balancing.
device(config-domain-zone)# location	<i>text</i>	Sets the location.
device(config-domain-zone)# location-additional-info	<i>text</i>	Sets the additional information location.
device(config-domain-zone)# mesh		Enables mesh networking.
device(config-domain-zone)# mesh-name	<i>name</i>	Sets the mesh name (ESSID).
device(config-domain-zone)# mesh-passphrase	<i>mesh-passphrase</i>	Sets the mesh passphrase.
device(config-domain-zone)# move	domainname	Moves the zone to another domain.
device(config-domain-zone)# node-affinity-profile	<i>profile-name</i>	Sets the node affinity profile
device(config-domain-zone)# protection-mode	2.4g <i>value</i>	Overrides the protection mode on 2.4 GHz radio
device(config-domain-zone)# recovery-ssid-enabled	disable	Overrides the enable recovery SSID broad case.
device(config-domain-zone)# rks-gre-profile	profile-name	Sets the AP Ruckus GRE tunnel profile.
device(config-domain-zone)# roam	2.4g 5g	Sets the smart roam.
device(config-domain-zone)# roam-macfilt-time	2.4g <i>seconds (0-600)</i> 5g <i>seconds (0-600)</i>	Sets the smart roam MAC filter time in seconds. The default value is 15 seconds. This configuration is only available at the Zone level.
device(config-domain-zone)# rogue-ap-detection	[disable enable] : Disables or enables rogue access points report-all[disable enable] : Enables or disables all rogue devices report-only-malicious[enable disable] : Enables or disables only malicious rogue device types report-ssid-spoofing [disable enable] : Enables or disables malicious rogue devices which have SSID spoofing	Sets the report rogue access point.
device(config-domain-zone)# secondary-channel	5g indoor [<i>Secondary channel</i>] 5g outdoor [<i>Secondary channel</i>]	Sets the secondary channel.
device(config-domain-zone)# smart-mon	intervalvalue thresholdvalue	Sets the smart monitor interval.
device(config-domain-zone)# smart-roam-disconnect-event		Enables smart roam disconnect event.
device(config-domain-zone)# soft-gre-profiles	<profile-name> <profile-name> <profile-name> - Select the first, second and third SoftGRE tunnel profile <profile-name> <profile-name> - Select the first and second SoftGRE tunnel profile <profile-name> - Select the first SoftGRE tunnel profile	Sets AP SoftGRE tunnel profiles

TABLE 9 Commands related to device(config-domain-zone) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone)# syslog-enabled		Enables the external syslog server for APs for the specified zone.
device(config-domain-zone)# syslog-facility	[Local6 Keep Original Local0 Local5 Local7 Local1 Local4 Local3 Local2]	Sets the syslog server facility,
device(config-domain-zone)# syslog-ip	ip	Sets the IP address for the syslog server.
device(config-domain-zone)# syslog-ip6	ipv6	Sets the IPv6 address for the syslog server.
device(config-domain-zone)# syslog-port	port	Sets the port number for the syslog server.
device(config-domain-zone)# syslog-priority	[Alert Info Critical Warning Notice Emergency All Error]	Sets the syslog server priority.
device(config-domain-zone)# timezone	<p>System : Follows the controller time zone setting</p> <p>System[time zone]</p> <p>Select the time zone from system database</p> <p>User-defined[time zone abbr.]</p> <p>User defined time zone</p> <p>Time zone abbreviation (example: GMT, CST, EST)</p>	Sets the timezone for zone.
device(config-domain-zone)# timezone-dst	[Start End] orderweekdaymonthhour	Sets the user defined timezone for daylight savings.
device(config-domain-zone)# timezone-gmt-offset	[hour hour:] minute: For example, 8, -7:45	Sets the user defined timezone for GMT offset.
device(config-domain-zone)# tunnel-profile	profile-name	Sets the AP GRE tunnel profile.
device(config-domain-zone)# tunnel-type	[gre gre-udp]	Sets the tunnel type.
device(config-domain-zone)# tx-power	<p>2.4g\${value}</p> <p>5g\${value}</p> <p>Value is minimum = 1 and maximum = 100</p>	Sets the TX power adjustment.
device(config-domain-zone)# usb-software	uploadftp-url	Sets the AP USB software package.
device(config-domain-zone)# venue-code	codeVenue Code	Sets the venue code.
device(config-domain-zone)# venue-profile	name	Sets the venue profile.
device(config-domain-zone)# vlan-overlapping		Enables the overlapping of VLAN pooling.
device(config-domain-zone)# vlan-pooling	name	Creates or updates the VLAN pooling profile.
device(config-domain-zone)# weak-bypass	<p>2.4g\${value}</p> <p>5g\${value}</p> <p>Value is minimum = 1 and maximum = 100</p>	Sets the weak bypass threshold of the client load balancing.
device(config-domain-zone)# web-authentication	name	Sets the web authentication.
device(config-domain-zone)# wechat	name: WeChat name	Create/update WeChat configuration.
device(config-domain-zone)# wlan	name	Creates or updates the WLAN/ ESSID configuration.
device(config-domain-zone)# wlan-group	name	Creates or updates the WLAN group configuration.
device(config-domain-zone)# wlan-scheduler	name	Creates or updates the WLAN scheduler configuration.

TABLE 10 Commands related device(config-domain-zone-aaa)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-aaa)# admin-domain		Enables the admin domain name.
device(config-domain-zone-aaa)# admin-domain-name	<i>admin-domain</i>	Creates or updates the admin domain.
device(config-domain-zone-aaa)# admin-password	<i>admin-password</i>	Creates or updates the admin password.
device(config-domain-zone-aaa)# backup	ip <i>ip</i> ipv6 <i>ipv6</i> port <i>port</i> shared-secret <i>shared-secret</i>	Enables backup of RADIUS support and set related settings.
device(config-domain-zone-aaa)# base-domain	<i>base-domain</i>	Set the base domain.
device(config-domain-zone-aaa)# description	<i>description</i>	Sets the description.
device(config-domain-zone-aaa)# global-catalog		Enables the global catalog support.
device(config-domain-zone-aaa)# ip	<i>ip</i>	Set IP addresses of primary RADIUS server.
device(config-domain-zone-aaa)# ipv6	<i>ipv6</i>	Set IPv6 addresses of primary RADIUS server.
device(config-domain-zone-aaa)# key-attribute	<i>key-attribute</i>	Sets the key attributes for the primary RADIUS server.
device(config-domain-zone-aaa)# password	<i>password</i>	Sets the password for the primary RADIUS server.
device(config-domain-zone-aaa)# port	<i>port</i>	Sets the port number of the primary RADIUS server.
device(config-domain-zone-aaa)# search-filter	<i>search-filter</i>	Sets the search filter.
device(config-domain-zone-aaa)# shared-secret	<i>shared-secret</i>	Sets the shared secret of the primary RADIUS server.
device(config-domain-zone-aaa)# test	<i>usernamepassword</i> [PAP CHAP]	Tests the RADIUS server based on the user credentials and protocol settings.
device(config-domain-zone-aaa)# test-acct		Tests the accounting server.
device(config-domain-zone-aaa)# type	[radius radius-acct LDAP AD]	Sets the RADIUS type.
device(config-domain-zone-aaa)# windows-domain	<i>windows-domain</i>	Sets the windows domain name.

TABLE 11 Commands related to device(config-domain-zone-ap-group)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-ap-group)# ani-ofdm-level	<i>ap-mode</i> : AP model name	Sets the AP adaptive noise immunity level for specific AP model.
device(config-domain-zone-ap-group)# channel		
device(config-domain-zone-ap-group)# channel	2.4g <i>{value}</i> 5g indoor <i>{value}</i> 5g outdoor <i>{value}</i>	Sets the channel.
device(config-domain-zone-ap-group)# channel-evaluation-interval	<i>seconds</i> : The interval value (60~3600 secs)	Sets the channel evaluation interval.
device(config-domain-zone-ap-group)# channel-range	2.4g [<i>channels</i> all]: 2.4GHz radio 5g indoor [<i>channels</i> all]: 5GHz radio 5g outdoor [<i>channels</i> all]: 5GHz radio	Set channel range.
device(config-domain-zone-ap-group)# channel-select-mode	2.4g <i>{value}</i> : 2.4GHz radio 5g <i>{value}</i> : 5GHz radio	Automatically adjusts the AP channels.

TABLE 11 Commands related to device(config-domain-zone-ap-group) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-ap-group)# channelfly-mtbc	2.4g <i>{number}</i> : 2.4GHz radio <i>number</i> : MTBC value range:100-1440 5g <i>{number}</i> : 5Hz radio <i>number</i> : MTBC value range:100-1440	Set MTBC value of Channelfly.
device(config-domain-zone-ap-group)# channelization	2.4g [20 40] 5g [40 20]	Sets the channelization.
device(config-domain-zone-ap-group)# client-admission-control	2.4g 5g 2.4g <i>minClientCount</i> <i>minClientCount</i> Min Client Count (Default: 10) 2.4g <i>maxRadioLoad</i> <i>maxRadioLoad</i> Max Radio Load (Default: 75%)	Enables the client admission control.
device(config-domain-zone-ap-group)# client-admission-control	2.4g <i>minClientThroughput</i> <i>minClientThroughput</i> : Min Client Throughput (Default: 0.0Mbps) 5g <i>minClientCount</i> <i>minClientCount</i> Min Client Count (Default: 20) 5g <i>maxRadioLoad</i> <i>maxRadioLoad</i> Max Radio Load (Default: 75%) 5g <i>minClientThroughput</i> <i>minClientThroughput</i> : Min Client Throughput (Default: 0.0Mbps)	Enables the client admission control.
device(config-domain-zone-ap-group)# description	<i>text</i>	Sets the description.
device(config-domain-zone-ap-group)# external-antenna	<i>ap-model</i> 5g[disable enable] <i>ap-model</i> 5g <i>gain</i> <i>gain</i> <i>ap-model</i> 2.4g <i>gain</i> <i>gain</i> <i>ap-model</i> 2.4g[enable disable] <i>ap-model</i> g <i>gain</i> <i>gain</i> <i>ap-model</i> [disable enable] <i>ap-model</i> 2.4g[3-antennas 2-antennas] <i>ap-model</i> 5g[3-antennas 2-antennas]	Sets the external antenna for specific AP model.
device(config-domain-zone-ap-group)# gps	<i>latitude</i> <i>longitude</i>	Displays the help.
device(config-domain-zone-ap-group)# gps-altitude	<i>altitude</i> [floor meters]	Sets the GPS altitude.
device(config-domain-zone-ap-group)# internal-heater	<i>ap-model</i> [enable disable]	Sets the internal heater for specific AP model.
device(config-domain-zone-ap-group)# lbs		Enables the location based service.
device(config-domain-zone-ap-group)# lbs-service		Sets the location based service.
device(config-domain-zone-ap-group)# led-mode	<i>ap-model</i>	Sets the LED mode for specific AP model.

TABLE 11 Commands related to device(config-domain-zone-ap-group) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-ap-group)# lldp	<i>ap-model</i> [enable disable]	Sets the LLDP for a specific AP model.
device(config-domain-zone-ap-group)# location		Sets the location.
device(config-domain-zone-ap-group)# location-additional-info	<i>text</i>	Sets the additional information location.
device(config-domain-zone-ap-group)# member	addap-mac move-toapgroup-nameap-mac removemac	Sets the AP group member. It adds a new access point to current AP group. The AP Mac address removes the access point from the current AP group and moves it to other AP group.
device(config-domain-zone-ap-group)# no	ani-ofdm-level channel2.4g channel5gindoor channel5goutdoor channel-evaluation-interval channel-select-mode channel-range channelization2.4g channelization5g client-admission-control description external-antennaap-model5g external-antennaap-model2.4g gps internalheater lbs led-mode lldp location location-additional-info	Disables / deletes the configuration settings.

TABLE 11 Commands related to device(config-domain-zone-ap-group) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-ap-group)# no	override-ap-mgmt-vlan override-channel-select-mode override-client-admission-control override-lbs override-zone-location override-zone-location-additional-info poe-operating-mode poe-out port-setting radio-band recovery-ssid status-leds tx-power2.4g tx-power 5g usb-port usb-software venue-profile wlan-group2.4g wlan-group5g	Disables / deletes the configuration settings.
device(config-domain-zone-ap-group)# override-ap-mgmt-vlan	<i>vlanTag</i>	Overrides the AP Management VLAN.
device(config-domain-zone-ap-group)# override-channel-select-mode	2.4g 5g	Overrides auto channel selection mode and ChannelFly MTBC.
device(config-domain-zone-ap-group)# override-client-admission-control	2.4g 5g	Overrides the client admission control settings.
device(config-domain-zone-ap-group)# override-lbs		Overrides the location based service to zone settings.
device(config-domain-zone-ap-group)# override-zone-location		Overrides the zone location setting.
device(config-domain-zone-ap-group)# override-zone-location-additional-info		Overrides the zone location additional information setting.
device(config-domain-zone-ap-group)# poe-operating-mode	<i>ap-model</i> : AP model name	Switches the PoE Operating Mode for specific AP model
device(config-domain-zone-ap-group)# poe-out	<i>ap-model</i> [enable disable]	Sets the PoE out port for a specific AP model.
device(config-domain-zone-ap-group)# port-setting	<i>ap-model</i>	Sets the port settings for specific AP model.
device(config-domain-zone-ap-group)# protection-mode	2.4g \${value}	Overrides the protection mode on 2.4 GHz radio
device(config-domain-zone-ap-group)# radio-band	<i>ap-model</i> [2.4g 5g]	Switches the radio band for a specific AP model.
device(config-domain-zone-ap-group)# recovery-ssid-enabled	disable	Overrides the enable recovery SSID broad case.
device(config-domain-zone-ap-group)# status-leds	<i>ap-model</i> [enable disable]	Sets the status LED for specific AP model.

TABLE 11 Commands related to device(config-domain-zone-ap-group) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-ap-group)# tx-power	2.4g {value} 5g {value}	Sets the TX power adjustment.
device(config-domain-zone-ap-group)# usb-port	ap-model[disable enable]	Sets the USB port for a specific AP model.
device(config-domain-zone-ap-group)# usb-software	ap-model:AP model name	Sets AP USB software package for a specific AP model
device(config-domain-zone-ap-group)# venue-profile	name: Venue profile	Sets the venue profile.
device(config-domain-zone-ap-group)# wlan-group	2.4g 5g	Sets the WLAN group configurations.

TABLE 12 Commands related to device(config-domain zone-ap-snmp configuration)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-ap-snmp)# ap-snmp		Enables AP SNMP.
device(config-domain-zone-ap-snmp)# no	ap-snmp snmp-v2-community name snmp-v3-username	Disables the settings that have been configured with these commands.
device(config-domain-zone-ap-snmp)# snmp-v2-community	name: Community name	Adds or updates the AP SNMPV2 community.
device(config-domain-zone-ap-snmp)# snmp-v3-user	name: User name	Adds or updates the AP SNMPV3 user.

TABLE 13 Commands related to device(config-domain-zone-ap-group lldp)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-ap-group-lldp)# lldp-ad-interval	seconds	Sets the LLDP advertise interval in seconds from the range 1 to 300.
device(config-domain-zone-ap-group-lldp)# lldp-hold-time	seconds	Sets the LLDP hold time in seconds from the range 60 to 1200.
device(config-domain-zone-ap-group-lldp)# lldp-mgmt		Enables the LLDP management IP TLV.

TABLE 14 Commands related to device(config-domain-zone-ap-group-port-setting)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-ap-group-port-setting)# dot1x	authsvr [Authenticator Server Name] accsvr name mac-auth-bypass [true false] supplicant user-name[user name password password] supplicant mac	Sets the 802.1x role

TABLE 14 Commands related to device(config-domain-zone-ap-group-port-setting) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-ap-group-port-setting)# lan	<i>port</i> <i>portuplink[general access trunk]</i> <i>portuntagvlan</i> <i>portmembervlan-members</i> <i>portdot1x[auth-mac-based disabled auth-port-based supplicant]</i>	Enables or disable specific port.
device(config-domain-zone-ap-group-port-setting)# no	dot1xaccsvr lanport	Disables or deletes the configuration settings.

TABLE 15 Commands related to device(config-zone-ap-model)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-ap-model)# ext-ant	2.4gnumber 2.4gnumber[3 2] 5gnumber 5gnumber[2 3]	Sets the external antenna.
device(config-domain-zone-ap-model)# internal- heater		Enables international heater.
device(config-domain-zone-ap-model)# lan1 device(config-domain-zone-ap-model)# lan2 device(config-domain-zone-ap-model)# lan3 device(config-domain-zone-ap-model)# lan4 device(config-domain-zone-ap-model)# lan5		Sets the LAN configurations from 1 to 5.
device(config-domain-zone-ap-model)# led		Enables the status of led.
device(config-domain-zone-ap-model)# led-mode		Sets the led mode description
device(config-domain-zone-ap-model)# lldp		Enables the Link Layer Discovery Protocol (LLDP).
device(config-domain-zone-ap-model)# lldp-ad- interval	<i>seconds</i>	Sets the LLDP advertise interval.
device(config-domain-zone-ap-model)# lldp-hold-time	<i>seconds</i>	Sets the LLDP hold time.
device(config-domain-zone-ap-model)# lldp-mgmt		Enables the LLDP management IP TLV.

TABLE 15 Commands related to device(config-zone-ap-model) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-ap-model)# no	ext-ant internal-heater lan1 lan2 lan3 lan4 lan5 led lldp lldp-mgmt poe-operating-mode poe-out-port radio-band usb-port usb-software	Disables or deletes the settings that have been configured.
device(config-domain-zone-ap-model)# poe-operating-mode	<i>\${value}</i>	Switches the PoE mode
device(config-domain-zone-ap-model)# poe-out-port		Enables the PoE out port
device(config-domain-zone-ap-model)# radio-band	<i>\${value}</i>	Switches the radio band for a specific AP model.
device(config-domain-zone-ap-model)# usb-port		Enables USB port.
device(config-domain-zone-ap-model)# usb-software		Sets AP USB software package.

TABLE 16 Commands related to device(config-domain-zone-ap-model-lan1)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-ap-model-lan1)# 8021x	<i>8021x-type</i>	Sets the 802.1x.
device(config-domain-zone-ap-model-lan1)# acct-service	<i>acct-service</i>	Sets the accounting service configurations.
device(config-domain-zone-ap-model-lan1)# auth-service	<i>auth-service</i>	Sets the authentication service configurations.
device(config-domain-zone-ap-model-lan1)# mac-bypass		Sets the MAC authentication bypass.
device(config-domain-zone-ap-model-lan1)# members	<i>members</i>	Sets the members.
device(config-domain-zone-ap-model-lan1)# no	acct-service mac-bypass	Disables or deletes the settings that have been configured.
device(config-domain-zone-ap-model-lan1)# profile	<i>profile</i> : Ethernet Port profile	Sets the Ethernet Port profile.
device(config-domain-zone-ap-model-lan1)# supplicant	mac <i>customusernamepassword</i>	Sets the supplicant.
device(config-domain-zone-ap-model-lan1)# type	[trunk-port access-port general-port]	Sets the port type.
device(config-domain-zone-ap-model-lan1)# vlan-untag-id	<i>vlan-untag-id</i>	Sets the VLAN untag ID.

TABLE 17 Commands related to device(config-domain-zone-ap-registration-rule)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-ap-registration-rule)# description	text	Sets the description.
device(config-domain-zone-ap-registration-rule)# gps	latitudelongitudedistance	Sets the GPS coordinates.
device(config-domain-zone-ap-registration-rule)# ip-range	ipip	Sets the IP address range from and to IP address.
device(config-domain-zone-ap-registration-rule)# provision-tag	tag	Sets the provision tags.
device(config-domain-zone-ap-registration-rule)# subnet	ipmask	Sets the subnet IP address and subnet mask.
device(config-domain-zone-ap-registration-rule)# type	[gps provision-tag ip-range subnet]	Sets the rule type.

TABLE 18 Commands related to device(config-domain-zone-block-client)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-block-client)# description	text	Sets the description.

TABLE 19 Commands related to device(config-domain-zone-bonjour-fencing-policy)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone- bonjour-fencing-policy)# description	text	Sets the description.
device(config-domain-zone- bonjour-fencing-policy)# no	description rule <i>rule index</i>	Sets to delete sub commands.
device(config-domain-zone- bonjour-fencing-policy)# rule	<i>index: rule index</i>	Sets the bonjour fencing rule.

TABLE 20 Commands related to device(config-domain-zone-bonjour-policy-rule)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-bonjour-policy-rule)# description	text	Sets the description.
device(config-domain-zone-bonjour-policy-rule)# no	rule <i>rule index</i>	Sets to delete sub commands.
device(config-domain-zone-bonjour-policy-rule)# rule	<i>index: rule index</i>	Sets the bonjour fencing rule.

TABLE 21 Commands related to device(config-domain-zone-bonjour-fencing-policy-rule)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-bonjour-fencing-policy-rule)# closest-ap	<text>	Sets the configuration to the closest AP.
device(config-domain-zone-bonjour-fencing-policy-rule)# description	<text>	Sets the description.
device(config-domain-zone-bonjour-fencing-policy-rule)# device-mac-list	#{value}	Lists the devices, which use MAC address.
device(config-domain-zone-bonjour-fencing-policy-rule)# device-type		Sets the device type.

TABLE 21 Commands related to device(config-domain-zone-bonjour-fencing-policy-rule) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-bonjour-fencing-policy-rule)# fence-range		Sets the fence range.
device(config-domain-zone-bonjour-fencing-policy-rule)# no	<i>device-mac-list</i>	Disables the configuration.
device(config-domain-zone-bonjour-fencing-policy-rule)# service-type		Sets the service type.

TABLE 22 Commands related to device(config-zone-domain-client-isolation-whitelist)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-client-isolation-whitelist)# auto		Enables the auto whitelist. Each entry must have an IP address in order to enable auto whitelist.
device(config-domain-zone-client-isolation-whitelist)# description	<i>text</i>	Sets the description.
device(config-domain-zone-client-isolation-whitelist)# entry	<i>index</i> : entry index	Sets the client isolation entry.
device(config-domain-zone-client-isolation-whitelist)# no	auto description entry	Sets to delete sub command

TABLE 23 Commands related to device(config-domain-zone-ap-snmp-options-snmp-v2-community configuration)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-ap-snmp-options-snmp-v2-community)# no	notification notification-target read snmp-v2-communityname snmp-v3-username write	Disables the settings that have been configured with these commands.
device(config-domain-zone-ap-snmp-options-snmp-v2-community)# notification		Enable notification privilege
device(config-domain-zone-ap-snmp-options-snmp-v2-community)# notification-target		Enable notification target configuration commands.
device(config-domain-zone-ap-snmp-options-snmp-v2-community)# notification-type		Sets the notification type
device(config-domain-zone-ap-snmp-options-snmp-v2-community)# read		Enable the read privilege.
device(config-domain-zone-ap-snmp-options-snmp-v2-community)# write		Enable the write privilege.

TABLE 24 Commands related to device(config-domain-zone-ap-snmp-options-snmp-v3-user configuration)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-ap-snmp-options-snmp-v3-user)# auth		Sets SNMPv3 user authentication.

TABLE 24 Commands related to device(config-domain-zone-ap-snmp-options-snmp-v3-user configuration) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-ap-snmp-options-snmp-v3-user)# no	notification notification-target read write snmp-v3-username	Disables the settings that have been configured with these commands.
device(config-domain-zone-ap-snmp-options-snmp-v3-user)# notification		Enable notification privilege.
device(config-domain-zone-ap-snmp-options-snmp-v3-user)# notification-target		Enable notification target configuration commands.
device(config-domain-zone-ap-snmp-options-snmp-v3-user)# notification-type		Sets the notification type
device(config-domain-zone-ap-snmp-options-snmp-v3-user)# privacy	none desprivacy-phrase : DES privacy phrase.	Set SNMPv3 user privacy.
device(config-domain-zone-ap-snmp-options-snmp-v3-user)# read		Enable the read privilege.
device(config-domain-zone-ap-snmp-options-snmp-v3-user)# write		Enable the write privilege.

TABLE 25 Commands related to device(config-domain-zone-bonjour-policy)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-bonjour-policy)# description	<i>text</i>	Sets the description.
device(config-domain-zone-bonjour-policy)# no rule	<i>priority</i>	Deletes the rules based on the rule priority.
device(config-domain-zone-bonjour-policy)# rule	<i>priority</i>	Sets the bonjour policy set of rules based on the rule priority.

TABLE 26 Commands related to device(config-domain-zone-bonjour-fencing-policy-rule)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-bonjour-fencing-policy-rule)# closest-ap	<text>	Sets the configuration to the closest AP.
device(config-domain-zone-bonjour-fencing-policy-rule)# description	<text>	Sets the description.
device(config-domain-zone-bonjour-fencing-policy-rule)# device-mac-list	#{value}	Lists the devices, which use MAC address.
device(config-domain-zone-bonjour-fencing-policy-rule)# device-type		Sets the device type.
device(config-domain-zone-bonjour-fencing-policy-rule)# fence-range		Sets the fence range.
device(config-domain-zone-bonjour-fencing-policy-rule)# no	<i>device-mac-list</i>	Disables the configuration.
device(config-domain-zone-bonjour-fencing-policy-rule)# service-type		Sets the service type.

TABLE 27 Commands related to device(config-domain-zone-bonjour-policy-rule)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-bonjour-policy-rule)# bridge-service	airdisk airplay airport-management airprint airtunes apple-file-sharing apple-mobile-devices (Allows sync with iTunes over Wi-Fi) appletv icloud-sync itunes-remote itunes-sharing open-directory-master optical-disk-sharing other screen-sharing secure-file-sharing secure-shell workgroup-manager www-http www-https xgrid	Sets the bridge service.
device(config-domain-zone-bonjour-policy-rule)# from-vlan	<i>int</i>	Sets the from VLAN.
device(config-domain-zone-bonjour-policy-rule)# notes	<i>int</i>	Sets the notes.
device(config-domain-zone-bonjour-policy-rule)# protocol		Sets the bridge service when it is 'other'.
device(config-domain-zone-bonjour-policy-rule)# to-vlan	<i>int</i>	Sets the VLAN.

TABLE 28 Commands related to device(config-domain-zone-device-policy)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-device-policy)# default-action	[allow block]	Sets the default action to either allow or block.
device(config-domain-zone-device-policy)# description	<i>text</i>	Sets the description.
device(config-domain-zone-device-policy)# do		Executes the do command.
device(config-domain-zone-device-policy)# no policy-rule	<i>Device Type</i>	Deletes the device policy rules.
device(config-domain-zone-device-policy)# policy-rule		Sets the device policy.

TABLE 29 Commands related to ruckus (config-domain-zone-device-policy-policy rule)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-device-policy-policy-rule)# action	[allow block]	Sets the default action to either allow or block.
device(config-domain-zone-device-policy-policy-rule)# description	<i>text</i>	Sets the description.
device(config-domain-zone-device-policy-policy-rule)# downlink	[<i>Rate Limiting</i>] Rate limiting (mbps)	Sets the downlink rate limiting.
device(config-domain-zone-device-policy-policy-rule)# no vlan		Resets the VLAN number.
device(config-domain-zone-device-policy-policy-rule)# type	[<i>Device Type</i>]	Sets the device type.
device(config-domain-zone-device-policy-policy-rule)# uplink	[<i>Rate Limiting</i>] Rate limiting (mbps)	Sets the uplink rate limiting.
device(config-domain-zone-device-policy-policy-rule)# vlan	[<i>VLAN Number</i>]	Sets the VLAN number.

TABLE 30 Commands related to device(config-domain-zone-diffserv)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-diffserv)# description	<i>text</i>	Sets the description.
device(config-domain-zone-diffserv)# downlink-diffserv	<i>value</i>	Enables the tunnel diffserv downlink and sets the diffserv number.
device(config-domain-zone-diffserv)# no	description downlink-diffserv preserved-diffserv uplink-diffserv	Disables various options.
device(config-domain-zone-diffserv)# preserved-diffserv	<i>value</i>	Adds the preserved diffserv number.
device(config-domain-zone-diffserv)# uplink-diffserv	<i>value</i>	Enables the tunnel diffserv uplink and sets the diffserv number.

TABLE 31 Commands related to device(config-domain-ethernet-port-profile)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-ethernet-port-profile)# 8021x	<i>text</i>	Sets the 802.1x.
device(config-domain-zone-ethernet-port-profile)# 8021x-enable		Enable 802.1x
device(config-domain-zone-ethernet-port-profile)# acct-service	<i>acct-service</i>	Sets the accounting service.
device(config-domain-zone-ethernet-port-profile)# auth-service	<i>auth-service</i>	Sets the authentication service.
device(config-domain-zone-ethernet-port-profile)# client-visibility		Enables client visibility regardless of 802.1X authentication
device(config-domain-zone-ethernet-port-profile)# dvlan		Enables the dynamic VLAN.
device(config-domain-zone-ethernet-port-profile)# guest-vlan	<i>guest-vlan-id</i>	Enables the dynamic guest VLAN.

TABLE 31 Commands related to device(config-domain-ethernet-port-profile) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-ethernet-port-profile)# mac-bypass		Enables the MAC authentication bypass.
device(config-domain-zone-ethernet-port-profile)# no	8021x-enable acct-service client-visibility dvlan mac-bypass proxy-acct proxy-auth tunnel	Disables various options.
device(config-domain-zone-ethernet-port-profile)# proxy-acct		Enables proxy accounting service.
device(config-domain-zone-ethernet-port-profile)# proxy-auth		Enables proxy authentication service.
device(config-domain-zone-ethernet-port-profile)# supplicant	mac - MAC IP address customusername password	Sets the supplicant.
device(config-domain-zone-ethernet-port-profile)# tunnel		Enables tunnel.
device(config-domain-zone-ethernet-port-profile)# type		Sets the port type.
device(config-domain-zone-ethernet-port-profile)# vlan-members	<i>vlan-members</i>	Sets the VLAN members.
device(config-domain-zone-ethernet-port-profile)# vlan-untag-id	<i>vlan-untag-id</i>	Sets the VLAN members.

TABLE 32 Commands related to ruckus (config-zone-guest-access)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-guest-access)# description	<i>text</i>	Sets the description.
device(config-domain-zone-guest-access)# do		Executes the do command.
device(config-domain-zone-guest-access)# enable-terms-and-conditions		Enables the web portal terms and conditions.
device(config-domain-zone-guest-access)# grace-period	<i>minutes</i>	Sets the grace period.
device(config-domain-zone-guest-access)# language		Sets the language.
device(config-domain-zone-guest-access)# logo	<i>ftp-url</i> FTP URL, format: <i>ftp://username:password@ip/file-path</i>	Sets the logo.
device(config-domain-zone-guest-access)# name	<i>name</i>	Sets the guess access service name.
device(config-domain-zone-guest-access)# no	enable-terms-and-conditions sms-gateway terms-and-conditions	Disables the various options.
device(config-domain-zone-guest-access)# session-timeout	<i>minutes</i>	Sets the session timeout as per the specified minutes.

TABLE 32 Commands related to ruckus (config-zone-guest-access) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-guest-access)# sms-gateway		Sets the guest pass for the SMS gateway.
device(config-domain-zone-guest-access)# start-page	original redirect <i>start-url</i>	Sets the start page.
device(config-domain-zone-guest-access)# terms-and-conditions		Sets the terms and conditions for the web portal.
device(config-domain-zone-guest-access)# title		Sets the title for the web portal.

TABLE 33 Commands related to device(config-domain-zone-hotspot)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-hotspot)# description	<i>text</i>	Sets the description.
device(config-domain-zone-hotspot)# do		Executes the do command.
device(config-domain-zone-hotspot)# grace-period	<i>minutes</i>	Sets the grace period.
device(config-domain-zone-hotspot)# https-redirect	<i>enable</i>	If enabled, the AP tries to redirect the HTTPS requests to the hotspot portal.
device(config-domain-zone-hotspot)# language		Sets the portal language.
device(config-domain-zone-hotspot)# location-id	<i>location-id</i>	Sets the location ID.
device(config-domain-zone-hotspot)# location-name	<i>name</i>	Sets the location name.
device(config-domain-zone-hotspot)# logo	<i>ftp-url</i>	Sets the logo.
device(config-domain-zone-hotspot)# logon-url	internal external <i>logon-url</i>	Sets the logon model
device(config-domain-zone-hotspot)# mac-address-format		Sets the MAC address format.
device(config-domain-zone-hotspot)# no	https-redirect show-terms-conditions walled-garden <i>walled-garden-list:</i> Allows unauthorized destinations. Comma-separated IP, IP range, CIDR and regular expression domain name list.	Disables the commands.
device(config-domain-zone-hotspot)# session-timeout	<i>minutes</i>	Sets the sessions timeout.
device(config-domain-zone-hotspot)# show-terms-conditions		Shows the terms and conditions.
device(config-domain-zone-hotspot)# smart-client-support	none enable only <i>instructions</i>	Sets the smart client support.
device(config-domain-zone-hotspot)# start-page	original <i>start-url</i>	Sets the start page.
device(config-domain-zone-hotspot)# terms-conditions	redirect	Sets the terms and conditions.
device(config-domain-zone-hotspot)# title	<i>title</i>	Sets the title.
device(config-domain-zone-hotspot)# walled-garden	<i>walled-garden-list</i>	Enables Walled Garden. Allows unauthorized destinations. Comma-separated IP, IP range, CIDR and regular expression domain name list

TABLE 34 Commands related to device(config-domain-zone-hotspot20-venue-profile)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-hotspot20-venue-profile)# description	text	Sets the description.
device(config-domain-zone-hotspot20-venue-profile)# do		Executes the do command.
device(config-domain-zone-hotspot20-venue-profile)# no	venue-names wan-at-capacity wan-sym-link	Disables the commands.
device(config-domain-zone-hotspot20-venue-profile)# venue-category	unspecifiedunspecified assembly [coffee-shop passenger-terminal restaurant bar arena library place-of-worship emergencycoordination-center museum stadium convention-center unspecified amphitheater amusement-park theater zoo-or-aquarium] business [unspecified on attorney-office professional-office research-and-development-facility doctor-ordentist-office fire-station post-office bank] educational [unspecified school-primary university-or-college school-secondary]	Sets the venue category
device(config-domain-zone-hotspot20-venue-profile)	factory-and-industrial [factory] institutional [hospital group-home unspecified prison-or-jail long-term-care-facility alcohol-and-drugrehabilitation-center] mercantile [grocery-market automotive-service-station unspecified retail-store gas-station shopping-mall] residential [unspecified private-residence hotel-or-motel dormitory boarding-house] storage unspecified utility-and-miscellaneous unspecified vehicular [train airplane ferry a bus motor-bike unspecified ship-or-boat] outdoor [unspecified city-park bus-stop traffic-control rest-area muni-mesh-network kiosks]	Sets the venue category.
device(config-domain-zone-hotspot20-venue-profile)# venue-names	<i>languagenames</i>	Sets the venue-names.
device(config-domain-zone-hotspot20-venue-profile)# wan-at-capacity		Sets the WAN capacity.
device(config-domain-zone-hotspot20-venue-profile)# wan-downlink-load	<i>downlink-load</i> : Load between 1 and 255	Sets the WAN downlink load.

TABLE 34 Commands related to device(config-domain-zone-hotspot20-venue-profile) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-hotspot20-venue-profile)# wan-downlink-speed	<i>speed</i>	Sets the WAN downlink speed in (kbps).
device(config-domain-zone-hotspot20-venue-profile)# wan-link-status	[link-up link-test link-down]	Sets the link status.
device(config-domain-zone-hotspot20-venue-profile)# wan-load-duration	<i>duration</i>	Sets the load measurement duration.
device(config-domain-zone-hotspot20-venue-profile)# wan-sym-link		Enables symmetric link.
device(config-domain-zone-hotspot20-venue-profile)# wan-uplink-load	<i>uplink-load</i>	Sets the WAN uplink load.
device(config-domain-zone-hotspot20-venue-profile)# wan-uplink-speed	<i>speed</i> : Uplink speed in kbps	Sets the WAN uplink speed.

TABLE 35 Commands related to device(config-domain-zone-hotspot20-wlan-profile)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-hotspot20-wlan-profile)# access-network-type		Sets the access network type.
device(config--domain-zone-hotspot20-wlan-profile)# asra		Sets the ASRA profile.
device(config--domain-zone-hotspot20-wlan-profile)# asra-dns-redirect	<i>url</i>	Sets the ASRA DNS redirection.
device(config--domain-zone-hotspot20-wlan-profile)# asra-http-redirect		Sets the ASRA HTTP redirection.
device(config--domain-zone-hotspot20-wlan-profile)# asra-online-signup	<i>ssid</i>	Sets the ASRA online signup.
device(config--domain-hotspot20-wlan-profile)# asra-terms-conditions	<i>url</i>	Sets the ASRA terms and conditions.
device(config--domain-zone-hotspot20-wlan-profile)# connect-capabilities	[pptp http voip-6 ipsec-vpn ikev2 ftp tls voip-17 icmp ssh esp][open unknown closed]	<p>Sets the connection capabilities.</p> <p>pptp: Protocol Number:6 Port:1723 Protocol Name: Used by PPTP VPNs</p> <p>http: Protocol Number:6 Port:80 Protocol Name: HTTP</p> <p>voip-6: Protocol Number:6 Port:5060 Protocol Name: VoIP</p> <p>ipsec-vpn: Protocol Number:17 Port:4500 Protocol Name: IPSec VPN</p> <p>ikev2: Protocol Number:17 Port:500 Protocol Name: Used by IKEv2(IPSec VPN)</p> <p>tls: Protocol Number:6 Port:443 Protocol Name: Used by TLS VPN</p> <p>voip-17: Protocol Number:17 Port:5060 Protocol Name: VoIP</p> <p>icmp: Protocol Number:1 Port:0 Protocol Name: ICMP</p>

TABLE 35 Commands related to device(config-domain-zone-hotspot20-wlan-profile) (continued)

Syntax and Type	Parameters (if any)	Description
device(config--domain-zone-hotspot20-wlan-profile)# connect-capabilities	[pptp http voip-6 ipsec-vpn ikev2 ftp tls voip-17 icmp ssh esp][open unknown closed]	ssh: Protocol Number:6 Port:22 Protocol Name: SSH esp: Protocol Number:50 Port:0 Protocol Name: ESP open: Open unknown: Unknown closed: Closed
device(config--domain-zone-hotspot20-wlan-profile)# cust-connect-capabilities	<i>protocol-name</i> <i>protocol-number</i>	Creates or updates the custom connection capabilities.
device(config--domain-zone-hotspot20-wlan-profile)# description	<i>text</i>	Sets the description.
device(config-domain-zone-hotspot20-wlan-profile)# identity-providers	<i>identityProvider</i> default	Sets the identity providers.
device(config-domain-zone-hotspot20-wlan-profile)# internet-option	enable	Enables the specified WLAN with Internet connectivity.
device(config-domain-zone-hotspot20-wlan-profile)# ipv4-address	[port-restrict-address single-nated-private-address double-nated-private-address port-restricted-address double-nated-address unknown public-address port-restricted-address-single-nated-address not-available]	Sets the IPv4 address.
device(config-domain-zone-hotspot20-wlan-profile)# ipv6-address	[not-available unknown available]	Sets the IPv6 address.
device(config-domain-zone-hotspot20-wlan-profile)# name	<i>name</i>	Sets the hotspot 2.0 WLAN profile name.
device(config-domain-zone-hotspot20-wlan-profile)# no	asra asra-dns-redirect asra-http-redirect asra-online-signup asra-terms-conditions cust-connect-capabilities identity-providers internet-option	Disables the commands.
device(config-domain-zone-hotspot20-wlan-profile)# operator	<i>name</i>	Sets the operator name.

TABLE 36 Commands related to device(config-domain-zone-hotspot20-wlan-profile-cust-connect-capabilities)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-hotspot20-wlan-profile-cust-connect-capabilities)# port	<i>port</i>	Set the port number.
device(config-domain-zone-hotspot20-wlan-profile-cust-connect-capabilities)# protocol	<i>protocol</i>	Sets the protocol number.
device(config-domain-zone-hotspot20-wlan-profile-cust-connect-capabilities) status	[closed unknown open]	Sets the status.

TABLE 37 Commands related to device(config-domain-zone-l2-acl)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-l2-acl)# action	[allow block]	Sets the handling action to allow or block.
device(config-domain-zone-l2-acl)# description	text	Sets the description.
device(config-domain-zone-l2-acl)# mac	`\${value}`	Sets the MAC value.
device(config-domain-zone-l2-acl)# no mac	`\${value}`	Disables the MAC value.

TABLE 38 Commands related to device(config-domain-zone-vlan-pooling)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-vlan-pooling)# algo	mac-hash	Sets the algorithm.
device(config-domain-zone-vlan-pooling)# description	text	Sets the description.
device(config-domain-zone-vlan-pooling)# do		Executes the do command.
device(config-domain-zone-vlan-pooling)# no	description pooling	Disables various option
device(config-domain-zone-vlan-pooling)# pooling	rangestart-valueend-value : VLAN range singlevalue : Single VLAN ID	Adds the VLAN pooling.

TABLE 39 Commands related to ruckus (config-domain-zone-web-authentication)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-web-authentication)# description	text	Sets the description.
device(config-domain-zone-web-authentication)# grace-period	minutes	Sets the grace period.
device(config-domain-zone-web-authentication)# language		Sets the language.
device(config-domain-zone-web-authentication)# session-timeout	minutes	Sets the session timeout as per the specified minutes.
device(config-domain-zone-web-authentication)# start-page	original redirectstart-url	Sets the start page.

TABLE 40 Commands related to device(config-domain-zone-wechat)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-wechat)# authentication-url	text	Sets the authentication URL.
device(config-domain-zone-wechat)#	text	Sets the black list.
device(config-domain-zone-wechat)#	text	Sets the description.
device(config-domain-zone-wechat)# dnat-destination	text	
device(config-domain-zone-wechat)# dnat-port-mapping	sourcedest	Sets the DNAT destination.
device(config-domain-zone-wechat)# do		Executes the do command.
device(config-domain-zone-wechat)# grace-period	minutes	Set the grace period as minutes.
device(config-domain-zone-wechat)# no	dnat-port-mapping white-list	Disables various options.

TABLE 40 Commands related to device(config-domain-zone-wechat) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-wechat)# white-list	<i>white-list</i> : Allow unauthorized destinations. Comma- separated IP, IP range, CIDR and regular expression domain name list.	Sets the white list.

TABLE 41 Commands related to device(config-domain-zone-wlan-group).

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-wlan-group)# description	<i>text</i>	Sets the description,
device(config-domain-zone-wlan-group)# do		Executes the do command.
device(config-domain-zone-wlan-group)# no	wlanname	Disables or removes WLAN from this group.
device(config-domain-zone-wlan-group)# wlan	<i>namevlanvlanTagnasidnasid</i> <i>namenasidnasidvlanvlanTag</i> <i>namevlanvlanTag</i> <i>namenasidnasid</i> <i>namevlan-poolingvlanPooling</i> <i>namevlan-poolingvlanPoolingnasid</i> <i>name</i>	Sets a WLAN in this group or overrides VLAN setting.

TABLE 42 Commands related to ruckus (config-domain-zone-wlan-scheduler)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-wlan-scheduler)# description	<i>text</i>	Sets the description,
device(config-domain-zone-wlan-scheduler)# no	description schedule-data [<i>weekday</i> <i>empty</i>] [<i>start time value</i> <i>empty</i>] [<i>end time value</i>] <i>\${weekday}</i>	Disables the commands.
device(config-domain-zone-wlan-scheduler)# schedule-data	[<i>weekday</i> <i>empty</i>][<i>start time value</i> <i>empty</i>][<i>end time value</i>] <i>\${weekday}</i>	Sets the schedule table.

dp-customized-config

Sets customized data plane configuration commands.

Syntax

dp-customized-config { *all* | *name* } *commandStr*

no dp-customized-config { *all* | *name* } *commandStr*

Command Default

Customized data plane configuration commands are not set.

Parameters

all

Specifies all data planes.

name

Specifies a data plane.

commandStr

Specifies all customized configurations.

Modes

Debug configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

The **no** form of the command disables customized data plane configuration commands.

Examples

The following example sets customized data plane configuration commands for a specified data plane.

```
device# debug
device(debug)# dp-customized-config NODE201-D1 string
```

The following disables customized data plane configuration commands for a all data planes.

```
device# debug
device(debug)# no dp-customized-config all
```

dp-group

Creates or updates the virtual SmartZone dataplane (vSZ-D) zone affinity profile configuration.

Syntax

dp-group *profile-name*

no dp-group *profile-name*

After the **enable** command is entered to allow the outbound traffic, the following configuration syntax is available:

```
{ allow-sess-on-acct-fail | auth token | cache-cleanup | ecgi-in-gtpv2-msg | error | error-message | expiration-interval | fast-reauth |  
gtp-nsapi | gtpv2-interface-type | host ip-address | imei-ie-in-gtp-msg | ip ip-address | ip-rule | local-host-name | local-network-  
indicator | local-realm-name | mcc country-code | mnc country-code | name SCI-profile-name | nat-ip-translation | ndc | password  
password | pasv-port | pattern pattern | peer-timeout seconds | policy | port port | read | retry-timeout | scg-rai-in-gtpv2-msg |  
scg-sai-in-gtpv2-msg | secret eap-sim-key | shared-secret secret-key | system-idsystem-id | tai-in-gtpv2-msg | test | type type |  
unit threshold | user user | user-id-privacy user-id-priv | value threshold-value | watch-dog-timeout seconds | write }
```

Command Default

No dp-group configuration is created or updated.

Parameters

profile-name

dp-group profile name.

allow-sess-on-acct-fail

Allows session on accounting fail.

auth

Sets SNMPv3 user authentication.

cache-cleanup

Enables cache cleanup setting.

ecgi-in-gtpv2-msg

Includes ECGI in GTPv2 messages.

error *number*

Sets the error code. Number from 2 to 5.

error-message *errmsg*

Sets the error message text.

expiration-interval *interval*

Sets the expiration interval using one of the following keywords: **day**, **hour**, **month**, **never**, **week**, **year**.

fast-reauth

Enables fast reauthentication support.

gtp-nsapi *number*

Sets the GTP Network Service Access Point Identifier (NSAPI).

gtpv2-interface-type *number*

Sets the GTPv2 interface type.

host *ip-address*

Sets the IP address of the host.

imei-ie-in-gtp-msg

Includes the IMEI IE in GTP messages.

ip *ip-address*

Sets the IP address of the primary RADIUS server.

local-host-name

Updates the local host name.

local-network-indicator

Sets the local network indicator.

local-realm-name

Updates the local realm name.

mcc *country-code*

Sets the mobile country code. Three-digit number.

mnc *network-code*

Sets the mobile network code. Three-digit number.

name *sci-prof-name*

Sets the SCI profile name.

nat-ip-translation

Enables network address translation (NAT) in FTP passive mode.

ndc *ndc-code*

Sets the network destination code.

password *password*

Sets the password.

pasv-port *password*

Sets the dynamic data transmission port range.

pattern *pattern*

Sets the user agent pattern.

peer-timeout *seconds*

Updates the peer expiry time, in seconds.

policy *seconds*

Sets the ALC policy.

port *port*

Sets the port.

read

Enables read privilege.

retry-timeout *seconds*

Updates the connection retry time, in seconds.

Commands D through F

dp-group

scg-rai-in-gtpv2-msg

Includes SCG-RAI in GTPv2 messages.

scg-sai-in-gtpv2-msg

Includes SCG-SAI in GTPv2 messages.

secret *EAP-SIM-key*

Sets the EAP-SIM secret key.

shared-secret *secret-key*

Sets the shared secret key of the primary RADIUS server.

system-id *system-id*

Sets the system ID.

tai-in-gtpv2-msg

Includes TAI in GTPv2 messages.

test

Tests the RADIUS server.

type *auth-type*

Sets the administration authentication type.

unit *threshold-unit*

Sets the threshold unit.

user *userid*

Sets the user ID.

user-id-privacy

Enables user ID privacy support.

value *threshold-value*

Sets the threshold value.

watch-dog-timeout *seconds*

Updates the device watch dog time, in seconds.

write

Enables write privilege.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command deletes the specified zone affinity profile.

The following table lists the related **dp-group** configuration commands.

Examples

The following example configures a cache cleanup for the vSZ-H zone named VSD.

```
device(config)# dp-group VSD  
device(config-dp-group)# cache-cleanup
```

dp-packet-capture

Enables or disables the data plane packet capture.

Syntax

```
dp-packet-capture { enable | disable | save }
```

Command Default

Data plane packet capture is not enabled.

Parameters

enable

Enables data plane packet capture.

disable

Disables data plane packet capture.

save

Saves captured packets.

Modes

Debug configuration mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.

Examples

The following example enables data plane packet capture.

```
device> debug  
device(debug)# dp-packet-capture enable
```

The following example disables data plane packet capture.

```
device> debug  
device(debug)# dp-packet-capture disable
```


eap-aka

Enters EAP AKA configuration mode to update EAP AKA configurations.

Syntax

eap-aka [**enable**]

After the **eap-aka** command is entered to enable EAP AKA configuration mode, the following configuration syntax is available:
[**cache-cleanup** | **fast-reauth** | **no** { **cache-cleanup** | **fast-reauth** | **secret key** | **user-id-privacy** } | **secret key** | **user-id-privacy**]

Command Default

EAP AKA configuration mode is not enabled.

Parameters

enables

Enables EAP AKA.

cache-cleanup

Enables the cache cleanup setting.

fast-reauth

Enables fast re-authentication support.

no

Disables configurations.

secretkey

Sets the EAP-AKA active secret key number.

user-id-privacykey

Enables user identity privacy support.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only.

Examples

The following example enables EAP AKA.

```
device# config
device(config)# eap-aka enable
```

Commands D through F

eap-aka

The following example enters EAP AKA configuration mode.

```
device# config
device(config)# eap-aka
device(config-eap-aka)#
```

The following example enables the cache cleanup setting.

```
device# config
device(config)# eap-aka
device(config-eap-aka)# cache-cleanup
```

eap-sim

Enables EAP SIM and enters EAP SIM configuration mode to update EAP SIM configurations.

Syntax

eap-sim [**enable**]

After the **eap-sim** command is entered to enable EAP SIM configuration mode, the following configuration syntax is available:

[**cache-cleanup** | **fast-reauth** | **no** { **cache-cleanup** | **fast-reauth** | **secret key** | **user-id-privacy** } | **secret key** | **user-id-privacy**]

Command Default

EAP SIM configuration mode is not enabled.

Parameters

enables

Enables EAP SIM.

cache-cleanup

Enables the cache cleanup setting.

fast-reauth

Enables fast re-authentication support.

no

Disables configurations.

secretkey

Sets the EAP-AKA active secret key number.

user-id-privacykey

Enables user identity privacy support.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only.

Examples

The following example enables EAP SIM.

```
device# config
device(config)# eap-sim enable
```

Commands D through F

eap-sim

The following example enters EAP SIM configuration mode.

```
device# config
device(config)# eap-sim
device(config-eap-sim)#
```

The following example enables the cache cleanup setting.

```
device# config
device(config)# eap-sim
device(config-eap-sim)# cache-cleanup
```

enable (new password)

Modifies the controller administrator password.

Syntax

enable

After the **enable** command is entered, the following configuration syntax is available:

```
{ old-password new password retype password }
```

Command Default

The password is not changed.

Parameters

old-password

The existing controller administrator password

new password

The new controller administrator password that you want to set.

retype password

Retype the new controller administrator password.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms.

Examples

The following example changes the controller administrator password.

```
ruckus# enable  
Old Password: *****  
New Password: *****  
Retype: *****  
Successful operation
```

enc-method

Specifies the encryption method to be used.

Syntax

`enc-method mixed | none | wep128 | wep64 | wpa | wpa2`

Command Default

No encryption method is specified.

Parameters

- mixed**
Specifies WPA mixed as the encryption method.
- none**
Specifies no encryption method.
- wep128**
Specifies WEP-128 (104 bits) as the encryption method.
- wep64**
Specifies WEP-64 (40 bits) as the encryption method.
- WPA**
Specifies WPA as the encryption method.
- WPA2**
Specifies WPA2 as the encryption method.

Modes

Zone WLAN configuration mode

Usage Guidelines

This command is available only after the **wlan** command is entered in zone configuration.

Examples

The following example creates a WLAN in zone Zone10, and sets the encryption method to be WPA2.

```
device# config
device(config)# zone zone10
device(config-zone)# wlan wlan20
device(config-zone-wlan)# enc-method WPA2
```

encrypt-mac-ip

Enables the encryption of MAC and IP addresses for Wireless Internet Service Provider roaming (WISPr) enriched URL.

Syntax

encrypt-mac-ip

no encrypt-mac-ip

Command Default

The encryption of MAC and IP addresses is not enabled.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

The **no** form of the command disables the encryption of MAC and IP addresses if it has been enabled.

Examples

The following example enables the encryption of MAC and IP addresses.

```
device(config)# encrypt-mac-ip  
Successful operation
```

The following disables the encryption of MAC and IP addresses.

```
device(config)# no encrypt-mac-ip  
Do you want to continue to disable (or input 'no' to cancel)? [yes/no]
```

encrypt-zone-name

Enables AP Zone name encryption for Wireless Internet Service Provider roaming (WISPr) enriched URL.

Syntax

encrypt-zone-name
no encrypt-zone-name

Command Default

AP zone name encryption is not enabled.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

The **no** form of the command disables AP zone name encryption if it has been enabled.

Examples

The following example enables AP zone name encryption.

```
device(config)# encrypt-zone-name  
Successful operation
```

The following disables AP zone name encryption.

```
device(config)# no encrypt-zone-name  
Do you want to continue to disable (or input 'no' to cancel)? [yes/no]
```

History

Release version	Command history
3.5.1	This command was introduced.

eth-port-validate-one-trunk

Enables the validator for an AP with at least one trunk port.

Syntax

```
eth-port-validate-one-trunk { disable | enable }
```

Command Default

The validator for an AP is not enabled with at least one trunk port.

Parameters

disable

Disables the validator for the AP with at least one trunk port.

enable

Enables the validator for the AP with at least one trunk port.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example enables the validator for the AP with at least one trunk port.

```
device(config)# eth-port-validate-one-trunk enable
```

The following example enables the validator for the AP with at least one trunk port.

```
device(config)# eth-port-validate-one-trunk disable
```

History

Release version	Command history
3.5.1	This command was introduced.

event

Updates event notification configurations.

Syntax

```
event { eventCode | db-persistence | email | snmp-notification }  
no event { db-persistence | email | snmp-notification }
```

Command Default

Event notification configurations are not updated.

Parameters

- eventCode*
Specifies a specified configuration event notification .
- db-persistence**
Enables data blade persistence for an event.
- email**
Enables email notifications.
- snmp-notification**
Enables selected SNMP notifications.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

The no form of the command disables configured event notifications.

Examples

The following example enables data blade persistence notifications for an event.

```
device(config)# event db-persistence
```

No.	Event Code	Category	Type	Email	Description	Severity
SNMP	OID				DB Persistence	
1	101	AP	AP discovery succeeded	Enabled	This event occurs when AP sends a discovery request to the SmartZone successfully.	Informational
Disabled	1.3.6.1.4.1.25053.2.10.1.46			Enabled		
2	103	AP	AP managed	Disabled	This event occurs when AP is approved by the SmartZone.	Informational
Disabled	1.3.6.1.4.1.25053.2.10.1.41			Disabled		
3	105	AP	AP rejected	Disabled	This event occurs when AP is rejected by the SmartZone.	Minor
Enabled	1.3.6.1.4.1.25053.2.10.1.28			Disabled		
4	106	AP	AP firmware updated	Disabled	This event occurs when AP successfully updates its firmware.	Informational
Disabled	1.3.6.1.4.1.25053.2.10.1.35			Disabled		
5	107	AP	AP firmware update failed	Disabled	This event occurs when the AP fails to update its firmware.	Major
Enabled	1.3.6.1.4.1.25053.2.10.1.34			Disabled		

Commands D through F
event

The following example enables SNMP notifications for an event.

```
device(config)# event snmp-notification
```

No. SNMP	Event OID	Code	Category	Type	Email	Description DB Persistence	Severity
1	101		AP	AP discovery succeeded	Enabled	This event occurs when AP sends a discovery request to the SmartZone successfully.	Informational
2	103		AP	AP managed	Disabled	This event occurs when AP is approved by the SmartZone.	Informational
3	105		AP	AP rejected	Disabled	This event occurs when AP is rejected by the SmartZone.	Minor
...							

event-email

Enters event email configuration mode to configure an event to email services.

Syntax

event-email

After the **event-email** command is entered to enable event email configuration mode, the following configuration syntax is available:
[**enable** | **no enable**]

After the **enable** command is entered to enable notification emails for events, the following configuration syntax is available::
[**mail-to** *email*]

Command Default

Notification emails for events is not enabled.

Parameters

enable

Enables notification emails for events.

noenable

Disables notification emails for events.

mail-to *email-address*

Specifies an email address.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example enters event email configuration mode and enables email notifications for events for a specified email address.

```
device(config)# event-email
device(config-event-email)# enable
device(config-event-email)# mail-to joe@company.com
```

The following example disables email notifications for events.

```
device(config)# event-email
device(config-event-email)# no enable
```

event-threshold

Enters event threshold configuration mode to update event threshold configurations.

Syntax

event-threshold *threshold*

After the **event-threshold** *threshold* command is entered to enable event email configuration mode, the following configuration syntax is available:

[**unit** | **value**]

Command Default

Event threshold configurations are not updated.

Parameters

threshold

Specifies an event threshold.

unit

Sets the threshold unit.

value

Sets the threshold value.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example enters event threshold configuration mode and sets the threshold value.

```
device(config)# event-threshold 904  
device(config-event-threshold)# value 55
```

export log

Exports the local system logs to an external FTP server.

Syntax

```
export log ftp-url app name
```

Command Default

Local system logs are not exported.

Parameters

ftp-url

Specifies an FTP URL.

app name

Specifies an application.

Modes

Debug configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example exports the local system logs to an external FTP server.

```
device# debug
device(debug)# export log ftp://mahan:ruckus1!@172.19.7.100
```

fips

Configures the Federal Information Processing Standards (FIPS) options.

Syntax

```
fips { disable | enable | showlog | status }
```

Command Default

FIPS is not configured.

Parameters

disable

Disables FIPS compliance.

enable

Enables the controller for FIPS compliance.

showlog

Show the bootup selftest log.

status

Indicates the status of FIPS compliance.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example enables the controller for FIPS compliance.

```
device# fips enable
Zeroization will be initiated using set factory and the FIPS mode will be set to Enable (or input 'no'
to cancel)? [yes/no]
```


fips

Configures the Federal Information Processing Standards (FIPS) options.

Syntax

```
fips { selftest | showlog | status }
```

Command Default

FIPS options are not configured.

Parameters

selftest

Specifies a FIPS self test.

showlog

Shows the bootup self-test log.

status

Indicates the status of system FIPS compliance.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.

Examples

The following example shows the bootup self-test log.

```
device# fips showlog

=====OpenSSL selftest=====
DRBG: PASSED
X931: PASSED
SHA1: PASSED
SHA2: PASSED
HMAC: PASSED
CMAC: PASSED
AES : PASSED
AES-CCM : PASSED
AES-GCM : PASSED
AES-XTS : PASSED
DES : PASSED
RSA : PASSED
ECDSA : PASSED
DSA : PASSED
DH : PASSED
ECDH : PASSED
ECP384 : PASSED
```

force-recover-escluster

Forces a recover ESCluster.

Syntax

force-recover-escluster

Command Default

Local system logs are not exported.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the SmartZone 100 controllers only.

Examples

The following example forces a recover ESCluster.

```
device# force-recover-escluster
This command would remove all the Elasticsearch data and re-sync again. Do you want to continue (or
input 'no' to cancel)? [yes/no] no
Cancel operation
```

fresh upgrade

Upgrades the controller firmware.

Syntax

fresh upgrade*file* | *ftp-url*

Command Default

The controller is not updated.

Parameters

file

Upgrades the controller files.

ftp-url

Upgrades the controller using firmware from the specified FTP path. FTP URL format is ftp://<username>:<password>@<ip-address>[filepath].

Modes

Privileged EXEC mode

Usage Guidelines

Wipe-out upgrade enables customers to upgrade real-box products .i.e. SZ100/vSZ-E and SZ300/vSZ-H before setting up the system. This feature is useful for service engineers and developers because it saves a lot of time. Wipe-out upgrade is not required for virtual products because deploying the VM instance is much easier.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example upgrades the controller with firmware from the specified FTP path.

```
device# fresh-upgrade
  <ftp-url>      Upgrade file, FTP URL Format: ftp://<username>:<password>@<ip>[/<
device# upgrade ftp://username:pwd234@10.10.8.100/tmp/filename.datfile-path]
```

ftp-server

Enters FTP server configuration mode to create or update a FTP server.

Syntax

ftp-server *name*

no ftp-server *name*

After the **ftp-server** *name* **app** *name* command is entered to enable FTP server configuration mode, the following configuration syntax is available:

[**host** *ip* | **password** | **port** *port number* | **protocol** { **ftp** | **sftp** } | **remote-directory** *directory* | **test** | **username** *username*]

Command Default

An FTP server is not created or updated.

Parameters

name

Name of FTP server.

host *IP*

Sets the FTP server IP address.

password

Sets a password.

port *port number*

Sets an FTP server port.

protocol

Sets the FTP protocol.

ftp

Specifies FTP.

sftp

Specifies SFTP.

remote-directory *directory*

Sets the FTP server remote directory.

test

Tests the FTP settings.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command deletes an FTP server. This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example enters FTP server configuration mode and updates the FTP server configurations.

```
device# configure
device(config)# ftp-server ftp1
ruckus(config-ftp-server)# host 1.1.1.1
ruckus(config-ftp-server)# port 21
ruckus(config-ftp-server)# protocol stp
ruckus(config-ftp-server)# username test
ruckus(config-ftp-server)# password
Password: ****
Retype: ****
ruckus(config-ftp-server)# exit
ruckus(config)#
```

The following example deletes an FTP server.

```
device# configure
device(config)# no ftp-server ftp1
```

ftp-test

Tests the FTP server connection.

Syntax

`ftp-testname`

Command Default

The FTP server connection is not tested.

Parameters

name

Specifies the FTP server.

Modes

Global configuration mode

Examples

The following example shows how to test the FTP server connection for a specified FTP server.

```
device(config)# ftp-server FTP-SERVER  
Fail to connection to FTP server
```

firmware-download-limit

Display the firmware download limitations.

firmware-download-limit [*integer* | *speedlimit*]

no firmware-download-limit

Command Default

The default concurrent connections for AP firmware download is 300 and the default bandwidth per AP firmware download connection is 1k to 256k bytes.

Parameters

integer

Enter the number of input connections in integer from (1 ~ 65535) [suggestion: 300].

speedlimit

Enter the download speed limit in KB [suggestion: 256k].

NOTE

For the second requested value, if 0 is entered, then the download speed is unlimited.

Modes

Global configuration mode

Usage Guidelines

This command allow users to limit concurrent connections and bandwidth for AP firmware download. The default concurrent connections for AP firmware download is 300 and the default bandwidth per AP firmware download connection is 0k bytes. Users can change the concurrent connections to the number between 1 and 65535 and bandwidth to the number between 0k and 2147483647k. However, users must be careful to update these parameters because it impacts the controller (SmartZone) network resources.

The no form of this command is set as *no limit* on AP Firmware Download. That means it will set the connection to 65535 and bandwidth to 0k. The 65535 is the maximum value of concurrent connections. The bandwidth 0k means there is no limitation for AP firmware download rate.

NOTE

Allocating too much bandwidth or too many concurrent connections for AP firmware download will impact other controller (SmartZone) services.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example enables certificate checking for APs.

```
device# config
device(config)# firmware-download-limit
The limited number of firmware download connection is 300 and the download speed per connection is not
limited.
Please input connections in integer(1 ~ 65535) [suggestion: 300]: 200
Please input download speed limit in KB [suggestion: 256k]: 500
Successful operation
% This configuration will take effect in a few minutes.
```

History

Release version	Command history
5.2.2	This command was introduced.

Commands G through I

gateway-advance

To set the gateway server advance options.

Syntax

gateway-advance

Command Default

Gateway advance options is not displayed.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The below example displays the gateway server advance options.

```
device# config
device(config)# gateway-advance
device(config-gateway-advance)#
  allow-sess-on-acct-fail    Allow Session on Accounting Fail
  do                        Do command
  ecgi-in-gtpv2-msg         Include ECGI in GTPV2 Messages
  end                       End the current configuration session and return to privileged EXEC mode
  exit                     Exit from the EXEC
  gtp-nsapi                 GTP Network Service Access Point Identifier [NSAPI]
  gtpv2-interface-type     Set GTPV2 interface type
  help                     Display this help message
  imei-ie-in-gtp-msg       Include IMEI IE in GTP Messages
  no                       Disable the Options
  scg-rai-in-gtpv2-msg     Include SCG-RAI in GTPV2 Messages
  scg-sai-in-gtpv2-msg     Include SCG-SAI in GTPV2 Messages
  tai-in-gtpv2-msg         Include TAI in GTPV2 Messages
```

gdpr-pii

To search and delete PII (Personally Identifiable Information) data based on GDPR (General Data Protection Regulation).

Syntax

```
gdpr-pii [delete | interrupt | progress | search]mac
```

Command Default

Interrupt PII data search and delete progress by device MAC.

Parameters

delete

Delete PII Data by device MAC.

interrupt

Interrupts the search or deletes process.

progress

Checks the progress on the search or delete process

search

Searches for PII data based on the device MAC address

mac

Specify the MAC device address

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The below example displays search and delete PII (Personally Identifiable Information) data based on GDPR (General Data Protection Regulation).

```
device# gdpr-pii
delete      Delete PII Data by device MAC
interrupt   Interrupt PII Data Search/Delete progress by device MAC
progress    Check PII Data Search/Delete progress by device MAC
search      Search PII Data by device MAC
```

ggsn-service

To create or update the APN resolution to GGSN/PGW configuration.

Syntax

ggsn-service [*apn* | *dns-retry* | *dns-server* | *dns-timeout* | *request-timer* | *response-timer* | *retry*]

Command Default

No ggsn-service is created or updated.

Parameters

apn <name>

apn - Creates or updates the APN resolution to GGSN / PGW configuration.

name - Name of the APN.

dns-retry <number>

dns-retry - Sets the number of DNS retry.

<number> - Number of DNS retries.

dns-server <ip> priority [down | up]

dns-server: Sets the DNS server.

<ip> DNS server IP address

priority [down | up]: Change DNS server priority by moving the priority either up or down.

dns-timeout <seconds>

dns-timeout: Sets the DNS response timeout in seconds.

<seconds>: DNS response timeout.

request-timer <seconds>

request-timer: Sets the echo request timer in seconds.

<seconds>: Echo request timeout.

response-timer <seconds>

response-timer: Sets the echo response timer in seconds.

<seconds>: Echo response timeout.

retry <number>

retry: Sets the number of retries.

<number>: Number of retries.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The below example displays options to create or update APN resolution to GGSN/PGW configuration.

```
device# config
device(config)# ggsn-service
apn          dns-retry          dns-server          dns-timeout          request-timer          response-
timer       retry
```

hlr-mnc-ndc

Setup the HLR service MNC to NDC mapping configuration.

Syntax

```
hlr-mnc-ndc{mcc | mnc | ndc}
```

Command Default

No mobile country code, network code and destination code can be setup.

Parameters

mcc	Set Mobile Country Code.
mnc	Set Mobile Network Code.
ndc	Set Network Destination Code.

Modes

Global configuration mode

Usage Guidelines

This command is supported only on the SmartZone 300/vSZ-H.

Examples

The below example displays setting up the HLR service from MNC to NDC mapping configuration.

```
device(config)# hlr-mnc-ndc
device(config-hlr-mnc-ndc)#
do          Do command
end        End the current configuration session and return to privileged EXEC mode
exit      Exit from the EXEC
help      Display this help message
mcc      Set Mobile Country Code
mnc      Set Mobile Network Code
ndc      Set Network Destination Code
```

hlr-service

Create or update the HLR service configuration.

Syntax

```
hlr-service {auth-caching | auth-map-version <version2> <version3> | av-caching | default-point-code-format <dottetd> <integer> | dest-gt-indicator <numbers> | dest-nature-addr-indicator <numbers> | dest-numbering-plan <numbers> | dest-translation-type <translation-type> | eap-sim-map-version <version2> <version3> | friendly-name | gt-point-code | local-point-code | name | routing-context | sccp-gtt <gt-digits> | sctp <ip> | source-gt-indicator | source-has-point-code | source-nature-addr-indicator | source-numbering-plan | source-translation-type}
```

Command Default

No HLR service can be created or updated.

Parameters

auth-caching

Enable authorization caching.

auth-map-version<version2><version3>

Set Authorization MAP version.

av-caching

Enable AV caching.

default-point-code-format<dottetd><interger>

Set Default Point Code format.

dest-gt-indicator<numbers>

Set Dest GT indicator.

dest-nature-addr-indicator<numbers>

Set Dest Nature Address of indicator.

dest-numbering-plan<numbers>

Set Dest Numbering Plan.

dest-translation-type<translation-type>

Set Dest Translation Type.

eap-sim-map-version<version2><version3>

Set EAP-SIM MAP version.

friendly-name

Set HLR Service friendly name.

gt-point-code

Set GT Point Code.

local-point-code

Set Local Point Code.

routing-context

Set Routing context

sccp-gtt<gt-digits>

Create/Update SCCP GTT table configuration.

sctp<ip>

Create/Update SCTP Association to Core Network configuration.

sgsn-isdn-addr<sgsn-isdn-address>

Set SGSN ISDN Address.

source-gt-indicator

Set Source GT Indicator.

source-has-point-code

Enables source has point code.

source-nature-addr-indicator

Set Source Nature Address of Indicator.

source-numbering-plan

Set Source Numbering Plan.

source-translation-type

Set Source Translation Type.

Modes

Global configuration mode

Usage Guidelines

This command is supported only on the SmartZone 300/vSZ-H.

Examples

The below example displays creating or updating the HLR service configuration.

```

device# config
device(config)# hlr-service name

device(config-hlr-service)#
  auth-caching           Enable authorization caching
  auth-map-version       Set Authorization MAP version
  av-caching             Enable AV caching
  default-point-code-format Set Default Point Code format
  description           Set Description
  dest-gt-indicator      Set Dest GT indicator
  dest-nature-addr-indicator Set Dest Nature Address of indicator
  dest-numbering-plan    Set Dest Numbering Plan
  dest-translation-type  Set Dest Translation Type
  do                    Do command
  eap-sim-map-version    Set EAP-SIM MAP version
  end                   End the current configuration session and return to privileged EXEC
mode
  exit                  Exit from the EXEC
  friendly-name        Set HLR Service friendly name
  gt-point-code        Set GT Point Code
  help                 Display this help message
  local-point-code     Set Local Point Code
  name                 Set HLR service name
  no                   No commands
  routing-context      Set Routing context
  sccp-gtt             Create/Update SCCP GTT table configuration
  sctp                 Create/Update SCTP Association to Core Network configuration
  sgsn-isdn-addr       Set SGSN ISDN Address
  source-gt-indicator  Set Source GT Indicator
  source-has-point-code Enable source has point code
  source-nature-addr-indicator Set Source Nature Address of Indicator
  source-numbering-plan Set Source Numbering Plan
  source-translation-type Set Source Translation Type

```

hlr-system-wide

Update HLR System Wide configuration.

Syntax

`hlr-system-wide`

Command Default

No hlr system wide configuration can be updated.

Modes

Global configuration mode

Usage Guidelines

This command is supported only on the SmartZone 300/vSZ-H.

Examples

The below example displays updating the HLR system wide configuration.

```
device# config
device(config)# hlr-system-wide
<cr>
```

hostname

Changes the hostname.

Syntax

hostname hostname

Command Default

Host name is not changed.

Parameters

hostname

Execute this command to change the hostname.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The below example displays **hostname** command:

```
device# config
device(config)# hostname
  <hostname>      Change hostname
device(config)# hostname ruckus
This command will restart some services. Do you want to continue (or input 'no' to cancel)? [yes/no]
```

hotspot

Create or update the hotspot (WISPr) configuration.

Syntax

hotspot [hotspot-name]

no hotspot[hotspot-name]

After **hotspot** command is entered, the following configuration syntax is available:

{**grace-period** mins | **https-redirect** language | **location-id** location-id | **session-timeout** mins | **sms-gateway** | **disabled** | **start-page** | **original** | **redirect** start-url | **walled-garden** network-IP-addresses}

After the **enable-terms-and-conditions** keyword is entered, the following configuration syntax is available:

[**terms-and-conditions**]

hotspot profile hotspot-name

Command Default

Hotspot (WISPr) is not created or updated.

Parameters

grace-period mins

Sets the EAP-SIM MAP version.

https-redirect language

Sets the portal language.

location-id location-id

Sets the location ID.

session-timeout mins

Sets the session timeout. Defined in minutes.

sms-gateway

Sets sms-gateway path.

disabled

Disables the set hotspot.

start-page

Sets the new start page as defined by the user.

original

Displays the original url.

redirect start-url

Sets the redirect url name as defined by the user.

walled-garden network-IP-addresses

Enables walled garden. Allows unauthorized destinations. Comma-separated IP, IP range, CIDR and regular expression domain name list.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command removes the user specified hotspots and the updates.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The below example displays **hotspot** details.

```
device(config)# hotspot hspl
device(config-hotspot-profile)#
  description          Set Description
  do                   Do command
  end                  End the current configuration session and return to privileged EXEC mode
  exit                Exit from the EXEC
  grace-period        Set Grace Period
  help                Display this help message
  location-id         Set Location ID
  location-name       Location Name
  logon-url           Set Logon Model
  mac-address-format  Set MAC Address Format
  name                Set Hotspot Service Name
  no                  No commands
  session-timeout     Set Session Timeout
  smart-client-support Set Smart Client Support
  start-page          Set Start Page
  walled-garden       Set Walled Garden
```

identity-provider

Create or update identity provider configuration.

Syntax

identity-provider{name}

no identity-provider{name}

After **identity-provider** command is entered, the following configuration syntax is available:

{**acct-enable** | **auth-profile** | **description** **home-ois** <name> | | **osu-enable** | **plmns** <mcc> | **realms** <name>}

Command Default

No identity provider configuration is updated or created.

Parameters

acct-enable

Enables Accounting.

auth-profile

Set Authentication Profile.

home-ois <name>

Set Home OIs.

osu-enable <minutes>

Enables Online Signup & Provisioning.

plmns <mcc>

Set PLMNs.

realms <name>

Set Realms.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command removes the user specified identity providers.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The below example displays creating or updating the **identity-provider** configuration.

```
device# config
device(config)# identity-provider name
device(config-identity-provider)#
  acct-enable      Enable Accounting
  auth-profile     Set Authentication Profile
  description      Set Description
  do              Do command
  end             End the current configuration session and return to privileged EXEC mode
  exit            Exit from the EXEC
  help            Display this help message
  home-ois        Set Home OIs
  name            Set Identity Provider Name
  no              Disable and delete commands
  osu-enable       Enable Online Signup & Provisioning
  plmns           Set PLMNs
  realms          Set Realms
```


hotspot-profile

Create or update the hotspot service profile configuration.

Syntax

hotspot profile[name]

no hotspot profile[name]

After the **hotspot profile** command is entered, to enable the hotspot profile configuration mode, the following configuration syntax is available:

```
{ grace-period <minutes> | location-id <location-id> | location-name <location-name> | logon-url <internal> <external> <ftp-url> |
mac-address-format <AA-BB-CC-DD-EE-FF> <AA:BB:CC:DD:EE:FF> <AABBCCDDEEFF> | <walled-garden-list> | session-timeout
<minutes> | smart-client-support <enable> <none> <only> | start-page <original> <redirect> | walled-garden}
```

Command Default

No hotspot profile is created or updated.

Parameters

grace-period <minutes>

Set Grace Period.

gt-point-code

Set GT Point Code.

location-id

Set Location ID.

location-name

Location Name.

logon-url <internal> <external> <ftp-url>

Sets the logon model and redirects unauthenticated user to the URL for authentication.

mac-address-format <AA-BB-CC-DD-EE-FF> <AA:BB:CC:DD:EE:FF> <AABBCCDDEEFF>

Sets the MAC address format.

session-timeout <minutes>

Set Session Timeout.

smart-client-support <enable> <none> <only>

Set Smart Client Support.

start-page <original> <redirect>

Sets Start Page and redirects to the defined URL.

walled-garden

Set Walled Garden.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command removes the user specified hotspot profiles.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The below example displays creating or updating the **hotspot profile** configuration.

```
device# config
device(config)# hotspot-profile name
device(config-hotspot-profile)#
  description          Set Description
  do                   Do command
  end                  End the current configuration session and return to privileged EXEC mode
  exit                 Exit from the EXEC
  grace-period         Set Grace Period
  help                 Display this help message
  location-id          Set Location ID
  location-name        Location Name
  logon-url            Set Logon Model
  mac-address-format   Set MAC Address Format
  name                 Set Hotspot Service Name
  no                   No commands
  session-timeout      Set Session Timeout
  smart-client-support Set Smart Client Support
  start-page           Set Start Page
  walled-garden        Set Walled Garden
```

interface

Setup interface configuration.

Syntax

The SZ300/vSZ-H displays the following syntax for **interface** command:

```
interface{cluster | control | management | user-defined <name>}
```

The SZ100/vSZ-E displays the following syntax for **interface** command:

```
interface{ ap-tunnel-data | mgmt-and-ap-control | user-defined <name>}
```

```
no interface {user-defined | <name>}
```

Command Default

No interface configuration is setup.

Parameters

cluster

Sets the cluster interface.

control

Sets the interface control configuration.

management

Sets the management interface configuration.

ap-tunnel-data

Sets the user defined access point tunnel data.

mgmt-and-ap-control

Sets the user defined management and access point controls.

user-defined <name>

Sets the user defined interface configuration and name.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes user defined interfaces.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Commands G through I

interface

Examples

The below example displays setting **interface** configuration for SZ100.

```
device# config

device(config)# interface
  ap-tunnel-data      AP Tunnel Data
  mgmt-and-ap-control Management & AP Control
  user-defined        User defined interface

device(config)# interface mgmt-and-ap-control

device(config-if)#
  data-plane      Update Data Plane configuration
  do              Do command
  end             End the current configuration session and return to privileged EXEC mode
  exit           Exit from the EXEC
  help           Display this help message
  ip             Update IP configuration
  no            Disable and delete commands
```

Examples

The below example displays setting **interface** configuration for SZ300.

```
device(config)# interface
  cluster      Cluster interface
  control      Control interface
  management   Management interface
  user-defined  User defined interface

device(config)# interface cluster

device(config-if)#
  do      Do command
  end     End the current configuration session and return to privileged EXEC mode
  exit   Exit from the EXEC
  help   Display this help message
  ip     Update IP configuration
```

internal-dp-group

Enables and sets the data plane grouping.

Syntax

```
internal-dp-group { dp-mac-group | <dp1-mac> | <dp2-mac> | <dp2-mac> }
no internal-dp-group
```

Command Default

No internal data plane groups are created.

Parameters

dp-mac-group

Internal Data Plane Groups (comma separated DP MAC addresses in a group, space separated groups). Ex: 3 DP, value can be like "<dp1-mac>, <dp2-mac>, <dp3-mac>"

Modes

Global configuration mode

Usage Guidelines

The data planes across the node in a cluster can be grouped and an AP in the node can be tunneled to the group of data planes. Data plane groups are comma separated DP MAC addresses in a group. For example, 3 DP value is seen as "<dp1-mac>,<dp2-mac><dp3-mac>."

The **no** form of this command removes the internal data plane groups.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example displays **internal-dp-group** configuration.

```
device# config
device(config)# internal-dp-group
  <dp-mac-group>      Internal Data Plane Groups (comma separated DP MAC addresses in a group,
space separated groups). Ex: 3 DP, value can be like "<dp1-mac>,<dp2-mac> <dp3-mac>"
device(config)# dp-mac-group dp1-172.19.7.100,dp2-172.19.8.120, dp3-172.19.9.130
```

History

Release version	Command history
6.0.0	This command was introduced.

ip

Sets up IP address.

Syntax

```
ip { control-nat | default-gateway | default-gateway-ipv6 | internal-subnet | ipv6-route | name-server | name-server-ipv6 | route | separate-access-core }
```

```
no ip { control-nat | ipv6-route | name-server | route | separate-access-core }
```

Command Default

No IP address is setup.

Parameters

control-nat

Set Control NAT IP.

default-gateway

Set default gateway.

default-gateway-ipv6

Set IPv6 default gateway.

internal-subnet

Set internal subnet prefix.

ipv6-route

Set IPv6 static routes.

name-server

Set name server.

name-server-ipv6

Set IPv6 name server.

route

Set static routes.

separate-access-core

Enable separate access and core gateway.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command removes the user specified ip addresses.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example displays setting up **ip** address.

```
device(config)# ip
control-nat          Set Control NAT IP
default-gateway      Set default gateway
default-gateway-ipv6 Set IPv6 default gateway
internal-subnet      Set internal subnet prefix
ipv6-route           Set IPv6 static routes
name-server          Set name server
name-server-ipv6     Set IPv6 name server
route                Set static routes
separate-access-core Enable separate access and core gateway
```

Examples

The below example displays **no ip** .

```
device(config)# no ip
control-nat          Delete Control NAT IP
ipv6-route           Delete IPv6 static routes
name-server          Delete all name servers
route                Delete static routes
separate-access-core Separate access and core gateway
```

ip control-nat

Sets up control NAT IP configuration.

Syntax

```
ip control-nat{ip}
```

Command Default

No control nat ip is configured.

Parameters

ip
The Control NAT IP.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example displays **ip control-nat** command options.

```
device(config)# ip control-nat  
<ip>      Control NAT IP  
  
device(config)# ip control-nat 172.172.18.9  
Successful operation
```


ip data-nat

Sets up external NAT IP address of the data interface.

Syntax

```
ip data-nat{address | port }
no ip data-nat
```

Command Default

No external NAT IP is setup.

Parameters

address
IP address to set the external NAT server.

port
NAT server port number.

Modes

Global configuration mode

Usage Guidelines

This command is supported only on the SmartZone Data Plane controller.

Examples

The following example displays **ip data-nat** configuration.

```
device(config)# ip data-nat
  data-nat                               Set external NAT IP address of data interface
device(config)# ip data-nat 172.172.18.9 80
The command was executed successfully. To save the changes, type 'end'.
```

Examples

The below example displays **no ip data-nat**.

```
beta-tmp-BDC(config)# no
  ip-data-nat                             Remove external NAT of data interface
beta-tmp-BDC(config)# no ip-data-nat
  ip-data-nat                             Remove external NAT of data interface
beta-tmp-BDC(config)# no ip-data-nat 172.172.18.9 80
The command was executed successfully. To save the changes, type 'end'.
```

ip default-gateway

Sets up default gateway configuration.

Syntax

```
ip default-gateway{cluster | control | management}
```

Command Default

Default gateway is not configured for IP.

Parameters

- cluster**
Displays cluster interface.
- control**
Displays control interface.
- management**
Displays management interface.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example displays **ip default-gateway** configuration.

```
NODE201(config)# ip default-gateway
cluster          Cluster interface
control          Control interface
management      Management interface
<interface>     Interface
```

ip default-gateway-ipv6

Setup default gateway configuration for IPv6.

Syntax

```
ip default-gateway-ipv6{cluster | control | management}
```

Command Default

IPv6 default gateway is not configured.

Parameters

cluster

Displays cluster interface.

control

Displays control interface.

management

Displays management interface.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example displays **ip default-gateway-ipv6** configuration.

```
device(config)# ip default-gateway-ipv6
cluster          Cluster interface
control          Control interface
management      Management interface
ruckus(config)# ip default-gateway-ipv6 cluster
This command will reload all SCG services. Do you want to continue (or input 'no ' to cancel)? [yes/no]
```

ip internal-subnet

Setup internal subnet for the IP address .

Syntax

```
ip internal-subnet{prefix}
```

Command Default

No internal subnet mask is setup for the IP address.

Parameters

prefix

Subnet prefix.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example displays **ip internal-subnet** configuration.

```
device# config
device(config)# ip internal-subnet
device(config)# ip internal-subnet 175.175.81
This command will reboot internal interfaces, data planes and SMF service. Do you want to continue
(or input 'no' to cancel)? [yes/no]
```

ip ipv6-route

Sets up IPv6 static rule configuration.

Syntax

ip ipv6-route{ip}

Command Default

No ipv6 route static rule is configured.

Parameters

ip

Destination network IPv6 address with prefix length.

Modes

Global configuration mode

Usage Guidelines

Configures a static IPv6 route where a static default IPv6 route is being configured on a control interface or management interface. This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The below example displays **ip ipv6-route** configuration.

```
device(config)# ip ipv6-route 193.12.30.10
```

History

Release version	Command history
5.1.1	This command was introduced.

ip name-server

Configures name of the IP server.

Syntax

```
ip name-server{ip}
```

Command Default

No IP server name is configured.

Parameters

ip
Primary DNS server.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example displays **ip name-server** configuration.

```
device# ip ipv6-route 193.12.30.10
```

ip name-server-ipv6

Configures the name of IPv6 server.

```
ip name-server-ipv6{ipv6-address}
```

Command Default

No IPv6 server name is configured.

Parameters

ipv6-address

IPv6 Primary DNS server.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example displays **ip name-server-ipv6** configuration.

```
device# ip name-server-ipv6 172.19.13.56  
Successful operation
```

Commands G through I

ip route

ip route

Configures the IP route.

ip route{ip | subnet mask | destination ip | interface}

Command Default

IP route is not configured.

Parameters

ip

Destination network IP address

subnet mask

Destination network mask

destination ip

Next hop IP address

interface

Interface

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example displays **ip route** command.

```
device# config
device(config)# ip route ip 193.12.30.10 255.255.255 10.9.0.254 management
```


ip separate-access-core

Enables access and core gateway.

ip separate-access-core{enable}

Command Default

IP separate access core is not enabled.

Parameters

enable

Enables access and core gateway.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example displays ip separate-access-core command.

```
device# config
device(config)# ip separate-access-core enable
If enabled, Management interface (core side) gateway is the system default.
Control interface (access side) gateway is used for access traffic only.
(or input 'no' to cancel)? [yes/no]
```

ip-support

Updates the IP version support.

ip-support { ipv4-ipv6 | ipv4-only }

Command Default

Supported IP version is not updated.

Parameters

ipv4-ipv6

To support both IPv4 and IPv6 versions.

ipv4-only

To support IPv4 version only.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone 300 controller only.

Examples

The following example displays ip-support command.

```
device# config
device(config)# ip-support
  ipv4-ipv6      IPv4 and IPv6
  ipv4-only      IPv4 only
```

ipsec-profile

Updates IPSEC profile configuration.

Syntax

ipsec[name]

no ipsec-profile

After **ipsec-profile** command is entered, the following configuration syntax is available:

{**auth-type** | **cara-server** | **cara-server-path** | **cara-subject-name** | **cmp-dhcp-opt43-subcode** | **cmp-subject-name-dhcp-opt43-subcode** | **description** | **dhcp-opt43-subcode** | **dpd-delay** | **esp-rekeytime** | **esp-type** | **failover-retry-interval** | **failover-retry-mode** | **failover-retry-period** | **ike-rekeytime** | **ike-type** | **ip-compression** | **keep-alive-interval** | **nat-traversal** | **replay-window** | **retry-limit** | **security-gateway**}

Command Default

IPSEC profile configuration is not updated.

Parameters

auth-type

Set Authentication Type.

cara-server

Set Certificate Management Protocol CA/RA Address.

cara-server-path

Set Certificate Management Protocol Server Path.

cara-subject-name

Set Certificate Management Protocol Subject Name of CA/RA.

cmp-dhcp-opt43-subcode

Set Certificate Management Protocol DHCP Option 43 Sub Code for CA/RA Address.

cmp-subject-name-dhcp-opt43-subcode

Set Certificate Management Protocol DHCP Option 43 Sub Code for Subject Name of CA/RA.

dhcp-opt43-subcode

Set DHCP Option 43 Sub Code for Security Gateway.

dpd-delay

Set Dead Peer Detection.

esp-rekeytime

Set ESP Rekey Time.

esp-type

Set ESP Proposal Type.

failover-retry-interval

Set Fail Over Retry Interval.

Commands G through I

ipsec-profile

failover-retry-mode

Set Fail Over Retry Mode.

failover-retry-period

Set Fail Over Retry Period.

ike-rekeytime

Set IKE Rekey Time.

ike-type

Set IKE Proposal Type.

ip-compression

Enable IP Compression.

keep-alive-interval

Set NAT-T Keep Alive Interval.

nat-traversal

Enable Force NAT-T.

replay-window

Set Replay Window.

retry-limit

Set Retry Limit.

security-gateway

Set Security Gateway.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command removes the user specified ipsec profiles.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example displays **ipsec-profile**.

```

NODE202# config

NODE202 (config)# ip
ip ipsec-profile

NODE202 (config)# ipsec-profile
<name> IPsec Profile name

NODE202 (config)# ipsec-profile xyz

NODE202 (config-ipsec-profile)#
auth-type Set Authentication Type
cara-server Set Certificate Management Protocol CA/RA Address
cara-server-path Set Certificate Management Protocol Server Path
cara-subject-name Set Certificate Management Protocol Subject Name of CA/RA
cmp-dhcp-opt43-subcode Set Certificate Management Protocol DHCP Option 43 Sub Code
for CA/RA Address
cmp-subject-name-dhcp-opt43-subcode Set Certificate Management Protocol DHCP Option 43 Sub Code
for Subject Name of CA/RA
description Set description
dhcp-opt43-subcode Set DHCP Option 43 Sub Code for Security Gateway
do Do command
dpd-delay Set Dead Peer Detection
end End the current configuration session and return to
privileged EXEC mode
esp-rekeytime Set ESP Rekey Time
esp-type Set ESP Proposal Type
exit Exit from the EXEC
failover-retry-interval Set Fail Over Retry Interval
failover-retry-mode Set Fail Over Retry Mode
failover-retry-period Set Fail Over Retry Period
help Display this help message
ike-rekeytime Set IKE Rekey Time
ike-type Set IKE Proposal Type
ip-compression Enable IP Compression
keep-alive-interval Set NAT-T Keep Alive Interval
name Set IPsec Profile Name
nat-traversal Enable Force NAT-T
no Disable and delete commands
replay-window Set Replay Window
retry-limit Set Retry Limit
security-gateway Set Security Gateway

NODE202 (config-ipsec-profile)# no
cara-server cara-server-path cara-subject-name dpd-delay esp-
rekeytime ike-rekeytime ip-compression
keep-alive-interval nat-traversal replay-window retry-limit security-gateway

```


Commands J through N

kdump

kdump is an advanced crash dumping mechanism.

Syntax

kdump enable

After the command is entered to enable the KDUMP service, the following configuration syntax is available:

kdump disable

Disables the **kdump** service.

kdump get {ftp/sftp username password | ip-addr ip-address}

Use the **get** command to get the latest **kdump** files.

Command Default

When enabled, the system is booted from the context of another kernel

Parameters

enable

Enables the **kdump** service.

disable

Disables the **kdump** service.

ftp/sftp username password

Specifies the FTP and SFTP server username and password to access **kdump** service.

ip-addr ip-address

Specifies the IP address to access **kdump** service.

Modes

Debug configuration mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.

To get the latest **kdump** files, use the **get** command by specifying username and password if you are using FTP/SFTP option or the server path in case you are using the IP address option.

Examples

The following example enables kdump service in debug mode.

```
device# debug
device(debug)# kdump enable
enable kdump Success
```

The following example disables kdump service in debug mode

```
device# debug
device(debug)# kdump disable
disable kdump Success
```

The following example gets the kdump service by specifying the IP address.

```
device# debug
device(debug)# kdump get ip-addr <ip-address>
device(debug)# kdump get ip-addr 10.206.6.36
```

The following example gets the kdump service by specifying the user name and address of the FTP server.

```
device# debug
device(debug)# kdump get ftp <username> <password>
device(debug)# kdump get ftp admin *****
```


I2-acl

Creates or updates the L2ACL configuration.

Syntax

l2-acl *acl-name*

no l2-acl

After the **l2-acl** command is entered to enable L2ACL configuration mode, the following configuration syntax is available:

{**action**{**allow**|**block**}|**mac***mac-value*}

Command Default

No L2ACL configuration is created or updated.

Parameters

acl-name

Name of the Layer 2 access control list (L2ACL).

action

Sets the handling action.

allow

Sets the handling action to allow traffic.

block

Sets the handling action to block traffic.

mac*mac-value*

Sets the device MAC address.

Modes

Domain configuration mode

WLAN configuration mode

Zone configuration mode

Usage Guidelines

This command is available only after one of the following commands is entered:

- domain
- wlan
- zone

The **no** form of the command deletes the specified L2ACL.

Commands J through N

l2-acl

In L2ACL configuration mode, the **no mac** command disables the MAC value. **config-zone-l2-acl** is seen when Zone is version 5.2 or previous AP firmware.

Examples

The following example configures a Layer 2 ACL named list2 to allow traffic for zone2.

```
device# config
device(config)# zone zone2
device(config-zone)# l2-acl list2
device(config-zone-l2-acl)# allow
```

I2ogre-profile

Creates or updates the L2oGRE profile (Layer 2 Services over GRE Tunnel Interfaces) configuration.

Syntax

l2ogre-profile *name*

After the **l2ogre-profile** command is entered to enable the L2oGRE configuration mode, the following configuration syntax is available:

[description *text* | **dhcp-relay** | **icmp-keep-alive-period** *seconds* | **icmp-keep-alive-retry** *number* | **name** *name* | | **no dhcp-relay secondary-gateway** | **primary-gateway** *ip* | **secondary-gateway** *ip* | **tunnel-mtu** *auto bytes*]

After the **dhcp-relay** command is entered, the following configuration syntax is available:

{dhcp-option82 | **dhcp-server1** *server-name* | **dhcp-server2** *server-name*}

After the **dhcp-option82** command is entered, the following configuration syntax is available:

{subopt1}{ap-ssid | ap-info-default | ap-info-location | ap-mac | format}

subopt150

subopt151{*ssidarea-name area-name*}

subopt2{*ap-ssid | ue-ssid | ue-mac | ap-mac*}

Command Default

The default L2oGRE Profile is used.

Parameters

name *name*

Sets the L2oGRE profile name.

description *text*

Sets the description of the L2oGRE profile for the user.

dhcp-relay

Enables DHCP relay agent.

no dhcp-relay

Disables DHCP relay.

icmp-keep-alive-period *seconds*

Sets the ICMP (The Internet Control Message Protocol) in seconds. The range is 01 to 32767 seconds.

icmp-keep-alive-retry *number*

Sets the number of ICMP (The Internet Control Message Protocol) retry. The range is 01 to 255.

primary-gateway *ip*

Sets the primary server.

secondary-gateway *ip*

Sets the secondary server.

no secondary-gateway *ip*

Disables the secondary gateway server.

Commands J through N

l2ogre-profile

tunnel-mtu *auto*

Sets the auto transmission unit size for the particular tunnel to 1500 bytes.

tunnel-mtu *bytes*

Sets the manual transmission unit size in bytes for the particular tunnel. Byte size is in the range 850–1500.

dhcp-option82

Enables DHCP Option82.

subopt1

Enables Subopt-1.

ap-ssid

Uses the Access Point (AP) MAC hex ESSID.

ap-info-default

Uses the default AP information in the following format: IF-Name:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC.

ap-info-location

Uses the AP location information in the following format: IF-Name:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC:Location.

ap-mac

Uses the AP MAC in the following format: AP-MAC-hex.

format

Uses the specified format.

subopt150

Enables Subopt-1.

subopt151

Enables Subopt-1.

subopt2

Enables Subopt-1.

dhcp-server1

Sets DHCP server 1.

dhcp-server2

Sets DHCP server 1.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only. If a user configures L2oGRE server as IPv6 address, DHCP relay is **not** supported in release 6.0 but is supported on IPv4 address.

Examples

The following example creates a l2ogre profile named newprofile123 and configures DHCP relay with DHCP Option82 parameters.

```
device# config
device(config)# l2ogre newprofile123
device(config-l2ogre-profile)# icmp-keep-alive-period 20
```

Examples

The following example enables Subopt-1.

```
device# config
device(config)# l2ogre newprofile123
device(config-l2ogre-profile)# dhcp-relay
device(config-l2ogre-profile)# dhcp-option82
device(config-l2ogre-profile-dhcp-option82)# subopt1 ap-ssid
```

The following example disables DHCP Relay when in the Zone configuration mode.

```
device(config-l2ogre-profile)# no dhcp-relay
Do you want to continue to disable (or input 'no' to cancel)? [yes/no] yes
Successful operation
```

lbs-service

Syntax

lbs-service *name*

After the **lbs-service** command is entered to enable the Location Services (SPoT) configuration mode, the following configuration syntax is available:

[**host** *host-ip-address* | **password** *pwd* | **port** *port-number* | **venue** *venue name*]

Command Default

The Location Services (SPoT) settings are not configured.

Parameters

name

Specifies an Location Services (SPoT) name.

host *ip-address*

Sets the LBS server host IP address.

password *pwd*

Sets the LBS server password.

port *port-num*

Sets the LBS server port number.

venue *name*

Sets the LBS venue name.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller. The default port number is 8883.

Examples

The following example shows how to configure various SPoT profile options.

```
device# config
device(config)# lbs-service spot
device(config-lbs-service)# host 10.10.2.3
device(config-lbs-service)# password Jxygl23
device(config-lbs-service)# port 3
device(config-lbs-service)# venue spot
```

ldap-service

Creates or updates the LDAP (Lightweight Directory Access Protocol) configuration.

Syntax

ldap-service *name*

After the **ldap-service** command is entered to enable the LDAP configuration mode, the following configuration syntax is available:

[**admin-domain-name** *admin-domain* | **admin-password** *admin-password* | **base-domain-name** *base-domain* | **description** *text* | **friendly-name** *friendly-name* | | **group-attrs** *attr-value* | **ip-address** *ip-address* **key-attr** *key-attribute* | **no group-attrs** | **port** *port-number* **search-filter** *search-filter*]

Command Default

The LDAP (Lightweight Directory Access Protocol) service settings are not configured.

Parameters

name *name*

Sets the LDAP service name.

admin-domain-name *admin-domain*

Creates or updates the admin domain. For example, cn=admin, dc=ldap, dc=com.

admin-password *admin-password*

Creates or updates the admin password.

base-domain *base-domain*

Creates or updates the base domain. For example, dc=ldap,dc=com

description *text*

Sets the description of the LDAP service for the user.

friendly-name *friendly-name*

Sets the LDAP service friendly name.

group-attrs *attr-value*

ip-address *ip-address*

Sets the IP address for the primary server.

key-attr *key-attribute*

Sets the key attribute to denote users. For example, default: uid.

no group-attrs

Disables group attributes.

port *number*

Sets the port for the primary server. Default port number is 389.

search-filter *search-filter*

Sets the search filter. Example, (objectClass=Person, show more...)

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Admin domain name : To query multiple organizational units, enter an admin domain name and -password with full search and read privileges.(example: uid=admin,dc=ldap,dc=com).

Examples

The following example configures an active LDAP service configuration mode.

```
device# config
device(config)# ldap-service lds
device(config-ldap-service)#
```

The following example sets the port for the primary server in LDAP service configuration mode.

```
device# config
device(config)# ldap-service lds
device(config-ldap-service)# port 1
```


legacy-ssh-algorithm

Disables/Enables legacy ssh algorithm from SmartZone SSH.

Syntax

[**legacy-ssh-algorithm**]*disable* | *enable*

Parameters

legacy-ssh-algorithm *disable*

Displays the warning message. After the confirmation the command is executed successfully.

legacy-ssh-algorithm *enable*

Legacy ssh algorithm is enabled successfully.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows how to disable/enable ssh-legacy-algorithm.

```
device# config
device(config)# legacy-ssh-algorithm disable
WARNING: ICX switches/routers running firmware lower than 09.10 will not be able to connect to the SZ
by disabling legacy ssh algorithm.
But connected switches with unsupported firmware continue to be registered until they are rejoined.
Do you want to continue? (or input 'no' to cancel)? [yes/no] yes
Successful operation

device(config)# legacy-ssh-algorithm enable
Successful operation
```

license cloud

Enables the cloud license server.

Syntax

license cloud enable

Command Default

License cloud is not enabled by default.

Parameters

enable

Enables the cloud license server.

Modes

Global configuration mode

Usage Guidelines

Cloud License Server also known as the SmartLicense server, is a cloud-based server that stores all of the licenses and support entitlements that you have purchased for the controller. For information on how to set up and activate your SmartLicense account, see the *SmartLicense User Guide*. This command is supported on the all SmartZone platforms except vSZ-D controller.

Examples

The following example of enabling cloud license.

```
device# config
device(config)# license cloud enable
Are you sure you want to change the license server configuration?
All current license data will be wipe out!! (or input 'no' to cancel)? [yes/no]
```

license export

Exports the license details.

Syntax

`license export ftp-url`

Command Default

License export is not configured by default.

Parameters

ftp-url

Specifies the FTP URL.

Modes

Global configuration mode

Usage Guidelines

Another scenario where this command can be used is when a user wants to shutdown the controller and return the installed licenses. The user can use **export license** to export the bin file and return to the license server.

This command is supported on the all SmartZone platforms except vSZ-D controller.

Enter the FTP URL in the following format: `ftp://username:password@ftp-host[/dir-path]`

Examples

The following example license export.

```
device# config
device(config)# license export ftp://mahan:ruckus1!@172.19.7.100/backup/AP_ad87453456fe.csv
```

license import

If the controller is disconnected from the Internet or is otherwise unable to communicate with the RUCKUS SmartLicense system (due to firewall policies, etc.), you can manually import a license entitlement file into the controller

Syntax

```
license import ftp-url
```

Command Default

License export is not configured by default.

Parameters

ftp-url

Specifies the FTP URL.

Modes

Global configuration mode

Usage Guidelines

The option to import a license file manually into the controller is only available if the controller is using the cloud license server. The controller, which cannot reach to the license server can import the licenses by downloading it from license server and then use the **import license** to install it.

This command is supported on the all SmartZone platforms except vSZ-D controller.

Enter the FTP URL in the following format: `ftp://username:password@ftp-host[/dir-path]`

Examples

The following example importing the license.

```
device# config
device(config)# license import ftp://mahan:ruckus1!@172.19.7.100/backup/AP_ad87453456fe.csv
```

license local

RUCKUS provides two options for managing the licenses that you have purchased for the controller - Cloud License Server and Local License Server (LLS).

license local *local-server*

Command Default

License local is not configured by default.

Parameters

local-server

Specifies the FQDN (fully qualified domain name) or IP address of the LLS.

Modes

Global configuration mode

Usage Guidelines

LLS allows you set up on the network by configuring the local server details by specifying either the domain name or the IP address. , and then configure the domain and port details. Each device will sync up the license with LLS once per day. Each LLS will sync up the license pool with the Cloud Server once per day. This command is supported on the all SmartZone platforms except vSZ-D controller.

Examples

The following example configures the local license.

```
device# config
device(config)# license local 10.174.84.201
Are you sure you want to change the license server configuration?
All current license data will be wipe out!! (or input 'no' to cancel)? [yes/no]
```

license sync-now

Automatically synchronizes the license information with the selected license server.

license sync-now

Command Default

License sync-now is not configured by default.

Modes

Global configuration mode

Usage Guidelines

The controller saves the selected license server configuration, deletes all of its saved license data, and then automatically synchronizes the license information with the selected license server. This command is supported on the all SmartZone platforms except vSZ-D controller.

Examples

The following example automatically synchronizes the license.

```
device# config
device(config)# license sync-now
<cr>
```

lineman

Sets up the workflow URL or uploads the workflow file.

Syntax

lineman

no lineman [*workflow-url*]

After the **lineman** command is entered, the following configuration syntax is available:

workflow-file *ftp-url*

workflow-url *url*

Parameters

workflow-file

Executes the work flow with the FTP URL.

workflow-url

Executes the work flow with the URL.

ftp-url

Specifies the FTP URL.

url

Specifies the URL.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the all SmartZone platforms except vSZ-D controller.

Examples

The following example on lineman workflow.

```
device# config
device(config)# ruckus(config)# lineman workflow-file https://172.19.10.4:8443
```

localdb-service

Creates or updates the local database service configuration.

Syntax

After the **localdb-service** command is entered to enable the local database service configuration mode, the following configuration syntax is available:

```
[description text | friendly-name friendly-name | | group-attrs attr-value ]
```

Command Default

The local database service settings are not configured.

Parameters

- description** *text*
Sets the description of the LDAP service for the user.
- friendly-name** *friendly-name*
Sets the LDAP service friendly name.
- group-attrs** *attr-value*
Sets the user traffic profile mapping.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows how to configure various local database service options.

```
device# config
device(config)# localdb-service
device(config-localdb-service)# friendly-name local
```


logging

Enables the logging of the console.

Syntax

After the **logging** command is entered to enable the logging service configuration mode, the following configuration syntax is available:

```
[console CaptivePortal | Cassandra | Ccmd | Ccmsync | Collectd | Communicator | Configurer | Core | DBlade | DeviceManager | EAut |  
ElasticSearch | EventReader | LogMgr | MdProxy | Mosquitto | MrProxy | MsgDist | NginX | Northbound | Observer | RabbitMQ |  
RadiusProxy | Redis | SNMP | ScgUniversalExporter | Scheduler | SessMgr | StatsHandler | SubscriberManagement | SubscriberPortal |  
Switchm | Web | CLI ]
```

```
no logging [ console ]
```

Command Default

The local database service settings are not configured.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller. The **no** form of the command disables all logging on the console and changes to default log level.

Examples

The following example shows how to configure login console options.

```
device# config  
device(config)# login console Switchm
```

Iwapp2scg

Updates the LWAPP2SCG configuration.

Syntax

lwapp2scg

no nat-ip-translation

After the **lwapp2scg** command is entered, the following configuration syntax is available:

[**nat-ip-translation** | **pasv-port** *port* | **policy** {*accept* | *accept-all* | | *deny* | *deny-all* | *seconds* }]

Command Default

The LWAPP2SCG settings is enabled on executing the command.

Parameters

nat-ip-translation

Enables network address translation (NAT) in FTP passive mode.

pasv-port *port*

Sets the minimum and maximum port for the dynamic data transmission port range.

policy {*accept* | *accept-all* | | *deny* | *deny-all* | *seconds* }

Sets the ALC policy.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the all SmartZone platforms except vSZ-D controller.

Parameter *nat-ip-translation* mode is enabled by default if the user's NAT cannot support PASV-mode FT. For parameter *pasv-port* PASV-mode FTP to work, the user has to set up a firewall that restricts the range of ports opened by the FTP server, thereby remaining secure, and enabling the download of AP firmware. Parameter *policy* the:

- *accept* option allows upgrade of individual APs as required by specifying the MAC address or serial number.
- *accept-all* option allows upgrade of all APs simultaneously. Make sure that there are no existing Zone Director (ZD) deployments in the same sub-net and are still in use. All the ZD APs will be affected and upgraded to the controller.
- *deny* option excludes specific APs from being upgraded to controller based on the MAC address or serial number.
- *deny-all* options excludes all APs from being upgraded to the controller.

Examples

The following example enables the network address translation.

```
device# config
device(config)# lwapp2scg
device(config-lwapp2scg)# nat-ip-translation
<cr>
```

manage-alias-ssh-port

Assigns and configures new port number for SSH traffic.

Syntax

`manage-alias-ssh-port { Set alias SSH port | Get alias SSH port | Delete alias SSH port }`

Command Default

A new port number is set for SSH traffic.

Parameters

Set alias SSH port

Enter the new port number.

Get alias SSH port

Assigns the new port number for SSH traffic.

Delete alias SSH port

Deletes the assigned port number.

Modes

Debug configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms.

Examples

```
device# debug

device(debug)# debug-tools
[Change to system]
Welcome to Debug CLI Framework!
(debug tool-set) system $ use sz
[Change to sz]
(debug tool-set) sz $ manage-alias-ssh-port

1.) Set alias SSH port
2.) Get alias SSH port
3.) Delete alias SSH port
Select Option (1/2/3): 1
Enter the port number: 6155
Done
[Execution Done!]
(debug tool-set) sz $ manage-alias-ssh-port

1.) Set alias SSH port
2.) Get alias SSH port
3.) Delete alias SSH port
Select Option (1/2/3): 2
6155
[Execution Done!]
(debug tool-set) sz $ manage-alias-ssh-port

1.) Set alias SSH port
2.) Get alias SSH port
3.) Delete alias SSH port
Select Option (1/2/3): 3
Done
[Execution Done!]
(debug tool-set) sz $
```

mgmt-acl

Creates or updates the management interface access control list configuration.

Syntax

mgmt-acl

no enable

After the **mgmt-acl** command is entered the following configuration syntax is available:

[**enable**]

After the **enable** command is entered, the following configuration syntax is available:

[**rule name**]

After the **mgmt-acl rule name** command is entered the following configuration syntax is available:

[**description text** | **restriction** { *ipv6-subnet <ip>* | *range <ip>* | *single <ip>* | *subnet <ip>* }]

Command Default

Management interface access settings is enabled on executing the command.

Parameters

enable

Enables the access control of the management interface.

rule name

Creates or updates the management interface ACL rule configuration.

description text

Sets the description of the LDAP service for the user.

restriction { *ipv6-subnet <ip>* | *range <ip>* | *single <ip>* | *subnet <ip>* }

Sets the restriction for the rule.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the all SmartZone platforms except vSZ-D controller.

- *ipv6-subnet <ip>* sets the subnet restriction along with network address and subnet mask .
- *range <ip>* set the IP range restriction with start and end IP addresses.
- *single <ip>* set the single IP restriction and IP address.
- *subnet <ip>* sets the subnet restriction along with network address.

Examples

The following example sets the rule name for management interface ACL.

```
device# config
device(config)# mgmt-acl
device(config-mgmt-acl)# enable
device(config-mgmt-acl)# rule ruleacl
<cr>
```

mvno

Creates or updates the Mobile Virtual Network Operator (MVNO) configuration.

Syntax

mvno *name*

no admin-radius capabilities zone

After the **mvno** command is entered the following configuration syntax is available:

[**admin** | **admin-radius** *name* | **capabilities** { *administration* | *configuration* | *device* | *identity* | *monitor* | *reports* | *capabilities-depth-1* }
| **description** *text* | **zone** *name*]

After the **mvno-admin** command is entered to enable the Admin configuration mode, the following configuration syntax is available:

[**email** *email-address* | **name** *name* | **password** | **phone** *number* | **real-name** *name* | **title** *job-title*]

After the **mvno-admin-radius** command is entered, the following configuration syntax is available:

[**ip** *ip-address* | **port** *port-number* | **shared-secret** *password* | | **type**{ *radius* | *tacacs*}]

Command Default

MVNO interface is enabled on specifying the MVNO interface name.

Parameters

admin *name*

Specifies an administrator account.

admin-radius *name*

Specifies the RADIUS server for administrators.

capabilities { *administration* | *configuration* | *device* | *identity* | *monitor* | *reports* | *capabilities-depth-1* }

Creates or updates the custom connection capabilities.

description *text*

Sets the description of the L2oGRE profile for the user.

zone *text*

Move the access point to another zone.

email *email-address*

Sets the email address for the user.

name *name*

Sets the administrator account name or the RADIUS server name.

password *password*

Sets the password for the account

phone *number*

Sets the phone number of the user.

real-name *name*

Sets the real name of the user.

title *job-title*

Sets the job title of the user.

ip-address *ip-address*

Sets the IP address for the primary RADIUS server.

portnumber

Sets the port number for the primary RADIUS server.

shared-secret *password*

Sets the shared secret for the primary RADIUS server. Valid values range from 1 through 255 characters.

type

Sets the authentication type.

radius

Specifies RADIUS authentication.

tacacs

Specifies TACACS authentication.

Modes

Global configuration mode

Usage Guidelines

A Mobile Virtual Network Operator (MVNO) uses a host carrier network to service its mobile users. An MVNO account is created for each operator and the MVNO page lists the accounts that are created. This command is supported only on SmartZone 300 and vSZ-H platforms.

- **capabilities** *administration* sets the xxx.
- **capabilities** *configuration* sets the xxx.
- **capabilities** *device* sets the xxx
- **capabilities** *identity* sets the xxx.
- **capabilities** *monitor* sets the xxx.
- **capabilities** *reports* sets the xxx.
- **capabilities** *capabilities-depth-1* sets the xxx.

Examples

The following example sets the RADIUS server for an MVNO account.

```
device# config
device(config)# mgmt-acl
device(config-mvno)# admin-radius radius
device(config-mvno-admin-radius)#
<cr>
```

nat

Creates or sets the NAT server configuration settings.

Syntax

nat nat

no set [*filter*]

nat name

After the **nat** command is entered the following configuration syntax is available:

[**nat-log-syslog** { *level value* } | **set filter**{ *private-ip ip-address* | *private-portport-number* | *public-ipip-address* | *public-portport-number* | *ue-mac mac-address*} | **show**]

After the **nat nat** command is entered the following configuration syntax is available to set a pool of NAT servers:

name

NOTE

The **show** command is documented as separate command in the Show Command chapter. Refer to [show nat](#) on page 383

Command Default

NAT server configurations is enabled on entering the **nat** command.

Parameters

nat-log-syslog *value*

Specifies the Syslog level in the range 1 to 7.

set *filter*

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.

- **set filter private-ip ip-address** sets the xxx.
- **set filter private-portport-number** sets the xxx.
- **set filter public-ipip-address** sets the xxx
- **set filter public-portport-number** sets the xxx.
- **setfilter ue-mac mac-address** sets the xxx.

Examples

The following example sets the filter for NAT server.

```
device# config
device(config)# nat
device((config-nat)# set filter
device(config-nat)# set filter private-port 90
Remember type "end" and type "show ue-nat-session" in first layer
<cr>
```

Commands J through N

no cls-sess msisdn

no cls-sess msisdn

Deletes the session information of the UE for the specified MSISDN.

no cls-sess msisdn*msisdn*

Command Default

The session information is not deleted.

Parameters

msisdn

Specifies the MSISDN value. The length of MSISDN should be between 10 to 15 digits.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone 300 only.

Examples

The following example deletes the session information of the UE for a specified MSISDN.

```
device# config
device(config)# no cls-sess msisdn 123456789012345
```

no control-plane

Removes the control plane from the cluster configuration.

no control-plane*name*

Command Default

The control plane is not removed from the cluster configuration.

Parameters

name

Specifies the name of the control plane.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone DataPlane and SmartZone 300.

Examples

The following example removes a control plane from the cluster configuration.

```
device# config
device(config)# no control-plane cp1
```

no data-plane

Removes a data plane and disables the STP package bridge.

Syntax

```
no data-plane name forward-stp
```

Command Default

Data plane configurations are not removed.

Parameters

name

Specifies a data plane.

forward-stp

Disables the STP package bridge.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone 100 and vSZ-H controllers only.

Examples

The following example removes a data plane and disables the STP package bridge.

```
device# configure
device(config)# no data-plane NODE202-D0 forward-stp

Do you want to continue to disable (or input 'no' to cancel)? [yes/no] yes
Successful operation
```

no domain

Deletes management domains or access point zones in a specific domain configuration.

Syntax

```
domain [ name zone zone-name [ aaa aaa-server-name | ap mac-address | ap-group group-name | ap-registration-rule priority |  
hotspot WISPr-name | wlan wlan-name | wlan-group name ] ]
```

Command Default

Management domains or access point zones are not deleted..

name

Specifies the domain name.

zone *name*

Specifies an AP zone of a domain.

aaa *aaa-server-name*

Specifies AAA Servers.

ap *mac-address*

Specifies an AP.

ap-group *group-name*

Specifies AP groups.

ap-registration-rule *priority*

Specifies AP registration rules.

hotspot *WISPr-name*

Specifies WISPr (Hotspot).

wlan *wlan-name*

Specifies WLANs.

wlan-group *name*

Specifies WLAN groups.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only.

Commands J through N
no domain

Examples

The following example deletes an AP zone for a domain.

```
device# config  
device(config)# no domain indus5-d zone zone1
```


no oauth-service

Deletes OAuth service configuration.

Syntax

no oauth-service *name*

Command Default

OAuth service configurations are not deleted.

Parameters

name

OAuth service name

Modes

Global configuration mode

Usage Guidelines

This command is supported for SmartZone 100 devices.

Examples

The following example shows how to disable the OAuth server named nam3.s.

```
device# config
device(config)# no oauth-service nam3
Do you want to continue to delete (or input 'no' to cancel)? [yes/no]
```

Commands J through N
no osu-portal-profile

no osu-portal-profile

Deletes OSU (Online SignUp) portal profile configurations.

Syntax

osu-portal-profile*name*

Command Default

OSU portal profile configurations are not deleted.

Parameters

name

Sets the operator profile name.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example disables all settings for the OSU portal profile named ops3.

```
device# config
device(config)# no osu-portal-profile ops3
Do you want to continue to delete (or input 'no' to cancel)? [yes/no] yes
```

no zone

Deletes specified configuration parameters from all AP zones, except the staging zone.

Syntax

no zone*zone-name*[**aaaaaa-server-name** | **ap***ap-mac-address* | **ap-group***ap-group-name* | **ap-registration-rule***priority* | **guest-access***guest-access-name* | **hotspot***wispr-name* | **web-authentication***guest-access-name* | **wlan***wlan-name* | **wlan-group***wlan-group-name* | **wlan-scheduler***guest-access-name*]

Command Default

AP zone configurations are not deleted.

Parameters

aaaaaa-server

Deletes the named AAA servers from the specified AP zone.

ap*mac-address*

Deletes the AP that matches the specified MAC address from the specified AP zone.

ap-group*ap-group-name*

Deletes the named AP groups from the specified AP zone.

ap-registration-rule*priority*

Deletes the AP registration rules from the specified AP zone.

guest-access*template-name*

Deletes the named guest access from the specified AP zone.

hotspot*wispr-name*

Deletes the WISPr (Hotspot) from the specified AP zone.

web-authentication*template-name*

Deletes web authentication from the specified AP zone.

wlan*wlan-name*

Deletes the named WLAN from the specified AP zone.

wlan-group*wlan-group-name*

Deletes the WLAN group from the specified AP zone.

web-authentication*template-name*

Deletes the named WLAN scheduler profiles from the specified AP zone.

Modes

Global configuration mode

Commands J through N

no zone

Usage Guidelines

A separate **zone** command exists with a **no** form in zone configuration mode to delete a specified zone configuration. For more details, see the **zone** command in the SmartZone Command Reference.

Examples

The following example deletes guest access from all APs in the zone for users specified in Template2.

```
device# config
device(config)# zone zone-discovery
device(config-zone)# no guest-access template2
Do you want to continue to delete (or input 'no' to cancel)? [yes/no] yes
```

node-affinity-config

Creates or updates the node affinity configuration.

Syntax

node-affinity-config

no enable

After the **node-affinity-config** command is entered the following configuration syntax is available:

[**enable**]

After the **enable** command is entered, the following configuration syntax is available:[**profile name** | **retry value**]

After the **node-affinity-config profile name** command is entered the following configuration syntax is available:

[{**blade-list** *node name* {*priority* | *up* | *down*}} | **description text**]

Command Default

The **node-affinity-config** settings is enabled on executing the command.

Parameters

enable

Enables the node affinity configuration set of commands.

profile name

Creates the Node Affinity Profile.

retry value

Sets the number of times an AP will attempt to connect to the preferred node. The default value is 3 and the accepted range is 1 to 10. If the AP is unable to connect to the preferred node, it will attempt to connect to the node that is next in the order of node priority.

blade-list *node name* {*priority* | *up* | *down*}

Sets the node order list by specifying it as Up or Down to position the node in the required order.

description text

Sets the description of the node profile for the user.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone 300 controller only. Node affinity enables administrators to manually configure the controller nodes to which APs will connect. To do this, set the order of preferred nodes on the node affinity page. Node affinity is implemented at the AP zone level, which means that all APs that belong to a zone will have the same node affinity settings. If you want APs that belong to the same zone to connect to the same node whenever possible, you can configure set the preferred node for a particular zone.

NOTE

1. An affinity profile defines the order of the nodes to which APs that belong to the same zone will connect.
2. Node affinity profile works only if it is restored in the same cluster. If the configuration must be restored to a different cluster, disable node affinity and remove the node affinity profiles containing nodes that are not available in the new cluster.

Examples

The following example enables the node affinity configuration.

```
device# config
device(config)# node-affinity-config
device(config-node-affinity-config)# enable
<cr>
```

The following example sets the node priority to UP.

```
device# config
device(config)# node-affinity-config
device(config-node-affinity-config)# enable
device(config-node-affinity-config)# profile prof
device(config-node-affinity-config-profile)# blade-list NODE201 priority up
NODE201 > KKK-SZ300
<cr>
```

non-tpm-switch-cert-validate

Enables validation of non TPM (Trusted Platform Module) switch certificate.

Syntax

non-tpm-switch-cert-validate

no non-tpm-switch-cert-validate

Command Default

non TPM (Trusted Platform Module) switch certificate is enabled.

Parameters

non-tpm-switch-cert-validate

Enables the certificate validation.

Modes

Global configuration mode

Usage Guidelines

On some ICX 7250, ICX 7450, or ICX 7750 devices, self-signed certificates are used. SmartZone honors these certificates when the **non-tpm-switch-cert-validate** command is entered on the SmartZone console. This command is supported on all platforms except SmartZone Data Plane. The no form of the command removes the validated non TPM (Trusted Platform Module) switch certificate.

Examples

The following example enables the non TPM (Trusted Platform Module) switch certificate.

```
device# config
device(config)# non-tpm-switch-cert-validate
ap-cert-check should enable first then change ap-cert-expired-check
<cr>
```

History

Release version	Command history
5.1	This command was added.

northbound-authtype

Sets the RADIUS authentication type to Northbound Portal interface.

Syntax

```
northbound-authtype [CHAP | PAP ]
```

Command Default

No authentication method is specified.

Parameters

CHAP

Specifies the Challenge Handshake Authentication Protocol (CHAP) protocol.

PAP

Specifies the Password Authentication Protocol (PAP) protocol.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all platforms except SmartZone Data Plane. To ensure that the controller administrators will be able to authenticate successfully with the RADIUS server authentication type that you selected.

Examples

The following example enables the authentication type.

```
device# config
device(config)# northbound-authtype
device(config)# northbound-authtype CHAP
<cr>
```


northbound-portal

Creates or modifies the Northbound Portal interface configuration.

Syntax

northbound-portal password

Command Default

No Northbound portal is specified.

Parameters

password

Sets the password for Northbound Interface support.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all platforms except SmartZone Data Plane. Third-party applications use the northbound portal interface to authenticate users and to retrieve user information during the UE (User Equipment) association.

Examples

The following example enables the Northbound Interface.

```
device# config
device(config)# northbound-portal
<password> Password
<cr>
```

ntp-server

Creates the NTP server configuration.

Syntax

ntp-server ntp-server

Command Default

No NTP server is specified.

Parameters

ntp-server

Sets the NTP server IP address or domain name.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all platforms except SmartZone Data Plane. The controller has three external Network Time Protocol (NTP) servers that are used to synchronize the time across Access Points, Cluster nodes, and vSZ-DPs.

Examples

The following example to set the NTP server configuration.

```
device# config
device(config)# ntp-server 10.174.84.201
<cr>
```

Commands O through Sh

operator-profile

Creates or updates a WiFi operator profile configuration.

Syntax

operator-profile *name*

no operator-profile *name*

After the **operator-profile** command is entered to enter Operator-profile configuration mode, the following configuration syntax is available:

```
{ domain-names domain-name | friendly-names language name | signup-security osen-cert cert# }
```

Command Default

A WiFi operator profile is not configured.

Parameters

name

Sets the operator profile name.

domain-names *domain-name*

Sets the domain name.

friendly-names *friendly-name*

Sets a user-friendly name seen by the user.

signup-security

Enables OSEN (Support for Anonymous Authentication).

osen-cert *cert#*

Uploads the specified operator certificate.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Although you can configure the options individually, you must configure all the options to create a WiFi operator profile.

Use the **no** form of this command without a profile name to disable the profile settings for all configured WiFi operators.

Examples

The following example shows how to create a WiFi operator profile with a domain name, friendly name and language, and to enable OSEN with an uploaded security certificate.

```
device# config
device(config)# operator-profile orangewifi
device(config-operator-profile)# domain-names domain-mktg
device(config-operator-profile)# friendly-names fre marketing
device(config-operator-profile)# signup-security
device(config-operator-profile)# osen-cert oc#12345
```

The following example disables all settings for the WiFi operator profile named orangewifi.

```
device# config
device(config)# no operator-profile orangewifi
Do you want to continue to delete (or input 'no' to cancel)? [yes/no] yes
```

outbound-firewall

Creates or updates the outbound firewall configuration.

Syntax

outbound-firewall

no outbound-firewall

After the **outbound-firewall** command is entered to enter Outbound Firewall configuration mode, the following configuration syntax is available:

[**enable** | **ip-rule** *profile-name* **out** { **sctp** | **tcp** | **udp** { **dport** *port* | **sport** *port* } }] [**dst** | **scr**] *ip-address*

no ip-rule *profile-name*

Command Default

An outbound firewall is not configured.

Parameters

enable

Enables all outbound traffic.

ip-rule *profile-name* **out**

Allows output traffic for the specified IP rule table profile through the outbound firewall.

sctp

Allows SCTP traffic.

tcp

Allows TCP traffic.

udp

Allows UDP traffic.

dport *port*

Destination port.

sport *port*

Source port.

dst *ip-address*

IP address for the specified destination port.

src *ip-address*

IP address for the specified source port.

Modes

Global configuration mode

Usage Guidelines

In Outbound Firewall configuration mode the **no ip-rule *profile-name*** command options removes the specified IP rule profile.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

The **no** form of this command disables the outbound firewall.

Examples

The following example shows how to allow TCP outbound traffic for the destination IP address 10.10.2.4 through the outbound firewall.

```
device# config
device(config)# outbound-firewall
device(config-outbound-firewall)# ip-rule profile1 out tcp dport eth2 dst 10.10.2.4
```

output-format

Enables output formatting.

Syntax

output-format

no output-format

Command Default

Output formatting is not enabled.

Modes

Debug configuration mode

Usage Guidelines

The **no** form of this command disables the output formatting.

Examples

The following example shows how to enable output formatting.

```
device# debug
device(debug)# output-format
```

patches

Uploads, applies and displays patch scripts.

Syntax

patches

no patches

After the **patches** command is entered, the following configuration syntax is available in patches configuration mode:
{ **apply** *script-name* [*script-options*] | **show** { **applied-patches** | **uploaded-patches** } | **upload** *ftp-url* }

Command Default

No patches are uploaded or applied.

Parameters

apply

Applies a patch script.

script-name

Name of script.

script-options

Optional script parameters.

show

Displays applied or uploaded script lists.

applied-scripts

Displays applied patches list.

uploaded-scripts

Displays uploaded patches list.

upload*ftp-url*

Uploads the patch script from a remote FTP server. The FTP URL must be in the following format: `ftp://<username>:<password>@<ftp-host>/<file-path>`

Modes

Privileged EXEC mode

Usage Guidelines

New AP models and firmware updates are supported without the need to upgrade the controller image by using AP patch files. Use the command to view patch scripts already applied or uploaded, and upload and apply scripts as required. Once a patch script has been applied, it cannot be reapplied.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

The **no** form of the command deletes a patch script. If the patch script is applied, it cannot be deleted.

Examples

The following example shows how to apply a patch file.

```
device# patches
device(patches)# upload ftp://ruckus:admin@commscope.com/files/julypatch.patch
device(patches)# apply julypatch.patch
```

ping

Sends an ICMP echo request to the network host.

Syntax

`ping options`

Command Default

No ICMP echo requests are sent.

Parameters

options

Specifies the desired response.

Modes

Privileged EXEC mode

Usage Guidelines

Use the command when troubleshooting to ping an IP address to determine connectivity issues and the network path to the network host server.

This command is supported on all the controllers including the SmartZone Data Plane.

Examples

The following example shows how to ping a network host at IP address 172.17.20.162.

```
device> ping 172.17.20.182
Start ping server (172.17.20.182) for 3 times...
PING 172.17.20.182 (172.17.20.182) 56(84) bytes of data.
64 bytes from 172.17.20.182: icmp_req=1 ttl=63 time=1.64 ms
64 bytes from 172.17.20.182: icmp_req=2 ttl=63 time=1.15 ms
64 bytes from 172.17.20.182: icmp_req=3 ttl=63 time=1.01 ms
--- 172.17.20.182 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 1.015/1.271/1.647/0.273 ms.
```

The following example shows what happens when a host cannot be found.

```
device> ping 10.15.5.3
Pinging 10.15.5.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

ping6

Sends an ICMP echo request to the network host.

Syntax

`ping6options`

Command Default

No ICMP echo requests are sent.

Parameters

options

Specifies the desired response.

Modes

Privileged EXEC mode

Usage Guidelines

Use the command when troubleshooting to ping an IPv6 address to determine connectivity issues and the network path to the network host server.

This command is supported on all the controllers including the SmartZone Data Plane.

Examples

The following example shows how to ping a network host at IPv6 address 2001:DB8::200C:417A.

```
device> ping6 2001:DB8::200C:417A
```

profile-based-nat

Enables or disables the display of NAT server configuration, when the customer logs in the next time.

Syntax

```
profile-based-nat { enable | disable }
```

Command Default

The NAT server configuration is hidden.

Parameters

enable

Displays the NAT server configuration after the next login.

disable

Hides the NAT server configuration after the next login.

Modes

Debug configuration mode

Usage Guidelines

Use the command to avoid displaying the NAT server configuration unless you need to update it.

This command is supported on the SmartZone Data Plane controllers only.

Examples

The following example enables the display of the NAT server configuration after you login again.

```
device> enable
device# debug
device(debug)# profile-based-nat enable
```

The following example disables the display of the NAT server configuration after you login again.

```
device> enable
device# debug
device(debug)# profile-based-nat disable
```

proxy-aaa

Creates or updates the proxy AAA server configuration settings.

Syntax

```
proxy-aaa name
```

Parameters

name

Proxy AAA server name.

Modes

Global configuration mode

Usage Guidelines

This command is supported for SmartZone 100 devices.

Examples

The following example shows how to create a proxy AAA server configuration.

```
device# config
device(config)# proxy-aaa proxy-server1
```

radius-service

Configures the RADIUS service options.

Syntax

radius-service *name*

no radius-service *name*

After the **radius-service** command is entered to enter RADIUS server configuration mode, the following configuration syntax is available:

{ **auto-fallback-disable** | **backup friendly-name** *language name* | **group-attrs** *attr-value user-role* | **ip** *ip-address* | **mor** *number* | **no-response-fail** | **out-of-band** | **port** *port-number* | **response-window** *window* | **revive-interval** *interval* | **sanity-timer** *seconds* | **shared-secret** *password* | **threshold** *number* | **type** [**radiusv** | **radius-acct**] | **zombie-period** *seconds* }

Command Default

A RADIUS server is not configured.

Parameters

name

RADIUS server name.

auto-fallback-disable

Disables auto fallback.

backup

Enables backup RADIUS support and related settings.

friendly-name *friendly-name*

Sets a user-friendly name for the RADIUS server.

group-attrs *attr-value user-role*

Sets attribute and user role values for the User Traffic Profile Mapping.

ip *ip-address*

Sets the IP address of the primary RADIUS server.

mor *number*

Sets the Maximum Outstanding Requests (MOR) per server. Number must be 0 or in the range of 10 to 4096.

no-response-fail

Enables the no response fail.

out-of-band

Enables the RFC 5580 Out of Band location delivery feature.

port *port-number*

Sets the port number for the primary RADIUS server

response-window *window*

Sets the response window, in seconds. Range from 5 to 30.

revive-interval *interval*

Sets the revive interval, in seconds. Range from 60 to 3600.

sanity-timer *seconds*

Sets the sanity timer, in seconds.

shared-secret *password*

Sets the shared secret password for the primary RADIUS server.

threshold *percentage*

Sets the threshold percentage. Range from 10 to 90 percent.

type radius *radius-acct*

Sets the RADIUS type.

zombie-period *seconds*

Sets the Zombie period in seconds. Range from 30 to 120.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command without a RADIUS server name to disable the configuration for all configured RADIUS servers.

Although you can configure the options individually and some are optional, you must configure the following options to create a basic RADIUS server configuration.

- **ip** *ip-address*
- **port** *port-number*
- **shared-secret** *password*

Before you can configure the **auto-fallback-disable** command and the backup options, you must enter the **backup** command without any options.

Examples

The following example shows how to create a proxy AAA server configuration.

```
device# config
device(config)# radius-service rad01
device(config-radius-service)# backup
device(config-radius-service)# backup ip 10.10.2.3
device(config-radius-service)# backup port 4
device(config-radius-service)# backup shared-secret
Password: ***
Retype: ***
```

The following example disables settings for all RADIUS server.

```
device# config
device(config)# no radius-service
Do you want to continue to delete (or input 'no' to cancel)? [yes/no] yes
```

History

Release version	Command history
3.5.1	This command was updated.

rbdump

Displays the board data of the controller.

Syntax

rbdump

Command Default

Controller board data is not displayed.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example displays the board data for the controller.

```
device# rbdump
name: Gallus
magic: 35333131
cksum: 6dd
rev: 5.4
Serial#: 00000089
Customer ID: ruckus
Model: SCG1k
V54 Board Type: Undef
V54 Board Class: AP71
Random#: 0000 0000 0000 0000 0000 0000 0000 0000
symings: no
ethport: 0
V54 MAC Address Pool: yes, size 32, base 00:1D:2E:89:00:00
major: 0
minor: 0
pciId: 0000
dblade0: yes 00:1D:2E:89:00:10
dblade1: yes 00:1D:2E:89:00:18
eth0: yes 00:1D:2E:89:00:00
eth1: yes 00:1D:2E:89:00:01
eth2: - 00:1D:2E:89:00:02
eth3: - 00:1D:2E:89:00:03
eth4: - 00:1D:2E:89:00:04
eth5: - 00:1D:2E:89:00:05
uart0: no
sysled: no, gpio 0
sysled2: no, gpio 0
sysled3: no, gpio 0
sysled4: no, gpio 0
Fixed Ctry Code: no
Antenna Info: no, value 0x00000000
Local Bus: disabled
factory: yes, gpio 8
serclk: internal
cpufreq: calculated 0 Hz
sysfreq: calculated 0 Hz
memcap: disabled
watchdog: enabled
```

rebalance-aps

Rebalances the AP load across control or dataplane nodes that exist within a cluster.

Syntax

rebalance-aps

Command Default

No rebalancing is performed.

Modes

Global configuration mode

Usage Guidelines

AP rebalancing helps distribute the AP load across nodes that exist within a cluster. When a multi-node cluster is upgraded, the node that reboots the last typically does not have any APs associated with it.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows how to rebalance the AP load.

```
device# config
device(config)# rebalance-aps
```

Commands O through Sh
reboot

reboot

Reboots the controller.

Syntax

reboot

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.

Examples

The following example reboots the controller.

```
device# reboot
```

reindex-elasticsearch-all

Reindexes all elastic search data.

Syntax

reindex-elasticsearch-all

Modes

Debug configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows how to reindex all elastic search data.

```
device# debug
device(debug)# reindex-elasticsearch-all
```

History

Release version	Command history
3.5.1	This command was introduced.

reload

Reloads the controller immediately or after a specified period of seconds.

Syntax

```
reload { now | seconds }
```

Command Default

The controller is not rebooted.

Parameters

now

Immediately reboots the controller.

seconds

Indicates the number of seconds before the controller reboots itself. Number between 1 and 60.

Modes

Privileged EXEC mode

Usage Guidelines

The *seconds* option allows a graceful reload.

To reboot an AP, use the **reload ap** command.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows how to reboot the controller after 20 seconds.

```
device# reload 20
Do you want to reboot system (yes/no)? yes
Server would be rebooted in 20 seconds.
Broadcast message from admin (Tue June 18 15:11:24 2020):
The system is going down for reboot NOW!
```

reload ap

Reboots an access point (AP).

Syntax

reload ap *mac-address*

Command Default

No AP is rebooted.

Parameters

mac-address

Reboots the AP with the specified MAC address.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows how to reboot the AP with the MAC address 00:1c:2d:ee:ff:cc

```
device# reload ap 00:1c:2d:ee:ff:cc  
Success to trigger AP (00:1c:2d:ee:ff:cc) reboot.
```

Commands O through Sh
reload data-plane

reload data-plane

Reboots a dataplane.

Syntax

reload data-plane *name*

Command Default

No dataplane is rebooted.

Parameters

name

Reboots the specified dataplane.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only.

Examples

The following example shows how to reboot the dataplane with the name NODE222

```
device# reload data-plane NODE222  
Success to trigger data plane (NODE222) reboot.
```


remote ap-cli

Executes remote access point (AP) CLI commands.

Syntax

remote ap-cli *mac command*

Command Default

No CLI commands are executed on remote APs.

Parameters

mac

MAC address of the remote AP.

command

Command to be executed. Use double quotation marks around the command.

Modes

Privileged EXEC mode

Usage Guidelines

Use the command on the controller when you need to run CLI commands on the AP remotely. You must have permission to access the remote AP.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows how to execute the **get version** command on the remote AP with the MAC address of 74:91:1A:2A:DB:80.

```
device# remote ap-cli 74:91:1A:2A:DB:80 "get version"
Ruckus 7962 Multimedia Hotzone Wireless AP
Version: 1.1.0.0.151
OK
```

remote-syslogd

Enables or disables the redirection of syslog to the remote syslog server.

Syntax

```
remote-syslogd { enable [ { udp | tcp } ip-address port ] | disable }
```

Command Default

No redirection of the syslog is enabled.

Parameters

enable

Enables the redirection of syslog to the remote syslog server.

udp

Uses UDP IP for transmitting the the syslog files.

tcp

Uses TCP IP for transmitting the the syslog files.

ip-address

IP address of the Syslog server.

port

Port number of the Syslog server.

disable

Disables the redirection of syslog to the remote syslog server.

Modes

Debug configuration mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.

Examples

The following example disables sending syslog messages to a remote syslog server.

```
device> enable  
device# debug  
device(debug)# remote-syslogd disable
```

report

Creates and updates the report configurations.

Syntax

report *report-title*

no report *report-title*

After the **report** command is entered to enter Report configuration mode, the following configuration syntax is available:

```
{ email email-address | enable-export | pdf-format | type { client-number | continuously-disconnected-aps | switch-traffic-statistics | system-resource-utilization | tx-rx-bytes }
```

```
{ resource-filter { device { ap ap-name | domain domain-name | zone zone-name } | radio { 2.4g | 5g } | ssid ssid }
```

```
{ schedule { daily hour minute minute | hourly minute | monthly date-of-month hour hour minute minute | weekly day-of-week hour hour minute minute }
```

```
{ time-filter { 3min | 15min | hourly } hours hour }
```

After the **enable-export** command is entered, the following configuration syntax is available:

```
[ export ftp-url ]
```

Command Default

A report is not configured.

Parameters

report-title

Name of the report.

email *email-address*

Sets email notification address.

enable-export

Enable the export report results to be sent to an FTP server.

pdf-format

Outputs the report to a PDF.

type

Sets the report type.

client-number

This report shows the historical view of the maximum and minimum number of clients connect to the system. Client number can be shown in different time intervals for a specified duration. The report can be generated based on specific management domain, AP zone, AP, SSID, or radio type.

continuously-disconnected-aps

This report shows the list of access points disconnected with specified time range. The report can be generated based on specific management domain and AP zone.

Commands O through Sh report

switch-traffic-statistics

This report shows the traffic statistics of switches, including the packets of InFrame, OutFrame, InMulticast, OutMulticast, InBroadcast, and OutBroadcast. The numbers of InError, OutError, CrcError, and InDiscard packets are also included.

system-resource-utilization

This report shows the historical view of the CPU and memory usage of the system. The CPU and memory usage can be shown in different time intervals for a specific duration. The report can be generated based on specific plane.

tx-rx-bytes

This report shows the historical view of the transmitted and received bytes of the system. The transmitted and received bytes can be shown in different time intervals for a specified duration. The report can be generated based on specific management domain, AP zone, AP, SSID or radio type.

resource-filter

Sets the resource filter criteria for the report.

device

Filtered by device parameters.

ap *ap-name*

Filtered by AP name.

domain *domain*

Filtered by domain name or the administration domain.

zone *zone-name*

Filtered by zone name.

radio

Filtered by radio frequency.

2.4g

Filtered by 2.4g.

5g

Filtered by 5g.

ssid *ssid*

SSID

schedule

Sets the schedule criteria for when the report is run.

daily

Run the report on a daily schedule.

hour

Specifies the hour.

minute *minute*

Specifies the minute.

hourly *minute*

Runs the report on the same minute every hour.

monthly *ssid*

Runs the report on a monthly schedule.

date-of-month
Specifies the day in the month.

hour *hour*
Specifies the hour.

minute *minute*
Specifies the minute.

monthly *ssid*
Runs the report on a monthly schedule.

day-of-week
Specifies the day in the week.

hour *hour*
Specifies the hour.

minute *minute*
Specifies the minute.

time-filter

Sets the period of time during which the data is gathered for the report.

3min
Sets the time period to 3 minutes.

15min
Sets the time period to 15 minutes.

hourly
Sets the time period to hourly.

hour *hour*
Specifies the hour.

export *ftp-url*

Sets the FTP URL to which the reports are exported. The FTP format is ftp://<username>:<pwd>@<ftp-host>[/<dir-path>].

Modes

Global configuration mode

Usage Guidelines

Although you can configure the options individually and some are optional, you must configure the following options to create and export a report.

- **email** *email-address*
- You must specify an FTP server for export.

Before you can configure the **export** command and the FTP server details, you must enter the **enable-export** command.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Use the **no** form of this command with a report name to remove the configuration for the specified report.

Examples

The following example shows how to create a report configuration to export a report in PDF format to an FTP server. The report type displays the historical view of the maximum and minimum number of clients connect to the system for the mktg-zone2 zone and it is scheduled to run daily at 32 minutes past the 20th hour.

```
device# config
device(config)# report report2
device(config-report)# email user2.mktg@commscope.com
device(config-report)# pdf-format
device(config-report)# resource-filter device zone mktg-zone2
device(config-report)# schedule daily 20 minute 32
device(config-report)# type client-number
device(config-report)# enable-export
device(config-report)# export ftp://user2:abc123@10.10.2.4/reports
Password: ***
Retype: ***
```

reset

Resets the DHCP server binding or profiles and NAT server profile.

Syntax

```
reset dhcp { binding { ip ip-addr | all } | profile profile }  
reset nat profile profile
```

Command Default

The DHCP server binding or profiles and NAT server profiles are not reset.

Parameters

dhcp
Resets DHCP server

binding
DHCP binding options.

ip *ip-addr*
Resets DHCP binding for the specified IP address.

all
Resets all the DHCP binding.

profile *profile*
Resets the specified DHCP or NAT profile.

nat
Deletes configuration options.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.

Examples

The following example resets the NAT profile, natprofile1

```
device# reset nat profile natprofile1
```

The following example resets the DHCP server binding for at 172.19.19.55.

```
device# reset dhcp binding 172.19.19.55
```

restore

Restores the local cluster or the entire cluster system.

Syntax

restore

Modes

Privileged EXEC mode

Usage Guidelines

After entering the restore command, you are prompted to restore either the entire cluster or the local cluster. The system detects backup files for you to select.



CAUTION

Choosing to restore the entire cluster or local cluster will start a reboot of the system.

Examples

The following example shows how to restore the local cluster or the entire cluster.

```
device# restore
Please choose a backup to restore or 'No' to cancel This action will reboot the system.
Do you want to restore "the entire" cluster system? (yes/no) # Yes: restore cluster, no: original
restore local
Do you want to restore the "local" system only? (yes/no) # Yes: start to restore local, No: cancel
operation
```

History

Release version	Command history
3.5.1	This command was introduced.

restore

Restores the controller configuration.

Syntax

```
restore ftp/tftp/sftp-filename ip-address
```

Parameters

ftp/tftp/sftp-filename

File name with the full path of the server. Specify the user name and password if you are using an FTP or SFTP server.

ip-address

IP address of the FTP, TFTP, or SFTP server.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.



CAUTION

Choosing to restore will start a reboot of the system.

Examples

The following example shows how to restore the controller configuration.

```
device# tftp 10.0.0.10 /tmp/filename.bak
```

Commands O through Sh
restore config

restore config

Restores a configuration backup file that you uploaded to the FTP server.

Syntax

`restore config`

Modes

Privileged EXEC mode

Usage Guidelines

When upgrading software you can create a backup file which is used to restore the device configuration after the upgrade or other event.



CAUTION

Choosing to restore the configuration will start a reboot of the system.

Examples

The following example shows how to restore the device configuration.

```
device# restore config
After restore configuration well done, Controller will be restarted,User need to re-login. Do you want
to restore configuration in this context (yes/no)? yes
Available backup configurations:
Available backup configurations:
1: Configuration_20201119071503GMT_1.1.0.0.246.bak 2020-11-19 07:15:03 GMT
Please choose a backup configuration to restore: (Or input 'No' to cancel)
Restore process starts
Restore process has been scheduled to run
```

restore network

Restores the network configuration.

Syntax

```
restore network
```

Modes

Privileged EXEC mode

Usage Guidelines

After entering the restore network command a list of backup files appears and you are prompted to select the backup file that you want to use to restore the network configuration on the controller.



CAUTION

Choosing to restore the network configuration will start a reboot of the system.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows how to restore the network configuration on the controller.

```
device# restore network
No.   Created on                Patch Version  File Size
-----
1     2020-10-05 12:32:14 GMT    3.0.0.0.479   160.3KB
Please choose a backup to restore or 'No' to cancel:
```

rks-gre

Creates or updates the RUCKUS GRE configuration.

Syntax

rks-gre *tunnel-name*

no rks-gre [*tunnel-name*]

After the **rks-gre** command is entered to enter RKS GRE configuration mode, the following configuration syntax is available:

{ **gateway-mtu** { **auto** | *manual-mtu-size* } | **tunnel-encryption** { **AES128** | **AES256** | **DISABLE** } | **tunnel-mode** { **gre** | **gre-udp** } }

Command Default

RUCKUS GRE is not configured.

Parameters

tunnel-name

RUCKUS GRE tunnel name.

gateway-mtu

Sets the WAN interface MTU.

auto

Enables auto discover for the MTU size.

manual-mtu-size

Manually sets the MTU size. Range is from 850 to 1500.

tunnel-encryption

Enables the tunnel encryption.

AES128

Uses the AES128 encryption algorithm.

AES256

Uses the AES256 encryption algorithm.

DISABLE

Disables the tunnel encryption.

tunnel-mode

Sets the tunnel mode.

gre

GRE tunnel mode.

gre-udp

GRE and UDP tunnel mode that supports APs behind Network Address Translation (NAT) tunnels.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

The **no** form of this command deletes the RUCKUS GRE configuration.

Examples

The following example shows how to configure RUCKUS GRE tunnel options.

```
device# config
device(config)# rks-gre GRE1
device(config-rks-gre)# gateway-mtu 950
device(config-rks-gre)# tunnel-encryption AES256
device(config-rks-gre)# tunnel-mode gre
```

route

Sets up the route configuration.

Syntax

route

After the **route** command is entered to enter Route configuration mode, the following configuration syntax is available:

add { *dst-network/dst-netmask next-hop* | **ip6** *dst6-network/prefixlen next-hop6* }

del { *dst-network/dst-netmask next-hop* | **ip6** *dst6-network/prefixlen next-hop6* }

show { **main** | **json** | **table-name** | **all** } [**ip6**]

Command Default

Only default route configuration exists.

Parameters

add

Adds configuration options.

dst-network

Destination IPv4 network address.

dst-netmask

Destination network mask.

next-hop

Next hop IPv4 address.

ip6

Adds IPv6 configuration options.

dst6-network

Destination IPv6 network address.

prefixlen

Destination IPv6 network prefix-length.

next-hop6

Next hop IPv6 address.

del

Deletes configuration options.

show

Displays route configuration.

main

Displays the main route.

json

Displays the route configuration in JSON format ?

table-name	Displays the table name.
all	Displays all route configuration in all the formats.
ip6	Displays the IPv6 route configuration.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.

Examples

The following example shows how to add an IPv4 route configuration with a destination network address and mask and the next hop address.

```
device# route
device(route)# add 10.254.32.0/24 10.10.2.1
```

The following example displays all the main route configuration.

```
device# route
device(route)# show main

--- main ---
default via 100.103.1.1 dev br0
10.254.32.0/24 dev br-tun proto kernel scope link src 10.254.32.15
100.103.1.0/24 dev br0 proto kernel scope link src 100.103.1.213
```

save-log

Saves the debug log to the remote controller.

Syntax

save-log controller

save-log { *ftp-url* | *sftp-url* | *tftp-url* } *ip-addr path* [*user*] [*password*]

save-log delete

Command Default

The debug log file is not saved.

Parameters

controller

Saves the debug log file to the controller.

ftp-url

Saves the debug log to the specified FTP URL server.

sftp-url

Saves the debug log to the specified SFTP URL server.

tftp-url

Saves the debug log to the specified TFTP URL server.

ip-addr

IP address of the server.

path

Path on the server for saving the file.

user

User name to access the server.

password

User password to access the server.

delete

Deletes all snapshots in /opt/ruckuswireless/wsg/log/dp_snapshot folder on the controller.

Modes

Debug configuration mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.

The optional *user* and *password* entries are only required when using the FTP or SFTP URLs.

Examples

The following example saves the debug log to a file on the controller.

```
device# debug
device(debug)# save-log controller
```

```
Package snapshot /opt/ruckuswireless/wsg/log/dp_snapshot/
97203WJ5REQJ0H2AFPD60R63GKNA000C295894A2000C295894AC_debug_support_info.tar.gz
```

scan-jmxport

Scans the JMX port.

Syntax

```
scan-jmxport ip-address
```

Command Default

The JMX port is not scanned.

Parameters

ip-address

Specifies the IP address.

Modes

Debug configuration mode

Usage Guidelines

Java Management Extensions (JMX) technology can be used to monitor and manage any Java technology-based applications (Java applications) that are running in either a local or a remote Java Virtual Machine (JVM).

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows how to scan the JMX port at the IP address 10.128.70.82.

```
device# debug
device(debug)# scan-jmxport 10.128.70.82
```

sci-profile

Enables the SCI profile settings.

Syntax

sci-profile *profile-name*

no sci-profile [*profile-name*]

After the **sci-profile** command is entered to enter SCI Profile configuration mode, the following configuration syntax is available:

{ **host** *host-ip-address* | **password** *pwd* | **port** *port-number* | **system-id** *system-id* | **user** *user* }

Command Default

SCI profile settings are not configured.

Parameters

host *host-ip-address*

Sets the SCI server host IP address.

password *pwd*

Sets the SCI server password.

port *port-num*

Sets the SCI server port number.

system-id *system-id*

Sets the SCI server system ID.

user *user*

Sets the SCI server user name.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

The **no** form of this command without any options deletes all the configured SCI profiles. Use the *profile-name* to delete just one SCI profile.

Examples

The following example shows how to configure various SCI profile options.

```
device# config
device(config)# sci-profile
device(config-sci-profile)# host 10.10.2.3
device(config-sci-profile)# password Jxygl23
device(config-sci-profile)# port 3
device(config-sci-profile)# system-id 12345
device(config-sci-profile)# user usermktg
```

History

Release version	Command history
3.5.1	This command was introduced.

screen-pagination

Enables the screen pagination.

Syntax

screen-pagination

no screen-pagination

Command Default

Screen pagination is not enabled.

Modes

Debug configuration mode

Usage Guidelines

This command is supported only on SmartZone 300 and vSZ-H platforms.

The **no** form of the command disables screen pagination.

Examples

The following example shows how to enable screen pagination.

```
device# debug
device(debug)# screen-pagination
```

service

Starts, stops, or restarts all the controllers services.

Syntax

service{restart|start}

no service

Command Default

All controller services are running by default.

Parameters

restart

Restarts all the controller services.

start

Starts all the controller services.

Modes

Privileged EXEC mode

Usage Guidelines

While the controller services are running by default, use the **service start** command if you have previously stopped the controller services using the **no service** command. Restoring a backup file to the controller requires restarting all of the controller services using the **service restart** command.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows how to start all the controller services. Use this option if the controller services have been stopped.

```
device# service start
Please note that this command will cause current SSH connection closed for SSH restart.
Do you want to start all services (yes/no)? yes
Starting all services...
wait for
(cassandra,communicator,eventreader,freeradius,memcached,monitor,northbound,replicated,scheduler,tomcat)
Up!
wait for
(cassandra,communicator,eventreader,freeradius,memcached,monitor,northbound,replicated,scheduler,tomcat)
Up!
wait for (communicator,eventreader,freeradius,memcached,monitor,northbound,replicated,scheduler,tomcat)
Up!
wait for (communicator,eventreader,monitor,northbound,replicated,scheduler,tomcat) Up!
wait for (communicator,eventreader,monitor,northbound,replicated,scheduler,tomcat) Up!
wait for (communicator,eventreader,monitor,northbound,replicated,scheduler,tomcat) Up!
wait for (communicator,eventreader,monitor,northbound,replicated,scheduler,tomcat) Up!
All services are up!
device# Connection to 10.2.6.230 closed by remote host.
```

The following example shows how to restart all the controller services. Use this option if you have restored a backup file to the controller.

```
device# service restart
Please note that this command will cause current SSH connection closed for SSH restart.
Do you want to restart all services (yes/no)? yes
Restarting all services...
```

The following example shows how to stop all the controller services.

```
device# no service
Please note that this command will cause current SSH connection closed for SSH restart.
Do you want to stop all services (yes/no)? yes
Stopping all services...
Connection to 10.2.6.230 closed by remote host.
```

session-timeout

Sets the local session timeout.

Syntax

session-timeout*minutes*

Command Default

The default local session timeout value is 30 minutes.

Parameters

minutes

Specifies the local session timeout in minutes. Maximum value is 1440 minutes and the default is 30.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows how to set the session timeout to 40 minutes.

```
device# session-timeout 40
```


set-factory

Resets the controller system to factory settings.

Syntax

`set-factory`

Modes

Privileged EXEC mode

Usage Guidelines



CAUTION

Resetting a node to factory settings will erase all of its system configuration settings, backup files, and cluster settings. Before resetting a node to factory settings, it is strongly recommends that you export all of the backup files on the controller to an FTP server using either the web interface or CLI.

This command is supported on all the controllers including the SmartZone Data Plane.

Examples

The following example shows how to reset the controller to factory settings. Before entering this command, export your backup files to an FTP server.

```
device# set-factory
```

Commands O through Sh
setup

setup

Sets up the controller network interface settings.

Syntax

setup

Modes

Privileged EXEC mode

Usage Guidelines

Use the command to help you configure the network interface settings using prompts.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example walks you through prompts to help you set up a SZ300 controller.

```
ruckus# setup

#####
Start controller setup process:
#####

Network is not setup.

*****
IP Version Support
*****
1. IPv4 only
2. IPv4 and IPv6
*****
Select address type: (1/2) 2

*****
IPv4 address setup for Control interface
*****
1. Manual
2. DHCP
*****
Select IP configuration: (1/2) 2

*****
IPv4 address setup for Cluster interface
*****
1. Manual
2. DHCP
*****
Select IP configuration: (1/2) 2

*****
IPv4 address setup for Management interface
*****
1. Manual
2. DHCP
*****
Select IP configuration: (1/2) 2

*****
Default Gateway Interface
*****
1. Control
2. Cluster
3. Management
*****
Select gateway interface: (1/2/3) 3
Primary DNS: 172.17.17.16
Secondary DNS:

*****
IPv6 address setup for Control interface
*****
1. Manual
2. DHCPv6
*****
Select IPv6 configuration: (1/2) 2

*****
IPv6 address setup for Management interface
*****
1. Manual
2. DHCPv6
*****
Select IPv6 configuration: (1/2) 2
```

Commands O through Sh
setup

```
*****
IPv6 Default Gateway Interface
*****
1. Control
2. Management
*****
Select IPv6 gateway interface: (1/2) 1
Primary IPv6 DNS:
Secondary IPv6 DNS:

*****
Current Network Settings (Before Applying)
*****
IP Version Support Settings:
*****
IP Version Support   : IPv4 and IPv6

Interface IPv4 settings:
*****
Control:
*****
IP Type           : DHCP
IP Address        : 192.168.2.53
Netmask          : 255.255.255.0
Gateway          : 192.168.2.219

*****
Cluster:
*****
IP Type           : DHCP
IP Address        : 192.168.100.88
Netmask          : 255.255.255.0
Gateway          :

*****
Management:
*****
IP Type           : DHCP
IP Address        : 172.17.25.55
Netmask          : 255.255.255.0
Gateway          :
Default Gateway   : yes

*****
DNS Server Settings:
*****
Primary DNS Server : 172.17.17.16
Secondary DNS Server :

Interface IPv6 settings:
*****
Control:
*****
IP Type           : DHCPv6
IP Address        :
Gateway Type      : RA
Gateway          :
Default Gateway   : yes

*****
Management:
*****
IP Type           : DHCPv6
IP Address        :
Gateway Type      : RA
Gateway          :

*****
DNS Server Settings:
*****
Primary DNS Server :
```

```

Secondary DNS Server :
*****
Enter 'y' to apply, 'n' to modify
Do you want to apply the settings? (y/n)
Please wait while sytem configures the network.
It may take a few minutes...

*****
Current Network Settings (After Applying)
*****
IP Version Support Settings:
*****
IP Version Support   : IPv4 and IPv6

Interface IPv4 settings:
*****
Control:
*****
IP Type              : DHCP
IP Address           : 192.168.2.53
Netmask              : 255.255.255.0
Gateway              :

*****
Cluster:
*****
IP Type              : DHCP
IP Address           : 192.168.100.88
Netmask              : 255.255.255.0
Gateway              :

*****
Management:
*****
IP Type              : DHCP
IP Address           : 172.17.25.55
Netmask              : 255.255.255.0
Gateway              : 172.17.25.1
Default Gateway      : yes

*****
DNS Server Settings:
*****
Primary DNS Server   : 172.17.17.16
Secondary DNS Server :

Interface IPv6 settings:
*****
Control:
*****
IP Type              : DHCPv6
IP Address           : fccc:192:168:2::eba/128
Gateway Type         : RA
Gateway              : fe80::20c:29ff:fef9:7e85
Default Gateway      : yes

*****
Management:
*****
IP Type              : DHCPv6
IP Address           : fccc:172:17:25::705/128
Gateway Type         : RA
Gateway              : fe80::20c:29ff:fef9:7e85

*****
DNS Server Settings:
*****
Primary DNS Server   :
Secondary DNS Server :
*****
Enter 'y' to accept, 'n' to modify

```

Commands O through Sh

setup

Accept these settings and continue? (y/n) y

```
SZ300# setup
#####
Start SZ300 setup process:
#####
Current Network Settings
*****
IP Version Support Settings:
*****
IP Version Support   : IPv4 and IPv6

Interface IPv4 settings:
*****
Control:
*****
IP Type              : DHCP
IP Address           : 192.168.2.53
Netmask              : 255.255.255.0
Gateway              :

*****
Cluster:
*****
IP Type              : DHCP
IP Address           : 192.168.100.88
Netmask              : 255.255.255.0
Gateway              :

*****
Management:
*****
IP Type              : DHCP
IP Address           : 172.17.25.55
Netmask              : 255.255.255.0
Gateway              : 172.17.25.1
Default Gateway      : yes

*****
DNS Server Settings:
*****
Primary DNS Server   : 172.17.17.16
Secondary DNS Server :

Interface IPv6 settings:
*****
Control:
*****
IP Type              : DHCPv6
IP Address           : fccc:192:168:2::eba/128
Gateway Type         : RA
Gateway              : fe80::20c:29ff:fef9:7e85
Default Gateway      : yes

*****
Management:
*****
IP Type              : DHCPv6
IP Address           : fccc:172:17:25::705/128
Gateway Type         : RA
Gateway              : fe80::20c:29ff:fef9:7e85

*****
DNS Server Settings:
*****
Primary DNS Server   :
Secondary DNS Server :
*****
Do you want to setup network? (y/n) n
(C)reate a new cluster or (J)oin an exist cluster (c/j): c
Cluster Name (cluster name can contain letters (a-z, A-Z), numbers (0-9), and dashes (-)): ruckus-
```

```

cluster-1
Controller Description: ruckus controller

*****
Create/Join      : create
DISCOVERY PROTOCOL: tcp
Cluster Name    : ruckus-cluster-1
Blade ID       : 83405b79-9286-4b57-8701-c7ecddf27c40
DESCRIPTION     : ruckus controller
*****
Are these correct (y/n): y
Enter the controller name of the blade ([a-zA-Z0-9-]): ruckus-controller
Is this controller behind NAT? (y/n) n
System UTC Time: 2020-02-06 07:39:53 UTC
NTP Server ([a-zA-Z0-9-.]): [ntp.ruckuswireless.com]
Check if NTP server [ntp.ruckuswireless.com] is reachable...
System time after synchronization: 2020-02-06 07:40:01 UTC
Convert ZoneDirector APs in factory settings to SZ300 APs automatically (y/n) [N]
Reset admin's password!
Enter admin password:
Enter admin password again:
Enter the CLI enable command password:
Enter the CLI enable command password again:
Reset admin's password done!
Setup configurations done. Starting setup process after 5 seconds...
/etc/init.d/snmpd restart
New hostname: ruckus-controller
Change admin password done!

*****
Check installation status
*****
Wait for cluster config operation start!
Wait for cluster config operation start!
Wait for cluster config operation start!
Wait for cluster config operation start!
Bootstrapping, Tue Feb 06 07:40:33 UTC 2020
Blade Channel Opened, Tue Feb 06 07:40:36 UTC 2020
Configurer Channel Opened, Tue Feb 06 07:40:46 UTC 2020
Cassandra Started, Tue Feb 06 07:41:59 UTC 2020
ElasticSearch Started, Tue Feb 06 07:43:08 UTC 2020
Cassandra Initialized, Tue Feb 06 07:47:31 UTC 2020
Certificate and Root Key created, Tue Feb 06 07:49:02 UTC 2020
SZ300 Apps Started, Tue Feb 06 08:03:58 UTC 2020
Available, Tue Feb 06 08:04:13 UTC 2020
[#####]100%
% System setup is finished. The current CLI session will be terminated. Please login again.

```

NOTE

At this point, log on to the controller CLI, and then run the setup command again.

```

ruckus# setup
#####
Start SCG setup process:
#####
Current network settings:
*****
Control (AP/Dataplane):
*****
IP TYPE : dhcp
IP Address : 10.2.6.231
Netmask : 255.255.0.0
Gateway : 10.2.0.1
Default Gateway : no
Primary DNS Server : 172.17.17.16
Secondary DNS Server : 168.95.1.1
*****
*****
Cluster:
*****
IP TYPE : dhcp

```

Commands O through Sh

setup

```
IP Address : 10.2.6.229
Netmask : 255.255.0.0
Gateway : 10.2.0.1
Default Gateway : no
Primary DNS Server : 172.17.17.16
Secondary DNS Server : 168.95.1.1
*****
*****
Management (Web):
*****
IP TYPE : dhcp
IP Address : 10.2.6.230
Netmask : 255.255.0.0
Gateway : 10.2.0.1
Default Gateway : yes
Primary DNS Server : 172.17.17.16
Secondary DNS Server : 168.95.1.1
*****
Server need to restart network after network setting.
Do you want to setup network? [YES/no]: no
(C)reate a new cluster or (J)oin an exist cluster: (c/j) c
Cluster Name ([a-zA-Z0-9_-]): test_cluster
Controller Description: test_cluster
*****
Create/Join : create
DISCOVERY PROTOCOL: tcp
Cluster Name : test_cluster
Blade ID : f7585769-6dd7-4e63-aa2c-e6da76501680
DESCRIPTION : test_cluster
*****
Are these correct? (y/n): y
Enter the controller name of the blade([a-zA-Z0-9_-]): test_cluster
NTP Server ([a-zA-Z0-9_-]): [pool.ntp.org]
Reset admin's password!
Enter admin password:
Enter admin password again:
Enter the enable password:
Enter the enable password again:
Reset admin's password done!
stty: standard input: Invalid argument
New hostname: test_cluster
Change admin password done!
*****
Check SCG installation status
*****
Wait for cluster config operation start!
Wait for cluster config operation start!
Wait for cluster config operation start!
Wait for cluster config operation start!
Bootstrapping, Tue Dec 18 15:25:32 GMT 2012
Blade Channel Jointed, Tue Dec 18 15:25:34 GMT 2012
Configurer Channel Jointed, Tue Dec 18 15:25:43 GMT 2012
Cassandra Started, Tue Dec 18 15:26:03 GMT 2012
Cassandra Initialized, Tue Dec 18 15:27:14 GMT 2012
First Time Initialization Process Done, Tue Dec 18 15:28:02 GMT 2012
Available, Tue Dec 18 15:29:47 GMT 2012
```


sha1

Enables Secure Hash Algorithm 1 (SHA1) support.

Syntax

sha1

no sha1

Command Default

SHA1 support is disabled.

Modes

Debug configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows how to enable SHA1 support.

```
device# debug
device(debug)# sha1

Wait for tomcat down...(0/120)
Wait for tomcat down...(2/120)
Stop service tomcat done!
Start service tomcat done!
      total      used      free      shared  buff/cache  available
Mem:    198054460  50570244  135203348  206444   12280868  145990120
Swap:         0         0         0
```

```
Wait for communicator down...(0/120)
Stop service communicator done!
Start service communicator done!
      total      used      free      shared  buff/cache  available
Mem:    198054460  50085552  135697744  206380   12271164  146475344
Swap:         0         0         0
```

Please make sure to enable/disable sha1 in all cluster nodes.
Successful operation

The following example shows how to disable SHA1 support.

```
device# debug
device(debug)# no sha1
```

History

Release version	Command history
3.5.1	This command was introduced.

shutdown

Shuts down the controller immediately, or after a specified period.

Syntax

```
shutdown { now | seconds }
```

On the SmartZone DP controllers:

```
shutdown { now | minutes }
```

Command Default

A controller is not shut down.

Parameters

now

Shuts down the controller immediately after 30 seconds.

seconds

Shuts down the controller after the specified number of seconds.

minutes

Shuts down the controller after the specified number of minutes. This variable is supported on the SmartZone Data Plane controllers only.

Modes

Privileged EXEC mode

Usage Guidelines

Use the command to define how quickly the controller is shut down.

This command is supported on all the controllers including the SmartZone Data Plane.

Examples

The following example shuts down the controller in 30 seconds.

```
device# shutdown now
Do you want to shutdown system? Y/N
Server would be shutdown in 30 seconds
```

The following example shuts down the controller in 90 seconds allowing for a graceful shutdown.

```
device# shutdown 90
Do you want to shutdown system? Y/N
Server would be shutdown in 90 seconds
```

Commands O through Sh

shutdown

The following example shuts down the SZ DP controller in 10 minutes allowing for a graceful shutdown.

```
device# shutdown 10
Do you want to shutdown system? Y/N
Server would be shutdown in 10 minutes
```

Show Commands

show (DP debug)

Shows the status of remote and data plane packet captures.

Syntax

show

Modes

Debug configuration mode

Usage Guidelines

This command is supported on the SmartZone Data Plane (DP) controllers only.

The command is only available under debug mode. Other DP **show** commands are available under Privileged EXEC mode.

Examples

The following example displays the output of the DP **show** command.

```
device# debug
device(debug)# show

Debug Settings:
  Remote Packet Capture: Enable
  Data Plane Packet Capture: Disable
```

Show Commands
show admin-activity

show admin-activity

Displays the activities of an administrator account.

Syntax

show admin-activity

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows output from the **show admin-activity** command.

```
device# show admin-activity
```

No.	Datetime	Administrator	From IP	Action	Resource	Description
1	2020-03-25 14:51:05 GMT	admin	10.45.246.91	Log on	Administrator	Administrator
	[admin] logged on from CLI.					
2	2020-03-25 10:18:41 GMT	admin	10.45.236.31	Terminate	Session	Succeeded to
	terminate the session [DA27XW3zzWOEM9aZkCKdyBsx8NxLlhWj].					
3	2020-03-24 09:47:02 GMT	admin	10.45.237.103	Log off	Administrator	Administrator
	[admin] logged off from CLI.					
4	2020-03-24 09:46:53 GMT	admin	10.45.237.103	Log on	Administrator	Administrator
	[admin] logged on from CLI.					
5	2020-03-24 09:42:18 GMT	admin	10.45.237.103	Log off	Administrator	Administrator
	[admin] logged off from CLI.					
6	2020-03-24 09:42:10 GMT	admin	10.45.237.103	Log on	Administrator	Administrator
	[admin] logged on from CLI.					
7	2020-03-24 08:40:42 GMT	admin	10.45.236.31	Update	AP Zone	Zone [Zone-699-Dual] updated.
8	2020-03-24 07:23:26 GMT	admin	10.45.236.31	Log on	Administrator	Administrator
	[admin] logged on from [10.45.236.31].					
9	2020-03-24 06:11:59 GMT	admin	10.45.236.31	Terminate	Session	Succeeded to
	terminate the session [MowYyEnrXHHJ7d0oHebMqjBZpe2uDdA7].					
10	2020-03-24 06:11:59 GMT	admin	10.45.237.66	Terminate	Session	Succeeded to
	terminate the session [RukKilInMgnAEs1VV30Y76mjZXhcXN1U].					
11	2020-03-24 06:11:59 GMT	admin	10.45.237.98	Terminate	Session	Succeeded to
	terminate the session [54rJboCibrYgmqhReeoPZZJI3pMFlvSm].					
12	2020-03-24 06:11:59 GMT	admin	10.174.84.9	Terminate	Session	Succeeded to
	terminate the session [ERxkX70tZ0wCNEm9CrTXSULLBwTVwGsR].					
13	2020-03-24 06:10:29 GMT	admin	10.45.237.103	Log off	Administrator	Administrator
	[admin] logged off from CLI.					
14	2020-03-24 06:10:12 GMT	admin	10.45.237.103	Log on	Administrator	Administrator
	[admin] logged on from CLI.					
15	2020-03-24 05:18:17 GMT	admin	10.174.84.9	Upgrade	Patch Image	System started
	upgrading to version [5.2.1.0.251].					
16	2020-03-24 05:07:50 GMT	admin	10.174.84.9	Upload	Patch Image	Upload patch file
	[5.2.1.0.251.ximg] triggered.					
17	2020-03-24 05:06:20 GMT	admin	10.174.84.9	Log on	Administrator	Administrator
	[admin] logged on from [10.174.84.9].					
18	2020-03-24 04:05:49 GMT	admin	10.45.237.103	Log off	Administrator	Administrator
	[admin] logged off from CLI.					
19	2020-03-24 04:05:41 GMT	admin	10.45.237.103	Log on	Administrator	Administrator
	[admin] logged on from CLI.					

Show Commands
show alarm

show alarm

Displays outstanding access point (AP) alarms.

Syntax

show alarm

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows partial output from the **show alarm** command.

```
device# show alarm
```

No.	Datetime	Code	Alarm Type	Severity	Status	Ack On	Cleared By
Cleared On		Comments		Activity			
1	2020-03-20 04:30:32 GMT	907	ipmiThempP	Major	Cleared		System
	2020-03-20 04:30:32 GMT	Auto Cleared	Processor [2] temperature [Too High] on control plane [24:79:2A:00:0B:00].				
2	2020-03-20 04:31:00 GMT	303	AP disconnected	Major	Outstanding		
			AP [RuckusAP@6C:AA:B3:3D:65:30] disconnected				
3	2020-03-20 04:31:00 GMT	303	AP disconnected	Major	Outstanding		
			AP [RuckusAP@94:BF:C4:14:F8:80] disconnected				
4	2020-03-20 04:31:00 GMT	303	AP disconnected	Major	Outstanding		
			AP [RuckusAP@EC:8C:A2:1F:92:20] disconnected				
5	2020-03-20 06:17:48 GMT	811	Cluster node rebooted	Major	Outstanding		
			Node [KKK-SZ300] in cluster [SZ300] rebooted				
.							
.							
.							

show ap

Displays details about a specific access point (AP) identified by its MAC address.

Syntax

```
show apmac-address[mesh{neighbors | topology}]
```

Parameters

mac-address

MAC address of the AP.

mesh

Displays AP mesh statistics.

neighbors

Displays the AP mesh neighbors.

topology

Displays the AP mesh topology.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Show Commands

show ap

Examples

The following example displays the mesh topology for the AP with the MAC address of 84:18:3A:39:C8:50

```
device# show ap DC:AE:EB:22:3E:D0
```

General Information

```
-----  
AP MAC Address      : DC:AE:EB:22:3E:D0  
AP Name             : dhcp-10-206-84-82  
Description         :  
Serial Number       : 272002000225  
Location            :  
GPS Coordinates     :  
Firmware Version    : 6.0.0.0.1582  
IP Address          : 10.206.84.82  
IP Type             : IPV4  
IPv6 Address        :  
IPv6 Type           : autoconf  
External IP Address : 10.206.84.82  
Model               : R550  
Mesh Role (Hops)    : Disabled  
Power Source        : DC  
Management VLAN     : 1
```

Status Summary

```
-----  
Connection Status   : Connect  
Uptime              : 3h 58m
```

...

show ap-certificate-status

To show the status of AP certificates.

Syntax

```
show ap-certificate-status{request|update}[zone-name]
```

Parameters

request

Displays AP certificate request status.

update

Displays AP certificate update status.

zone-name

Target zone name.

Modes

Privileged EXEC mode

Usage Guidelines

If the *zone-name* is not specified, the status of all AP certificates is displayed.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following examples display the AP certificate update status.

```
device# show ap-certificate-status request
```

No.	AP Name	Description	Model	Serial Number	Status
1	RuckusAP		H320	241702002977	Yes

```
device# show ap-certificate-status request JILANI
```

No.	AP Name	Description	Model	Serial Number	Status
1	RuckusAP		H320	241702002977	

Yes

```
device# show ap-certificate-status request
```

No.	AP Name	Description	Model	Serial Number	Status
1	RuckusAP		H320	241702002977	NO

```
device# show ap-certificate-status update JILANI
```

No.	AP Name	Description	Model	Serial Number	Status
1	RuckusAP		H320	241702002977	Updating

show ap-stats

Displays the AP statistics.

Syntax

Syntax for a SZ100 controller:

```
show ap-stats mac-address type {air-timeradio {2.4g | 5g} | ap-traffic | client-association | client-count | client-os} {ap | zone zone-name | wlan wlan-ssid} | rks-gre period {1-h | 7-d | 14-d | 24-h}
```

Syntax for a SZ300 controller:

```
show ap-stats mac-address type {air-timeradio {2.4g | 5g} | ap-traffic | client-association | client-count | client-os | rks-gre} period {1-h | 24-h}
```

Parameters

mac-address

MAC address of the AP.

type

Type of AP statistics to display.

airtimeradio

Displays statistics for radio air time by bandwidth.

2.4g

2.4 GHz bandwidth.

5g

5 GHz bandwidth.

ap-traffic

Displays the AP mesh topology.

client-association

Displays statistics for client associations.

client-count

Displays statistics for client count.

client-os

Displays statistics for client model names.

ap

Displays statistics by AP.

zone zone-name

Displays statistics by specified zone.

wlan wlan-ssid

Displays statistics by specified WLAN.

rks-gre

Displays statistics for RUCKUS GRE tunnel usage.

period

Displays the specified AP statistics for a specified period of time.

- 1-h**
Displays statistics for the last hour.
- 7-d**
Displays statistics for the last 7 days. This option is not available for zone statistics on the SZ100 or on the SZ300 controllers.
- 14-d**
Displays statistics for the last 14 days. This option is not available on SZ300 controllers.
- 24-h**
Displays statistics for the last 24 hours.

Modes

Privileged EXEC mode

Usage Guidelines

NOTE

The supported syntax is different between the SmartZone 100 and vSZ-E controllers and the SmartZone 300 and vSZ-H controllers. See the Syntax section.

Examples

The following example shows the AP traffic statistics from the AP with a MAC address of 11:20:56:D7:E5:87 for the last hour. Only partial output is displayed.

```
device# show ap-stats 11:20:56:D7:E5:87 type ap-traffic ap period 1-h
```

No.	Time	Total (Bytes)	2.4G (Bytes)	5G (Bytes)
1	2020-03-25 14:19:38	17581	11230	6351
2	2020-03-25 14:21:08	17799	10378	7421
3	2020-03-25 14:22:38	17547	9456	8091
4	2020-03-25 14:24:08	17089	13579	3510
5	2020-03-25 14:25:38	15795	8545	7250
6	2020-03-25 14:27:08	20170	15211	4959
7	2020-03-25 14:28:38	20162	13412	6750
8	2020-03-25 14:30:08	25624	17211	8413
9	2020-03-25 14:31:38	16634	9753	6881
10	2020-03-25 14:33:08	16072	10470	5602
11	2020-03-25 14:34:38	16758	7624	9134
.				
.				
.				

Show Commands

show ap-stats

The following example from a SZ100 controller shows the RUCKUS GRE tunnel usage statistics from the AP with a MAC address of 11:20:56:D7:E5:87 for the last 7 days.

```
device# show ap-stats 11:20:56:D7:E5:87 type rks-gre period 7-d
```

No.	Time	RX-Rate	TX-Rate	RX-Bytes	TX-Bytes	RX-Packets	TX-Packets
1	2020-03-18 15:45:00 GMT	0	0	0	0	0	0
2	2020-03-19 15:45:00 GMT	0	0	0	0	0	0
3	2020-03-20 15:45:00 GMT	0	0	0	0	0	0
4	2020-03-21 15:45:00 GMT	0	0	0	0	0	0
5	2020-03-22 15:45:00 GMT	0	0	0	0	0	0
6	2020-03-23 15:45:00 GMT	0	0	0	0	0	0
7	2020-03-24 15:45:00 GMT	0	0	0	0	0	0

show ap-subnet-discovery-status

Displays AP subnet discovery service status.

Syntax

```
show ap-subnet-discovery-status
```

Modes

Debug configuration mode

Usage Guidelines

This command is supported for SmartZone 100 devices.

The command is only available under debug mode.

Examples

The following example shows that the AP subnet discovery service is disabled.

```
device# debug
device(debug)# show ap-subnet-discovery-status

AP Subnet Discovery Status: Disabled
```

Show Commands

show backup

show backup

Displays a list of available system backup versions.

Syntax

show backup

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to verify that the backup file has been created successfully. Backups are useful, for example, to create backups of clusters that need to be restored.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows the output from the **show backup** command.

```
device# show backup
```

No.	Created on	Patch Version	File Size
1	2019-03-03 10:36:49 GMT	3.0.0.0.599	869.7MB

show backup-config

Displays a list of available configuration backup versions.

Syntax

```
show backup-config
```

Modes

Privileged EXEC mode

Usage Guidelines

When backing up the controller configuration from the CLI, use this command to verify that the backup file of the CLI configuration was successful.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows the output from the **show backup-config** command on a SZ300 controller.

```
device# show backup-config
```

```
Available backup configurations:
```

```
1: Configuration_20191219071503GMT_1.1.0.0.246.bak 2019-12-19 07:15:03 GMT
```

The following example shows the output from the **show backup-config** command on a SZ100 controller.

```
device# show backup-config
```

No.	Created on	Version	CP Version	DP Version	Created By	Type	Backup	Elapsed	File Size
1	2019-03-03 11:14:31 GMT	3.1.0.0.187	3.1.0.0.381	3.1.0.0.33	admin	Manual Backup	1		48.1KB

Show Commands

show backup-config-state

show backup-config-state

Displays the status of the available configuration backup.

Syntax

show backup-config-state

Modes

Privileged EXEC mode

Usage Guidelines

When backing up the controller configuration from the CLI, use this command to verify the status of the backup CLI configuration file.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows the output from the **show backup-config-state** command.

```
device# show backup-config-state  
  
Operation : Successful  
Progress Status : Completed
```

show backup-network

Displays backup network configuration versions.

Syntax

show backup-network

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to verify the backup file of the controller network configuration, including the control plane and data plane information. The controller creates a backup of its network configuration on its database.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows output from the **show backup-network** command.

```
device# show backup-network
```

No.	Created on	Patch Version	File Size
1	2019-02-11 16:53:26 GMT	3.1.0.0.401	1.2KB

Show Commands

show backup-schedule

show backup-schedule

Displays the schedule of system backup versions.

Syntax

show backup-schedule

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows output from the **show backup-schedule** command.

```
device# show backup-schedule  
No running configuration
```

show backup-state

Displays the system backup state.

Syntax

show backup-state

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows output from the **show backup-state** command.

```
device# show backup-state  
No running configuration
```

Show Commands

show backup-upgrade-state

show backup-upgrade-state

Displays the system backup and upgrade state.

Syntax

show backup-upgrade-state

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows output from the **show backup-upgrade-state** command.

```
device# show backup-upgrade-state
No running configuration
```

show client

Displays current AP associated client sessions.

Syntax

show client *client-mac*

Parameters

client-mac

Displays AP client sessions for the specified client MAC address.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows output from the **show client** command.

```
device# sshow client F2:AD:E0:A6:81:D3

General Information
-----
STA MAC Address       : F2:AD:E0:A6:81:D3
IP Address            : 10.206.84.55 / ::
User Name             : N/A
Auth Method           : Standard+Open
Encryption Method     : None
Connected Since       : 2021-03-30 07:09:07 GMT
Status                : AUTHORIZED
AP Zone               : zone1
Access Point          : dhcp-10-206-84-82
Model Name            : Android 11
Host Name             : Galaxy-A50
-----
Channel               : 40
VLAN                  : 1
SNR (dB)              : 65
Packets from Client   : 9.7KB
Bytes from Client     : 3.1MB
Packets to Client     : 30.2KB
Bytes to Client       : 37.3MB
Dropped Packets to Client : 0
AP Rx Signal (db)    : 31
...

```

Show Commands

show clock

show clock

Displays the current GMT date and time.

Syntax

show clock

Modes

User EXEC mode

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example displays the date as March 26, 2020 at 6:09pm Greenwich Mean Time (GMT).

```
device> show clock
```

```
2020-03-26 18:09:53 GMT
```


show cls-sess

Displays the session information of a user equipment at a node level as per the MSISDN or by date and time.

Syntax

```
show cls-sess{msisdnmsisdn|date-time}
```

Parameters

msisdnmsisdn

MSISDN and MSISDN value.

date-time

Displays session information by date and time in the following format: dd/mm/yy/hh/mm/ss.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only.

Examples

The following example shows the session information for March 3, 2020 at 8:10:30 am.

```
device# show cls-sess 03/03/20/08/10/30
```

```
No. MSISDN IMSI   DHCP IP   DNS IP   Auth Server IP Acct Server IP Charging Type PDP IP   TEID GGSN IP
SESS Type
-----
```

Show Commands

show cluster

show cluster

Displays the system cluster settings.

Syntax

```
show cluster{ip-list|name}
```

Parameters

ip-list

Displays the cluster node IP list.

name

Displays the cluster name.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows output from the **show cluster** command with the **ip-list** option.

```
device# show cluster ip-list
Cluster Node IPs: 10.1.96.128
```

The following example shows output from the **show cluster** command with the **name** option.

```
device# show cluster name
Cluster Name: SZ300
```

show cluster-node

Displays the cluster node information.

Syntax

```
show cluster-node[name]
```

Parameters

name

Cluster node name.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported for SmartZone 100 devices.

Run the **show cluster-node** command to view information for all the cluster nodes configured on the controller. Use the *name* option to display information for a specific cluster node.

Examples

The following example shows output from the **show cluster-node** command.

```
device# show cluster-node
```

No.	Cluster Node	Description	Model	Serial Number	# of APs	CP IP	CP MAC	CP Version
1	aish	aish	SZ124	501526006045	0	10.174.84.161	F8:E7:1E:20:0C:A0	5.2.1.0.252
	DP IP	DP MAC		DP Status	Cluster Role	Uptime		
	182.168.20.161	F8:E7:1E:20:0C:B0		Managed	Leader	1d 5h 38m		

Show Commands
show cluster-node

The following example shows output from a specific cluster node.

```
device# show cluster-node mktg
```

```
Cluster Node : mktg
-----
Serial Number : 501526006045
Model         : SZ124
Description   : mktg
Role          : Leader
Status        : In_Service
Total Memory  : 31.3GB
Total Disk    : 241.1GB
# of Ports    : 6

Control Plane : Mktg-C
-----
MAC Address   : F8:E7:1E:20:0C:A0
Firmware      : 5.2.1.0.252
IP Address    : 10.174.84.161
# of APs      : 0

Data Plane    : Mktg-C
-----
MAC Address   : F8:E7:1E:20:0C:B0
IP Address    : 182.168.20.161
Model         : SZ124

Network Settings
-----

IPv4 Interface
-----
IP Mode       : Static
IP Address    : 10.174.84.161
Subnet Mask   : 255.255.254.0
Gateway       : 10.174.84.1

IPv6 Interface
-----
IP Mode       : Static
IP Address    : 2070::161/64
Gateway       : 2070::1

IPv6 RA
-----
No.   Interface   IP Address
-----
1     Control

IPv6 DHCP
-----
No.   Interface   IP Address
-----
1     Control

DNS Servers
-----
No.   Priority  Server
-----
1     1         4.2.2.2
2     2         8.8.8.8

User Defined Interfaces
-----

Routes
-----
No.   Network Address Subnet Mask   Gateway   Interface   Metric
-----
```

```
1    0.0.0.0      0.0.0.0      10.174.84.1  Control Interface  0
2    10.174.84.0  255.255.254.0  0.0.0.0     Control Interface  0
```

IPv6 Routes

```
-----  
No. Network Address Gateway Interface Metric  
-----  
1  2070::/64      ::          Control Interface  256  
2  ::/0           2070::1    Control Interface  1
```

Show Commands
show cluster-state

show cluster-state

Displays the system cluster and node state.

Syntax

show cluster-state

Modes

Privileged EXEC mode

Usage Guidelines

Use this command when you need to view the statuses of the node and the cluster before restoring a backup file for example.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows output from the **show cluster-state** command.

```
device# show cluster-state

Current Management Service Status : In service
Current Node Status : In service
Cluster Status : In service
Cluster Operation : None
System Mode : None

Cluster Node Information
-----
No.   Name                Role
-----
1     RRR-SZ300-C         LEADER
```

show controller

Displays the vSZ-related configuration.

Syntax

```
show controller[cli_upload_cert_chain|current_cert_chain|connect_status]
```

Parameters

cli_upload_cert_chain

Displays user upload certificate chain.

current_cert_chain

Displays the vSZ-related current server certificate chain.

connect_status

Displays the vSZ-D connection status to the controller.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.

Examples

The following example displays the vSZ-related current server certificate chain.

```
device# device# show controller
vsz Address: 10.1.2.250
```

Show Commands
show control-plane

show control-plane

Displays the list of, and information about, control planes on the controller.

Syntax

```
show control-plane [ cp-name ]
```

Parameters

cp-name
Control plane name.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only.

Control planes and data planes are used to control traffic. The control plane manages and exchanges routing table information. The control plane packets are processed by the router to update the routing table information. The data plane forwards the traffic along the path according to the logic of the control plane.

Run the **show control-plane** command to view information for the specified control plane.

Examples

The following example shows output from the **show control-plane** command.

```
device# show control-plane
```

No.	Name	CP MAC Address	Model	Serial Number	# of APs	Description	Firmware	Management IP
Cluster	IP	Control IP	Cluster	Role	Uptime			
1	MKT-SZ300-C	24:79:2A:00:0B:00	SZ300	161737000069	2	MKT-SZ300	5.2.1.0.223	10.174.84.128
	10.1.96.128	10.1.13.128	Leader	2d 12h 47m				

The following example shows partial output from the **show control-plane** command displaying detailed information about the MKT-SZ300-C controller.

```
device# show control-plane MKT-SZ300-C

MKT-SZ300-C
-----
Serial Number   : 161737000069
Model           : SZ300
Description     : KKK-SZ300
Management IP   : 10.174.84.128
Cluster IP     : 10.1.96.128
Control IP     : 10.1.13.128
Firmware       : 5.2.1.0.223
Status         : In_Service
Role           : Leader
# of APs       : 2
Total Memory    : 127.9GB
Total Disk     : 1TB
# of Ports     : 6

Network Settings
-----
Control Interface  Cluster Interface  Management Interface
IP Model           Static              Static              Static
IP Address         10.1.96.128        10.1.13.128        10.174.84.128
Subnet Mask        255.255.255.0     255.255.255.0     255.255.254.0
Gateway            10.1.96.1          10.1.13.1          10.174.84.1

IPv6 Network Settings
-----
Control Interface  Cluster Interface  Management Interface
IP Model           Static              Static
IP Address         2005::128         2070::128/64
Gateway            2005::1           2070::1

IPv6 RA
-----
No.  Interface  IP Address
-----
1    Control
2    Cluster
3    Management

IPv6 DHCP
-----
No.  Interface  IP Address
-----
1    Control
2    Cluster
3    Management

DNS Servers
-----
No.  Priority  Server
-----
1    1         10.9.0.250
2    2         8.8.8.8
3    3         2001::1

User Defined Interfaces
-----

Routes
-----
No.  Network Address  Subnet Mask  Gateway  Interface  Metric
-----
1    0.0.0.0          0.0.0.0     10.174.84.1  Management Interface  0
2    10.1.13.0       255.255.255.0  0.0.0.0     Control Interface     0
3    10.1.96.0       255.255.255.0  0.0.0.0     Cluster Interface     0
4    10.174.84.0    255.255.254.0  0.0.0.0     Management Interface  0
```

Show Commands
show control-plane

5	140.138.0.0	255.255.0.0	10.1.13.1	Control Interface	0
6	182.168.0.0	255.255.0.0	10.1.13.1	Control Interface	0
7	192.168.0.0	255.255.0.0	10.1.13.1	Control Interface	0

IPv6 Routes

No.	Network Address	Gateway	Interface	Metric
1	2005::/64	::	Control Interface	256
2	2070::/64	::	Management Interface	256
3	::/0	2070::1	Management Interface	1

show control-plane-stats

To display control plane status, use the following command:

Syntax

```
show control-plane-stats c-plane-name type{cpu | disk | interface interface-type | memory | port port-number} period{7-d | 8-h | 24-h | 30-d}
```

Parameters

c-plane-name

Control plane name.

type

Type of control plane statistics to display.

cpu

Displays control plane cpu usage statistics.

disk

Displays control plane disk usage statistics.

interface*interface-type*

Displays control plane usage statistics for the specified interface type. One of the following; cluster, control, management, or user-defined.

memory

Displays control plane memory usage statistics.

port*port-number*

Displays control plane usage statistics for the specified port.

period

Displays the specified control plane statistics for a specified period of time.

7-d

Displays statistics for the last 7 days.

8-h

Displays statistics for the last 8 hours.

24-h

Displays statistics for the last 24 hours.

30-d

Displays statistics for the last 30 days.

Modes

Privileged EXEC mode

Show Commands

show control-plane-stats

Usage Guidelines

Use this command to verify that the backup file has been created successfully. Backups are useful, for example, to create backups of clusters that need to be restored.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows control plane memory statistics for the MKTG-SZ399-C controller over the last 24 hours.

```
device# show control-plane-stats MKTG-SZ300-C type memory period 24-h
```

No.	Time	MAX	AVG	MIN
1	2020-03-25 18:00:00 GMT	16.9%	16.86%	16.84%
2	2020-03-25 19:00:00 GMT	16.91%	16.86%	16.83%
3	2020-03-25 20:00:00 GMT	16.91%	16.86%	16.83%
4	2020-03-25 21:00:00 GMT	16.91%	16.86%	16.83%
5	2020-03-25 22:00:00 GMT	16.89%	16.86%	16.84%
6	2020-03-25 23:00:00 GMT	16.92%	16.87%	16.84%
7	2020-03-26 00:00:00 GMT	16.93%	16.87%	16.84%
8	2020-03-26 01:00:00 GMT	16.93%	16.87%	16.67%
9	2020-03-26 02:00:00 GMT	16.92%	16.88%	16.84%
10	2020-03-26 03:00:00 GMT	16.93%	16.88%	16.84%
11	2020-03-26 04:00:00 GMT	16.91%	16.87%	16.84%
12	2020-03-26 05:00:00 GMT	16.92%	16.88%	16.85%
13	2020-03-26 06:00:00 GMT	16.92%	16.88%	16.86%
14	2020-03-26 07:00:00 GMT	16.92%	16.88%	16.85%
15	2020-03-26 08:00:00 GMT	16.92%	16.88%	16.85%
16	2020-03-26 09:00:00 GMT	17.17%	16.9%	16.86%
17	2020-03-26 10:00:00 GMT	16.96%	16.91%	16.88%
18	2020-03-26 11:00:00 GMT	16.96%	16.91%	16.88%
19	2020-03-26 12:00:00 GMT	16.95%	16.91%	16.88%
20	2020-03-26 13:00:00 GMT	16.96%	16.91%	16.88%
21	2020-03-26 14:00:00 GMT	16.95%	16.91%	16.88%
22	2020-03-26 15:00:00 GMT	16.94%	16.92%	16.9%
23	2020-03-26 16:00:00 GMT	16.95%	16.91%	16.89%
24	2020-03-26 17:00:00 GMT	16.97%	16.92%	16.89%

The following example shows control plane statistics for the control interface of the MKTG-SZ399-C controller over the last 7 days.

```
device# show control-plane-stats MKTG-SZ300-C type interface control period 7-d
```

No.	Time	RX-Rate	TX-Rate	RX-Bytes	TX-Bytes	RX-Packets	TX-Packets
1	2020-03-19 GMT						
2	2020-03-20 GMT	3436	21316	37117479	230215337	350290	205834
3	2020-03-21 GMT	2744	263	29637647	2848958	374836	25811
4	2020-03-22 GMT	2757	264	29780459	2853072	376911	25816
5	2020-03-23 GMT	1774323	1181554	19162691683	12760783562	47448311	38298290
6	2020-03-24 GMT	4348998	1395874	46969182265	15075445859	72050014	52834038
7	2020-03-25 GMT	1475	492	15939300	5318891	176237	47758

show counter

Displays the database counter values.

Syntax

```
show counter{devices|users}
```

Parameters

devices

Displays number of devices.

users

Displays information about users.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows the number of devices.

```
device# show counter devices

Total Devices: 0
```

The following example shows the number of users for each user type.

```
device# show counter users

Guest credentials   : 1
Local users         : 1
Remote users        : 0
-----
Total users         : 2
```

Show Commands

show cpuinfo

show cpuinfo

Displays the current CPU usage status.

Syntax

show cpuinfo

Modes

User EXEC mode

Privileged EXEC mode

Usage Guidelines

Use this command when you are troubleshooting a slow device because a high CPU usage can result in a slower processing of the traffic through a device.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example output from the **show cpuinfo** command displays information about all the processors and the percentage of the current CPU in use.

```
device# show cpuinfo

processor      : 0
model name    : Intel(R) Xeon(R) CPU E5-2695 v3 @ 2.30GHz
processor      : 1
model name    : Intel(R) Xeon(R) CPU E5-2695 v3 @ 2.30GHz
processor      : 2
model name    : Intel(R) Xeon(R) CPU E5-2695 v3 @ 2.30GHz
processor      : 3
.
.
.
processor      : 54
model name    : Intel(R) Xeon(R) CPU E5-2695 v3 @ 2.30GHz
processor      : 55
model name    : Intel(R) Xeon(R) CPU E5-2695 v3 @ 2.30GHz
%Cpu(s): 21.7 us,  4.1 sy,  0.0 ni, 74.0 id,  0.2 wa,  0.0 hi,  0.0 si,  0.0 st
```

show data-plane

Displays information about the data planes on the controller.

Syntax

```
show data-plane [ dp-name [ ip route | ping host ] ]
```

Parameters

dp-name

Data plane name.

ip route

Displays the IP routing table for the specified data plane.

ping host

Displays the ping information to a specific IP host address for the specified data plane.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only.

Control planes and data planes are used to control traffic. The control plane manages and exchanges routing table information. The control plane packets are processed by the router to update the routing table information. The data plane forwards the traffic along the path according to the logic of the control plane.

Run the **show data-plane** command to view information and traffic for the specified data plane.

Show Commands

show data-plane

Examples

The following example shows output from the **show data-plane** command for the SALES-SZ300-D0 data plane

```
device# show data-plane SALES-SZ300-D0

SALES-SZ300-D0
-----
Serial Number       : 24:79:2A:00:0B:10
Model               : SZ300
Firmware            : 5.2.1.0.270
MAC Address         : 24:79:2A:00:0B:10
IP Address          : 10.148.124.36
IPv6 Address        : 2148::4e8:34ad:18d4:e3d2
Status              : Managed

Access and Core Tunnel Summary
-----
Ruckus GRE Tunnels      : 0
Access L2oGRE Tunnels  : 0
Access Q-in-Q Layer 2 Tunnels : 0
Core L2oGRE Tunnels    : 0
Core L3oGRE Tunnels    : 0
GGSN Count             : 0
```


show data-plane-stats

Displays data plane statistics.

Syntax

```
show data-plane-stats dp-name type port { Port0 | Port1 } period { 7-d | 8-h | 24-h | 30-d }
```

Parameters

dp-name

Data Plane name.

type

Statistics data type.

port

Displays port usage statistics

Port0

Port 0.

Port1

Port 1

period

Displays statistics for the specified period.

7-d

The last 7 days.

8-h

The last 8 hours.

24-h

The last 24 hours.

30-d

The last 30 days.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only.

Control planes and data planes are used to control traffic. The control plane manages and exchanges routing table information. The control plane packets are processed by the router to update the routing table information. The data plane forwards the traffic along the path according to the logic of the control plane.

Run the **show data-plane-stats** command to view traffic statistics for the specified data plane.

Show Commands

show data-plane-stats

Examples

The following example shows partial output from the **show data-plane-stats** command displaying the traffic through Port 0 on the MKTG-SZ300-D1 controller for the last eight hours.

```
device# show data-plane-stats MKTG-SZ300-D1 type port Port0 period 8-h
```

No.	Time	RX-Rate	TX-Rate	RX-Bytes	TX-Bytes	RX-Packets	TX-Packets
1	2020-04-07 07:45:00 GMT	1645	54	185088	6078	2904	66
2	2020-04-07 08:00:00 GMT	1634	58	183904	6532	2885	70
3	2020-04-07 08:15:00 GMT	1616	53	181880	5992	2873	65
4	2020-04-07 08:30:00 GMT	1664	54	187280	6164	2933	67
5	2020-04-07 08:45:00 GMT	1636	58	184090	6532	2888	70
6	2020-04-07 09:00:00 GMT	1866	53	210029	5992	2993	65
7	2020-04-07 09:15:00 GMT	1694	53	190687	5992	2948	65
8	2020-04-07 09:30:00 GMT	1620	58	182324	6532	2869	70
9	2020-04-07 09:45:00 GMT	1658	54	186616	6164	2923	67
10	2020-04-07 10:00:00 GMT	1629	54	183336	6078	2896	66
.							
.							
.							

show dhcp binding

Displays the DHCP binding or profile for a vSZ-D controller.

Syntax

```
show dhcp binding{ue-mac-address|pool_namepool-name}
```

Parameters

binding

Displays DHCP binding information.

ue-mac-address

Display the DHCP binding information for the device specified by the MAC address.

pool_name*pool-name*

Display the DHCP binding information for the specified device pool.

Modes

Privileged EXEC mode

Usage Guidelines

Run the **show dhcp** command to display DHCP information configured on the controller for troubleshooting purposes.

This command is supported on the SmartZone Data Plane controllers only.

Examples

The following example displays DHCP binding information for a single device specified by its MAC address.

```
device# show dhcp binding pool_name DHCP-POOL-01  
  
>> Dynamic IPs: shown=0 (detected: expired=0, actv=0  
    Fixed IPs: shown=0 (detected: expired=0, actv=0)
```

Show Commands

show dhcp-relay-stats

show dhcp-relay-stats

Displays a list of DHCP relay statistics.

Syntax

```
show dhcp-relay-stats
```

Modes

Privileged EXEC mode

Usage Guidelines

Run the **dhcp-relay** command to enable DHCP Relay functionality and generate statistics before entering this command.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows information about DHCP Relay.

```
device# show dhcp-relay-stats
```

No.	Data Plane	DHCP Server IP	DISCOVER	OFFER	REQUEST	ACK	DHCP Opt82	DHCP Pkts Dropped
1	vDP-23-2-5210 389-1	1.1.1.15	4	4	3	2	6	1

show diskinfo

Displays the current disk usage on the controller.

Syntax

```
show diskinfo
```

Modes

Privileged EXEC mode

Usage Guidelines

Run the **show diskinfo** command to determine the current disk size of the node if you need to backup a cluster, for example.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows output from the **show diskinfo** command.

```
device# show diskinfo

Total Disk: 1.03086 TB
Used Disk: 44.4 GB
Free Disk: 1011.2 GB
```

Show Commands

show dp-customized-config

show dp-customized-config

Displays customized data plane configuration commands.

Syntax

```
show dp-customized-config{all|name}
```

Parameters

all

Displays all customized data plane configuration commands.

name

Displays customized configuration commands for a specific data plane.

Modes

Debug configuration mode

Usage Guidelines

The command is only available under debug mode.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows customized configuration for all data planes.

```
device# debug
device(debug)# show dp-customized-config all

Data Plane Name          Customized Configuration
-----
RRR-SZ300-D0
RRR-SZ300-D1
```

show event

Displays events on the controller.

Syntax

show event

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all the controllers including the SmartZone Data Plane.

Examples

The following example shows partial output from the **show event** command run on a SZ300 controller.

```
device# show event
```

No.	Datetime	Event Code	Event Type	Severity	Activity
1	2020-04-07 15:57:57 GMT	508	Data plane IP address updated	Informational	Data plane [RRR-SZ300-D1@24:79:2A:00:0B:18] IP address changed.
2	2020-04-07 15:57:56 GMT	508	Data plane IP address updated	Informational	Data plane [RRR-SZ300-D0@24:79:2A:00:0B:10] IP address changed.
3	2020-04-07 15:57:48 GMT	2502	Node IPv6 address deleted	Informational	Network interface [pow0] on node [RRR-SZ300-D0] deleted IPv6 address [2148::2679:2aff:fe00:b10].
4	2020-04-07 15:57:48 GMT	2502	Node IPv6 address deleted	Informational	Network interface [pow0] on node [RRR-SZ300-D1] deleted IPv6 address [2148::2679:2aff:fe00:b18].
5	2020-04-07 15:56:00 GMT	508	Data plane IP address updated	Informational	Data plane [RRR-SZ300-D0@24:79:2A:00:0B:10] IP address changed.
6	2020-04-07 15:56:00 GMT	508	Data plane IP address updated	Informational	Data plane [RRR-SZ300-D1@24:79:2A:00:0B:18] IP address changed.
7	2020-04-07 15:55:52 GMT	2501	Node IPv6 address added	Informational	Network interface [pow0] on node [RRR-SZ300-D1] added IPv6 address [2148::2679:2aff:fe00:b18].

Show Commands

show event

The following example shows partial output from the **show event** command run on a vSZ-D controller.

```
device# show event

2019-03-18T17:28:57+00:00 vDP-243 vdp_cli[566]: @@99214,dpUserLogout,
"dpKey"="97H0T58MTPWU263XS6N432G7X55Q000C297375FB000C29737505", "source"="10.206.67.253", "account"="admin
"

2019-03-18T17:38:47+00:00 vDP-243 vdp_cli[27580]: @@99221,dpSessionIdleTerminated,
"dpKey"="97H0T58MTPWU263XS6N432G7X55Q000C297375FB000C29737505", "source"="Console"

2019-03-18T17:38:47+00:00 vDP-243 vdp_cli[27580]: @@99214,dpUserLogout,
"dpKey"="97H0T58MTPWU263XS6N432G7X55Q000C297375FB000C29737505", "source"="Console", "account"="admin"

2019-03-21T11:19:05+00:00 vDP-243 vdp_cli[14105]: @@99212,dpUserLogin,
"dpKey"="97H0T58MTPWU263XS6N432G7X55Q000C297375FB000C29737505", "source"="10.206.67.253", "account"="admin
"
```


show ggsn-cnxxn-stats

Displays Gateway GPRS Serving Node (GGSN) connections statistics.

Syntax

show ggsn-cnxxn-stats

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only.

The Gateway GPRS Support Node (GGSN) is a main component of the General Packet Radio Service (GPRS) network. The GGSN is responsible for the interworking between the GPRS network and external packet switched networks such as the Internet and X. 25 networks. You must be aware of the GGSN session settings on the controller to monitor the health of the controller. Run the **show ggsn-cnxxn-stats** command to view response times between the GGSN and the controller.

Examples

The following example shows output from the **show ggsn-cnxxn-stats** command.

```
device# show ggsn-cnxxn-stats
      No.   Control Plane  GGSN IP           Echo Req Sent  Echo Rsp Rcvd  Echo Req Rcvd  Echo Rsp
Sent PathFailure  Created On           Last Modified On
-----
0      1      74:FE:48:08:A  10.174.84.143    5              0              0
      0              2021-03-24 12:03:58 GMT  2021-03-24 12:03:58 GMT
      F:A6
-----
```

Show Commands
show ggsn-gtpc-stats

show ggsn-gtpc-stats

Displays Gateway GPRS Serving Node (GGSN) statistics for GPRS Tunneling Protocol control plane (GTP-C) sessions.

Syntax

show ggsn-gtpc-stats

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only.

The Gateway GPRS Support Node (GGSN) is a main component of the General Packet Radio Service (GPRS) network. The GGSN is responsible for the interworking between the GPRS network and external packet switched networks such as the Internet and X. 25 networks. You must be aware of the GGSN session settings on the controller to monitor the health of the controller. Run the **show ggsn-gtpc-stats** command to view statistics related to the tunnels between the GGSN and the controller.

Examples

The following example shows output from the **show ggsn-gtpc-stats** command.

```
device# show ggsn-gtpc-stats

No. MVNO Account Control Plane  GGSN IP      Created On      Last Modified On  PDP Context  GGSN
Init Update
-----
SCG Init Update(Roaming)  SCG Init Update(CoA from AAA)  SCG Init Update(Events from HLR)  GGSN Init
Delete
-----
SCG Init Delete(Error)  DM Init Delete  SCG Init Delete(Event from HLR)  SCG Init Delete(Timeout)
AP Init Delete
-----
DP Init Delete  Client Init Delete  Admin Init Delete
-----
```

show history

Displays a list of CLI commands that have recently been executed.

Syntax

show history

Modes

Privileged EXEC mode

Usage Guidelines

Run the **show history** command to find a command that you have entered in the current CLI session. Press the up arrow to locate the command from the history list at the CLI prompt if you want to reenter the command.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows output from the **show history** command.

```
device# show history
0. enable
1. show domain "Administration Domain"
2. show dp-group
3. show ftp-server
4. show history
```

show interface

Displays the interface runtime status or configuration information.

Syntax

SZ300 syntax:

```
show interface[cluster | control | management | user-defined]
```

SZ100 syntax:

```
show interface[ap-tunnel-data | mgmt-and-ap-control | user-defined]
```

vSZ-D syntax:

```
show interface[access-core-sep-config | current-access-core-separate | current-data | current-management | data-config | management-  
config]
```

Parameters

cluster

Displays cluster interface information.

control

Displays control interface information.

management

Displays management interface information.

user-defined

Displays user-defined interface information.

ap-tunnel-data

Displays AP tunnel interface information.

mgmt-and-ap-control

Displays management and AP control interface information.

access-core-sep-config

Displays access core separate interface configuration.

current-access-core-separate

Displays access core separate interface runtime information.

current-data

Displays access core separate interface configuration.

current-management

Displays management interface runtime information.

data-config

Displays data interface configuration.

management-config

Displays management interface configuration.

Modes

Privileged EXEC mode

Usage Guidelines

Run the **show interface** command without any keywords to view information about all types of interfaces configured on the controller.

This command is supported on all the controllers including the SmartZone Data Plane.

Examples

The following example shows output from the **show interface cluster** command on a SZ300 controller.

```
device# show interface cluster

Interface      : Cluster
IP Mode       : Static
IP Address    : 10.1.96.128
Subnet Mask   : 255.255.255.0
Gateway      : 10.1.96.1
```

The following example shows output from the **show interface control** command on a SZ300 controller.

```
device# show interface control

Interface      : Control
IP Mode       : Static
IP Address    : 10.1.13.128
Subnet Mask   : 255.255.255.0
Gateway      : 10.1.13.1

IPv6 Mode     : Static
IPv6 Address  : 2005::128/64
IPv6 Gateway  : 2005::1
```

The following example shows output from the **show interface ap-tunnel** command on a SZ100 controller.

```
device# show interface ap-tunnel

Interface      : AP Tunnel Data
IP Mode       : Static
IP Address    : 182.168.20.161
Subnet Mask   : 255.255.255.0
Gateway      : 182.168.20.1

IPv6 Mode     : Auto
IPv6 Address  : 2078::fae7:1eff:fe20:cb0/64
IPv6 Gateway  : fe80::82e0:1dff:fe76:cbd6
```

The following example shows output from the **show interface management-config** command on a vSZ-D controller.

```
device# show interface management-config

Configure Management interface:
proto: static
proto6: auto
address:10.206.67.243
netmask:255.255.255.0
gateway:10.206.67.254
```

Show Commands

show internal-subnet

show internal-subnet

Displays the runtime internal subnet prefix.

Syntax

show internal-subnet

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows output from the **show internal-subnet** command.

```
device# show internal-subnet  
Internal Subnet Prefix: 10.254.1
```

show ip

Displays information about the IP static route configured on the controller.

Syntax

show ip routestatic

Parameters

routestatic

Displays IP static route information.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows output from the **show ip route static** command.

```
device# show ip route static
Static Routes
-----
No. Network Address Subnet Mask Gateway Interface Metric
-----
1 10.1.31.0 255.255.255.0 172.19.9.1 Control 0
```

Show Commands

show ip (DP)

show ip (DP)

Displays IP information for SmartZone Data Plane controllers.

Syntax

```
show ip{name-server|data-nat-ip}
```

Parameters

name-server

Displays DNS server information.

data-nat-ip

Displays NAT server information.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.

Examples

The following example shows output from the **show ip name-server** command.

```
device# show ip name-server
IP Name Server: 10.8.8.8
```


show license

Displays information about the current controller licenses.

Syntax

```
show license
```

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Show Commands

show license

Examples

The following example shows output from the **show license** command on a SZ300 controller.

```
device# show license
```

```
License Server Status
```

```
-----  
License Server           : RUCKUS Cloud License Server  
Last Sync                : 2020-04-07 00:59:26 GMT  
30 Days Statistics       : Success:19 Error:0  
Historical Sync Status  
-----
```

```
-----  
No.  Date                Status  
-----  
1    2020-04-07 00:59:26 GMT OK  
2    2020-04-06 00:29:29 GMT OK  
3    2020-04-05 00:18:51 GMT OK  
4    2020-04-04 00:49:10 GMT OK  
5    2020-04-03 00:07:59 GMT OK  
-----
```

```
License Summary
```

```
-----  
No.  License Type                #of Units Total #of Units Consumed #of Units Available  
-----  
1    AP Capacity License           1010             1002 (99.208%)     8 (0.792%)  
2    AP Direct Tunnel License      4                 0 (0%)             4 (100%)  
3    URL Filtering Capacity License 0                 0 (100%)           0 (0%)  
4    Switch Capacity License       0                 0 (100%)           0 (0%)  
5    AP Split Tunnel Capacity License 0                 0 (100%)           0 (0%)  
-----
```

This table shows the currently installed licenses

```
Installed Licenses [Customer: RUCKUS-Internal]
```

```
-----  
---  
No. Node      Feature          Capacity Description                Start Date      Expiration  
Date  
-----  
1    KKK-SZ300 CAPACITY-AP  1000    AP Capacity License                2014-08-04 GMT 2022-04-04  
GMT  
2    KKK-SZ300 CAPACITY-RMNO 11      Temporary RMNO License              2014-08-04 GMT 2022-04-04  
GMT  
3    KKK-SZ300 CAPACITY-VSZD 2        License for 1 Virtual Data Plane     2015-05-21 GMT Permanent  
4    KKK-SZ300 CAPACITY-RXGW 4        Tunnel Capacity license              2014-08-11 GMT Permanent  
5    KKK-SZ300 SUP-SZ300-EU  1        WatchDog Premium Support for SmartZone 2017-02-09 GMT 2022-02-09  
GMT  
300(SZ300) with redundant DC power,  
5 year, Smart Licensing  
6    KKK-SZ300 CAPACITY-AP  10      SZ/(v)SCG AP license for 1 AP       2015-12-08 GMT Permanent  
-----
```

show logs-filter

Displays the LMA signalling status.

Syntax

```
show logs-filter client mac-address [copyftp-url]
```

Parameters

client mac-address

Client STA MAC address.

copyftp-url

Copies the STA real-time tracing log to an external FTP server. FTP directory URL format: ftp://<username>:<password>@<ftp-host>[</dir-path>]

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows output for the **show logs-filter** command.

```
device# show logs-filter
show logs-filter client 6E:6D:3D:45:EE:92
2021-03-30 08:17:24+00:00 127.0.83.187 hostapd: @@236,clientInfoUpdate,"apMac"="dc:ae:eb:
22:3e:d0","clientMac"="6e:6d:3d:45:ee:92","ssid"="aaa_rvin","bssid"="dc:ae:eb:22:3e:dc",
userId="",wlanId="2","iface"="wlan32","tenantUUID"="839f87c6-d116-497e-afce-
aa8157abd30c","apName"="dhcp-10-206-84-82","clientIP"="10.206.84.162","userName"="6e6d3d45ee92",
"vlanId"="1","radio"="a/n/
ac","encryption"="None","fwVersion"="6.0.0.0.1582","model"="R550","zoneUUID"="be61b0d2-3e5a-4fd2-8dfc-31
d4a158a9d0","zoneName"="zone1","timeZone"="UTC+0",
"apLocation"="",apGps="",apIpAddress="10.206.84.82","apIpv6Address","",apGroupUUID"="691029d9-5fc9-
4d30-8324-7d8486632039","domainId"="8b2081d5-9662-40d9-a3db-2a3cf4dde3f7",
serialNumber"="272002000225","domainName"="Administration Domain","wlanGroupUUID"="4305b192-9106-11eb-
b8d6-2a735728af2d","idealEventVersion"="3.5.1","apDescription"=""
2021-03-30 08:17:22+00:00 127.0.83.187 hostapd: @@202,clientJoin,"apMac"="dc:ae:eb:
22:3e:d0","clientMac"="6e:6d:3d:45:ee:92","ssid"="aaa_rvin","bssid"="dc:ae:eb:22:3e:dc",
userId="",wlanId="2","iface"="wlan32","tenantUUID"="839f87c6-d116-497e-afce-
aa8157abd30c","apName"="dhcp-10-206-84-82","vlanId"="1","radio"="a/n/ac","encryption"="None",
"Instantaneous
rssi"="0","Xput"="0","fwVersion"="6.0.0.0.1582","model"="R550","zoneUUID"="be61b0d2-3e5a-4fd2-8dfc-31d4a
158a9d0","zoneName"="zone1","timeZone"="UTC+0","apLocation"="",
"apGps"="",apIpAddress="10.206.84.82","apIpv6Address","",apGroupUUID"="691029d9-5fc9-4d30-8324-7d8486
632039","domainId"="8b2081d5-9662-40d9-a3db-2a3cf4dde3f7","serialNumber"="272002000225",
"domainName"="Administration Domain","wlanGroupUUID"="4305b192-9106-11eb-
b8d6-2a735728af2d","idealEventVersion"="3.5.1","apDescription"=""
```

Show Commands

show md-stats

show md-stats

Displays the MD-Statistics captured on this controller.

Syntax

```
show md-stats{ap-macmac-address|node-idnode-id|peer-scg-macmac-address|remote|scg|scg-app-name}
```

Parameters

ap-macmac-address

Display the statistics for the connected AP at the controller.

node-idnode-id

Displays the statistics for node IDs stats; Valid value: actual node id + 1

peer-scg-macmac-address

Display the statistics for other SCG-MD connections at the controller.

remote

Display the statistics from remote AP/DP; Valid value: ap / dp .

mac

Provide MAC of AP/DP

app-name

Provide app-name from AP/DP; Valid value: ap_md / dp_md

scg

Display the local MD shared memory statistics.

scg-app-name

Displays the local application statistics; application names must be one of the following (scg_md/scg_sessmgr/md_proxy/scg_hip/scg_cnr/scg_communicator/scg_sciagent/scg_web/scg_eventreader/scg_nbi/scg_publicapi/scg_memproxy/scg_observer/scg_logmgr/logclient/scg_idm/scg_ccd/scg_push/scg_greyhound/scg_snmp/scg_cached)

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows partial output from the **show md-stats scg** command.

```
device# show md-stats scg

=====
MD Stats collected From      : [Apr14 2020 09:32:29] Till: [Apr14 2020 10:02:24]
MD -> App Success           : 371
MD -> App Failure           : 0
App -> MD Success           : 371
App -> MD Failure           : 0
AP MD connected             : 0
AP MD disconnected           : 0
DP MD connected             : 0
DP MD disconnected           : 0
Other MD connected          : 0
Other MD disconnected        : 0
PartialWriteTcpDiscCount    : 0
MPS Achieved                : 0
RAC Msg from ssh(Rx)        : 0
RAC Msg to MD(Rx)           : 0
MD to ssh Rac Msg(Tx)       : 0
MD to RAC, Rac msg(Tx)     : 0
=====
MD Stats collected From      : [Apr14 2020 10:02:29] Till: [Apr14 2020 10:32:24]
MD -> App Success           : 372
MD -> App Failure           : 0
App -> MD Success           : 372
App -> MD Failure           : 0
AP MD connected             : 0
AP MD disconnected           : 0
DP MD connected             : 0
DP MD disconnected           : 0
Other MD connected          : 0
Other MD disconnected        : 0
PartialWriteTcpDiscCount    : 0
MPS Achieved                : 0
RAC Msg from ssh(Rx)        : 0
RAC Msg to MD(Rx)           : 0
MD to ssh Rac Msg(Tx)       : 0
MD to RAC, Rac msg(Tx)     : 0
=====
.
.
.
```

Show Commands

show meminfo

show meminfo

Displays the current memory usage status.

Syntax

```
show meminfo
```

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows output from the **show meminfo** command.

```
device# show meminfo

Total Memory: 127.9 GB
Used Memory: 22.2 GB
Free Memory: 105.7 GB
```

show nat

Displays the NAT server configuration settings.

Syntax

```
show nat { stats | summary public-ip | filter | }
```

Parameters

stats

Displays the NAT service status.

summary

Displays NAT server information.

public-ip

Displays NAT server information.

filter

Displays NAT server filter information.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.

Examples

The following example shows output from the **show nat** status command.

```
device# config
device(config)# nat
device((config-nat)# # show stats
>> NAT stats: write stats into file '/etc/dp_config/nat_stats.txt'
upstream rate (from private): 0 kbps
downstream rate (from public): 0 kbps
port-mapping assignment rate: 0 /sec
public-vlan: 0
Pools(0) assigned port count: ('active' ones only)
```

Show Commands

show radius-proxy-stats

show radius-proxy-stats

Displays RADIUS proxy statistics on controller.

Syntax

show radius-proxy-stats

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example displays RADIUS proxy statistics captured on an SZ300 controller. The DM (NAS), CoA (NAS) and CoA Autz Only fields are not supported on SmartZone 100 controllers.

```
device# show radius-proxy-stats
```

```
No.   MVNO Account Control Plane AAA IP Created On Last Modified
On NAS Type Auth Accounting ACCESS Request ACCESS Challenge
ACCESS Accept ACCESS Reject Account Request Accounting Response
CoA (AAA)  DM (AAA)    DM (NAS)    Dropped requests due to rate
Limiting (Auth/Acc) AP Accounting AP Accounting Request/
Response CoA (NAS)  CoA Autz Only
-----
1 Super INDUS4-C 104.0.0.25 2015-03-20 12:46:20 GMT 2015-03-24
09:37:47 GMT Ruckus AP 0/0/0 0/0 6/6 0/0 0/0 0/0 6/6 0/0 0/0/0
0/0/0 0/0/0 0/0 0/2 6/0 0/0/0 0/0/0
2 Super INDUS4-C 104.0.0.2 2015-03-20 10:29:33 GMT 2015-03-24
09:37:47 GMT Ruckus AP 25/50/0 17/0 117/117 36/36 25/25 50/50
48/48 45/45 0/0/0 0/0/0 0/0/0 0/0 11/1 35/32 0/0/0 0/0/0
```


show radshm-stats

Displays RADIUS KPI (key performance indicators) captured per AAA server on the controller.

Syntax

```
show radshm-stats{display|kill|sendip-address}
```

Parameters

display

Display the Radius KPI statistics captured on this controller.

kill

Stops sending the Radius KPI statistics collected to the elastic search database.

sendip-address

Starts sending the Radius KPI statistics collected to the specified elastic search server IP address.

Modes

Privileged EXEC mode

Usage Guidelines



CAUTION

Use the *sendip-address* option with caution because the output is displayed on the console screen if the server IP address is not found.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example stops sending Radius KPI statistics captured on the controller to an elastic search server.

```
device# show radshm-stats kill
```

History

Release version	Command history
3.5.1	This command was introduced.

Show Commands
show report-result

show report-result

Displays specific report results.

Syntax

```
show report-result report-title
```

Parameters

report-title
Report title.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example displays the report results for Report1.

```
ruckus# show report-result report1
```

No.	Date and Time	Title Report	Template	Result Links	Status	Time Taken
1	2020-04-25 09:02:26 GMT	Report1	Client Number	CSV	Success	43ms
2	2020-04-25 00:00:02 GMT	Report1	Client Number	CSV	Success	19ms
3	2020-04-24 00:00:02 GMT	Report1	Client Number	CSV	Success	23ms
4	2020-04-23 00:00:02 GMT	Report1	Client Number	CSV	Success	20ms

show rogue-aps

Displays information about rogue access points.

Syntax

show rogue-aps

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows output for the show rogue-aps command.

```

device# show rogue-aps
show rogue-aps
No.    Rogue MAC          Type          Channel  Radio
SSID
Encryption  Last Detected
-----
-----
-----
1      0C:F4:D5:13:39:F8  Rogue        11       802.11 g
RVParks_W
          iFi          Open        2021-03-23 16:50:56 GMT
2      0C:F4:D5:53:39:FC  Rogue        153      802.11 a
RVParks_A
          dmin        Encrypted   2021-03-23 16:49:16 GMT
3      0C:F4:D5:93:39:FC  Rogue        153      802.11
a
          Open        2021-03-23 16:49:16 GMT

WLAN8616
          -OPEN
4      18:4B:0D:1C:A2:4C  Rogue        44       802.11 a   Clone
of
          SARAVANAN  Encrypted   2021-03-23 16:50:56 GMT

Repo
          rt
...
-11k-

```

Show Commands
show running-config

show running-config

Displays the current system configuration or the current configuration for the specified command.

Syntax

```
show running-config command-name [command-options]
```

DP syntax

```
show running-config [dhcp | nat]
```

Parameters

command-name *command-options*

Display the running configuration for the specified command and any options, if applicable.

Modes

Privileged EXEC mode

Usage Guidelines

Use the command to view the current configuration of a specific command or to view the entire configuration. Most configuration commands are available with this command, use the Tab+Tab or ? to view the supported list.

NOTE

Viewing the entire running configuration may require you to scroll down several "pages" of content.

On vSZ-D controllers only DHCP and NAT configuration information is displayed.

This command is supported on all the controllers including the SmartZone Data Plane.

Examples

The following example displays the current WLAN configuration for the zone named Zone-699-Dual.

```
device# show running-config zone Zone-699-Dual wlan
```

No.	Name	SSID	Auth Method	Encryption
1	5.2.1_ENG_MADHAV_S GRE_SZ300	5.2.1_ENG_MADHAV_S GRE_SZ300	OPEN	WPA2

The following example displays the current NTP server configuration.

```
device# show running-config ntp-server
```

```
Current System Time      : 2020-04-14 16:24:50 UTC
Current System UTC Time  : 2020-04-14 16:24:50 UTC
Current System Time Zone : UTC
NTP Server                : ntp.ruckuswireless.com
```

show service

Displays status information for system services.

Syntax

```
show service[service-name]
```

Parameters

service-name

Name of system service.

Modes

Privileged EXEC mode

Usage Guidelines

service-name

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example displays the status of the SNMP service.

```
NODE201# show service Cassandra
No.   Application Name   Status   Uptime   Memory   CPU   PID   Log Level   # of Logs
-----
1     Cassandra           Online   2-00:38:49  3.3GB   3.4   42662                20
```

Show Commands

show service

The following example displays the status of the all system services running on a SZ300 controller.

```
NODE201# show service
CaptivePortal
Cassandra
Ccmd
Ccmsync
Collectd
Communicator
Configurer
Core
Courier
DBlade
DeviceManager
EAut
ElasticSearch
EventReader
LogMgr
MdProxy
Mosquitto
MrProxy
MsgDist
NginX
Northbound
Observer
RabbitMQ
RadiusProxy
Redis
SNMP
ScgUniversalExporter
Scheduler
SessMgr
StatsHandler
SubscriberManagement
SubscriberPortal
Switchm
Web
<name>          System Service name
<cr>
```

show sha1-state

Displays the Secure Hash Algorithm 1 (SHA1) support state.

Syntax

`show sha1-state`

Modes

Debug configuration mode

Usage Guidelines

The command is only available under debug mode.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows that SHA1 is currently supported.

```
device# debug
device(debug)# show sha1-state

SHA1 support : true
```

History

Release version	Command history
3.5.1	This command was introduced.

Show Commands

show snapshot-disk-state

show snapshot-disk-state

Displays a snapshot of the disk state.

Syntax

```
show snapshot-disk-state
```

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the SmartZone vSZ-E and vSZ-H controllers only.

Examples

The following example shows a snapshot of the disk state.

```
device# show snapshot-disk-state
Info      :
Progress : 0
```


show ssh-rekey-limit-state

Displays the Secure Shell (SSH) rekey interval support state.

Syntax

```
show ssh-rekey-limit-state
```

Modes

Debug configuration mode

Usage Guidelines

The command is only available under debug mode. FIPS must be enabled before the command can be entered.

SSH rekey is disabled by default in non-FIPS mode. The SSH rekey interval is defined either by the maximum number of minutes or the maximum amount of data before SSH rekey is initiated. SSH rekey feature cannot be disabled in FIPS/CC mode.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows that the SSH rekey interval is currently supported.

```
device# debug
device(debug)# show ssh-rekey-limit-state

SSH Rekey support : true
RekeyLimit 100K 1d
```

Show Commands
show stats

show stats

Displays the current traffic statistics and basic system configuration of a vSZ-D controller.

Syntax

show stats

Modes

Privileged EXEC mode

Usage Guidelines

Run the **show stats** command to gather information about the traffic generated or managed by the controller for troubleshooting purposes.

This command is supported on the SmartZone Data Plane controllers only.

Examples

The following example displays traffic and system information for a v-SZ-D controller.

```
device# show stats
vSZ-D System/Total-Traffic Statistics:
-----
|System Uptime      |CPU Core|CPU Util|Mem Util|RAM Total (M)  |RAM Free (M)  |RAM Shared (M) |RAM
Buffer (M) |Current Process|
-----
|      72d, 3h,10m, 1s|      3| 99.0(%)| 94.9(%) |      5966.6|      306.7|
0.0|          0.1|          306|
-----
|Interface Name|Rx Pkts  |Tx Pkts  |Rx Bytes  |Tx Bytes  |Rx Error  |Tx Error  |Rx Drop  |Tx
Drop  |MulticastRcv|
-----
|Mgmt:br0      |      23.8M|      18.4M|      2.9G|      2.0G|          0|          0|
0|          0|          0|
-----
|Data:pow0     |      74.2M|      28.5M|      3.2G|      2.1G|          0|          0|
0|          12|          0|
-----
|Tunnel:br-tun |      8.9M|      9.6M|      1.4G|      1.4G|          0|          0|
0|          0|          0|
-----
-----
```

show status

Displays the current network settings and connection status of a vSZ-D controller.

Syntax

show status

Modes

Privileged EXEC mode

Usage Guidelines

Run the **show status** command to gather information about the network to which the controller is attached for troubleshooting purposes.

This command is supported on the SmartZone Data Plane controllers only.

Show Commands

show status

Examples

The following example displays network information for a v-SZ-D controller.

```
device# show status
vSZ-D Status:
-----
Current Date/Time: 2021-03-24 12:09:44 UTC
vSZ-D Uptime:      72d, 3h,11m,30s
-----
vSZ-D SETUP: Done
vSZ-D Version Number: 6.0.0.0.1108
vSZ-D Bandwidth: 1G
-----Management Interface-----
vSZ-D Management Interface Name: br0
vSZ-D Management Interface MAC: 00:2C:29:48:14:A3
vSZ-D Management Interface IP: 10.10.1.10
vSZ-D Management Interface Netmask: 255.255.255.220
vSZ-D Management Interface Gateway: 100.123.10.1
vSZ-D Management Interface DNS 1: 9.8.8.9
vSZ-D Management Interface DNS 2:
-----Data Interface-----
vSZ-D Data Interface Name: pow0
vSZ-D Data Interface MAC: 00:2C:29:48:94:AC
vSZ-D Data Interface Model: vSZ-D
vSZ-D Data Interface IP: 0.0.0.0
-----vSZ Connection Status-----
vSZ Active Server IPList(0): 10.102.1.151
vSZ Active Server IPList(1): 10.102.1.152
vSZ Current Server IP: 10.102.1.152
vSZ Cert Validation: Disable
vSZ-D to vSZ Connection State: [Connected]
vSZ-D Tunnel IP: 10.25.31.6
vSZ-D Tunnel Netmask: 255.255.4.4
vSZ-D Tunnel Uptime:      6d,19h,57m,27s
vSZ Tunnel IP: 10.254.32.1
vSZ-D-to-vSZ Tunnel Ping Test: ([10.254.32.6] --> [10.25.31.6])
*****
PING 10.254.32.1 (10.25.31.6) 56(84) bytes of data.
64 bytes from 10.25.31.6: icmp_seq=1 ttl=64 time=10.4 ms
64 bytes from 10.25.31.6: icmp_seq=2 ttl=64 time=0.577 ms
64 bytes from 10.25.31.6: icmp_seq=3 ttl=64 time=0.624 ms

--- 10.25.31.6 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2014ms
rtt min/avg/max/mdev = 0.577/3.871/10.414/4.626 ms

*****
-----
```

show strict-wfa-compliance-state

Displays the current state of Wi-Fi Alliance (WFA) compliance.

Syntax

`show strict-wfa-compliance-state`

Modes

Privileged EXEC mode

Debug configuration mode

Usage Guidelines

To enable or disable strict WFA compliance, use the **strict-wfa-compliance** command.

NOTE

We recommend that you contact Ruckus customer support before enabling or disabling the **strict-wfa-compliance** command.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example displays the WFA compliance state. Note that the command is entered in debug mode in this example.

```
device# debug
device(debug)# show strict-wfa-compliance-state
Strict WFA compliance state : Enabled
```

History

Release version	Command history
3.5.1	This command was introduced.

Show Commands

show system-capacity

show system-capacity

Displays the system capacity.

Syntax

show system-capacity

Modes

Privileged EXEC mode

Usage Guidelines

Examples

The following example displays the system capacity for the virtual SZ controller.

```
device# show system-capacity

System Capacity of Cluster:
Total Capacity: 10000 APs (2000 Switches)
Connected AP: 0 APs
Connected Switch: 0 Switches
Remaining AP: 10000 APs
Remaining Switch: 2000 Switches
```

show tlsv1-state

Displays the Transport Layer Security version 1 (TLSv1) support state.

Syntax

show tlsv1-state

Modes

Debug configuration mode

Usage Guidelines

The command is only available under debug mode.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows that TLSv1 is supported.

```
device# debug
device(debug)# show tlsv1-state

TLSv1.0 support : true
```

History

Release version	Command history
3.5.1	This command was introduced.

Show Commands

show ttg-client

show ttg-client

Displays the current Tunnel Terminating Gateway (TTG) client sessions.

Syntax

```
show ttg-client client-mac
```

Parameters

client-mac

Client MAC address.

Modes

Privileged EXEC mode

Usage Guidelines

Examples

The following example displays the TTG client sessions for MAC address A1:87:45:34:56:FE.

```
device# show ttg-client 48:5A:3F:76:11:3F

General Information
-----
STA MAC Address       : 48:5A:3F:76:11:3F
IP Address            : 10.1.220.6
User Name             : 1405803123321186@wlan.mnc803.mcc405.3gppnetwork.org
Auth Method           : Standard+802.1X
Encryption Method     : WPA2-AES
Connected Since       : 2021-03-31 06:23:13 GMT
Status                : AUTHORIZED
AP Zone               :
Access Point          :
Model Name            :
Host Name             : android-17c8e7a56ca740eb
-----
Channel               :
VLAN                  : 1
SNR (dB)              :
Packets from Client   : 18
Bytes from Client     : 2.5KB
Packets to Client     : 2
Bytes to Client       : 304
Dropped Packets to Client : 0
WLAN                  : 6.1331-SZ300-WLAN-TTG
```


show ue-nat-session

Displays the status of the datacore filter for NAT.

Syntax

```
show ue-nat-session
```

Modes

User EXEC mode

Privileged EXEC mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.

Examples

The following example displays the status of the NAT datacore filter.

```
device# show ue-nat-session  
  
NAT filter clear, done.
```

Show Commands

show upgrade

show upgrade

Displays the previous upgrade information for a vSZ-D controller.

Syntax

show upgrade

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.

Examples

The following example displays the previous upgrade information for a vSZ-D controller.

```
device# show upgrade
vSZ-D Previous Upgrade Info:
-----
Triggered by: WebGUI

vSZ-D MAC: 00:0c:39:68:94:a2

Old Version: 10.0.0.0.1009

New Version: 10.0.0.0.1108

Upgrade Start Time: 2020-12-16 02:34:40 AM UTC

Upgrade Stop Time: 2020-12-16 02:43:14 AM UTC

Upgrade Fail Reason: None

Upgrade Result: Success
-----
```

show upgrade-history

Displays system upgrade history.

Syntax

show upgrade-history

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all the controllers including the SmartZone Data Plane.

Examples

The following example displays the system upgrade history on a controller.

```
device# show upgrade-history
```

No.	Start time	SmartZone System Version	Control Plane version	Data Plane version	AP
Firmware version	File name	Elapsed			
1	2015-03-03 10:41:20 GMT	3.0.0.0.599->3.1.0.0.187	3.0.0.0.1624->3.1.0.0.3	3.0.0.0.157->3.1.0	
		3.0.0.0.438->3.1.0.	scge-install_3.1	22m 14s	
2	2015-03-03 09:37:50 GMT	3.0.0.0.599	3.0.0.0.1624	3.0.0.0.157	
		3.0.0.0.438	Fresh Install	15m 11s	

Show Commands
show upgrade-state

show upgrade-state

Displays the system upgrade state.

Syntax

show upgrade-state

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example shows that a system upgrade is not currently running on the controller.

```
device# show upgrade-state  
No running operation
```

show version

Displays the controller version.

Syntax

show version

Modes

User EXEC mode

Privileged EXEC mode

Usage Guidelines

This command is supported on all the controllers including the SmartZone Data Plane.

Examples

The following example shows version details for a SZ300.

```
device# show version

Model                : SZ300
Serial #             : 161737000069
SZ Version           : 5.2.1.0.251
Control Plane Software Version : 5.2.1.0.223
Data Plane Software Version   : 5.2.1.0.251
AP Firmware Version   : 5.2.0.0.1170, 5.2.0.0.1192, 5.2.0.0.1221, 5.2.0.0.1232, 5.2.0.0.1246,
                        5.2.0.0.1281, 5.2.0.0.1316, 5.2.0.0.1326, 5.2.0.0.1348, 5.2.0.0.1367,
                        5.2.0.0.1381, 5.2.0.0.1386, 5.2.0.0.1392, 5.2.0.0.1412, 5.2.1.0.341
```

The following example shows version details for a SZ100.

```
device# show version

Model                : SZ124
Serial #             : 501526006045
SZ Version           : 5.2.1.0.282
Control Plane Software Version : 5.2.1.0.252
Data Plane Software Version   : 5.2.1.0.73
AP Firmware Version   : 5.1.1.0.413, 5.1.2.0.368, 5.2.0.0.1103, 5.2.0.0.1129, 5.2.0.0.1160,
                        5.2.0.0.1192, 5.2.0.0.1221, 5.2.0.0.1232, 5.2.0.0.1316, 5.2.0.0.1326,
                        5.2.0.0.1348, 5.2.0.0.1367, 5.2.0.0.1378, 5.2.0.0.1381, 5.2.0.0.1386,
                        5.2.0.99.942, 5.2.0.99.961, 5.2.0.99.971, 5.2.0.99.985, 5.2.0.99.1002,
                        5.2.0.99.1007, 5.2.0.99.1018, 5.2.0.99.1028, 5.2.0.99.1041,
                        5.2.1.0.198,
                        5.2.1.0.206, 5.2.1.0.213, 5.2.1.0.220, 5.2.1.0.231, 5.2.1.0.242,
                        5.2.1.0.253, 5.2.1.0.267, 5.2.1.0.274, 5.2.1.0.294, 5.2.1.0.304,
                        5.2.1.0.334, 5.2.1.0.361, 5.2.1.0.390, 5.2.1.0.400
```

The following example shows version details for a vSZ-D.

```
device# show version

Model                : vSZ-D
vSZ-D Serial Number  : 972MTWA3W5H3XMHGWTXU5CN5FMJQ000C29135A53000C29135A5D
vSZ-D Version        : 5.2.1.0.20200401054522
```

Show Commands
show wired- client

show wired- client

Displays the wired client sessions associated with the current AP.

Syntax

show wired-client*wired-client-mac*

Parameters

wired-client-mac

Wired client MAC address.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example displays the sessions associated with the current AP for the wired client with the specified MAC address.

```
device# show wired-client
<wired-client-mac>      Wired Client MAC address

sz300-1# show wired-client D4:BE:D9:48:89:31
General Options
-----
MAC Address              : D4:BE:D9:48:89:31
Auth Status              : AUTHORIZED
User                     : guest3
VLAN                     : 1
IP Address               : 192.168.43.79
IPv6 Address             : fdff:a040::ce4a
AP MAC                   : C8:03:F5:2C:80:E0
LAN                       : 1
Connected Since         : 2021-03-30 09:02:48 GMT
Packets from Client     : 99
Bytes from Client       : 9.1KB
Packets to Client       : 68
Bytes to Client         : 11KB
```

History

Release version	Command history
3.5.1	This command was introduced.

show zone

Displays information about AP zone states.

Syntax

```
show zone[zone-name{ap[ap-mac-address]|client[client-mac-address]|wired-client[wired-client-mac-address]]
```

Parameters

zone-name

Zone name

ap*ap-mac-address*

Displays information for the specified AP zone or all AP zones.

client*client-mac-address*

Displays information for the specified client list of a specific AP zone.

wired-client*wired-client-mac-address*

Displays information for the specified wired client list of a specific AP zone.

Modes

Privileged EXEC mode

Usage Guidelines

The **show zone** command without any options displays information about all AP zones.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example displays the output for the **show zone** command without any options.

```
device# show zone
```

No.	Zone Name	Management Domain	Description	AP Firmware	# of
Alarms	# of APs	# of WLANs	# of Clients	AP IP Mode	
1	3.6_ZONE	Administration Domain		6.0.0.99.11	
0/0/0/0	0 (0/0/0/0/0)	7	0	Dual	85
2	Staging Zone	Administration Domain	Staging Zone		
0/1/0/0	1 (0/1/0/0/0)	0	0		
3	6.1315-Wired-ZONE	Administration Domain	6.1315-Wired-ZONE	6.0.0.99.12	
0/0/0/0	1 (1/0/0/0/0)	0	0	IPv4	59
4	6.1213-GP-AP-ZONE	Administration Domain	6.1213-GP-AP-ZONE	6.0.0.99.12	
0/0/0/0	0 (0/0/0/0/0)	1	0	IPv4	59
5	GA_ZONE	Administration Domain		6.0.0.0.158	
0/0/0/0	0 (0/0/0/0/0)	1	0	Dual	1

Show Commands

show zone

The following example displays the output for the **show zone** command for the GA Zone.

```
device# show zone GA_ZONE
ap          client          wired-client
```


Commands Si - Z

sms-server

Enters SMS configuration mode to enable SMS server configurations.

Syntax

sms-server

After the **enable** command is entered to enable the SMS server, the following configuration syntax is available:

{**account-sid***sid* | **auth-token***token* | **fromemail** | **server-name***server-name*}

Command Default

No SMS server configurations are created.

Parameters

server-name*server-name*

Sets a server name for the SMS server.

account-sid*sid*

Sets the account SID, which is a 34 character string that uniquely identifies this account. The SID must start with "AC" and only the following characters are allowed: 'a-z' , 'A-Z' , '0-9'.

auth-token*token*

Sets the authorization token identifier.

fromemail

Identifies the email address from which the SMS server sends alert messages.

Modes

Global configuration mode

Usage Guidelines

The **no enable** command in SMS server configuration mode disables the SMS server configuration.

Examples

The following example shows how to enter SMS server configuration mode, enable the configuration, and configure SMS parameters.

```
device# config
device(config)# sms-server
device(config-sms-server)# enable
device(config-sms-server)# server-name sname
device(config-sms-server)# account-sid AC12345678912345678912345678912345
device(config-sms-server)# auth-token smstoken
device(config-sms-server)# from username@company.com
```

The following example shows how to disable the SMS server.

```
device# config
device(config)# sms-server
device(config-sms-server)# no enable
```

smtp-server

Enables and configures the SMTP server.

Syntax

smtp-server

After the **enable** command is entered to enable the SMTP server, the following configuration syntax is available:

{**fromemail**|**host***host-name*|**password***password*|**personalname***display-name*|**port***port*|**test**|**tls**|**toemail**|**username***user-name*}

Command Default

No SMTP server configurations are updated.

Parameters

fromemail

Identifies the email address from which the SMS server sends alert messages.

host*host-name*

Sets the SMTP server IP address or domain name.

password*password*

Sets a password for the SMTP server.

personalname*display-name*

Sets a display name for the SMTP server.

port*port*

Sets the port number for the SMTP server.

test

Tests the SMTP server settings.

tls

Enables TLS encryption on the SMTP server.

toemail

Identifies the email address to which the SMS server sends alert messages.

username*user-name*

Sets a logon name for the SMTP server.

Modes

Global configuration mode

Usage Guidelines

The **no enable** command in SMTP Server configuration mode disables the SMTP server configuration.

Examples

The following example shows how to enter SMTP server configuration mode.

```
device# config
device(config)# smtp-server
device(config-smtp-server)# enable
device(config-smtp-server)# host 10.10.1.2
device(config-smtp-server)# tls
device(config-smtp-server)# from admin@commscope.com
device(config-smtp-server)# to user2@commscope.com
```

The following example shows how to disable the SMTP server.

```
device# config
device(config)# smtp-server
device(config-smtp-server)# no enable
Do you want to continue to disable (or input 'no' to cancel)? [yes/no] yes
Successful operation
```

snmp-notification

Enables SNMP notifications.

Syntax

snmp-notification

no snmp-notification

Command Default

SNMP notifications are not enabled.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables SNMP notifications.

Examples

The following example shows how to enable SNMP notifications.

```
device# config
device(config)# snmp-notification
```

The following example shows how to disable SNMP notifications.

```
device# config
device(config)# no snmp-notification
Do you want to continue to disable (or input 'no' to cancel)? [yes/no]
```

snmp-v2-community

Configures the SNMPV2 community.

Syntax

snmp-v2-community*community*

no snmp-v2-community*community*

After the **snmp-v2-community** command is entered to enable the SNMP v2 Community configuration mode, the following configuration syntax is available:

[**notification** | **read** | **write**]

After the **notification** command is entered in SNMP v2 Community configuration mode, the following additional configuration syntax is available:

[**notification-target***ip-address[port]* | **notification-type**(**inform** | **trap**)]

Command Default

No SNMP communities are configured.

Parameters

community

Community name.

notification

Enables notification privilege. This keyword is supported on the SmartZone 100 and vSZ-E controllers only.

notification-target

Enables notification target by setting the IP address and port.

ip-address

Specifies the IP address.

port

Specifies the port number. The range is from 1 to 65535.

notification-type

Specifies the notification type. This keyword is supported on the SmartZone 100 and vSZ-E controllers only.

inform

Specifies the notification type as informational.

trap

Specifies the notification type as an SNMP trap.

read

Enables SNMP read privileges.

write

Enables SNMP write privileges.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command deletes the SNMP community when entered in Configuration mode. In SNMP v2 Community Configuration mode, the **no** form is available for the **notification**, **notification-target**, **read**, and **write** keywords and applicable variables.

NOTE

The **notification** and **notification-type** keywords are supported on the SmartZone 100 and vSZ-E controllers only.

Examples

The following example shows how to create an SNMP community named comm3 and configure related parameters. The **notification** syntax in this example is supported on the SmartZone 100 and vSZ-E controllers only.

```
device# config
device(config)# snmp-v2-community comm3
device(config-snmp-v2-community)# read
device(config-snmp-v2-community)# notification
device(config-snmp-v2-community)# notification-target 10.10.1.2 port
device(config-snmp-v2-community)# notification-type inform
```

The following example shows how to disable the read privileges from the SNMP community named comm3.

```
device# config
device(config)# snmp-v2-community comm3
device(config-snmp-v2-community)# no read
```

The following example shows how to delete an SNMP community named comm3.

```
device# config
device(config)# no snmp-v2-community comm3
```

snmp-v3-user

Configures an SNMPv3 user.

Syntax

snmp-v3-user*user*

no snmp-v3-user*user*

After the **snmp-v3-user** command is entered to enable the SNMP v3 User configuration mode, the following configuration syntax is available:

[**auth**{**md5***auth-pwd* | **none** | **sha***auth-pwd*} | **notification** | **read** | **write**]

After the **auth md5** or the **auth sha** commands are entered in SNMP v3 User configuration mode, the following additional configuration syntax is available:

[**privacy**{**aes***privacy-phrase* | **des***privacy-phrase* | **none**}]

After the **notification** command is entered in SNMP v3 User configuration mode, the following additional configuration syntax is available:
[**notification-target***ip-address*[*port*] | **notification-type**{**inform** | **trap**}]

Command Default

No SNMPv3 users are configured.

Parameters

user

The SNMPv3 user name.

auth

Sets SNMPv3 user authentication.

md5*auth-pwd*

Sets the authentication method to MD5 and specifies an authentication password phrase.

none

Sets no authentication method.

sha*auth-pwd*

Sets the authentication method to SHA and specifies an authentication password phrase.

privacy

Sets SNMPv3 user privacy configuration.

aes*privacy-phrase*

Sets SNMPv3 user privacy to use AES and specifies a privacy phrase.

des*privacy-phrase*

Sets SNMPv3 user privacy to use DES and specifies a privacy phrase.

none

Sets no SNMPv3 user privacy.

notification

Enables notification privilege. This keyword is supported on the SmartZone 100 and vSZ-E controllers only.

notification-target

Enables notification target by setting the IP address and port.

ip-address

Specifies the IP address.

port

Specifies the port number. The range is from 1 to 65535.

notification-type

Specifies the notification type. This keyword is supported on the SmartZone 100 and vSZ-E controllers only.

inform

Specifies the notification type as informational.

trap

Specifies the notification type as an SNMP trap.

read

Enables SNMP read privileges.

write

Enables SNMP write privileges.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command deletes the SNMP v3 user when entered in Configuration mode. In SNMP v3 User Configuration mode, the **no** form is available for the **notification**, **notification-target**, **read**, and **write** keywords and applicable variables.

NOTE

The **notification** and **notification-type** keywords are supported on the SmartZone 100 and vSZ-E controllers only.

Examples

The following example configures an SNMPv3 user named user3 and enters SNMPv3 configuration mode. Read, authentication, privacy, and notification parameters are configured for user3. The notification syntax in this example is supported on the SmartZone 100 and vSZ-E controllers only.

```
device# config
device(config)# snmp-v3-user user3
device(config-snmp-v3-user)# read
device(config-snmp-v3-user)# auth md5 mylongerpwd
device(config-snmp-v3-user)# privacy aes mypassphrase
device(config-snmp-v3-user)# notification-type inform
```

The following example shows how to disable the read privileges for the SNMPv3 user named user3.

```
device# config
device(config)# snmp-v3-user user3
device(config-snmp-v3-user)# no read
```

Commands Si - Z

snmp-v3-user

The following example deletes an SNMPv3 user named user3.

```
device# config
device(config)# no snmp-v3-user user3
```

soft-gre

Creates or updates the soft GRE tunnel profile configuration.

Syntax

soft-gre*name*

no soft-gre[*name*]

After the **soft-gre** command is entered to enable the Soft GRE configuration mode, the following configuration syntax is available:

[device-ip-mode{*ipv4* | *ipv6*} | **force-disassociate-client** | **gateway***ip-address*{**primary** | **secondary**} | **gateway-mtu**{**auto** | *manual-mtu-size*} | **icmp-period***seconds* | **icmp-retry***retries* | **name**]

If the **device-ip-mode** keyword is entered with the **ipv6** keyword in Soft GRE configuration mode, the following configuration syntax is available instead of the **gateway** keyword:

[gateway6*ipv6-address*{**primary** | **secondary**}]

Command Default

No soft GRE tunnel profiles are configured.

Parameters

name

Soft GRE profile name.

device-ip-mode

Sets the gateway IP mode version.

ipv4

Sets the gateway IP mode to IPv4.

ipv6

Sets the gateway IP mode to IPv6.

force-disassociate-client

Enables the Force Disassociate Client function.

gateway*ip-address*

Sets the IPv4 gateway address.

primary

Sets the primary gateway address.

secondary

Sets the secondary gateway address.

gateway-mtu

Sets the MTU size for the gateway.

auto

Sets the MTU size automatically.

Commands Si - Z

soft-gre

mtu-size

Manually specifies the MTU size. The range for IPv4 is from 850 to 1500, and the range for IPv6 is from 1384 to 1500.

icmp-period*seconds*

Sets the ICMP keepalive period, in seconds. The range is from 1 to 180.

icmp-retry*retries*

Sets the number of ICMP keepalive retries. The range is from 2 to 20.

name*name*

Specifies the Soft GRE profile name.

gateway6*ipv6-address*

Sets the IPv6 gateway address.

primary

Sets the primary gateway address.

secondary

Sets the secondary gateway address.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command in configuration mode deletes the soft GRE tunnel profile.

Soft GRE creates a tunnel profile.

Examples

The following example creates the soft GRE tunnel profile named GRE1.

```
device# configure terminal
device(config)# soft-gre GRE1
device(config-soft-gre)# device-ip-mode ipv4
device(config-soft-gre)# gateway 10.10.2.4 primary
```

ssh-rekey-limit

This command is used to trigger the time or data limit for a session.

Syntax

ssh-rekey-limit

Modes

Debug configuration mode

Examples

```
device# debug
device(debug)# ssh-rekey-limit 100k,1d
Reloading sshd configuration (via systemctl): [ OK ]
Successful Operation
```

History

Release version	Command history
5.2.1	This command was introduced.

stats-upload

Updates the FTP server for uploading statistical data. If you add an FTP server to the controller, the controller will export statistics files to that FTP server, either on demand or based on a schedule.

Syntax

stats-upload

After the **enable** command is entered to update the FTP server, the following configuration syntax is available:
[ftp-servervalue | stats-intervalhourly | test]

Command Default

The command is disabled by default.

Parameters

ftp-server{value}

Specifies values for the FTP server.

stats-interval

Sets the interval at which the statistics are uploaded.

hourly

Sets the statistical data upload to occur hourly.

test

Tests the FTP server settings.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone 300 and vSZ-H controllers only.

The **no enable** command in Stats Upload configuration mode disables the statistical data upload to the FTP server.

Examples

The following example updates the ftp server for uploading statistical data with the statistical upload interval.

```
device# config
device(config)# stats-upload
device(config-stats-upload)# enable
device(config-stats-upload)# stats-interval weekly
```

The following example disables the statistical data uploads to the FTP server.

```
device# config
device(config)# stats-upload
device(config-stats-upload)# no enable
Do you want to continue to disable (or input 'no' to cancel)? [yes/no] yes
Successful operation
```

strict-wfa-compliance

Enables strict Wi-Fi Alliance (WFA) compliance.

Syntax

strict-wfa-compliance

no strict-wfa-compliance

Modes

Debug configuration mode

Usage Guidelines

Use this command to ensure that all your Access Points (APs) are conforming to the strict WFA standards.

Use the **no** form of this command if you have some APs that may not conform completely to the WFA standards.

Examples

The following example enables strict WFA compliance.

```
device# debug
device(debug)# strict-wfa-compliance

Successful operation
```

The following example disables WFA compliance.

```
device# debug
device(debug)# no strict-wfa-compliance
```


subpackages

Creates or updates the subscription package configuration.

Syntax

subpackages*package-name*

After the **enable** command is entered to enable the Subscription Package configuration mode, the following configuration syntax is available:

[**expiration-interval**{**day** | **hour** | **month** | **never** | **week** | **year**} | **name***package-name*]

Command Default

No subscription packages are created.

Parameters

package-name

Name of the subscription package.

expiration-interval

Sets the interval after which the subscription package expires.

day

Sets the subscription package to expire in one day.

hour

Sets the subscription package to expire in one hour.

month

Sets the subscription package to expire in one month.

never

Sets the subscription package to never expire.

week

Sets the subscription package to expire in one week.

year

Sets the subscription package to expire in one year.

name*package-name*

Specifies the name of the subscription package.

Modes

Global configuration mode

Usage Guidelines

Before configuring this command, ensure the subscription interval is appropriate.

Examples

The following example creates a subscription package named sub1 and sets the package to expire after one week.

```
device# config
device(config)# subpackages sub1
device(config-subpackages)# expiration-interval week
```

support-admin

Configures support administrator configuration.

Syntax

support-admin

After the **enable** command is entered to enable support administration configuration, the following configuration syntax is available:
[change-password]

Command Default

Support administrator configuration is not enabled.

Parameters

change-password

Prompts the user to enter and validate a new password.

Modes

Global configuration mode

Usage Guidelines

The **no enable** command in Support Admin configuration mode disables the support administrator configuration.

Examples

The following example enables support administrator configuration and changes the password.

```
device# config
device(config)# support-admin
device(config-support-admin)# changepassword
New Password: *****
Retype: *****
```

syslog

Configures the device to use the Syslog server.

Syntax

syslog

After the **syslog** command is entered to enable the Syslog configuration mode, the following configuration syntax is available:

[dhcp{enable | disable} | nat{enable | disable} | show | syslog-serverip-addressport]

Command Default

The device does not use the Syslog server.

Parameters

dhcp

Sets the DHCP messaging options for the Syslog server.

enable

Enables forwarding of DHCP messages to the Syslog server.

disable

Disables forwarding of DHCP messages to the Syslog server.

nat

Sets the NAT messaging options for the Syslog server.

enable

Enables forwarding of NAT messages to the Syslog server.

disable

Disables forwarding of NAT messages to the Syslog server.

show

Displays Syslog server information.

syslog-serverip-addressport

Configures the Syslog server IP address and port number.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.

Examples

The following example configures the device to use the Syslog server, enables DHCP, and sets the Syslog server IP address and port number. The show command displays information about the configuration of the Syslog server.

```
device# config
device(config)# syslog
device(config-syslog)# dhcp enable
device(config-syslog)# syslog-server 10.10.2.2 4
device(config-syslog)# show
syslog server ip: 10.10.2.2
syslog server port: 4
syslog server dhcps: enable
syslog server nat: disable
```

syslog-server

Updates the syslog server configurations.

Syntax

syslog-server

Command Default

The syslog server configurations are not updated.

Modes

Global configuration mode

Usage Guidelines

The following table lists the relate **syslog-server** configuration commands.

TABLE 43 Commands related to the syslog-server command

Syntax and Type	Parameters (if any)	Description
ruckus(config-syslog-server)# appfacility Type: Privileged	[Local2 Local7 Local0 Local6 Local4 Local5 Local3 Local1]	Remote syslog server to send the application log files.
ruckus(config-syslog-server)# auditfacility Type: Privileged	[Local6 Local4 Local2 Local3 Local0 Local5 Local7 Local1]	Remote syslog server to send the audit log files.
ruckus(config-syslog-server)# eventfacility Type: Privileged	[Local7 Local6 Local3 Local4 Local0 Local2 Local1 Local5]	Remote syslog server to send the event log files.
ruckus(config-syslog-server)# filter Type: Privileged	[severity exclude-client all] severity: All events above a severity exclude-client: All events except client associate/disassociate events all: All events	Sets the settings for filtering events.
ruckus(config-syslog-server)# filter-severity Type: Privileged	[Critical Warning Major Info Debug Minor]	Sets the event severity filter settings.
ruckus(config-syslog-server)# host Type: Privileged	ip	Sets the syslog server IP address.
ruckus(config-syslog-server)# no Type: Privileged	enable secondary-host	Disables the syslog server and secondary settings.
ruckus(config-syslog-server)# port Type: Privileged	port	Sets the syslog server port.
ruckus(config-syslog-server)# priority Type: Privileged	[Minor Critical Debug Info Warning Major][Debug Warning Info Error]	Sets the priority for events. The event severity and syslog-severity is based on priority.

TABLE 43 Commands related to the syslog-server command (continued)

Syntax and Type	Parameters (if any)	Description
ruckus(config-syslog-server)# protocol Type: Privileged	tcp udp	Sets the primary Syslog server protocol.
ruckus(config-syslog-server)# secondary-protocol Type: Privileged	tcp udp	Sets the secondary Syslog server protocol.
ruckus(config-syslog-server)# redundancy-mode Type: Privileged	[Primary/Backup Active/Active]	Sets forwarding syslog server mode.
ruckus(config-syslog-server)# secondary-host Type: Privileged	<i>ip</i> : IP address	Sets the secondary syslog server IP.
ruckus(config-syslog-server)# secondary-port Type: Privileged	<i>port</i> : Port	Sets the secondary syslog server port.

Examples

The following example enables syslog server configuration.

```
device# config
device(config)# syslog-server
```

tlsv1

Enables Transport Layer Security version 1 (TLSv1) support.

Syntax

tlsv1

no tlsv1

Command Default

TLSv1 is not supported.

Modes

Debug configuration mode

Usage Guidelines

Use the **no** form of this command to disable TLSv1 support.

Examples

The following example enables TLSv1 support.

```
device# debug
device(debug)# tlsv1

Wait for tomcat down...(0/120)
Wait for tomcat down...(2/120)
no tWait for tomcat down...(4/120)
lsvWait for tomcat down...(6/120)
lWait for tomcat down...(8/120)
Stop service tomcat done!
Start service tomcat done!
      total      used      free      shared  buff/cache  available
Mem:   198054460  53146476  134929828  194428   9978156  143483400
Swap:      0         0         0

Wait for communicator down...(0/120)
Stop service communicator done!
tart service communicator done!
      total      used      free      shared  buff/cache  available
Mem:   198054460  52804616  135280780  194356   9969064  143825496
Swap:      0         0         0
```

Please make sure to enable/disable tlsv1 in all cluster nodes.
Successful operation

History

Release version	Command history
3.5.1	This command was introduced.

tlsversion

Set TLS version for LBS profile.

Syntax

```
tlsversion tlsv1|tlsv1.1|tlsv1.2
```

Parameters

tlsversion

Displays the tls version for LBS profile.

tlsv1

Sets the tls version number for LBS profile.

tlsv1.1

Sets the tls version number for LBS profile.

tlsv1.2

Sets the tls version number for LBS profile.

Modes

Global configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example sets the tls version for LBS profile.

```
device# config
device(config)# lbs-service
device(config-lbs-service)#
do                Do command
end              End the current configuration session and return to privileged EXEC mode
exit            Exit from the EXEC
help           Display this help message
host           Set Server Address
password       Set Password
port           Set Port
tlsversion     Set TLS version
venue          Set LBS venue

device(config-lbs-service)# tlsversion
<tlsVersion>    TLS Version
device(config-lbs-service)# tlsVersion tlsv1.0
This field should be a valid TLS version (tlsv1, tlsv1.1, tlsv1.2).
device(config-lbs-service)# tlsversion tlsv1
device(config-lbs-service)# tlsversion tlsv1.1
device(config-lbs-service)# tlsVersion tlsv1.2
Set TLS version for LBS profile to [tlsv1]
```

tracert

Displays the route that packets take to the network host.

Syntax

```
tracert[-4][6][-d][-F][-ffirst_ttl][-gateway,...][-I][-T][-idevice][-mmax_ttl][-Nsqueries][-pport][-ttos][-lflow_label][-wwaittime][-qnqueries][-r][-ssrc_addr][-zsendwait]host-addr[packetlen]
```

Command Default

Tracert is disabled.

Parameters

- 4** Displays IPv4 hops.
- 6** Displays IPv6 hops.
- d** Enables socket-level debugging.
- F** Does not fragment the packets.
- ffirst ttl** Starts from the first_ttl hop (instead from 1).
- gateway** Routes packets through the specified gateway. (maximum 8 for IPv4 and 127 for IPv6).
- I** Uses ICMP ECHO for tracerouting.
- T** Uses TCP SYN for tracerouting. Default port is 80.
- idevice** Specifies a network interface with which to operate.
- mmax ttl** Sets the max number of hops (max TTL to be reached). Default is 30.
- Nsqueries** Sets the number of probes to be tried simultaneously (default is 16).
- pport** Sets the destination port to use. It is either initial udp port value for "default" method (incremented by each probe, default is 33434), or initial seq for "icmp" (incremented as well, default from 1), or some constant destination port for other methods (with default of 80 for "tcp", 53 for "udp", etc.) .
- ttos** Sets the TOS (IPv4 type of service) or TC (IPv6 traffic class) value for outgoing packets.

Commands Si - Z

traceroute

-lflow_label

Uses specified flow_label for IPv6 packets.

-wwaittime

Sets the number of seconds to wait for response to a probe (default is 5.0). Non-integer (float point) values allowed too.

-qnqueries

Sets the number of probes per each hop. Default is 3.

-r

Bypasses the normal routing and sends the probes directly to a host on an attached network.

-ssrc_address

Uses source src_addr for outgoing packets.

-zsendwait

Minimal time interval between probes (default 0). If the value is more than 10, then it specifies a number in milliseconds, else it is a number of seconds (float point values allowed too).

host-address

The IPv4 host address to which tracerouting is applied.

packetlen

Sets the packet length.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **traceroute** command to help troubleshoot network access or network performance issues.

This command is supported on all the controllers including the SmartZone Data Plane.

Examples

The following example uses IPv4 addresses to trace the route from the device to the host at 10.1.31.105

```
device# traceroute -4 10.1.31.105
traceroute to 10.1.31.105 (10.1.31.105), 30 hops max, 60 byte packets
 1 10.174.84.1 (10.174.84.1)  2.712 ms  2.796 ms  2.893 ms
 2 77.77.77.2 (77.77.77.2)  0.292 ms  0.292 ms  0.408 ms
 3 10.174.86.1 (10.174.86.1)  0.680 ms  0.859 ms  1.053 ms
 4 10.174.127.17 (10.174.127.17)  4.397 ms  4.823 ms  5.191 ms
 5 10.7.136.30 (10.7.136.30)  0.922 ms  0.862 ms  0.907 ms
 6 10.7.136.225 (10.7.136.225)  1.335 ms  0.990 ms  0.971 ms
 7 172.16.2.50 (172.16.2.50)  3.127 ms  3.310 ms  3.228 ms
 8 172.16.4.242 (172.16.4.242)  222.211 ms  218.514 ms  222.099 ms
 9 172.16.4.241 (172.16.4.241)  216.834 ms  220.216 ms  220.244 ms
10 172.23.128.13 (172.23.128.13)  219.387 ms  223.637 ms  219.072 ms
11 10.7.2.243 (10.7.2.243)  223.541 ms  223.656 ms  219.682 ms
12 * * *
13 * * *
.
.
.
28 * * *
29 * * *
30 * * *
```

The following example sets the maximum number of hops to 15 tracing a route to the host at 10.1.31.105.

```
device> traceroute -m 15 10.1.31.105
traceroute to 10.1.31.105 (10.1.31.105), 15 hops max, 60 byte packets
 1 10.174.84.1 (10.174.84.1)  2.876 ms  2.861 ms  2.893 ms
 2 77.77.77.2 (77.77.77.2)  0.370 ms  0.370 ms  0.334 ms
 3 10.174.86.1 (10.174.86.1)  0.604 ms  0.722 ms  0.842 ms
 4 10.174.127.17 (10.174.127.17)  4.321 ms  4.317 ms  4.489 ms
 5 10.7.136.30 (10.7.136.30)  0.839 ms  0.831 ms  0.794 ms
 6 10.7.136.225 (10.7.136.225)  1.132 ms  1.086 ms  1.054 ms
 7 172.16.2.50 (172.16.2.50)  2.800 ms  2.849 ms  2.890 ms
 8 172.16.4.242 (172.16.4.242)  220.259 ms  219.940 ms  219.844 ms
 9 172.16.4.241 (172.16.4.241)  216.658 ms  217.896 ms  216.566 ms
10 172.23.128.13 (172.23.128.13)  218.914 ms  219.710 ms  219.962 ms
11 10.7.2.243 (10.7.2.243)  219.888 ms  219.760 ms  219.764 ms
12 * * *
13 * * *
14 * * *
15 * * *
```

traceroute6

Displays the route that packets take to the network IPv6 host.

Syntax

```
traceroute6[-4][6][-d][-F][-ffirst_ttl][-gateway,...][-I][-T][-idevice][-mmax_ttl][-Nsqueries][-pport][-ttos][-lflow_label][-wwaittime][-qnqueries]
[-r][-ssrc_addr][-zsendwait]host-addr[packetlen]
```

Command Default

Traceroute IPv6 is disabled.

Parameters

- 4** Displays IPv4 hops.
- 6** Displays IPv6 hops.
- d** Enables socket-level debugging.
- F** Does not fragment the packets.
- ffirst ttl** Starts from the first_ttl hop (instead from 1).
- gateway** Routes packets through the specified gateway. (maximum 8 for IPv4 and 127 for IPv6).
- I** Uses ICMP ECHO for tracerouting.
- T** Uses TCP SYN for tracerouting. Default port is 80.
- idevice** Specifies a network interface with which to operate.
- mmax ttl** Sets the max number of hops (max TTL to be reached). Default is 30.
- Nsqueries** Sets the number of probes to be tried simultaneously (default is 16).
- pport** Sets the destination port to use. It is either initial udp port value for "default" method (incremented by each probe, default is 33434), or initial seq for "icmp" (incremented as well, default from 1), or some constant destination port for other methods (with default of 80 for "tcp", 53 for "udp", etc.) .
- ttos** Sets the TOS (IPv4 type of service) or TC (IPv6 traffic class) value for outgoing packets.

- lflow_label**
Uses specified flow_label for IPv6 packets.
- wwaittime**
Sets the number of seconds to wait for response to a probe (default is 5.0). Non-integer (float point) values allowed too.
- qnqueries**
Sets the number of probes per each hop. Default is 3.
- r**
Bypasses the normal routing and sends the probes directly to a host on an attached network.
- ssrc_address**
Uses source src_addr for outgoing packets.
- zsendwait**
Minimal time interval between probes (default 0). If the value is more than 10, then it specifies a number in milliseconds, else it is a number of seconds (float point values allowed too).
- host-address**
The IPv6 host address to which tracerouting is applied.
- packetlen**
Sets the packet length.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **tracert6** command to help troubleshoot network access or network performance issues.

This command is supported on all the controllers including the SmartZone Data Plane.

Examples

The following example uses IPv6 addresses to trace the route from the device to the IPv6 host at 2001:DB8::200C:417A.

```
device# tracert6 -6 2001:DB8::200C:417A
tracert6 to 2001:DB8::200C:417A (2001:db8::200c:417a), 30 hops max, 80 byte packets
 1  2070::1 (2070::1)  8.239 ms !N  8.286 ms !N  8.375 ms !N
```

ttg-pdg-profile

Creates or updates the Tunnel Terminating Gateway (TTG) and Packet Data Gateway (PDG) profile configurations.

Syntax

ttg-pdg-profile*profile-name*

no ttg-pdg-profile*profile-name*

After the **ttg-pdg-profile** command is entered to enter ttg pdg profile configuration mode, the following configuration syntax is available:

{acct-retry*retry-times***|acct-retry-timeout***seconds***|apn-format-ggsn****[dns|string]****|apn-oi|default|dhcp-option82|dhcp-relay|dhcp-server1** *ip-address* **|dhcp-server2** *ip-address* **|name***profile-name***|pdgue-idle-timeout***seconds* **|realm** *realm***}**

{apn**[ni|nioi]***apn-name***{route-type****{gtpv1|gtpv2|pdg}}****}**

Command Default

TTG and PDG profiles are not created.

Parameters

profile-name

TTG+PDG profile name.

acct-retry*retry-times*

Specifies the interval, in minutes, at which the controller will recheck the primary TTG+PDG RADIUS profile, if it is available. The default is 5 minutes with a range of 1 to 10.

acct-retry-timeout*seconds*

Sets the timeout period, in seconds, after which an expected response message is considered to have failed.

apn-format-ggsn

Sets the APN format to GGSN.

dns

Uses DNS as the APN format.

string

Uses a string as the APN format.

apn-oi

Enables APN-OI for DNS resolution.

default

Creates or updates default APN configuration.

no-match-realm*apn-name*

Uses the specified *apn-name* as the default when no matching is found. Existing APNs are displayed as a choice.

no-realm*apn-name*

Uses the specified *apn-name* as the default when no realm is specified. Existing APNs are displayed as a choice.

dhcp-relay

Enables DHCP relay.

dhcp-option82

Enables DHCP option 82.

dhcp-server1 *ip-address*

Sets DHCP server 1.

dhcp-server2 *ip-address*

Sets DHCP server 2.

name*profile-name*

Sets the default TTG PDG profile name.

pdgue-idle-timeout

Sets the PDG UE session idle timeout, in seconds.

realm*realm*

Creates or updates the default APN for realm.

apn

Creates or updates the APN configuration to allow for overrides of the Network Identifier (NI) or Operator Identifier (OI).

ni*apn-name*

Uses the specified *apn-name* to override the supplied NI.

noi*apn-name*

Uses the specified *apn-name* to override the supplied OI.

route-type

Specifies a route type.

gtpv1

Specifies the GTPv1 route type.

gtpv2

Specifies the GTPv2 route type.

pdg

Specifies the PDG route type.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to delete a TTG+PDG profile.

This command is supported on the SmartZone 300 only.

Examples

The following example creates a TTG+PDG profile named newprofile123 and configures some other parameters.

```
device# config
device(config)# ttg-pdg-profile newprofile123
NODE-63(config-ttg-pdg-profile)# acct-retry 6
NODE-63(config-ttg-pdg-profile)# acct-retry-timeout 20
device(config-ttg-pdg-profile)# pdgue-idle-timeout 45
device(config-ttg-pdg-profile)# apn ni ruckus-new
device(config-ttg-pdg-profile-apn)# route-type pdg
```

upload ap-certificate-status

Uploads the AP certificate to the controller.

Syntax

```
upload ap-certificate-status ftp-url
```

Command Default

No AP certificates are loaded on the controller.

Parameters

ftp-url

Uploads the AP certificate from the specified FTP path. FTP URL format is ftp://<username>:<password>@<ip-address>[filepath]

Modes

Privileged EXEC mode

Examples

The following example uploads an AP certificate from the specified FTP path

```
device# upload ap-certificate-status ftp://username:pwd123@172.19.7.100
```

Commands Si - Z

use sz

use sz

Changes the debug tool-set category to SZ.

Syntax

use sz

Command Default

Debug tool-set category is changed to SZ.

Modes

Debug configuration mode

Usage Guidelines

This command is supported on all SmartZone platforms.

Examples

```
device# debug

device(debug)# debug-tools
[Change to system]
Welcome to Debug CLI Framework!
(debug tool-set) system $ show categories
ap      dp      system  sz
(debug tool-set) system $ use sz
[Change to sz]
(debug tool-set) sz $ ?
Debug Tools (sz):
Command      Help
=====
ccm-cli      List CCM Config folder and inspect GPB content
clear-maintenance-mode clear maintenance mode
dump-upload  dump file uploader via FTP
manage-alias-ssh-port Manage alias SSH port
network-dia  Run Network Diagnostic Tool
show-counter-devicemanager show DeviceManager counter
show-counter-subscriberportal show SubscriberPortal counter
show-es-cat-aliases show ES cat aliases info
show-es-cat-health show ES cat health info
show-es-cat-indices show ES cat indices info
show-es-cat-master show ES cat master info
show-es-cat-nodes show ES cat nodes info
show-es-cat-shards show ES cat shards info
show-es-cluster-settings show ES cluster settings
show-es-folder-info show ES folder info
skip-setup-capability-check skip vsz setup capability check
start-all-services Start all services
stop-all-services Stop all services
test-cp-storage Run test script for CP storage

Debug framework commands:
=====
exit help show use
```

user-agent-blacklist

Creates and updates the user agent blacklisted configuration.

Syntax

user-agent-blacklist*name*

no user-agent-blacklist*name*

After the **user-agent-blacklist** command is entered with an associated user name to enter user agent blacklist configuration mode, the following configuration syntax is available:

{**error***error-code* | **error-message***msg* | **name***agent-name* | **pattern***agent-pattern*}

Command Default

No user agent is blacklisted.

Parameters

name

Name of the blacklist to be configured.

error*error-code*

Sets the error code to be displayed. The range is from 400 to 599.

error-message*msg*

Sets the error message to be displayed.

name*agent-name*

Specifies a user agent name to be blacklisted.

pattern*agent-pattern*

Sets the pattern to be used.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of the command to delete the specified user agent blacklist.

Examples

The following example creates a user agent blacklist named `blst1` and specifies the name of the agent to be blacklisted and the error code to be displayed.

```
device# config
device(config)# user-agent-blacklist agent1
device(config-user-agent-blacklist)# name agent1
device(config-user-agent-blacklist)# error 450
```

user-group

Creates and updates user group configuration.

Syntax

user-group*name*

no user-group*name*

After the **user-group** command is entered to enter user group configuration mode, the following configuration syntax is available:
{**domain***domain-name* | **name***name* | **permission***permission-type* | **resource***resource*[**full-access** | **modify** | **read**] | **user***user-name*}

Command Default

No user groups are configured.

Parameters

name

Specifies the name of the user group.

domain

Specifies the domain for the user group. This command is supported on the SmartZone 300 controller only.

name*name*

Specifies the name of the user group.

permission*permission-type*

Specifies the permission type for the user group. Some permission types are preset such as "AP Admin," "Guest Pass Admin," "Network Admin," and "Super Admin." These options must be entered as shown including the parentheses.

resource*resource*

Specifies the resource type for the user group. This command is supported on the SmartZone 300 controller only.

full-access

Allows the resource full access to the device.

modify

Allows the resource to make changes to the device.

read

Allows the resource read access only to the device.

user*user-type*

Specifies the user. Some user types are preset such as ap-admin, ap_guest, guest, mvno, and super. These options must be entered as shown. Additional syntax options are available after entering the user type of mvno. See the syntax section for more details.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the specified user group.

Examples

The following example configures user group group1 and gives the user group permission to be an AP administrator

```
device# config
device(config)# user-group group1
device(config-user-group)# description user group from marketing
device(config-user-group)# permission "AP Admin"
```

user-role

Creates and updates the user role configuration.

Syntax

user-role*role-name*

no user-role[*role-name*]

After the **user-role** command is entered to enter user role configuration mode, the following configuration syntax is available:
{**firewall-profile***firewall-name* | **max-devices**{*number* | **unlimited**} | **user-traffic-profile***traffic-profile-name*}

Command Default

No user roles are defined.

Parameters

role-name

Specifies the user role name.

firewall-profile*firewall-name*

Specifies the firewall profile name to be used.

max-devices*number*

Specifies the maximum number of devices.

number

Specifies the maximum number of devices. Number from 1 to 10.

unlimited

Specifies an unlimited number of devices.

user-traffic-profile*traffic-profile-name*

Specifies the user traffic profile name to be used. See the Usage Guidelines section for details about

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command deletes user roles. If no *role-name* is specified, all user roles will be deleted.

If no *firewall-profile* is specified, all fire wall profile will be deleted.

The **user-traffic-profile** command can be used to specify the user traffic profile to be used. To configure the user traffic profile parameters, use the **user-traffic-profile** command in configuration mode.

Examples

The following example creates a user role, user1, adds a firewall and traffic profile and sets the maximum number fo devices to 3.

```
device# config
device(config)# user-role user1
device(config-user-role)# firewall-profile 5.2_Firewall
device(config-user-role)# max-devices 3
device(config-user-role)# user-traffic-profile "System Default"
```

The following example deletes all the configured user roles.

```
device# config
device(config)# no user-role
Do you want to continue to delete (or input 'no' to cancel)? [yes/no] yes
```

History

Release version	Command history
5.2	(config-user-role)# firewall-profile and(config-user-role)# no firewall-profile commands were introduced.

user-traffic-profile

Creates and updates the user traffic profile configuration.

Syntax

user-traffic-profile*profile-name*

no user-traffic-profile*profile-name*

After the **user-traffic-profile** command is entered to enter user traffic profile configuration mode, the following configuration syntax is available:

{acl | default-action{allow | block} | downlinkrate-limiting | nameprofile-name | uplinkrate-limiting

After the **acl** keyword is entered in user traffic profile configuration mode, the following configuration syntax is available:

{action{allow | block} | {destination-ip | source-ip}{hostip-address | networknetwork-addresssubnet-mask} | {destination-port | source-port}port-number | directionupstream | protocolprotocol-number |

Command Default

No user traffic profiles are created.

Parameters

profile-name

Specifies the user traffic profile name.

acl

Specifies the network access control list (ACL).

default-action

Sets a default action for traffic.

allow

Allows configured traffic.

block

Blocks configured traffic.

downlinkrate-limiting

Specifies the downlink rate limits in mbps. Range is from 0.1 to 200.

name*profile-name*

Specifies a name for the user traffic profile.

uplinkrate-limiting

Specifies the uplink rate limits in mbps. Range is from 0.1 to 200.

action

Sets an action for traffic.

allow

Allows configured traffic.

block

Blocks configured traffic.

destination-ip

Specifies the host IP or network address of the destination.

hostip-address

Specifies the host IP address.

networknetwork-addresssubnet-mask

Specifies the network address and subnet mask.

destination-port

Specifies the destination port number or range of ports.

port-number

Specifies the port number.

rangeport-numberport-number

Specifies the destination port range numbers.

directionupstream

Specifies the traffic direction as upstream.

protocolprotocol

Specifies the protocol number.

source-ip

Specifies the source IP address or network address.

source-port

Specifies the source port number or range of ports.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command deletes the specified user traffic profile.

Examples

The following example configures the downlink and uplink rate-limiting speeds for user traffic profile tprof1.

```
device# config
device(config)# user-traffic-profile tprof1
device(config-user-traffic-profile)# downlink 50
device(config-user-traffic-profile)# uplink 30
```

The following example configures an access control list for the tprof2 user traffic profile that matches traffic from source ports 2 through 4.

```
device# config
device(config)# user-traffic-profile tprof2
device(config-user-traffic-profile)# acl
device(config-user-traffic-profile-acl)# source-port range 2 4
```

usgv6

Runs the US Government IPv6 (USGv6) automation tests.

Syntax

usgv6

no usgv6

After the **usgv6** command is entered to enable USGv6 configuration mode, the following configuration syntax is available:

[**backup-dns-config-n-modify** *dns-server* | **flush-v6-neigh** *device-name* | **ping6** | **restart-device** *device-name* | **restore-dns-config** | **set-dev-mtu** *device-name mtu-size*]

Command Default

The USGv6 automation tests are not run.

Parameters

backup-dns-config-n-modify *dns-server*

Backs up and modifies the configuration file for the specified DNS server

flush-v6-neigh *device-name*

Flushes IPv6 neighbor's entries for the specified device.

ping6

Pings the IPv6 utility.

restart-device *device-name*

Restarts the specified device.

restore-dns-config

Restores the backup DNS configuration file.

set-dev-mtu *device-name mtu-size*

Sets the specified device and MTU size.

Modes

Privileged EXEC mode

Usage Guidelines

The **no** form of the command in configuration mode stops the USG automation tests.

This command is supported on the SmartZone Data Plane controllers only.

Examples

The following example runs the USGv6 automation tests and configures an MTU size of 1400 for device3.

```
device> enable
device# usgv6
device(usgv6)# set-dev-mtu device3 1400
```

vlan-pooling

Creates or updates VLAN pooling configuration.

Syntax

vlan-pooling*vlan-name*

no vlan-pooling[*vlan-name*]

After the **vlan-pooling** command is entered to enter VLAN pooling configuration mode, the following configuration syntax is available:
{**algot**mac-hash | **name***vlan-pool-name* | **pooling**{**range***start-numberend-number* | **single***vlan-number*}

Command Default

No VLAN pooling is defined.

Parameters

vlan-name

Specifies the user role name.

algotmac-hash

Specifies the algorithm to be used.

name*vlan-pool-name*

Specifies the VLAN pooling profile name.

pooling

Specifies the user traffic profile name to be used.

range*start-numberend-number*

Specifies a range of VLANs.

single*vlan-number*

Specifies a single VLAN.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command in configuration mode deletes the VLAN pooling profile. The **no pooling** command in VLAN pooling configuration mode deletes a single VLAN or a range of VLANs from the pooling profile.

Examples

The following example creates a VLAN pooling profile, vpool1, adds the use of the MAC hash algorithm, and defines a range of VLANs.

```
device# config
device(config)# vlan-pooling vpool1
device(config-vlan-pooling)# algo mac-hash
device(config-vlan-pooling)# pooling range 5 10
device(config-user-role)# user-traffic-profile "System Default"
```

The following example deletes a range of VLANs from the current VLAN pool.

```
device(config-vlan-pooling)# no pooling 5-10
Do you want to continue to delete (or input 'no' to cancel)? [yes/no] yes
Successful operation
```

vpn

Configures the Virtual Private Network (VPN) settings.

Syntax

vpn

After the **vpn** command is entered to enable VPN configuration mode, the following configuration syntax is available:

```
[show[all | sites | stats | summary] | sitesite-ip | ue-ip-filter{enable | disable}]
```

After the **show** command is entered in VPN configuration mode, the following configuration syntax is available:

```
[all[countnum | site{all | summary}] | tidtunnel-id]
```

After the **site site-ip** command is entered in VPN configuration mode, the following configuration syntax is available:

```
[ip-address[calea_serverip-address | crypto{enable | disable}] | keys ivbyte-lengthhex-value | keys pskbit-lengthhex-value | server_ipip-address/mask | site_DC{yes | no} | site_vlanvlan-id | udpport | ue_ipip-address/mask | ue_vlanvlan-id]
```

Command Default

No VPN settings are configured.

Parameters

show

Displays global VPN configuration information.

all

Displays all VPN information.

sites

Displays VPN information for the specified site.

stats

Displays VPN statistical information.

summary

Displays summary VPN information.

sitesite-ip

Specifies the site IP address.

ue-ip-filter

Controls the user-enabled (UE) IP filtering.

enable

Enables the UE IP filter.

disable

Disables the UE IP filter.

countnum

Displays the VPN count information for the specified number from the data core.

tid*tunnel-id*

Displays VPN tunnel information for the specified tunnel ID.

site*site-ip*

Specifies the site configuration.

ip-address

Specifies the IP address of the site.

calea-server*ip-address*

Specifies the IP address of the calea server.

crypto

Controls the use of VPN cryptographic security.

enable

Enables VPN cryptographic security.

disable

Disables VPN cryptographic security.

keys iv*byte-lengthhex-value*

Specifies the use of IV keys with the specified byte length and hex value.

keys psk*bit-lengthhex-value*

Specifies the use of PSK keys with the specified bit length and hex value.

server-ip*ip-address/mask*

Specifies the IP address and mask of the server.

site_DC

Controls the use of the DC site.

yes

Enables VPN cryptographic security.

no

Disables VPN cryptographic security.

site_vlan*vlan-id*

Specifies the VLAN ID of the site.

udp*port*

Specifies the UDP protocol and port number.

ue-ip*ip-address/mask*

Specifies the IP address and mask of the UE.

ue-vlan*vlan-id*

Specifies the UDP protocol and port number.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the SmartZone Data Plane controllers only.

Examples

The following example configures a site and server for the VPN.

```
device# configure
device(config)# vpn
device(config-vpn)# site site-ip 10.10.1.2
device(config-vpn)# server-ip 10.20.2.3/16
```

The following example displays VPN summary information.

```
device# configure
device(config)# vpn
device(config-vpn)# show summary
>>> -----
VPNGRE-Free-Pool: 1023 entries, max=1024; cli_cfg_count=2
  vpngret_hash_entry_cnt=0, number_sites=0
  Gbl CALEA: site=0.0.0.0 vlan=0 vpntid=0 l2gre=0.0.0.0
  UE_subnet_filter='disabled'
  Ingress: pkts=0 (drops=0), bytes=0
  Egress:  pkts=0, bytes=0, drops=0
  Actv VPNGRE: ACC  NB=0, SB=0 (past 4-sec)
  Actv VPNGRE: CORE NB=0, SB=0 (past 4-sec)
  Rx unconfigured VPNGRE (pkts=0, bytes=0)
  Err: LL_full=0  sip_no_tunl=0
  pow0_IP: 10.6.236.131, pow0_MAC: 00:0C:29:13:5A:5D
```

weak-cipher-allowed

Enables weak SSL cipher.

Syntax

weak-cipher-allowed

no weak-cipher-allowed

Command Default

Weak SSL cipher is enabled.

Parameters

This command has no parameters.

Modes

Global configuration mode

Usage Guidelines

This command can be used to configure Nginx accepting weak SSL cipher.

The **no** form of the command disables weak SSL ciphers.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example allows a client to make TLS connections to SZ with weak cipher.

```
device# config
device(config)# weak-cipher-allowed
Successful operation
% This configuration will take effective in a few minutes.
```

The following example disallows a client to make TLS connection to SZ with weak cipher.

```
device# config
device(config)# no weak-cipher-allowed
Do you want to continue to disable (or input 'no' to cancel)? [yes/no] yes
Successful operation
% This configuration will take effective in a few minutes.
```

web-authentication

To create or update the web authentication configurations, use the following command.

Syntax

web-authentication{*name*}

no web-authentication

After the **web-authentication** command is entered to enter web authentication configuration mode, the following configuration syntax is available:

{**grace-period***minutes* | **language***language* | **session-timeout***minutes* | **start-page**{**original** | **redirect***start-url*}}

Command Default

No web authentication is configured.

Parameters

name

Web authentication name.

grace-period*minutes*

Specifies the grace period, in minutes.

language*language*

Specifies the language.

session-timeout*minutes*

Specifies the number of minutes before the session times out when no activity has occurred.

start-page

Specifies the start page.

original

Specifies the start page as the original first page.

redirect*start-url*

Specifies a redirect link with a specific start page.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes web authentication configuration.

This command is supported for SmartZone 100 devices.

Examples

The following example configures web authentication.

```
device# config
device(config)# web-authentication webauth1
device((config-web-authentication)# grace-period 15
device((config-web-authentication)# start-page original
```

The following example deletes all web authentication configuration.

```
device(config)# no web-authentication
Do you want to continue to delete (or input 'no' to cancel)? [yes/no]
```

wechat

Creates or updates a WeChat portal configuration.

Syntax

wechat*name*

no wechat[*name*]

After the **wechat** command is entered to enter wechat configuration mode, the following configuration syntax is available:

{**authentication-url***auth-url* | **blacklist***blacklist* | **dnat-destination***dest* | **dnat-port-mappings***sourcedest* | **grace-period***mins* | **whitelist***whitelist*}

Command Default

No WeChat portal is configured.

Parameters

name

Specifies the Wechat portal name.

authentication-url*auth-url*

Specifies a link to an authentication interface URL on a third party authentication server. When a managed AP receives a WeChat logon request from a client device, it will send the request to this authentication URL and get the authorization result.

blacklist*blacklist*

Specifies the network destinations that the controller automatically blocks associated wireless clients from accessing. Use a comma to separate multiple entries.

dnat-destination*dest*

Specifies the DNAT destination server address to which the controller forwards HTTP requests from unauthenticated client devices. The DNAT destination server and the authentication server do not have to be the same server.

dnat-port-mappings*sourcedest*

Specifies the DNAT port mappings.

grace-period*mins*

Specifies the grace period before which the user does not have to reauthenticate, in minutes. The default is 60 with a range from 1 to 14399.

whitelist*whitelist*

Specifies the network destinations that the controller automatically allows associated wireless clients to access. You can add a single entry or multiple entries. Allowed entries are comma-separated IP addresses, IP address ranges, CIDR and regular expression domain name lists.

Modes

AP group configuration mode

Domain configuration mode

Zone configuration mode

Usage Guidelines

This command is supported only on SmartZone 300 and vSZ-H platforms.

The **no** form of the command deletes the WeChat portal.

The **wechat** command is only visible after specific commands are entered. These commands include **ap-group**, **domain**, and **zone**. Ruckus controllers only support the WeChat mobile app.

A WeChat portal defines the third party authentication server, also known as the equipment service provider (ESP) server, to which the controller forwards all WeChat authentication requests from wireless devices that are associated with controller-managed APs. In turn, the third party authentication server forwards these authentication requests to the WeChat server.

Examples

The following example creates a WeChat portal with an authentication server and sets the grace period to 30 minutes.

```
device# config
device(config)# zone zone-discovery
device(config-zone)# wechat chat2
device(config-wechat)# authentication http://authserver.examplecompany.com
device(config-wechat)# grace-period 45
```

with-public-key-change

Renews default certificate with/without updating private key.

Syntax

with-public-key-change

Command Default

Default certificate is renewed.

Parameters

This command has no parameters.

Modes

Global configuration mode

Usage Guidelines

This command is only for "Default Certificate". To generate certificate by new private key and remind user to update AP public key with this change.

This command is supported on all SmartZone platforms except SmartZone Data Plane controller.

Examples

The following example generate certificate with new private key.

```
device# config
device(config)# cert-store cert "Default Certificate"
device(config-cert)# with-public-key-change
device(config-cert)# end
Do you want to update this context configuration?
It will renew default certificate with updating key.
The Web GUI session will be terminated. Please login again. (or input 'no' to cancel)? [yes/no] yes
```


wlan

Creates or updates WLAN configurations.

Syntax

wlan *name*

no wlan [*name*]

After the **wlan** command is entered to access WLAN configuration mode, the following configuration syntax is available (see several sections below):

{ **access-network** | **acct-service** { **disabled** | *service-name* } | **acct-service-use-proxy** | **assoc-rssi-threshold** *num* | **auth-rssi-threshold** *num* | **bss-minrate** { **1mbps** | **2mbps** | **5.5mbps** | **12mbps** | **24mbps** | *rate* } }

{ **called-sta** { **apgroup** | **apmac** | **bssid** | **none** } | **client-fingerprinting** | **client-tx-rx-statistics** | | **dhcp-option-82** | **directed-multicast** | **directed-threshold** *num* | **disable-load-balancing** | **dtim-interval** | **enable-type** { **always-off** | **always-on** | **specific** } | **external-nas** }

{ **flow-log** | **force-dhcp** *seconds* | **hessid** *id* | **hide-ssid** | **inactivity-timeout** *mins* | **max-clients** *num* | **mgmt-tx-rate** *rate* | **ofdm-only** | **single-session-id-acct** | **ssid** *ssid* | **ssid-rate-limiting** | **support-802-11d** | **support-802-11k** | **transient-client-mgmt** | **venue-code** *code* | **vlan-id** *vlan-id* | **wireless-client-isolation** }

Command Default

No WLANs are configured.

Parameters

name

Specifies the WLAN name or ESSID.

access-network

Enables tunnel WLAN traffic to the controller.

acct-service *radius-server*

Specifies the RADIUS Accounting server that you want to use for this WLAN. The server must already be set up.

acct-service-use-proxy

Allows the controller to proxy accounting messages to the AAA server.

assoc-rssi-threshold *threshold*

Specifies the minimum client Received Signal Strength Indicator (RSSI) threshold to allow joining. Range is from -60 through -90 dBm.

auth-rssi-threshold *threshold*

Specifies the authentication RSSI threshold.

bss-minrate

Specifies the BSS minute rate.

1mbps

Sets 1 Mbps as the BSS minute rate.

2mbps

Sets 2 Mbps as the BSS minute rate.

Commands Si - Z

wlan

5.5mbps

Sets 5.5 Mbps as the BSS minute rate.

12mbps

Sets 12 Mbps as the BSS minute rate.

24mbps

Sets 24 Mbps as the BSS minute rate.

rate

Specifies the BSS minute rate.

called-sta

Specifies the Called Station ID format which is sent to the RADIUS server as a decision attribute.

agroup

Sets the AP Group number as the Called Station ID format.

apmac

Sets the AP MAC address as the Called Station ID format.

bssid

Sets the BSS ID as the Called Station ID format.

none

Sets none as the Called Station ID format.

client-fingerprinting

Enables client fingerprinting.

client-tx-rx-statistics

Stops the controller from monitoring traffic statistics for unauthorized clients.

dhcp-option82

Enables DHCP option 82. Other sub-options may be available.

directed-multicast

Enables directed multicast.

directed-threshold num

Sets the directed MC/BC threshold. Defines the per radio client count at which an AP stops converting group addressed data traffic to unicast. Number from 0 to 128.

disable-load-balancing

Disables client load balancing on the WLAN.

dtim-interval num

Sets the frequency at which the Delivery Traffic Indication Message (DTIM) will be included in beacon frames. Number from 1 to 255.

enable-type

Specifies the WLAN service enable type.

always-on

The WLAN service is always turned on.

always-off

The WLAN service is always turned off.

specific

The WLAN service is turned on and off by schedule.

external-nas

Enables external NAS IP.

flow-log

Enables the sending of flow log messages to the external server.

force-dhcp *seconds*

Requires the clients to obtain a valid IP address from DHCP within the specified number of seconds.

hessid *ssid*

Sets the WLAN HESS ID. Number from ?.

hide-ssid

Hides the SSID in a beacon broadcast.

inactivity-timeout *seconds*

Sets the duration, in seconds, after which idle clients will be disconnected.

max-clients *max-num*

Limits the number of clients that can associate with this WLAN per AP radio. Default is 100.

mgmt-tx-rate *rate*

Sets the transmit rate for management frames type such as beacon and probes. The rate can be one of the following: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 mbps.

ofdm-only

Disconnects 802.11b devices from the WLAN and all devices are forced to use higher data rates for more efficient airtime usage. Only affects 2.4GHz radio.

single-session-id-acct

Allows the APs to maintain one accounting session for a client roaming between APs.

ssid *ssid*

Specifies the SSID for the WLAN.

ssid-rate-limiting

Enforces an aggregate rate limit for all users of the WLAN. Rates from uplink and downlink are combined.

uplink *rate*

Sets rate to be limited on uplink.

downlink *rate*

Sets rate to be limited on downlink.

support-802-11d

Enables support for 802.11d.

support-802-11k

Enables 802.11k neighbor reports.

transient-client-mgmt

Enables transient client management.

venue-codecode

Specifies the venue code.

Commands Si - Z

wlan

vlan *vlan-id*

Tags the WLAN traffic with a VLAN ID in the range of 2 to 4094. By default, all client traffic will be assigned to the native (untagged) VLAN on the Ethernet port of the AP, which we represent as VLAN ID 1.

wireless-client-isolation

Prevents wireless clients from communicating with each other.

Modes

AP group configuration mode

Domain configuration mode

Zone configuration mode

Usage Guidelines

The **no** form of the command deletes the WLAN configuration.

The **wlan** command is only visible after specific commands are entered. These commands include **ap-group**, **domain**, and **zone**. RUCKUS controllers only support the WeChat mobile app.

The following list of commands are available under zone WLAN configuration mode (config-zone-wlan) and are all documented as separate commands in the *RUCKUS SmartZone Command Reference*.

- auth-method
- auth-type
- calea
- dhcp-option-82
- dns-server-profile
- priority
- proxy-arp
- qos-map-enable
- radius-nas-max-retries
- radius-nas-reconnect-primary
- radius-nas-request-timeout
- radius-nas-type
- roam
- roam-factor
- user-traffic-profile
- vlan-pooling

Examples

The following example creates a WLAN with an authentication method of 802.1x EAP, a BSS minute rate of 5.5Mbps, and a timeout in 120 seconds when no activity is detected.

```
device# config
device(config)# zone zone-discovery
device(config-zone)# wlan wlan2
device(config-zone-wlan)# auth-method 8021x
device(config-zone-wlan)# bss-minrate 5.5
device(config-zone-wlan)# inactivity-timeout 120
```

The following example deletes a WLAN named WLAN20 from zone-discovery zone.

```
device# config
device(config)# zone zone-discovery
device(config-zone)# no wlan wlan20
Do you want to continue to delete (or input 'no' to cancel)? [yes/no] yes
Operation successful
```

wlan-group

Creates or updates WLAN group configurations

Syntax

wlan-group*name*

no wlan-group[*name*]

After the **wlan-group** command is entered to enter WLAN group configuration mode, the following configuration syntax is available:
{*wlan-name* | **nasid***nas-id* | **vlan***vlan-tag* | **vlan-pooling***vlan-name*}

Command Default

No WLAN groups are configured.

Parameters

name

Specifies the WLAN group name.

wlan-name

Specifies the WLAN name.

nasid*nas-id*

Defines the ID sent to the RADIUS server, which identifies the AP.

vlan*vlan-tag*

Tags the WLAN traffic with a VLAN ID between 2 and 4094. By default, all client traffic will be assigned to the native (untagged) VLAN on the Ethernet port of the AP, which we represent as VLAN ID 1.

vlan-pooling*vlan-name*

Enables VLAN pooling with the specified VLAN IDs to be associated with the WLAN group.

Modes

AP group configuration mode

Domain configuration mode

Zone configuration mode

Usage Guidelines

This command is supported for SmartZone 100 devices.

The **no** form of the command deletes the WLAN group.

The **wlan-group** command is only visible after specific commands are entered. These commands include **ap-group**, **domain**, and **zone**.

Examples

The following example creates a WLAN group and specifies a WLAN to be associated with the group. Note that you must enter zone configuration mode to be able to configure the WLAN group.

```
device# config
device(config)# zone zone-discovery
device(config-zone)# wlan-group wgroup3
device(config-wlan-group)# wlan wlan4
```

The following example removes a WLAN group configuration.

```
device# config
device(config)# zone zone-discovery
device(config-zone)# no wlan-group wgroup3
Do you want to continue to delete (or input 'no' to cancel)? [yes/no] yes
```

wlan-scheduler

To create or update the WLAN scheduler configurations, use the following command.

Syntax

wlan-scheduler*name*

no wlan-scheduler

After the **wlan-scheduler** command is entered to enter WLAN scheduler configuration mode, the following configuration syntax is available:

{**name***profile-name* | **schedule-data**[*weekday*][*start-time*][*end-time*]}

Command Default

No WLAN scheduler configurations are created.

Parameters

name

WLAN scheduler name.

name*profile-name*

Sets the WLAN scheduler profile name.

schedule-data

Sets the schedule table.

weekday

Sets the WLAN schedule to a specified weekday. If no weekday is entered, the default value is all days.

start-time

Sets the WLAN schedule to start from a time value set in 15-minute intervals from 00:00 to 23:45. If no start time is entered, the default value is the whole day.

end-time

Sets the WLAN schedule to end at a time value set in 15-minute intervals from 00:15 to 24:00.

Modes

Global configuration mode

Usage Guidelines

This command is supported for SmartZone 100 devices.

The **no form** deletes all WLAN scheduler configurations.

Examples

The following example creates a WLAN scheduler named schedule1 to run on Tuesdays from 7am to 6pm.

```
device# config
device(config)# wlan-scheduler schedule1
device((config-wlan-scheduler)# schedule-data tuesday 07:00 18:00
```

The following example deletes all WLAN scheduler configurations.

```
device(config)# no wlan-scheduler
```

zone

To create or update the Access Point (AP) zone configurations, use the following command.

Syntax

zone*zone-name*

After the **zone** command is entered to access Zone configuration mode, the following configuration syntax is available:

[**ap-firmware** *ap-firmware* | **template** *template-name* | **template-apply***template-name* | | **trigger-prefer-node** *name*]

no zone[*zone-name*]

Command Default

AP zone configurations are not created.

Parameters

zone-name

AP zone name.

ap-firmware*ap-firmware*

Changes the AP firmware to the specified version.

template*template-name*

Creates an AP zone from the specified zone template.

template-apply*template-name*

Apply the specified zone template.

trigger-prefer-node*template-name*

Apply the trigger preference for the node from the specified zone template.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command in zone configuration mode deletes a zone configuration. The below **no** commands are supported for SmartZone 100 devices.

A separate **no zone** command exists in configuration mode to delete specific features of a specified AP zone. For more details, see the **no zone** command in the SmartZone Command Reference.

The following list of commands are available under zone configuration mode (config-zone) and are all documented as separate commands in the SmartZone Command Reference. Some of the following commands have other syntax configuration modes associated with them.

- **ap-group**
- **ap-model**
- **bonjour-policy**

- **device-policy**
- **diffserv**
- **guest-access**
- **hotspot**
- **hotspot20-venue-profile**
- **hotspot20-wlan-profile**
- **l2-acl**
- **vlan-pooling**
- **web-authentication**
- **wechat**
- **wlan-group**
- **wlan-scheduler**

The following tables contain commands that are available in the specified sub-configuration mode. Many of these options are also available in other commands.

TABLE 44 Commands related to device(config-zone)

Syntax and Type	Parameters (if any)	Description
device(config-zone)# aaa	<i>name</i>	Creates or updates the AAA server configuration.
device(config-zone)# adj-threshold	2.4g { <i>value</i> } 5g { <i>value</i> } Value is minimum = 1 and maximum = 100	Sets the adjacent radio threshold of the client load balancing.
device(config-zone)# ap-firmware	<i>ap-firmware</i>	Sets the AP firmware.
device(config-zone)# ap-group	<i>name</i>	Creates or updates the AP group configuration.
device(config-zone)# ap-ip-mode	[ipv4 ipv6 dual]	Sets the AP IP mode to either IPv4 or IPv6.
device(config-zone)# ap-logon	<i>logon-id</i>	Sets the login ID for the AP administrator.
device(config-zone)# ap-mgmt-vlan	<i>lvlanTag</i> : VLAN Tag (1-4094); enter 'keep' to keep APs setting.	Sets the AP management VLAN.
device(config-zone)# ap-model	<i>name</i>	Sets the AP model configuration.
device(config-zone)# ap-password		Sets the password for the AP administrator.
device(config-zone)# ap-ping-latency-interval	<i>enable</i> <i>disable</i>	Sets the AP latency detection by enabling or disabling the AP ping.
device(config-zone)# ap-reboot-timeout	default-gateway [<i>hours and minutes</i>] : Sets the default gateway timeout in hours and minutes. control-interface <i>hours</i> : Sets the control interface timeout in hours.	Sets the AP reboot timeout.
device(config-zone)# ap-registration-rule	<i>priority</i>	Creates or updates the AP registration rule configuration.
device(config-zone)# ap-snmp-options		Sets the AP SNMP options.
device(config-zone)# background-scan	2.4g <i>seconds</i> 5g <i>seconds</i>	Sets the background scanning.

TABLE 44 Commands related to device(config-zone) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-zone)# band-balancing	2.4g <i>int</i> 2.4g 2.4G band <i>int</i> : Percentage of clients on 2.4G band	Sets the band balance.
device(config-zone)# block-client	<i>mac</i> : Client MAC Address	Sets to block clients.
ruckus(config-zone)# bonjour-fencing	<i>name</i>	Bonjour Fencing provides a mechanism to limit the scope of Bonjour (mDNS) service discovery in the physical/spatial domain.
ruckus(config-zone)# bonjour-fencing-policy	<i>name</i>	Creates or updates the bonjour fencing policy.
device(config-zone)# bonjour-gateway		Enables the bonjour gateway.
device(config-zone)# bonjour-policy	<i>name</i>	Creates or updates the bonjour policy.
device(config-zone)# channel	2.4g <i>channel</i> 5g indoor <i>channel</i> 5g outdoor <i>channel</i>	Sets the channel.
device(config-zone)# channel-evaluation-interval	<i>seconds</i> : The interval value (Range: 60~3600 sec)	Sets the channel evaluation interval.
device(config-zone)# channel-range	2.4g [<i>channel</i> all] 5g indoor [<i>channel</i> all] 5g outdoor [<i>channel</i> all]	Sets the channel range.
device(config-zone)# channel-select-mode	2.4g { <i>value</i> } 5g { <i>value</i> }	Set a mode to automatically adjust AP channels.
device(config-zone)# channelfly-mtbc	2.4g <i>number</i> : MTBC value (Range: 100~1440) 5g <i>number</i>	Sets the MTBC value of ChannelFly.
device(config-zone)# channelization	2.4g [20 40] 5g [40 20]	Sets the channelization.
device(config-zone)# client-admission-control	2.4g 5g 2.4g <i>minClientCount</i> <i>minClientCount</i> 2.4g <i>maxRadioLoad</i> <i>maxRadioLoad</i> 2.4g <i>minClientThroughput</i> <i>minClientThroughput</i> 5g <i>minClientCount</i> <i>minClientCount</i> 5g <i>maxRadioLoad</i> <i>maxRadioLoad</i> 5g <i>minClientThroughput</i> <i>minClientThroughput</i>	Enables the client admission control.
device(config-zone)# client-isolation-whitelist	<i>name</i> : Client isolation whitelist name	Creates or updates the client isolation whitelist.
device(config-zone)# country-code	<i>country-code</i>	Sets the country code.
device(config-zone)# description	<i>text</i>	Sets the description,
device(config-zone)# device-policy	<i>name</i>	Sets the device policy.
device(config-zone)# dfs-channel		Enable DFS channels for the US country code.
device(config-zone)# difserv	<i>name</i>	Creates or updates the diff server profile.

TABLE 44 Commands related to device(config-zone) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-zone)# dos-protection	<i>dosBarringPeriod</i> : DoS protection period <i>dosBarringThreshold</i> : DoS protection threshold <i>dosBarringCheckPeriod</i> : DoS protection checkperiod	Enables DoS (Denial-of-service) protection.
device(config-zone)# ethernet-port-profile	<i>name</i>	Sets the Ethernet Port profile.
device(config-zone)# gps	<i>latitude</i> <i>longitude</i>	Displays the help.
device(config-zone)# gps-altitude	<i>altitude</i> [floor meters] <i>altitude</i> value floor meters	Sets the GPS altitude.
device(config-zone)# guest-access	<i>name</i>	Sets the guest access.
device(config-zone)# headroom	2.4g <i>client</i> 5g : 5 GHz radio	Sets the headroom (# of clients) of client load balancing.
device(config-zone)# hotspot	<i>name</i>	Creates or updates the WISPr hotspot configuration.
device(config-zone)# hotspot20-venue-profile	<i>name</i>	Creates or updates the venue profile for hotspot release 2 configuration.
device(config-zone)# hotspot20-wlan-profile	<i>name</i>	Creates or updates the WLAN profile for hotspot release 2 configuration.
device(config-zone)# indoor-channel		Enables the indoor channels.
device(config-zone)# ipsec-profile	<i>profile-name</i>	Sets the IPsec profile.
device(config-zone)# ipsec-tunnel-profile	<i>{value}</i>	Sets the IPsec Tunnel Profile.
device(config-zone)# l2-acl	<i>name</i>	Sets the layer 2 access control list.
device(config-zone)# lbs		Enables the location based service.
device(config-zone)# lbs-service		Sets the location based service.
device(config-zone)# load-balancing	2.4g 5g	Sets the client load balancing.
device(config-zone)# location	<i>text</i>	Sets the location.
device(config-zone)# location-additional-info	<i>text</i>	Sets the additional information location.
device(config-zone)# mesh		Enables mesh networking.
device(config-zone)# mesh-name	<i>name</i>	Sets the mesh name (ESSID).
device(config-zone)# mesh-passphrase	<i>mesh-passphrase</i>	Sets the mesh passphrase.
device(config-zone)# move	domain <i>name</i>	Moves the zone to another domain.
device(config-zone)# name	<i>name</i>	Sets the AP zone name.

TABLE 44 Commands related to device(config-zone) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-zone)# no	aaa name ap-group name ap-registration-rule priority background-scan 2.4g 5g band-balancing block-client bonjour-fencing bonjour-fencing-policy bonjour-gateway bonjour-policy channel-select-mode 2.4g 5g client-admission-control 2.4g 5g client-isolation-whitelist description device-policy dfs-channel diffserv dos-protection dosBarringPeriod ethernet-port-profile gps gps-altitude altitude guest-access hotspot name hotspot20-venue-profile name hotspot20-wlan-profile name indoor-channel ipsec-profile l2-acl lbs load-balancing location location-additional-info mesh protection-mode roam smart-mon smart-roam-disconnect-event soft-gre-profiles syslog-enabled syslog-facility syslog-ip syslog-ip6	Disables and deletes command configuration.

TABLE 44 Commands related to device(config-zone) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-zone)# no	timezone timezone-dst timezone-dst timezone-gmt-offset tunnel-profile tunnel-type tx-power venue-codename venue-profile vlan-overlapping weak-bypass web-authentication wechatname wlan name wlan-group name wlan-scheduler name	Disables and deletes command configuration.
device(config-zone)# node-affinity-profile	<i>profile-name</i>	Sets the node affinity profile
device(config-zone)# protection-mode	2.4g \${value}	Overrides the protection mode on 2.4 GHz radio
device(config-zone)# recovery-ssid-enabled	disable	Overrides the enable recovery SSID broad case.
device(config-zone)# rks-gre-profile	profile-name	Sets the AP Ruckus GRE tunnel profile.
device(config-zone)# roam	2.4g 5g	Sets the smart roam.
device(config-zone)# roam-macfilt-time	2.4g <i>seconds (0-600)</i> 5g <i>seconds (0-600)</i>	Sets the smart roam MAC filter time in seconds. The default value is 15 seconds. This configuration is only available at the Zone level.
device(config-zone)# rogue-ap-detection	[disable enable] : Disables or enables rogue access points report-all[disable enable] : Enables or disables all rogue devices report-only-malicious[enable disable] : Enables or disables only malicious rogue device types report-ssid-spoofing [disable enable]: Enables or disables malicious rogue devices which have SSID spoofing	Sets the report rogue access point.

TABLE 44 Commands related to device(config-zone) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-zone)# rogue-ap-detection	<p>report-same-network [enable disable]: Enables or disables malicious rogue devices which have same network</p> <p>report-mac-spoofing [disable enable]: Enables or disables malicious rogue devices which have MAC IP address spoofing</p> <p>protect-from-malicious [disable enable]: Enables or disables the network from malicious rogue access points</p>	Sets the report rogue access point.
device(config-zone)# secondary-channel	<p>5g indoor [<i>Secondary channel</i>]</p> <p>5g outdoor [<i>Secondary channel</i>]</p>	Sets the secondary channel.
device(config-zone)# smart-mon	<p>interval<i>value</i></p> <p>threshold<i>value</i></p>	Sets the smart monitor interval.
device(config-zone)# smart-roam-disconnect-event		Enables smart roam disconnect event.
device(config-zone)# soft-gre-profiles	<p><profile-name> <profile-name> <profile-name> - Select the first, second and third SoftGRE tunnel profile</p> <p><profile-name> <profile-name> - Select the first and second SoftGRE tunnel profile</p> <p><profile-name> - Select the first SoftGRE tunnel profile</p>	Sets AP SoftGRE tunnel profiles
device(config-zone)# syslog-enabled		Enables the external syslog server for APs for the specified zone.
device(config-zone)# syslog-facility	[Local6 Keep Original Local0 Local5 Local7 Local1 Local4 Local3 Local2]	Sets the syslog server facility,
device(config-zone)# syslog-ip	<i>ip</i>	Sets the IP address for the syslog server.
device(config-zone)# syslog-ip6	<i>ipv6</i>	Sets the IPv6 address for the syslog server.
device(config-zone)# syslog-port	<i>port</i>	Sets the port number for the syslog server.
device(config-zone)# syslog-priority	[Alert Info Critical Warning Notice Emergency All Error]	Sets the syslog server priority.
device(config-zone)# timezone	<p>System : Follows the controller time zone setting</p> <p>System[<i>time zone</i>]</p> <p>Select the time zone from system database</p> <p>User-defined[<i>time zone abbr.</i>]</p> <p>User defined time zone</p> <p>Time zone abbreviation (example: GMT, CST, EST)</p>	Sets the timezone for zone.
device(config-zone)# timezone-dst	[<i>Start</i> <i>End</i>] <i>orderweekdaymonthhour</i>	Sets the user defined timezone for daylight savings.
device(config-zone)# timezone-gmt-offset	[<i>hour</i> <i>hour:</i>] <i>minute</i> : For example, 8, -7:45	Sets the user defined timezone for GMT offset.
device(config-zone)# tunnel-profile	<i>profile-name</i>	Sets the AP GRE tunnel profile.

TABLE 44 Commands related to device(config-zone) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-zone)# tunnel-type	[gre gre-udp]	Sets the tunnel type.
device(config-zone)# tx-power	2.4g\${value} 5g\${value} Value is minimum = 1 and maximum = 100	Sets the TX power adjustment.
device(config-zone)# usb-software	uploadftp-url	Sets the AP USB software package.
device(config-zone)# venue-code	codeVenue Code	Sets the venue code.
device(config-zone)# venue-profile	name	Sets the venue profile.
device(config-zone)# vlan-overlapping		Enables the overlapping of VLAN pooling.
device(config-zone)# vlan-pooling	name	Creates or updates the VLAN pooling profile.
device(config-zone)# weak-bypass	2.4g\${value} 5g\${value} Value is minimum = 1 and maximum = 100	Sets the weak bypass threshold of the client load balancing.
device(config-zone)# web-authentication	name	Sets the web authentication.
device(config-zone)# wechat	name: WeChat name	Create/update WeChat configuration.
device(config-zone)# wlan	name	Creates or updates the WLAN/ ESSID configuration.
device(config-zone)# wlan-group	name	Creates or updates the WLAN group configuration.
device(config-zone)# wlan-scheduler	name	Creates or updates the WLAN scheduler configuration.

TABLE 45 Commands related to device(config-zone-aaa)

Syntax and Type	Parameters (if any)	Description
device(config-zone-aaa)# admin-domain		Enables the admin domain name.
device(config-zone-aaa)# admin-domain-name	admin-domain	Creates or updates the admin domain.
device(config-zone-aaa)# admin-password	admin-password	Creates or updates the admin password.
device(config-zone-aaa)# backup	ipip ipv6ipv6 portport shared-secretshared-secret	Enables backup of RADIUS support and set related settings.
device(config-zone-aaa)# base-domain	base-domain	Set the base domain.
device(config-zone-aaa)# description	description	Sets the description.
device(config-zone-aaa)# global-catalog		Enables the global catalog support.
device(config-zone-aaa)# ip	ip	Set IP addresses of primary RADIUS server.
device(config-zone-aaa)# ip6	ipv6	Set IPv6 addresses of primary RADIUS server.
device(config-zone-aaa)# key-attribute	key-attribute	Sets the key attributes for the primary RADIUS server.
device(config-zone-aaa)# no	backup global-catalog	Disables or deletes configuration settings.
device(config-zone-aaa)# password	password	Sets the password for the primary RADIUS server.
device(config-zone-aaa)# port	port	Sets the port number of the primary RADIUS server.
device(config-zone-aaa)# search-filter	search-filter	Sets the search filter.

TABLE 45 Commands related to device(config-zone-aaa) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-zone-aaa)# shared-secret	<i>shared-secret</i>	Sets the shared secret of the primary RADIUS server.
device(config-zone-aaa)# test	<i>usernamepassword</i> [PAP CHAP]	Tests the RADIUS server based on the user credentials and protocol settings.
device(config-zone-aaa)# test-acct		Tests the accounting server.
device(config-zone-aaa)# type	[radius radius-acct LDAP AD]	Sets the RADIUS type.
device(config-zone-aaa)# windows-domain	<i>windows-domain</i>	Sets the windows domain name.

TABLE 46 Commands related to device(config-zone-ap-group)

Syntax and Type	Parameters (if any)	Description
device(config-zone-ap-group)# ani-ofdm-level	<i>ap-mode</i> : AP model name	Sets the AP adaptive noise immunity level for specific AP model.
device(config-zone-ap-group)# ap-snmp-options		Enables AP SNMP options.
device(config-zone-ap-group)# channel	2.4g { <i>value</i> } 5g indoor { <i>value</i> } 5g outdoor { <i>value</i> }	Sets the channel.
device(config-zone-ap-group)# channel-evaluation-interval	<i>seconds</i> : The interval value (60~3600 secs)	Sets the channel evaluation interval.
device(config-zone-ap-group)# channel-range	2.4g [<i>channels</i> all]: 2.4GHz radio 5g indoor [<i>channels</i> all]: 5GHz radio 5g outdoor [<i>channels</i> all]: 5GHz radio	Set channel range.
device(config-zone-ap-group)# channel-select-mode	2.4g { <i>value</i> }: 2.4GHz radio 5g { <i>value</i> }: 5GHz radio	Automatically adjusts the AP channels.
device(config-zone-ap-group)# channelfly-mtbc	2.4g { <i>number</i> }: 2.4GHz radio <i>number</i> : MTBC value range:100-1440 5g { <i>number</i> }: 5Hz radio <i>number</i> : MTBC value range:100-1440	Set MTBC value of Channelfly.
device(config-zone-ap-group)# channelization	2.4g [20 40] 5g [40 20]	Sets the channelization.
device(config-zone-ap-group)# client-admission-control	2.4g <i>minClientThroughput</i> <i>minClientThroughput</i> : Min Client Throughput (Default: 0.0Mbps) 5g <i>minClientCount</i> <i>minClientCount</i> Min Client Count (Default: 20) 5g <i>maxRadioLoad</i> <i>maxRadioLoad</i> Max Radio Load (Default: 75%) 5g <i>minClientThroughput</i> <i>minClientThroughput</i> Min Client Throughput (Default: 0.0Mbps)	Enables the client admission control.
device(config-zone-ap-group)# description	<i>text</i>	Sets the description.

TABLE 46 Commands related to device(config-zone-ap-group) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-zone-ap-group)# external-antenna	<i>ap-model5g</i> [disable enable] <i>ap-model5g</i> gaingain <i>ap-model2.4g</i> gaingain <i>ap-model2.4g</i> [enable disable] <i>ap-model</i> gaingain <i>ap-model</i> [disable enable] <i>ap-model2.4g</i> [3-antennas 2-antennas] <i>ap-model5g</i> [3-antennas 2-antennas]	Sets the external antenna for specific AP model.
device(config-zone-ap-group)# gps	<i>latitude</i> <i>longitude</i>	Displays the help.
device(config-zone-ap-group)# gps-altitude	<i>altitude</i> [floor meters]	Sets the GPS altitude.
device(config-zone-ap-group)# internal-heater	<i>ap-model</i> [enable disable]	Sets the internal heater for specific AP model.
device(config-zone-ap-group)# lbs		Enables the location based service.
device(config-zone-ap-group)# lbs-service		Sets the location based service.
device(config-zone-ap-group)# led-mode	<i>ap-model</i>	Sets the LED mode for specific AP model.
device(config-zone-ap-group)# lldp	<i>ap-model</i> [enable disable]	Sets the LLDP for a specific AP model.
device(config-zone-ap-group)# location		Sets the location.
device(config-zone-ap-group)# location-additional-info	<i>text</i>	Sets the additional information location.
device(config-zone-ap-group)# member	add <i>ap-mac</i> move-to <i>apgroup-nameap-mac</i> remove <i>mac</i>	Sets the AP group member. It adds a new access point to current AP group. The AP Mac address removes the access point from the current AP group and moves it to other AP group.

TABLE 46 Commands related to device(config-zone-ap-group) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-zone-ap-group)# no	ani-ofdm-level channel2.4g channel5gindoor channel5goutdoor channel-evaluation-interval channel-select-mode channel-range channelization2.4g channelization5g client-admission-control description external-antennaap-model5g external-antennaap-model2.4g gps internalheater lbs led-mode lldp location location-additional-info	Disables / deletes the configuration settings.

TABLE 46 Commands related to device(config-zone-ap-group) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-zone-ap-group)# no	override-ap-mgmt-vlan override-ap-snmp-options override-channel-select-mode override-client-admission-control override-lbs override-zone-location override-zone-location-additional-info poe-operating-mode poe-out port-setting protection-mode <2.4g> radio-band recovery-ssid secondary-channel status-leds tx-power2.4g tx-power 5g usb-port usb-software venue-code venue-profile wlan-group2.4g wlan-group5g	Disables / deletes the configuration settings.
device(config-zone-ap-group)# override-ap-mgmt-vlan	<i>vlanTag</i>	Overrides the AP Management VLAN.
device(config-zone-ap-group)# override-ap-snmp-options		Overrides the AP SNMP options.
device(config-zone-ap-group)# override-channel-select-mode	2.4g 5g	Overrides auto channel selection mode and ChannelFly MTBC.
device(config-zone-ap-group)# override-client-admission-control	2.4g 5g	Overrides the client admission control settings.
device(config-zone-ap-group)# override-lbs		Overrides the location based service to zone settings.
device(config-zone-ap-group)# override-venue-code		Overrides the zone's venue code .
device(config-zone-ap-group)# override-zone-location		Overrides the zone location setting.
device(config-zone-ap-group)# override-zone-location-additional-info		Overrides the zone location additional information setting.
device(config-zone-ap-group)# poe-operating-mode	<i>ap-model</i> : AP model name	Switches the PoE Operating Mode for specific AP model
device(config-zone-ap-group)# poe-out	<i>ap-model</i> [enable disable]	Sets the PoE out port for a specific AP model.

TABLE 46 Commands related to device(config-zone-ap-group) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-zone-ap-group)# port-setting	<i>ap-model</i>	Sets the port settings for specific AP model.
device(config-zone-ap-group)# protection-mode	2.4g <i>{value}</i>	Overrides the protection mode on 2.4 GHz radio
device(config-zone-ap-group)# radio-band	<i>ap-model</i> [2.4g 5g]	Switches the radio band for a specific AP model.
device(config-zone-ap-group)# recovery-ssid	enabled disable	Enables or disables the recovery SSID broad case.
device(config-zone-ap-group)# secondary-channel	5g indoor [<i>secondary channel</i>] 5g outdoor [<i>secondary channel</i>]	Sets the secondary channel.
device(config-zone-ap-group)# status-leds	<i>ap-model</i> [enable disable]	Sets the status LED for specific AP model.
device(config-zone-ap-group)# tx-power	2.4g <i>{value}</i> 5g <i>{value}</i>	Sets the TX power adjustment.
device(config-zone-ap-group)# usb-port	<i>ap-model</i> [disable enable]	Sets the USB port for a specific AP model.
device(config-zone-ap-group)# usb-software	<i>ap-model</i> :AP model name	Sets AP USB software package for a specific AP model
device(config-zone-ap-group)# venue-code		Sets the venue code.
device(config-zone-ap-group)# venue-profile	<i>name</i> : Venue profile	Sets the venue profile.
device(config-zone-ap-group)# wlan-group	2.4g 5g	Sets the WLAN group configurations.

TABLE 47 Commands related to device(config-zone-ap-snmp-options configuration)

Syntax and Type	Parameters (if any)	Description
device(config-zone-ap-snmp-options)# ap-snmp		Enables AP SNMP.
device(config-zone-ap-snmp-options)# no	ap-snmpname snmp-v2-communityname snmp-v3-username	Disables the settings that have been configured with these commands.
device(config-zone-ap-snmp-options)# snmp-v2-community	<i>name</i>	Adds or updates the AP SNMPv2 community.
device(config-zone-ap-snmp-options) # snmp-v3-user	<i>name</i>	Adds or updates the AP SNMPv3 user.

TABLE 48 Commands related to device(config-zone-ap-snmp-options-snmp-v2-community configuration)

Syntax and Type	Parameters (if any)	Description
device(config-zone-ap-snmp-options-snmp-v2-community)# no	notification notification-target read write	Disables the settings that have been configured with these commands.
device(config-domain-zone-ap-snmp-options-snmp-v2-community)# notification		Enable notification privilege
device(config-domain-zone-ap-snmp-options-snmp-v2-community)# notification-target		Enable notification target configuration commands.
device(config-domain-zone-ap-snmp-options-snmp-v2-community)# notification-type		Sets the notification type
device(config-domain-zone-ap-snmp-options-snmp-v2-community)# read		Enable the read privilege.

TABLE 48 Commands related to device(config-zone-ap-snmp-options-snmp-v2-community configuration) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-ap-snmp-options-snmp-v2-community)# write		Enable the write privilege.

TABLE 49 Commands related to device(config-zone-ap-snmp-options-snmp-v3-user configuration)

Syntax and Type	Parameters (if any)	Description
device(config-zone-ap-snmp-options-snmp-v3-user)# auth		Sets SNMPv3 user authentication.
device(config-zone-ap-snmp-options-snmp-v3-user)# no	notification' notification-target read write snmp-v3-username	Disables the settings that have been configured with these commands.
device(config-zone-ap-snmp-options-snmp-v3-user)# notification		Enable notification privilege.
device(config-zone-ap-snmp-options-snmp-v3-user)# notification-target		Enable notification target configuration commands.
device(config-zone-ap-snmp-options-snmp-v3-user)# notification-type		Sets the notification type
device(config-zone-ap-snmp-options-snmp-v3-user)# privacy	none desprivacy-phrase: DES privacy phrase.	Set SNMPv3 user privacy.
device(config-zone-ap-snmp-options-snmp-v3-user)# read		Enable the read privilege.
device(config-zone-ap-snmp-options-snmp-v3-user)# write		Enable the write privilege.

TABLE 50 Commands related to device(config-zone-ap-group lldp)

Syntax and Type	Parameters (if any)	Description
device(config-zone-ap-group-lldp)# lldp-ad-interval	<i>seconds</i>	Sets the LLDP advertise interval in seconds from the range 1 to 300.
device(config-zone-ap-group-lldp)# lldp-hold-time	<i>seconds</i>	Sets the LLDP hold time in seconds from the range 60 to 1200.
device(config-zone-ap-group-lldp)# lldp-mgmt		Enables the LLDP management IP TLV.

TABLE 51 Commands related to device(config-zone-ap-group-port-setting)

Syntax and Type	Parameters (if any)	Description
device(config-zone-ap-group-port-setting)# lan	<i>port</i> <i>portuplink[general access trunk]</i> <i>portuntagvlan</i> <i>portmembervlan-members</i> <i>portdot1x[auth-mac-based disabled auth-port-based supplicant]</i>	Enables or disable specific port.
device(config-zone-ap-group-port-setting)# no	lanport	Disables or deletes the configuration settings.

TABLE 52 Commands related to device(config-zone-ap-model)

Syntax and Type	Parameters (if any)	Description
device(config-zone-ap-model)# ext-ant	2.4gnumber 2.4gnumber[3 2] 5gnumber 5gnumber[2 3]	Sets the external antenna.
device(config-zone-ap-model)# internal-heater		Enables international heater.
device(config-zone-ap-model)# lan1 device(config-zone-ap-model)# lan2 device(config-zone-ap-model)# lan3 device(config-zone-ap-model)# lan4 device(config-zone-ap-model)# lan5		Sets the LAN configurations from 1 to 5.
device(config-zone-ap-model)# led		Enables the status of led.
device(config-zone-ap-model)# led-mode		Sets the led mode description
device(config-zone-ap-model)# lldp		Enables the Link Layer Discovery Protocol (LLDP).
device(config-zone-ap-model)# lldp-ad-interval	<i>seconds</i>	Sets the LLDP advertise interval.
device(config-zone-ap-model)# lldp-hold-time	<i>seconds</i>	Sets the LLDP hold time.
device(config-zone-ap-model)# lldp-mgmt		Enables the LLDP management IP TLV.
device(config-zone-ap-model)# no	ext-ant internal-heater lan1 lan2 lan3 lan4 lan5 led lldp lldp-mgmt poe-operating-mode poe-out-port radio-band usb- usb-software	Disables or deletes the settings that have been configured.
device(config-zone-ap-model)# poe-operating-mode	<i>value</i>	Switches the PoE mode
device(config-zone-ap-model)# poe-out-port		Enables the PoE out port
device(config-zone-ap-model)# radio-band	<i>value</i>	Switches the radio band for a specific AP model.
device(config-zone-ap-model)# usb	<i>port</i>	Enables USB port.
device(config-zone-ap-model)# usb-software		Sets AP USB software package.

TABLE 53 Commands related to device(config-zone-ap-model-lan1)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-ap-model-lan1)# profile	<i>profile</i>	Sets the Ethernet Port profile. By default the access port or default trunk port (LAN) or default trunk port (WAN).

TABLE 54 Commands related to device(config-zone-ap-registration-rule)

Syntax and Type	Parameters (if any)	Description
device(config-zone-ap-registration-rule)# description	<i>text</i>	Sets the description.
device(config-zone-ap-registration-rule)# type <i>gps</i>	<i>latitude</i> <i>longitude</i> <i>distance</i>	Sets the GPS coordinates.
device(config-zone-ap-registration-rule)# type <i>ip-range</i>	<i>ipip</i>	Sets the IP address range from and to IP address.
device(config-zone-ap-registration-rule)# type <i>provision-tag</i>	<i>tag</i>	Sets the provision tags.
device(config-zone-ap-registration-rule)# type <i>subnet</i>	<i>ipmask</i>	Sets the subnet IP address and subnet mask.
device(config-zone-ap-registration-rule)# type	[gps provision-tag ip-range subnet]	Sets the rule type.

TABLE 55 Commands related to device(config-zone-block-client)

Syntax and Type	Parameters (if any)	Description
device(config-zone-block-client)# description	<i>text</i>	Sets the description.

TABLE 56 Commands related to device(config-zone-bonjour-fencing-policy)

Syntax and Type	Parameters (if any)	Description
device(config-zone- bonjour-fencing-policy)# description	<i>text</i>	Sets the description.
device(config-zone- bonjour-fencing-policy)# no	description rulerule index	Sets to delete sub commands.
device(config-zone- bonjour-fencing-policy)# rule	<i>index: rule index</i>	Sets the bonjour fencing rule.

TABLE 57 Commands related to device(config-zone-bonjour-fencing-policy-rule)

Syntax and Type	Parameters (if any)	Description
device(config-zone-bonjour-fencing-policy-rule)# closest-ap	<text>	Sets the configuration to the closest AP.
device(config-zone-bonjour-fencing-policy-rule)# description	<text>	Sets the description.
device(config-zone-bonjour-fencing-policy-rule)# device-mac-list	#{value}	Lists the devices, which use MAC address.
device(config-zone-bonjour-fencing-policy-rule)# device-type		Sets the device type.
device(config-zone-bonjour-fencing-policy-rule)# fence-range		Sets the fence range.
device(config-zone-bonjour-fencing-policy-rule)# no	<i>device-mac-list</i>	Disables the configuration.
device(config-zone-bonjour-fencing-policy-rule)# service-type		Sets the service type.

TABLE 58 Commands related to device(config-zone-bonjour-policy)

Syntax and Type	Parameters (if any)	Description
device(config-zone-bonjour-policy)# description	<i>text</i>	Sets the description.
device(config-zone-bonjour-policy)# no	description rule <i>rule index</i>	Sets to delete sub commands.
device(config-zone-bonjour-policy)# rule	<i>index: rule index</i>	Sets the Bonjour fencing rule.

TABLE 59 Commands related to device(config-zone-bonjour-policy-rule)

Syntax and Type	Parameters (if any)	Description
device(config-zone-bonjour-policy-rule)# bridge-service	airdisk airplay airport-management airprint airtunes apple-file-sharing apple-mobile-devices (Allows sync with iTunes over Wi-Fi) appletv icloud-sync itunes-remote itunes-sharing open-directory-master optical-disk-sharing other screen-sharing secure-file-sharing secure-shell workgroup-manager www-http www-https xgrid	Sets the bridge service.
device(config-zone-bonjour-policy-rule)# from-vlan	<i>int</i>	Sets the from VLAN.
device(config-zone-bonjour-policy-rule)# notes	<i>int</i>	Sets the notes.
device(config-zone-bonjour-policy-rule)# protocol		Sets the bridge service when it is 'other'.
device(config-zone-bonjour-policy-rule)# to-vlan	<i>int</i>	Sets the VLAN.

TABLE 60 Commands related to device(config-zone-client-isolation-whitelist)

Syntax and Type	Parameters (if any)	Description
device(config-zone-client- isolation-whitelist)# auto		Enables the auto whitelist. Each entry must have an IP address in order to enable auto whitelist.
device(config-zone-client- isolation-whitelist)# description	<i>text</i>	Sets the description.

TABLE 60 Commands related to device(config-zone-client-isolation-whitelist) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-zone-client- isolation-whitelist)# entry	<i>index</i> : entry index	Sets the client isolation entry.
device(config-zone-client- isolation-whitelist)# no	auto description entry	Sets to delete sub command

TABLE 61 Commands related to device(config-zone-client-isolation-whitelist-entry)

Syntax and Type	Parameters (if any)	Description
device(config-zone-client- isolation-whitelist-entry)# description	<i>text</i>	Sets the description.
device(config-zone-client- isolation-whitelist-entry)# ip	<i>ip-address</i>	Sets the IP address.
device(config-zone-client- isolation-whitelist-entry)# mac	<i>mac-address</i>	Sets the MAC IP address.
device(config-zone-client- isolation-whitelist-entry)# no	description ip	Sets to delete sub command

TABLE 62 Commands related to device(config-zone-device-policy)

Syntax and Type	Parameters (if any)	Description
device(config-zone-device-policy)# default-action	[allow block]	Sets the default action to either allow or block.
device(config-zone-device-policy)# description	<i>text</i>	Sets the description.
device(config-zone-device-policy)# no policy-rule	<i>Device Type</i>	Deletes the device policy rules.
device(config-zone-device-policy)# policy-rule		Sets the device policy.

TABLE 63 Commands related to ruckus (config-zone-device-policy-policy rule)

Syntax and Type	Parameters (if any)	Description
device(config-zone-device-policy-policy-rule)# action	[allow block]	Sets the default action to either allow or block.
device(config-zone-device-policy-policy-rule)# description	<i>text</i>	Sets the description.
device(config-zone-device-policy-policy-rule)# downlink	[<i>Rate Limiting</i>] Rate limiting (mbps)	Sets the downlink rate limiting.
device(config-zone-device-policy-policy-rule)# no vlan		Resets the VLAN number.
device(config-zone-device-policy-policy-rule)# type	[<i>Device Type</i>]	Sets the device type.
device(config-zone-device-policy-policy-rule)# uplink	[<i>Rate Limiting</i>] Rate limiting (mbps)	Sets the uplink rate limiting.
device(config-zone-device-policy-policy-rule)# vlan	[<i>VLAN Number</i>]	Sets the VLAN number.

TABLE 64 Commands related to device(config-zone-diffserv)

Syntax and Type	Parameters (if any)	Description
device(config-zone-diffserv)# description	<i>text</i>	Sets the description.
device(config-zone-diffserv)# downlink-diffserv	<i>value</i>	Enables the tunnel diffserv downlink and sets the diffserv number.

TABLE 64 Commands related to device(config-zone-diffserv) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-zone-diffserv)# no	description downlink-diffserv preserved-diffserv uplink-diffserv	Disables various options.
device(config-zone-diffserv)# preserved-diffserv	<i>value</i>	Adds the preserved diffserv number.
device(config-zone-diffserv)# uplink-diffserv	<i>value</i>	Enables the tunnel diffserv uplink and sets the diffserv number.

TABLE 65 Commands related to device(config-zone-ethernet-port-profile)

Syntax and Type	Parameters (if any)	Description
device(config-zone-ethernet-port-profile)# 8021x	<i>text</i>	Sets the 802.1x.
device(config-zone-ethernet-port-profile)# 8021x-enable		Enable 802.1x
device(config-zone-ethernet-port-profile)# acct-service	<i>acct-service</i>	Sets the accounting service.
device(config-zone-ethernet-port-profile)# auth-service	<i>auth-service</i>	Sets the authentication service.
device(config-zone-ethernet-port-profile)# client-visibility		Enables client visibility regardless of 802.1X authentication
device(config-zone-ethernet-port-profile)# dvlan		Enables the dynamic VLAN.
device(config-zone-ethernet-port-profile)# guest-vlan	<i>guest-vlan-id</i>	Enables the dynamic guest VLAN.
device(config-zone-ethernet-port-profile)# mac-bypass		Enables the MAC authentication bypass.
device(config-zone-ethernet-port-profile)# no	8021x-enable acct-service client-visibility dvlan mac-bypass proxy-acct proxy-auth tunnel	Disables various options.
device(config-zone-ethernet-port-profile)# proxy-acct		Enables proxy accounting service.
device(config-zone-ethernet-port-profile)# proxy-auth		Enables proxy authentication service.
device(config-zone-ethernet-port-profile)# supplicant	<i>mac \${value}</i> customusername <i>password</i>	Sets the supplicant.
device(config-zone-ethernet-port-profile)# tunnel		Enables tunnel.

TABLE 65 Commands related to device(config-zone-ethernet-port-profile) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-zone-ethernet-port-profile)# type	<i>access-port</i> <i>general-port</i> <i>trunk-port</i>	Sets the port type. The Ethernet port type defines how the AP will manage VLAN frames. You can set Ethernet ports on an AP to one of the following types: Trunk Port, Access Port, or General Port.
device(config-zone-ethernet-port-profile)# vlan-members	<i>vlan-members</i>	Enter the VLAN IDs that you want to use to tag WLAN traffic that will use this profile. You can enter a single VLAN ID or a VLAN ID range (or a combination of both). The valid VLAN ID range is from 1 through 4094.
device(config-zone-ethernet-port-profile)# vlan-untag-id	<i>vlan-untag-id</i>	Enter the ID of the native VLAN (typically 1), which is the VLAN into which untagged ingress packets are placed upon arrival. If your network uses a different VLAN as the native VLAN, configure the VLAN Untag ID of the AP Trunk port with the native VLAN used throughout your network.

TABLE 66 Commands related to ruckus (config-zone-guest-access)

Syntax and Type	Parameters (if any)	Description
device(config-zone-guest-access)# description	<i>text</i>	Sets the description.
device(config-zone-guest-access)# enable-terms-and-conditions		Enables the web portal terms and conditions.
device(config-zone-guest-access)# grace-period	<i>minutes</i>	Sets the grace period.
device(config-zone-guest-access)# language		Sets the language.
device(config-zone-guest-access)# logo	<i>ftp-url</i> FTP URL, format: <i>ftp://username:password@ip/file-path</i>	Sets the logo.
device(config-zone-guest-access)# name	<i>name</i>	Sets the guess access service name.
device(config-zone-guest-access)# no	enable-terms-and-conditions sms-gateway terms-and-conditions	Disables the various options.
device(config-zone-guest-access)# session-timeout	<i>minutes</i>	Sets the session timeout as per the specified minutes.
device(config-zone-guest-access)# sms-gateway		Sets the guest pass for the SMS gateway.
device(config-zone-guest-access)# start-page	original redirect <i>start-url</i>	Sets the start page.
device(config-zone-guest-access)# terms-and-conditions		Sets the terms and conditions for the web portal.
device(config-zone-guest-access)# title		Sets the title for the web portal.

TABLE 67 Commands related to device(config-zone-hotspot)

Syntax and Type	Parameters (if any)	Description
device(config-zone-hotspot)# description	<i>text</i>	Sets the description.
device(config-zone-hotspot)# grace-period	<i>minutes</i>	Sets the grace period.

TABLE 67 Commands related to device(config-zone-hotspot) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-zone-hotspot)# https-redirect	<i>enable</i>	If enabled, the AP tries to redirect the HTTPS requests to the hotspot portal.
device(config-zone-hotspot)# language		Sets the portal language.
device(config-zone-hotspot)# location-id	<i>location-id</i>	Sets the location ID.
device(config-zone-hotspot)# location-name	<i>name</i>	Sets the location name.
device(config-zone-hotspot)# logo	<i>ftp-url</i>	Sets the logo.
device(config-zone-hotspot)# logon-url	internal external <i>logon-url</i>	Sets the logon model
device(config-zone-hotspot)# mac-address-format		Sets the MAC address format.
device(config-zone-hotspot)# no	https-redirect show-terms-conditions walled-garden <i>walled-garden-list</i> : Allows unauthorized destinations. Comma-separated IP, IP range, CIDR and regular expression domain name list.	Disables the commands.
device(config-zone-hotspot)# session-timeout	<i>minutes</i>	Sets the sessions timeout.
device(config-zone-hotspot)# show-terms-conditions		Shows the terms and conditions.
device(config-zone-hotspot)# smart-client-support	none enable only <i>instructions</i>	Sets the smart client support.
device(config-zone-hotspot)# start-page	original <i>start-url</i>	Sets the start page.
device(config-zone-hotspot)# terms-conditions	redirect	Sets the terms and conditions.
device(config-zone-hotspot)# title	<i>title</i>	Sets the title.
device(config-zone-hotspot)# walled-garden	<i>walled-garden-list</i>	Enables Walled Garden. Allows unauthorized destinations. Comma-separated IP, IP range, CIDR and regular expression domain name list

TABLE 68 Commands related to device(config-zone-hotspot20-venue-profile)

Syntax and Type	Parameters (if any)	Description
device(config-zone-hotspot20-venue-profile)# description	<i>text</i>	Sets the description.
device(config-zone-hotspot20-venue-profile)# no	venue-names wan-at-capacity wan-sym-link	Disables the commands.

TABLE 68 Commands related to device(config-zone-hotspot20-venue-profile) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-zone-hotspot20-venue-profile)# venue-category	<p>unspecifiedunspecified</p> <p>assembly [coffee-shop passenger-terminal restaurant bar arena library place-of-worship emergencycoordination-center museum stadium convention-center unspecified amphitheater amusement-park theater zoo-or-aquarium]</p> <p>business[unspecified on attorney-office professional-office research-and-development-facility doctor-ordentist-office fire-station post-office bank]</p> <p>educational[unspecified school-primary university-or-college school-secondary]</p>	Sets the venue category
device(config-zone-hotspot20-venue-profile) venue-category	<p>factory-and-industrial[factory]</p> <p>institutional[hospital group-home unspecified prison-or-jail long-term-care-facility alcohol-and-drugrehabilitation-center]</p> <p>mercantile[grocery-market automotive-service-station unspecified retail-store gas-station shopping-mall]</p> <p>residential[unspecified private-residence hotel-or-motel dormitory boarding-house]</p> <p>storageunspecified</p> <p>utility-and-miscellaneousunspecified</p> <p>vehicular [train airplane ferry a bus motor-bike unspecified ship-or-boat]</p> <p>outdoor[unspecified city-park bus-stop traffic-control rest-area muni-mesh-network kiosk]</p>	Sets the venue category.
device(config-zone-hotspot20-venue-profile)# venue-names	<i>language</i> names	Sets the venue-names.
device(config-zone-hotspot20-venue-profile)# wan-at-capacity		Sets the WAN capacity.
device(config-zone-hotspot20-venue-profile)# wan-downlink-load	<i>downlink-load</i> : Load between 1 and 255	Sets the WAN downlink load.
device(config-zone-hotspot20-venue-profile)# wan-downlink-speed	<i>speed</i>	Sets the WAN downlink speed in (kbps).
device(config-zone-hotspot20-venue-profile)# wan-link-status	[link-up link-test link-down]	Sets the link status.
device(config-zone-hotspot20-venue-profile)# wan-load-duration	<i>duration</i>	Sets the load measurement duration.
device(config-zone-hotspot20-venue-profile)# wan-sym-link		Enables symmetric link.

TABLE 68 Commands related to device(config-zone-hotspot20-venue-profile) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-zone-hotspot20-venue-profile)# wan-uplink-load	<i>uplink-load</i>	Sets the WAN uplink load.
device(config-zone-hotspot20-venue-profile)# wan-uplink-speed	<i>speed</i> : Uplink speed in kbps	Sets the WAN uplink speed.

TABLE 69 Commands related to device(config-zone-hotspot20-wlan-profile)

Syntax and Type	Parameters (if any)	Description
device(config-zone-hotspot20-wlan-profile)# access-network-type		Sets the access network type.
device(config-zone-hotspot20-wlan-profile)# asra		Sets the ASRA profile.
device(config-zone-hotspot20-wlan-profile)# asra-dns-redirect	<i>url</i>	Sets the ASRA DNS redirection.
device(config-zone-hotspot20-wlan-profile)# asra-http-redirect		Sets the ASRA HTTP redirection.
device(config-zone-hotspot20-wlan-profile)# asra-online-signup	<i>ssid</i>	Sets the ASRA online signup.
device(config-hotspot20-wlan-profile)# asra-terms-conditions	<i>url</i>	Sets the ASRA terms and conditions.
device(config-zone-hotspot20-wlan-profile)# connect-capabilities	[pptp http voip-6 ipsec-vpn ikev2 ftp tls voip-17 icmp ssh esp][open unknown closed]	Sets the connection capabilities. pptp: Protocol Number:6 Port:1723 Protocol Name: Used by PPTP VPNs http: Protocol Number:6 Port:80 Protocol Name: HTTP voip-6: Protocol Number:6 Port:5060 Protocol Name: VoIP ipsec-vpn: Protocol Number:17 Port:4500 Protocol Name: IPSec VPN ikev2: Protocol Number:17 Port:500 Protocol Name: Used by IKEv2(IPSec VPN) tls: Protocol Number:6 Port:443 Protocol Name: Used by TLS VPN voip-17: Protocol Number:17 Port:5060 Protocol Name: VoIP icmp: Protocol Number:1 Port:0 Protocol Name: ICMP
device(config-zone-hotspot20-wlan-profile)# connect-capabilities	[pptp http voip-6 ipsec-vpn ikev2 ftp tls voip-17 icmp ssh esp][open unknown closed]	ssh: Protocol Number:6 Port:22 Protocol Name: SSH esp: Protocol Number:50 Port:0 Protocol Name: ESP open: Open unknown: Unknown closed: Closed
device(config-zone-hotspot20-wlan-profile)# custom-connect-capabilities	<i>protocol-name</i> <i>protocol-number</i>	Creates or updates the custom connection capabilities.
device(config-zone-hotspot20-wlan-profile)# description	<i>text</i>	Sets the description.

TABLE 69 Commands related to device(config-zone-hotspot20-wlan-profile) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-hotspot20-wlan-profile)# identity-providers	<i>identityProvider</i> default	Sets the identity providers.
device(config-domain-zone-hotspot20-wlan-profile)# internet-option	enable	Enables the specified WLAN with Internet connectivity.
device(config-domain-zone-hotspot20-wlan-profile)# ipv4-address	[port-restrict-address single-nated-private-address double-nated-private-address port-restricted-addressdouble-nated-address unknown public-address port-restricted-address-single-nated-address not-available]	Sets the IPv4 address.
device(config-domain-zone-hotspot20-wlan-profile)# ipv6-address	[not-available unknown available]	Sets the IPv6 address.
device(config-domain-zone-hotspot20-wlan-profile)# name	<i>name</i>	Sets the hotspot 2.0 WLAN profile name.
device(config-domain-zone-hotspot20-wlan-profile)# no	asra asra-dns-redirect asra-http-redirect asra-online-signup asra-terms-conditions cust-connect-capabilities identity-providers internet-option	Disables the commands.
device(config-domain-zone-hotspot20-wlan-profile)# operator	<i>name</i>	Sets the operator name.

TABLE 70 Commands related to device(config-zone-hotspot20-wlan-profile-cust-connect-capabilities)

Syntax and Type	Parameters (if any)	Description
device(config-zone-hotspot20-wlan-profile-cust-connect-capabilities)# port	<i>port</i>	Set the port number.
device(config-zone-hotspot20-wlan-profile-cust-connect-capabilities)# protocol	<i>protocol</i>	Sets the protocol number.
device(config-zone-hotspot20-wlan-profile-cust-connect-capabilities) status	[closed unknown open]	Sets the status.

TABLE 71 Commands related to device(config-zone-l2-acl)

Syntax and Type	Parameters (if any)	Description
device(config-zone-l2-acl)# action	[allow block]	Sets the handling action to allow or block.
device(config-zone-l2-acl)# description	<i>text</i>	Sets the description.
device(config-zone-l2-acl)# mac	<i>value</i>	Sets the MAC value.
device(config-zone-l2-acl)# no mac	<i>value</i>	Disables the MAC value.

TABLE 72 Commands related to ruckus (config-zone-web-authentication)

Syntax and Type	Parameters (if any)	Description
device(config-zone-web-authentication)# description	text	Sets the description.
device(config-zone-web-authentication)# grace-period	minutes	Sets the grace period.
device(config-zone-web-authentication)# language		Sets the language.
device(config-zone-web-authentication)# session-timeout	minutes	Sets the session timeout as per the specified minutes.
device(config-zone-web-authentication)# start-page	original redirectstart-url	Sets the start page.

TABLE 73 Commands related to device(config-zone-wechat)

Syntax and Type	Parameters (if any)	Description
device(config-zone-wechat)# authentication-url	text	Sets the authentication URL.
device(config-zone-wechat)# black-list	text	Sets the black list.
device(config-zone-wechat)# description	text	Sets the description.
device(config-zone-wechat)# dnat-destination	text	
device(config-zone-wechat)# dnat-port-mapping	sourcedest	Sets the DNAT destination.
device(config-zone-wechat)# grace-period	minutes	Set the grace period as minutes.
device(config-zone-wechat)# no	dnat-port-mapping white-list	Disables various options.
device(config-zone-wechat)# white-list	white-list: Allow unauthorized destinations. Comma- separated IP, IP range, CIDR and regular expression domain name list.	Sets the white list.

TABLE 74 Commands related to device(config-zone-wlan)

Syntax and Type	Parameters (if any)	Description
device(config-zone-wlan)# aaa-vlan-override		Enables AAA VLAN override.
device(config-zone-wlan)# access-network		Enables tunnel WLAN traffic to the controller.
device(config-zone-wlan)# acct-delay-time		Enables the acct-delay time.
device(config-zone-wlan)# acct-interval	minutes	Set the authentication service. Enables accounting interval to send interim updates.
device(config-zone-wlan)# acct-service	name	Sets the accounting service.
device(config-zone-wlan)# acct-service-use-proxy		Set the accounting service: Uses the controller as proxy.
device(config-zone-wlan)# acct-ttg-session		Sets the accounting service. Enables accounting for TTG sessions.
device(config-zone-wlan)# app-visibility		Sets the application to visible mode.
device(config-zone-wlan)# assoc-rssi-threshold	numbers	Sets the associated RSSI threshold ranging from -60 to -90.
device(config-zone-wlan)# auth-method		Sets the authentication method.
device(config-zone-wlan)# auth-rssi-threshold	numbers	Sets the authentication RSSI threshold ranging from -60 to -90.
device(config-zone-wlan)# auth-service	name	Sets the authentication service.
device(config-zone-wlan)# auth-service-use-proxy		Sets the authentication service. Enables accounting for TTG sessions.

TABLE 74 Commands related to device(config-zone-wlan) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-zone-wlan)# auth-type		Sets the authentication type.
device(config-zone-wlan) #bss-minrate	[5.5mbps 24mbps 12mbps 1mbps 2mbps]	Sets the BSS minimum rate.
device(config-zone-wlan) #bypass-cna		Enables to bypass CNA server.
device(config-zone-wlan)# calea		Enables Calea server.
device(config-zone-wlan)# called-sta	[bssid apmac none apgroup]	Sets the called STA ID.
device(config-zone-wlan)# client-fingerprinting		Sets the client fingerprinting.
device(config-zone-wlan)# client-tx-rx-statistics		Enables ignore statistics from unauthorized clients.
device(config-zone-wlan)# description	text	Sets the description,
device(config-zone-wlan)# device-policy	policy name	Sets the device policy.
device(config-zone-wlan)# dgaf		Disables downstream group-address frame forwarding.
device(config-zone-wlan)# dhcp-option-82		Enables an AP to encapsulate additional information (such as VLAN ID, AP name, SSID, and MAC address) into DHCP request packets before forwarding them to the DHCP server.
device(config-zone-wlan)# dhcp-option-82-format	[soft-gre ruckus-gre subopt-1]	Enables an AP to encapsulate additional information into DHCP request packets before forwarding them to the DHCP server.
device(config-zone-wlan)# dhcp-option-82-subopt	[1 2 150 151 mac-format]	Enables DHCP option 82 format options. Subopt-1 with format and select the option. The options are : <ul style="list-style-type: none"> ● AP-MAC ● AP-MAC ESSID ● AP-NAME ESSID Subopt-2 with format and select the option. The options are : <ul style="list-style-type: none"> ● Client-MAC ● AP-MAC ● AP-MAC ESSID ● AP-NAME Subopt -150 with VLAN-ID. Subopt -151 with AREA-NAME. Subopt -Mac format delimiter .
device(config-zone-wlan)# diffserv-profile	name	Sets the Diffserv profile.
device(config-zone-wlan)# directed-multicast		Sets the per-radio-client count at which an AP stops converting group addressed data traffic to unicast.
device(config-zone-wlan)# directed-threshold	number Directed threshold should range from 0 to 128	Sets the directed MC/BC threshold
device(config-zone-wlan)# disable-band-balancing		Disables radio band balancing on WLAN.
device(config-zone-wlan)# disable-load-balancing		Disables client load balancing on WLAN.
device(config-zone-wlan)# disable-wlan		Disables this WLAN service.

TABLE 74 Commands related to device(config-zone-wlan) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-zone-wlan)# dnlk-limit		Sets the downlink rate limiting.
device(config-zone-wlan)# dns-server-profile		Sets the DNS server profile.
device(config-zone-wlan)# dp-tunnel-nat		Enables the DP tunnel NAT server.
device(config-zone-wlan)# dpsk-effective-type		Sets the DPSK expiration effective type.
device(config-zone-wlan)# dpsk-expiration		Sets DPSK expiration.
device(config-zone-wlan)# dpsk-length	<i>number</i> : key length (8-62)	Sets the DPSK length. The range is 8-62.
device(config-zone-wlan)# dpsk-type		Sets the DPSK type.
device(config-zone-wlan)# drop-random-probes		Sets the option, drop random probes.
device(config-zone-wlan)# dtim-interval	<i>number</i> : DTIM interval must range from 1 to 255	Sets the frequency at which the Delivery Traffic Indication Message (DTIM) will be included in Beacon frames.
device(config-zone-wlan)# eap-acct-ip-attr-ignore		Accounting service - enables the attribute <i>ignore</i> for EAP Accounting IP address.
device(config-zone-wlan)# enable-rfc5580-support		Enables this attribute to deliver the location information only for those APs where location attribute is configured.
(config-zone-wlan)# enable-type		Enables the WLAN service type.
device(config-zone-wlan)# enc-algorithm		Sets the encryption algorithm.
device(config-zone-wlan)# enc-method		Sets the encryption method.
device(config-zone-wlan)# enc-mfp		Sets the MFP.
device(config-zone-wlan)# enc-passphrase	<i>password</i>	Sets the encryption passphrase.
device(config-zone-wlan)# enc-wep-key	<i>wep-key-index wep-key</i> WEP key (HEX), length should be 10 (WEP-64) or 26 (WEP-128)	Sets WEP key (HEX).
device(config-zone-wlan)# external-nas		Enables the external NAS IP address.
device(config-zone-wlan)# flow-log		Enables the flow log.
device(config-zone-wlan)# force-dhcp	timeout seconds timeout : Sets the disconnect client timeout interval seconds : Sets the disconnect client timeout in intervals of 5 - 15 seconds	Sets the timeout for DHCP in seconds.
device(config-zone-wlan)# forwarding-policy		Sets the forwarding policy configurations.
device(config-zone-wlan)# guest-access	<i>name</i>	Sets the guest access service.
device(config-zone-wlan)# guest-access-acct-service		Sets the accounting server.
device(config-zone-wlan)# guest-access-auth-service		Sets the authentication server.
device(config-zone-wlan)# hessid	<i>hessid</i>	Sets the WLAN HESSID value.
device(config-zone-wlan)# hide-ssid		Hides SSID in beacon broadcast.
device(config-zone-wlan)# hotspot	<i>name</i>	Sets the hotspot service.
device(config-zone-wlan)# hotspot2	<i>name</i>	Sets the hotspot 2.0 configuration.
device(config-zone-wlan)# hotspot20-osu-support		Enables the hotspot 2.0 device registration from the guest portal.
device(config-zone-wlan)# inactivity-timeout	<i>number</i>	Sets the inactivity timeout. Terminates idle user sessions after the specified seconds of inactivity.

TABLE 74 Commands related to device(config-zone-wlan) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-zone-wlan)#ipsec-profile	<i>\$ { value }</i>	Sets an IPSec profile (Soft GRE only).
device(config-zone-wlan)#join-accept-timeout	<number>: Sets the join expire time ranging from 1 to 300.	Sets the join expire time.
device(config-zone-wlan)#join-ignore-threshold	<number>: Sets the wait threshold ranging from 1 to 50.	Sets the wait threshold time.
device(config-zone-wlan)#join-ignore-timeout	<number>: Sets the wait time ranging from 1 to 60.	Sets the wait time.
device(config-zone-wlan)# l2-acl	[ACL Name]	Sets the layer 2 access control list.
device(config-zone-wlan)# mac-address-format		Sets the MAC address format.
device(config-zone-wlan)# mac-auth	<i>password</i>	Sets the MAC authentication.
device(config-zone-wlan)# max-clients	<i>number</i>	Sets the maximum clients. Allows clients per AP radio to associate with this WLAN. Range is between 1 and 512.
device(config-zone-wlan)# mgmt-tx-rate	[11mbps 1mbps 54mbps 24mbps 36mbps 12mbps 5.5mbps 9mbps 48mbps 2mbps 18mbps 6mbps]	Sets the management Tx rates.
device(config-zone-wlan)# mobility-domain-id	<i>number</i> : ID number (1-65535)	Sets the mobility domain identifier (for 802.11r).

TABLE 74 Commands related to device(config-zone-wlan) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-zone-wlan)# no	aaa-vlan-override access-network acct-delay-time acct-service acct-service-use-proxy acct-ttg-session auth-service-use-proxy app-visibility assoc-rssi-threshold auth-rssi-threshold auth-service-use-proxy bss-minrate bypass-cna calea client-fingerprinting client-tx-rx-statistics device-policy dgaf dhcp-option-82 dhcp-option-82-subopt diffserv-profile diffserv-profile directed-multicast disable-band-balancing disable-load-balancing disable-wlan dnlink-limit dns-server-profile dp-tunnel-nat drop-random-probes	Disables or deletes the configuration settings.

TABLE 74 Commands related to device(config-zone-wlan) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-zone-wlan)# no	eap-acct-ip-attr-ignore enable-rfc5580-support external-nas flow-log force-dhcp hessid hide-ssid hotspot20-osu-support ipsec-profile l2-acl mac-auth ofdm-only (Orthogonal Frequency Division Multiplexing) okc-support onboarding-auth-service onboarding-auth-service-use-proxy pmk-caching-support probe-rssi-threshold proxy-arp qos-map-enable roam single-session-id-acct split-tunnel-profile ssid-rate-limiting support-802-11d support-802-11k support-802-11r transient-client-mgmt uplink-limit user-traffic-profile venue-code vlan-enabled vlan-pooling wireless-client-isolation wireless-client-isolation-whitelist zero-it-activation zero-it-onboarding	Disables or deletes the configuration settings.

TABLE 74 Commands related to device(config-zone-wlan) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-domain-zone-wlan)# ofdm-only		Enables OFDM (Orthogonal Frequency Division Multiplexing) rates.
device(config-zone-wlan)# okc-support		Enables OKC support.
device(config-zone-wlan)# onboarding-auth-service	<i>service-name</i> local realm <i>service-name</i> remote realm <i>service-name</i> local realm never <i>service-name</i> local realm hour expiration-value: Expiration value between 1 and 175200. <i>service-name</i> local realm day expiration-value: Expiration value between 1 and 7300. <i>service-name</i> local realm week expiration-value: Expiration value between 1 and 1040. <i>service-name</i> local realm month expiration-value - Expiration value between 1 and 240.	Sets the onboarding authentication service.
device(config-zone-wlan)# onboarding-auth-service-use-proxy		Sets the onboarding authentication service using the controller proxy server.
device(config-zone-wlan)# onboarding-portal	<i>name</i>	Sets the onboarding portal.
device(config-zone-wlan)# operator-realm		Sets the operator realm.
device(config-zone-wlan)# pmk-caching-support		Enables the PMK caching support.
device(config-zone-wlan)# priority		Sets the priority as either low or high.
device(config-zone-wlan)# probe-rssi-threshold		Probes the RSSI threshold.
device(config-zone-wlan)# proxy-arp		Enables proxy ARP.
device(config-zone-wlan)# qos-map	<i>priority</i>	Updates the QoS map.
device(config-zone-wlan)# qos-map-enable		Enables the QoS map.
device(config-zone-wlan)# radius-nas-id	<i>number</i>	Sets the RADIUS NAS ID.
device(config-zone-wlan)# radius-nas-ip	<i>ip</i>	Sets the RADIUS NAS IP address.
device(config-zone-wlan)# radius-nas-ip-type	[<i>sz-mgmt-ip</i> disabled <i>user</i> <i>sz-control-ip</i>]	Sets the RADIUS NAS IP type.
device(config-zone-wlan)# radius-nas-max-retries	<i>times</i>	Sets the maximum number of retries for RADIUS NAS.
device(config-zone-wlan)# radius-nas-reconnect-primary	<i>minutes</i>	Sets the reconnection to the primary RADIUS NAS.
device(config-zone-wlan)# radius-nas-request-timeout	<i>seconds</i>	Sets the RADIUS NAS request timeout.
device(config-zone-wlan)# radius-nas-type		Sets the RADIUS NAS type.
device(config-zone-wlan)# roam		Enables roaming.
device(config-zone-wlan)# roam-factor	2.4g value 5g value	Sets the roam factor.
device(config-zone-wlan)# scheduler	[<i>Profile Name</i>]	Sets the WLAN scheduler profile.
device(config-zone-wlan)# single-session-id-acct		Enables Single Session ID Accounting.
device(config-zone-wlan)# split-tunnel-profile	<i>\${value}</i>	Sets a split tunnel profile.
device(config-zone-wlan)# ssid	<i>ssid</i>	Sets the WLAN SSID configuration.
device(config-zone-wlan)# ssid-rate-limiting	<i>uplinkdownlink</i>	Sets the SSID rate limit as either uplink or downlink with the range 1-200 mbps.
device(config-zone-wlan)# support-802-11d		Enables support for 802.11d.

TABLE 74 Commands related to device(config-zone-wlan) (continued)

Syntax and Type	Parameters (if any)	Description
device(config-zone-wlan)# support-802-11k		Enables support for 802.11k neighbor reports.
device(config-zone-wlan)# support-802-11r		Enables 802.11r fast BSS transition.
device(config-zone-wlan)# transient-client-mgmt		Sets the transient client management.
device(config-zone-wlan)# tunnel-profile	<i>value</i>	Sets the GRE tunnel profile.
device(config-zone-wlan)# uplink-limit		Sets the uplink rate limiting.
device(config-zone-wlan)# user-traffic-profile		Sets the user traffic profile.
device(config-zone-wlan)# venue-code		Enables venue code.
device(config-zone-wlan)# vlan-enabled		Enables dynamic VLAN.
device(config-zone-wlan)# vlan-id	<i>vlan-id</i>	Sets the VLAN ID.
device(config-zone-wlan)# vlan-pooling	<i>name</i>	Enables and sets the VLAN pooling profile.
device(config-zone-wlan)# web-authentication	<i>name</i>	Sets the web authentication service.
device(config-zone-wlan)# wechat	<i>name</i>	Sets the WeChat services.
device(config-zone-wlan)# wireless-client-isolation		Sets the wireless client Isolation.
device(config-zone-wlan)# wireless-client-isolation-whitelist	<i>whitelist name</i>	Sets the wireless client Isolation whitelist. The whitelist can only contain wired destinations. Wireless clients are not supported on the whitelist.
device(config-zone-wlan)# zero-it-activation		Enables zero-it activation (WLAN users are provided with wireless configuration installer after they log in).
device(config-zone-wlan)# zero-it-onboarding		Enables zero-it device registration from the guest portal.

TABLE 75 Commands related to device(config-zone-wlan-group).

Syntax and Type	Parameters (if any)	Description
device(config-zone-wlan-group)# description	<i>text</i>	Sets the description,
device(config-zone-wlan-group)# no	wlanname	Disables or removes WLAN from this group.
device(config-zone-wlan-group)# wlan	<i>namevlanvlanTagnasidnasid namenasidnasidvlanvlanTag namevlanvlanTag namenasidnasid namevlan-poolingvlanPooling namevlan-poolingvlanPoolingnasid name</i>	Sets a WLAN in this group or overrides VLAN setting.

TABLE 76 Commands related to device(config-zone-wlan-qos-map)

Syntax and Type	Parameters (if any)	Description
device(config-zone-wlan-qos-map)# dscp-range	<i>dscp-low-value dscp-high-value</i>	Sets the range as either high or low values for DSCP.
device(config-zone-wlan-qos-map)# enable		Enables the QoS map setting.

TABLE 76 Commands related to device(config-zone-wlan-qos-map) (continued)

Syntax and Type	Parameters (if any)	Description
ruckus(config-zone-wlan-qos-map)# excp-dscp-values Type: Privileged		Sets the exception values for DSCP.
device(config-zone-wlan-qos-map)# no	enable excp-dscp-values	Disables the commands.

TABLE 77 Commands related to ruckus (config-zone-wlan-scheduler)

Syntax and Type	Parameters (if any)	Description
device(config-zone-wlan-scheduler)# description	text	Sets the description,
device(config-zone-wlan-scheduler)# no	description schedule-data [weekday empty] [start time value empty] [end time value] \$ {weekday}	Disables the commands.
device(config-zone-wlan-scheduler)# schedule-data	[weekday empty][start time value empty][end time value] \${weekday}	Sets the schedule table.

Examples

The following example creates an AP zone and changes the AP firmware for that zone to be version 5.2.1.0.400.

```
device# config
device(config)# zone zone-discovery ap-firmware 5.2.1.0.400
device(config-zone)#
```

The following example deletes a zone named zone-discovery.

```
device# config
device(config)# no zone zone-discovery
Do you want to continue to delete (or input 'no' to cancel)? [yes/no] yes
Operation successful
```

The following example deletes the profile of a blocked client with the MAC address 84:18:3A:39:C8:50.

```
device# config
device(config)# no block-client 84:18:3A:39:C8:50
```

zone-template

Creates or updates zone template configurations.

Syntax

zone-template*template-name*[**export***ftp-url* | **extract***zone-name*]

zone-template**import***ftp-url*

no zone-template*template-name*

Command Default

No zone templates are created or updated.

Parameters

template-name

AP zone template name.

export

Exports an AP zone template to an FTP server.

ftp-url

FTP URL, format: *ftp://username:password@ftp-host/file-path*

extract

Extracts an AP zone template from an existing AP zone.

zone-name

AP zone name.

import

Imports an AP zone template from an FTP server.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command deletes a zone template.

Examples

The following example creates a new zone template named *acct-profile*.

```
device# config
device(config)# zone-template acct-profile
```

Commands Si - Z

zone-template

The following example imports a zone template from the FTP server named ftp1.

```
device# config
device(config)# zone-template import ftp://myname:pwd@ftp1/z://import/zone-templates
```



© 2023 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
<https://www.commscope.com>