



ExtremeWireless[™] CLI Reference Guide

Release V10.11.02

Copyright © 2016 Extreme Networks, Inc. All rights reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:

www.extremenetworks.com/company/legal/trademarks

Support

For product support, including documentation, visit: <http://www.extremenetworks.com/support/>

For information, contact:

Extreme Networks, Inc.

145 Rio Robles

San Jose, California 95134

USA

Table of Contents

Preface.....	8
Text Conventions.....	8
Providing Feedback to Us.....	8
Getting Help.....	9
Related Publications.....	9
Chapter 1: About This Guide.....	11
Who Should Use This Guide.....	11
How to Use This Guide.....	11
Chapter 2: Introduction to the CLI.....	13
CLI Wizard.....	13
CLI Structure.....	18
Account Types.....	19
Chapter 3: Common Commands.....	21
apply.....	21
end.....	21
exit.....	22
help.....	22
logout.....	23
no.....	24
show.....	24
Chapter 4: root Commands.....	25
audit.....	28
availability.....	28
backup.....	31
no backup.....	31
copy.....	31
host-attributes.....	34
export.....	36
no export.....	37
flash.....	38
no flash.....	38
healthpoll.....	38
import.....	39
key.....	39
lanset.....	41
loglevel.....	42
ping.....	43
radtest.....	44
radtest_mba.....	45
reset.....	45
restart.....	46
restore.....	46
secureconnection.....	47
show.....	47
shutdown.....	86

tech_support.....	87
traceroute.....	88
upgrade ac.....	89
upgrade apup.....	91
upgrade_backup_dest.....	91
upgrade_image_src.....	92
Chapter 5: ap Commands.....	93
ap Context.....	93
Radio Commands.....	140
DCS Commands.....	158
logs.....	163
maintain_cycle.....	165
Chapter 6: I2ports Commands.....	168
esaN.....	168
jumbo-frames.....	168
portN.....	169
show.....	170
<named-LAG-port>.....	170
Chapter 7: ip Commands.....	172
route.....	172
ospf.....	173
Chapter 8: login Commands.....	180
apply.....	180
auth.....	181
auth-order.....	183
move.....	184
show.....	185
Chapter 9: Radar Commands.....	186
mitigator Context.....	186
Common Scan /Profile Commands.....	193
Chapter 10: mobility Commands.....	203
backupmanagerip.....	203
mrole.....	204
mport.....	204
mheartbeat.....	205
slpreg.....	205
agent.....	205
secmode.....	206
mdismethod.....	206
mmanagerip.....	207
Chapter 11: schedule_backup Commands.....	208
destination.....	209
dir.....	209
freq.....	209
password.....	210
protocol.....	211

server.....	211
starttime.....	211
type.....	212
user.....	212
Chapter 12: schedule_upgrade Commands.....	214
schld_upgrd.....	214
upgrade_backup.....	215
Chapter 13: snmp Commands.....	217
contact	218
context.....	218
enable	218
engine-id.....	219
location.....	219
port.....	220
publish-ap.....	220
rcommunity.....	221
rwcommunity.....	221
severity.....	221
show.....	222
trap-manager-v1v2.....	222
trap-manager-v3.....	223
user.....	223
Chapter 14: syslog Commands.....	225
audmsg.....	225
facility.....	226
stationevents.....	226
svcmmsg.....	227
syslogip.....	227
Chapter 15: time Commands.....	229
clock.....	229
date.....	230
ntp.....	230
ntpip.....	230
tz.....	231
Chapter 16: traffic_capture Commands.....	232
file_name.....	232
size.....	233
interface.....	233
delete.....	234
list.....	234
start.....	235
stop.....	235
show.....	235
show interfaces.....	236
Chapter 17: users Commands.....	237
id.....	237
pwd.....	238

Chapter 18: VNS Commands (vnsmode)	239
adminctr	240
create	247
custom-app	247
das	249
default-role	249
delete	252
nac	252
netflow-mirror	254
radius	255
rateprofile	268
redirection-url-list	270
<named-VNS>	271
Common Filter Configuration Commands	274
Chapter 19: wlans Commands	282
clients	282
create	286
delete	287
remote-ssid	287
show	287
<WLAN-service-name>	289
hotspot	346
Chapter 20: role Commands	368
role Context	368
create	369
delete	369
show	370
<named-role>	370
Common Filter Configuration Commands	379
Chapter 21: topology Commands	387
create	387
delete	388
internal-vlanid	389
multicast-support	389
show	390
<named-topology>	390
topology-group	418
Chapter 22: Location-Based-Service (lbs) Commands	423
multicast	423
port	424
service	424
server-ip	425
show	425
Related commands	426
Chapter 23: web Commands	427
guestportal-admin-timeout	427
timeout	428

showvns.....	428
show.....	429
Chapter 24: cos Commands.....	430
create.....	430
delete.....	431
show.....	431
<named-cos>.....	432
Chapter 25: site Commands.....	438
create.....	438
delete.....	439
show site.....	439
<named-site>.....	439
Chapter 26: RF Location Commands.....	454
location-engine.....	454
default-height.....	455
auto-tracking.....	455
default-env-mode.....	456
floor-plan.....	456
on-demand.....	458
publish.....	458
show.....	459
area-tracking.....	459
Chapter 27: Publish Commands.....	461
push.....	461
interval.....	462
unit.....	462
push-list.....	462
push-client-reporting.....	463

Preface

Text Conventions

The following tables list text conventions that are used throughout this guide.

Table 1: Notice Icons






Icon	Notice Type	Alerts you to...
	General Notice	Helpful tips and notices for using the product.
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.
	New	This command or section is new for this release.

Table 2: Text Conventions

Convention	Description
Screen displays	This typeface indicates command syntax, or represents information as it appears on the screen.
The words enter and type	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
[Key] names	Key names are written with brackets, such as [Return] or [Esc] . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del]
<i>Words in italicized type</i>	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short [online feedback form](#). You can also email us directly at internalinfodev@extremenetworks.com.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

- **Global Technical Assistance Center (GTAC) for Immediate Support**
 - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
 - **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- **GTAC Knowledge** — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- **The Hub** — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- **Support Portal** — Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related Return Material Authorization (RMA) numbers

Related Publications

ExtremeWireless and ExtremeWireless AP documentation can be found on Extreme Documentation page at: <http://documentation.extremenetworks.com>

Extreme recommends the following guides for users of ExtremeWireless products:

- *ExtremeWireless AP3935i & AP3935e Installation Guide*
- *ExtremeWireless AP3965i & AP3965e Installation Guide*
- *ExtremeWireless Appliance C5210 Quick Reference*
- *ExtremeWireless Appliance C5110 Quick Reference*
- *ExtremeWireless Appliance C4110 Quick Reference*
- *ExtremeWireless Appliance C25 Quick Reference*
- *ExtremeWireless Appliance C35 Quick Reference*

- *ExtremeWireless CLI Reference Guide*
- *ExtremeWireless End User License Agreements*
- *ExtremeWireless External Antenna Site Preparation and Installation Guide*
- *ExtremeWireless External Antenna with Wave 2 Site Preparation and Installation Guide*
- *ExtremeWireless Getting Started Guide*
- *ExtremeWireless Integration Guide*
- *ExtremeWireless Maintenance Guide*
- *ExtremeWireless Open Source Declaration*
- *ExtremeWireless User Guide*
- *IdentiFi Wireless WS-AP3865e Installation Guide*
- *IdentiFi Wireless WS-AP3825i & WS-AP3825e Installation Guide*
- *IdentiFi Wireless WS-AP3805i & WS-AP3805e Installation Guide*

1 About This Guide

Who Should Use This Guide How to Use This Guide

The Command Line Interface (CLI) is used to configure the ExtremeWireless Appliance. It is accessible directly on the controller's console port, or via Secure Shell (SSH) access on the ESA or Management ports.

Who Should Use This Guide

This guide is intended for system test, network administrators, and development engineers who understand all components of the ExtremeWireless.

How to Use This Guide

This guide contains the following chapters

- [Introduction to the CLI](#) on page 13 describes the overall context structure of the CLI.
- [Common Commands](#) on page 21 describes commands that appear within every context level of the CLI.
- [root Commands](#) on page 25 describes commands available from the root context of the Wireless Appliance.
- [ap Commands](#) on page 93 describes commands that manage the functions of Wireless APs on a system using the Wireless Appliance.
- [l2ports Commands](#) on page 168 describes commands to enable and disable L2 ports on the Wireless Controller.
- [ip Commands](#) on page 172 describes commands to configure routing information.
- [login Commands](#) on page 180 describes commands to configure the login authentication modes — local authentication and RADIUS-based authentication.
- [Radar Commands](#) on page 186 describes configurable options for the detection of rogue Access Points, DoS attacks, and other potential network intrusion events.
- [mobility Commands](#) on page 203 describes commands to manage the exchange of client session information across a network.
- [schedule_backup Commands](#) on page 208 describes commands to schedule data backups.
- [schedule_upgrade Commands](#) on page 214 describes commands to configure scheduling an upgrade and back up of the controller's software.
- [snmp Commands](#) on page 217 describes commands to manage Simple Network Management Protocol (SNMP) settings for the Wireless Appliance.
- [syslog Commands](#) on page 225 describes commands to configure System Log settings.
- [time Commands](#) on page 229 describes commands to set the system time for the Wireless Appliance, and configure network time protocol options.

- [traffic_capture Commands](#) on page 232 describes commands to manage the TCPDump.
- [users Commands](#) on page 237 describes commands used to manage user accounts on the network.
- [VNS Commands \(vnsmode\)](#) on page 239 VNS Commands (vnsmode), describes commands for the setup of virtual network services (VNS) for the network.
- [wlans Commands](#) on page 282 describes commands used to define and configure WLAN services for the network.
- [role Commands](#) on page 368 describes commands used to define and configure policies for the Wireless Appliance.
- [topology Commands](#) on page 387 describes commands used to define and configure topology objects used by policy and VNS objects.
- [Location-Based-Service \(lbs\) Commands](#) on page 423 describes commands used to configure the Wireless APs for use with an AeroScout or Ekahau location-based service.
- [web Commands](#) on page 427 describes commands used to configure the web settings.
- [cos Commands](#) on page 430 describes commands for configuring Classes of Service that can be applied to policies.
- [site Commands](#) on page 438 describes commands for configuring sites that have their own local authentication server defined.
- [RF Location Commands](#) on page 454 describes commands used to enable and configure the Radio Frequency (RF) Location engine on a Wireless Appliance to determine location and perform tracking on wireless mobile users through Wireless APs.
- [Publish Commands](#) on page 461 describes commands used in the publish context.

Keyboard Shortcuts

There are several keyboard shortcuts available to assist in navigating within the contexts of the CLI.

- To display options within a context or to complete partial entries of commands at the prompt, use **[CTRL] + I**, **[Tab]**, or the **[?]** key.
- To transpose mi--typed characters at the command prompt, use **[CTRL] + T**.
- To recall previous commands executed for the session, use the UP arrow.
- To cycle forward through previously executed commands, use the DOWN arrow.

2 Introduction to the CLI

CLI Wizard
CLI Structure
Account Types

The commands of the CLI are structured in a hierarchical set of contexts. Each context contains commands which relate to a specific type of function. For example, the radio1 context is a set of commands available for configuring operational parameters on the Radio1 radio of an access point. To configure default Radio1 parameters for AP3710s, you must move down from the root context through the ap, default, ap37xx, radio1 contexts (ap:defaults:ap37xx:radio1) to reach, set, and apply those parameters. To configure Radio1 parameters for a specific access point for which you know the ID (serial number), move down from the root context through the ap, <serial>, and radio1 contexts (ap:0409920200000000:radio1).

CLI Wizard

The CLI wizard is designed to configure administrative settings on the controller. The CLI wizard begins automatically when a user with administrative access logs into the controller for the first time or when the system has been reset to the factory default. Instructions display when the wizard starts. Each screen in the wizard presents the default response in square brackets []. Simply press **Enter** to accept the default response. You can exit the wizard by pressing **[CTRL] + [C]**.

Take the following steps to configure the controller through the CLI wizard:

- 1 Press **Enter** to begin.
- 2 Change the admin password on the account?
 - Press **Enter** to change the password, or
 - Type **n** and press **Enter** to keep the default password.

When changing the password:

- The password must be 8-24 characters.
- Do not use special characters ` ' " \ : or blank characters

Retype the new password and press **Enter** to accept the changes.

3 Change AP access password?

**Note**

For the initial configuration, you must change the factory default AP password.

- Press **Enter** to change the AP access password.

The Secure Shell (SSH) password must be 5 to 30 alpha numeric and can include special characters [.-_ space].

Retype the new password and press **Enter** to accept the changes.

- If this is not the initial configuration, you have the option to accept the existing AP access password. Type **n** and press **Enter** to accept the existing password.

4 Change port Physical 1 settings?

- Press **Enter** to change settings on port Physical 1, or
- Type **n** and press **Enter** to accept all default settings.

When modifying Physical 1 port settings:

- Type an IP address and press **Enter** or press **Enter** to accept the default IP address value.
- Type a netmask value and press **Enter** or press **Enter** to accept the default netmask value.
- Type a VLAN ID and press **Enter** or press **Enter** to accept the default VLAN ID value.

5 Will the interface transmit tagged frames?

- Press **Enter** for No, or
- Type **y** and press **Enter** for Yes.

6 Would you like to enable management?

- Press **Enter** for Yes, or
- Type **n** and press **Enter** for No.

7 Would you like to enable AP registration?

- Press **Enter** for Yes, or
- Type **n** and press **Enter** for No.

A summary of configured Data Plane Settings is displayed. Press **Enter** to accept the settings or type **n** and press **Enter** to reconfigure the Data Plane Settings.

8 Would you like to change the host attributes?

- Press **Enter** for Yes, or
- Type **n** and press **Enter** for No.

When modifying host attributes:

- Type the host name for the appliance and press **Enter**, or press **Enter** to accept EWC.
- Type the IP address for the Admin Port and press **Enter**, or press **Enter** to accept the default IP address value.
- Type the IP netmask for the Admin Port and press **Enter**, or press **Enter** to accept the default netmask value.

9 Do you want to have a name server? (Primary DNS)

- Press **Enter** for Yes, and enter an IP address for the name server, or
- Type **n** and press **Enter** for No. Go to [step 11](#).

- 10 Do you want to have a secondary name server? (Secondary DNS)
- Press **Enter** for No, or
 - Type **y** and press **Enter** for Yes. Then, enter an IP address for the name server.
- 11 Enter the domain name for the appliance.
- Press **Enter** to accept the default domain name for the appliance.
 - Enter a unique domain name and press enter.
- 12 Would you like to configure a global default gateway?
- Press **Enter** to configure a global default gateway, and enter the global default gateway IP address, or
 - Type **n** and press **Enter** for No.

A summary of host attribute settings is displayed. Press **Enter** to accept the settings, or type **n** and press enter to reconfigure the host attribute settings.

- 13 Would you like to enable SNMP?
- Press **Enter** for Yes, or
 - Type **n** and press **Enter** for No.

When enabling SNMP:

- Type the SNMP3 account user name and press **Enter**, or press **Enter** to accept the default user name.
- Type the authentication password (8-32 characters) and press **Enter**, or press **Enter** to accept the default authentication password.
- Enter a privacy password (8-32 characters) and press **Enter**, or press **Enter** to accept the default privacy password.

A summary of SNMP settings is displayed. Press **Enter** to accept the settings or type **n** and press **Enter** to reconfigure the SNMP settings.

- 14 Change time settings?
- Press **Enter** to change time settings, or
 - Type **n** and press **Enter** to accept default time settings.
- a Change time zone?
- Press **Enter** to change time zone, or
 - Type **n** and press **Enter** to accept default settings.

To change time zone:

- 1 Enter the continent code. See [Table 3: Continent Codes for Time Settings](#) on page 16. For continents with multiple zones, the first letter of the city is in parentheses.
- 2 Enter a country code or city code where applicable. See [Table 4: Country and City Codes for Time Settings](#) on page 16.



Note

The ExtremeWireless graphical user interface (GUI) offers valid time zone options that you can select from drop list fields. Consider using the GUI to configure time zones. For more information, see the *Wireless User Guide*.

Table 3: Continent Codes for Time Settings

Continent	Code
Africa (A-J)	0
Africa (K-W)	1
America (A-A)	2
America (B-D)	3
America (E-I)	4
America (J-M)	5
America (N-R)	6
America (S-Y)	7
Antarctica	8
Arctic	9
Asia (A-G)	10
Asia (H-O)	11
Asia (P-V)	12
Asia (Y-Y)	13
Atlantic	14
Australia	15
Europe (A-L)	16
Europe (M-U)	17
Europe (V-Z)	18
Indian (V-Z)	19
Pacific (A-N)	20
Pacific (P-W)	21

Table 4: Country and City Codes for Time Settings

Country/City	Code
Nassau	0
New York	1
Nipigon	2
Nome	3
Noronha	4
North Dakota/Center	5
North Dakota/New Salem	6
Panama	7
Pangnirtung	8

Table 4: Country and City Codes for Time Settings (continued)

Country/City	Code
Paramaribo	9
Phoenix	10
Port-au-Prince	11
Port of Spain	12
Porto_Velho	13
Puerto-Rico	14
Rainy-River	15
Rankin_Inlet	16
Recife	17
Regina	18
Resolute	19
Rio_Branco	20
America/Montreal	21

- b Change time?
- 1 Press **Enter** for No, or
 - 2 Type **y** and press **Enter** for Yes. Then, enter a date and time in format (mm-dd-yyyy hh:mm) and press **Enter**. The time is in 24-hour format.
- c Run NTP as a client?
- Press **Enter** for Yes, or
 - Type **n** and press **Enter** for No.

If running NTP as a client, enter the fully qualified domain name or IP address of the NTP server.

- d Enter a second NTP server?
- Press **Enter** for No.
 - Type **y** and press **Enter** for Yes.

If entering a second NTP server, enter the fully qualified domain name or IP address of the NTP server.

You can configure up to three NTP servers.

- e Make this controller an NTP server?
- Press **Enter** for No.
 - Type **y** and press **Enter** for Yes.

A summary of Time Settings is displayed. Press **Enter** to accept the settings or type **n** and press **Enter** to reconfigure the Time Settings.

- 15 The Controller Post Configuration options appear. Review the full configuration. To return to a portion of the configuration wizard, enter the number that corresponds to that portion of the configuration wizard. To save and exit, press **Enter**.

**Note**

If you exit the wizard without saving changes, the wizard will run the next time you access the controller.

- **1** - Return to the Change Admin Password screen from which you can change the administrator's password.
- **2** - Return to the Change AP Password screen from which you can change the AP access password.
- **3** - Return to the Data Plane Settings screen from which you can change the settings for physical ports on the controller.
- **4** - Return to the Host Attribute Settings screen from which you can change the host attributes for the controller.
- **5** - Return to the Current SNMP Settings screen from which you can change the SNMP settings for the controller.
- **6** - Return to the Time Settings screen from which you can change the date and time settings and configure NTP servers.
- **7** - Save your changes and exit the wizard.
- **8** - Exit the wizard without saving your changes.

The wizard is complete. This guide provides information about individual commands available in the CLI. For additional information about configuration and setup information for both the wireless controller and APs, refer to the *Wireless User Guide*.

CLI Structure

The following diagram shows the root context. Many of the commands move to a context (ap, topology) and some are commands that perform a system function (export, login). This kind of structure applies at every context level.

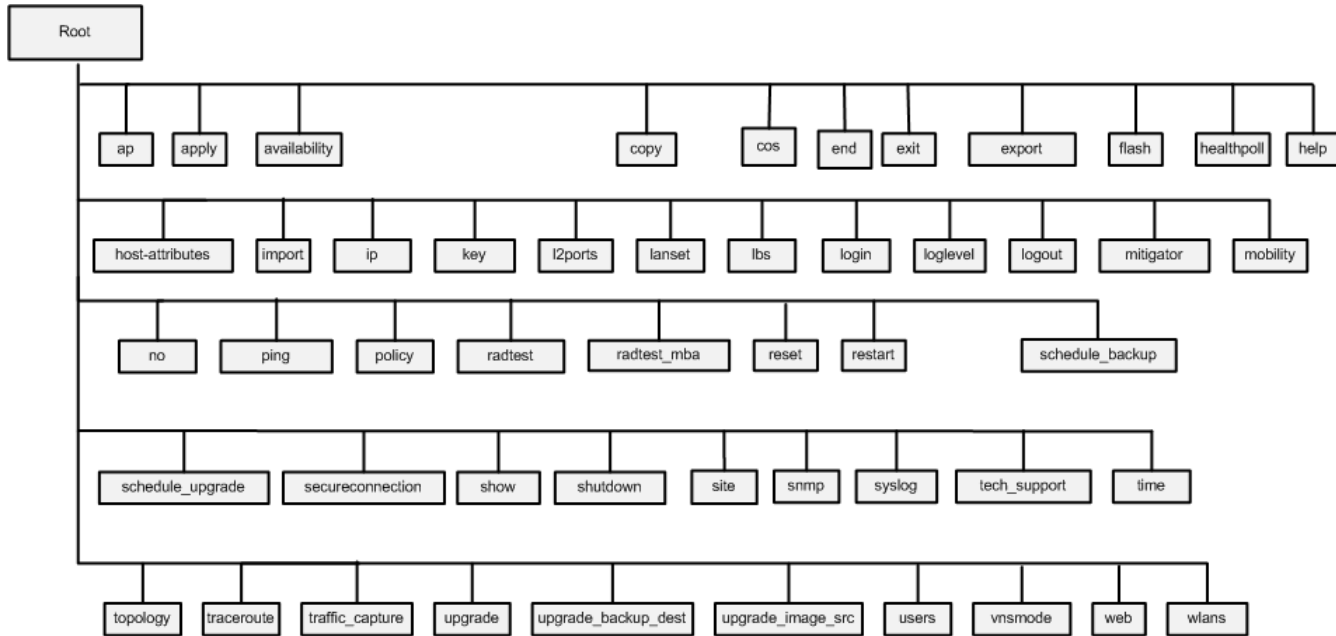


Figure 1: CLI Root Structure

Account Types

Access to the CLI varies for two account types: "admin" and "user". The admin account provides administrator access to all the contexts and features in the CLI, while the user account provides no access to contexts and command availability is limited.

The following example displays commands available in the root context for the admin account type.

```

EWC.extremenetworks.com# help
Available commands are:
ap                Modify Access Point settings
availability      Modify availability settings
copy             Transfer files between the controller and an
external server.
cos              Configure Controller cos settings
end              Return to the base mode
exit             Return to the previous mode
export           Export Controller data to a file
flash           Mount/Unmount flash drive
healthpoll      Set healthpoll timeout
host-attributes  Configure Controller host attributes settings
import          Restore Controller data/configuration from
file
ip              Modify controller route
key             Modify License Keys
l2ports         Configure Controller L2 Ports settings
lanset          Set Ethernet link parameters
lbs             Modify settings for AP location based service.
login           Configure login settings.
loglevel        Set a log level
logout          Logout
mitigator       Modify Mitigator settings to assist in
  
```

detection of rogue AP	
mobility	Modify access controller mobility settings
no	Clear the command setting
ping	Ping a host or gateway.
policy	Configure Controller policy settings
radtest	Test Radius Server connectivity, Caotive authentication
Portal and EAP	
radtest_mba	Test Radius Server connectivity and MAC-based
authorization	
reset	Reset database configuration
restart	Restart a process
schedule_backup	Modify backup schedule.
schedule_upgrade	Scheduled upgrade
secureconnection	Modify access controller secure connection
settings	
show	Display settings
shutdown	Used to safely halt or reboot the controller
site	Configure site settings
snmp	Configure SNMP settings
syslog	Change syslog settings
tech_support	Collect tech support data
time	Configure network time for the Controller
topology	Configure Controller topology settings
traceroute	Traceroute a host or gateway.
traffic_capture	Traffic capture on interface
upgrade	Utility for upgrading AC software (AC), or AP
software (APUP)	
upgrade_backup_dest	Set ftp parameters for full disk clone backup
upgrade_image_src	Set location of upgrade image, if remote
upgrade is being	performed
users	Change Controller user settings
vnsmode	Modify Controller VNS(Virtual Network
Segment) settings	
web	Modify web settings
wlans	Configure WLAN Service settings

3 Common Commands

```
apply
end
exit
help
logout
no
show
```

The following commands are used universally throughout the CLI shell.

apply

Use the `apply` command, after a command or a series of commands have been executed, for the configuration of the Wireless Appliance to take affect. Unless otherwise noted, run the `apply` command for configuration changes to take effect.

apply

Parameters

None

Examples

The following example disables the DNS server configuration.

```
EWC.extremenetworks.com.com:dns# no dns 192.1.1.3
EWC.extremenetworks.com.com:dns# apply
```

end

Use the `end` command to return to the base context.

end

Parameters

None

Examples

The following example returns you to the base context from the ap:defaults context.

```
EWC.extremenetworks.com:ap:defaults# end
EWC.extremenetworks.com#
```

exit

Use the `exit` command to return to the previous context, or to exit the shell if you are in the base context.

exit

Parameters

None

Examples

The following example exits a context and moves up one level to the previous context.

```
EWC.extremenetworks.com:policy:p1# exit
EWC.extremenetworks.com:policy#
```

The following example exits the shell from the base context.

```
EWC.extremenetworks.com# exit
```

help

Use the `help` command to display available commands in a context, or obtain usage information for a specified command.

help *help command*

Parameters

<i>command</i>	Specifies the command for which you need usage information.
----------------	---

Examples

The following example displays the available commands in the ap:defaults context:

```
EWC.extremenetworks.com:ap:defaults# help
Available commands are:
3935FCC                Modify 3935FCC ap defaults settings
ap37xx                 Modify ap37xx and W78xC ap defaults settings
ap3801                 Modify ap3801 ap defaults settings
ap38xx                 Modify ap38xx ap defaults settings
apply                  Commit AP default changes.
assign                 Modify AP default VNS assignment settings
```

```

end
exit
learnac          Enable/disable learn on the AP.
logout
no              Clear the command setting
show           Display settings

```

The following example displays the usage information for the serial command:

```

EWC.extremenetworks.com:ap:# help serial
Create a new AP entry
Usage: serial <ap serial number> <name> <hardware type> <ap_role>
[<description>]
Usage: no serial <serial#>
<hardware type> is one of:
  AP3705i (Wireless AP3705i Internal)
  AP3710e (Wireless AP3710e External)
  AP3710i (Wireless AP3710i Internal)
  AP3715e (Wireless AP3715e External)
  AP3715i (Wireless AP3715i Internal)
  AP3715i-1 (Wireless AP3715i-1 Internal)
  AP3765e (Wireless AP3765e External)
  AP3765i (Wireless AP3765i Internal)
  AP3767e (Wireless AP3767e External)
  AP3801i (Wireless AP3801i Internal)
  AP3805e (Wireless AP3805e External)
  AP3805i (Wireless AP3805i Internal)
  AP3825e (Wireless AP3825e External)
  AP3825i (Wireless AP3825i Internal)
  AP3865e (Wireless AP3865e External)
  AP3935e-FCC (Wireless AP3935e-FCC External)
  AP3935i-FCC (Wireless AP3935i-FCC Internal)

```

logout

Use the `logout` command to exit the shell immediately.

logout

Parameters

None

Examples

The following example exits the shell:

```

EWC.extremenetworks.com:topology:Admin:l3# logout

```

no

Use the `no` option to disable a function of a command. Use the command's syntax without the `no` form to enable it. The `no` option can also be used to delete settings or files when used with certain commands. Not all commands within the CLI include a `no` option.

Syntax

`no`

Parameters

None

Examples

The following example configures and displays a gateway IP address, then disables it with the `no` command and displays the change.

```
EWC.extremenetworks.com:topology:Admin:13# gateway 192.176.3.4
EWC.extremenetworks.com:topology:Admin:13# show gateway
gateway 192.176.3.4
EWC.extremenetworks.com:topology:Admin:13# no gateway
EWC.extremenetworks.com:topology:Admin:13# show gateway
no gateway
```

show

Use the `show` command to display the current configuration within a context.

`show`

Parameters

None

Examples

The following example displays the DNS configuration.

```
EWC.extremenetworks.com:dns# show
dns 1 192.1.1.3
dns 2 192.1.2.3
dns 3 192.1.3.3
```


4 root Commands

```
audit
availability
backup
no backup
copy
host-attributes
export
no export
flash
no flash
healthpoll
import
key
lanset
loglevel
ping
radtest
radtest_mba
reset
restart
restore
secureconnection
show
shutdown
tech_support
traceroute
upgrade ac
upgrade apup
upgrade_backup_dest
upgrade_image_src
```

The root context of the CLI displays available commands relating to the Wireless Appliance's configuration, as well as available sub-contexts.

All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

This chapter documents root context commands not associated with features documented in other chapters. See [Table 5: Root Commands Documented in Feature Chapters](#) on page 26 for a listing and description of root commands documented outside of this chapter.

The following commands are available in the root context:

- [availability](#) on page 28
- [copy](#) on page 31
- [host-attributes](#) on page 34
- [export](#) on page 36
- [no export](#) on page 37
- [flash](#) on page 38
- [no flash](#) on page 38
- [healthpoll](#) on page 38
- [import](#) on page 39
- [key](#) on page 39
- [lanset](#) on page 41
- [loglevel](#) on page 42
- [ping](#) on page 43
- [radtest](#) on page 44
- [radtest_mba](#) on page 45
- [reset](#) on page 45
- [restart](#) on page 46
- [secureconnection](#) on page 47
- [show](#) on page 47
- [shutdown](#) on page 86
- [tech_support](#) on page 87
- [traceroute](#) on page 88
- [upgrade ac](#) on page 89
- [upgrade apup](#) on page 91
- [upgrade_backup_dest](#) on page 91
- [upgrade_image_src](#) on page 92

Table 5: Root Commands Documented in Feature Chapters

Command	Description
ap	The <code>ap</code> command moves you to the ap context of the CLI, providing access to commands required to manage the basic functions of the Wireless APs on the system. See ap Commands on page 93.
cos	The <code>cos</code> command moves you to the cos context, where you can configure Class of Service (CoS) settings to be applied to policies. See cos Commands on page 430.
exit	The <code>exit</code> command returns to the previous context or exits the shell if you are in the base context. See exit on page 22.

Table 5: Root Commands Documented in Feature Chapters (continued)

Command	Description
ip	The <code>ip</code> command moves you to the ip context of the CLI, providing access to commands for the configuration of routing information. See ip Commands on page 172.
l2ports	The <code>l2ports</code> command moves you to the l2ports context of the CLI, providing access to commands for the enabling and disabling of ports. See l2ports Commands on page 168.
login	The <code>login</code> command moves you to the login context of the CLI, providing access to commands for the configuration of the login authentication modes. See login Commands on page 180.
logout	The <code>logout</code> command exits the shell immediately. See logout on page 23.
mitigator	The <code>mitigator</code> command moves you to the mitigator context of the CLI, providing commands that assist in the detection of network intrusion, including DoS attacks, rogue Access Points, and other forms of network intrusion. See Radar Commands on page 186.
mobility	The <code>mobility</code> command moves you to the mobility context of the CLI, providing commands that configure the sharing and exchanging of client session information, which enables a wireless device to roam between Wireless APs on different ExtremeWireless without service interruption. See mobility Commands on page 203.
policy	The <code>policy</code> command moves you to the policy context of the CLI, providing commands for the defining and configuring of policy for the ExtremeWireless. See role commands .
schedule_backup	The <code>schedule_backup</code> command moves you to the schedule_backup context of the CLI, providing commands for backup scheduling of software configurations, CDR, log, and audit. See schedule_backup Commands on page 208.
schedule_upgrade	The <code>schedule_upgrade</code> command moves you to the schedule_upgrade context of the CLI, providing commands for scheduling an upgrade and back up of the controller's software. See schedule_upgrade Commands on page 214.
site	The <code>site</code> command moves you to the site context of the CLI, providing commands for configuration of sites that can perform autonomous local authentication. See site Commands on page 438.
snmp	The <code>snmp</code> command moves you to the snmp context of the CLI, providing for the management of SNMP settings for the ExtremeWireless. See snmp Commands on page 217.
syslog	The <code>syslog</code> command moves you to the syslog context of the CLI, providing for the configuration of system log settings on the ExtremeWireless. See syslog Commands on page 225.
time	The <code>time</code> command moves you to the time context of the CLI, providing for synchronization network elements on the ExtremeWireless to a universal clock using the ExtremeWireless's own system time or the Network Time Protocol. See time Commands on page 229.
topology	The <code>topology</code> command moves you to the topology context of the CLI, providing for defining and configuration of topology objects used by policy and VNS objects. See topology Commands on page 387.

Table 5: Root Commands Documented in Feature Chapters (continued)

Command	Description
traffic_capture	The <code>traffic_capture</code> command moves you to the <code>traffic_capture</code> context of the CLI, providing for the management of the TCPDump. See traffic_capture Commands on page 232.
users	The <code>users</code> command moves you to the users context of the CLI, providing for commands used to create and manage user accounts on the network. See users Commands on page 237.
vnsmode	The <code>vnsmode</code> command moves you to the <code>vnsmode</code> context of the CLI, providing for commands used to define and configure Virtual Network Services (VNS) for the network. See VNS Commands (vnsmode) on page 239.
web	The <code>web</code> command moves you to the web context of the CLI, providing for commands to configure the web settings. See web Commands on page 427.
wlans	The <code>wlans</code> command moves you to the <code>wlans</code> context of the CLI, providing for commands used to define and configure WLAN services for the network. See wlans Commands on page 282.

audit

The `audit` command is deprecated.

availability

Move to the availability context from the root context to access the following commands on the Wireless Appliance pair.

The following commands are available in the availability context:

- [pair](#) on page 28
- [pairip](#) on page 29
- [pairrole](#) on page 29
- [fast_failover](#) on page 29
- [link_timeout](#) on page 30
- [sync-config](#) on page 30
- [sync-mu](#) on page 30

pair

Use the `pair` command to set up two Wireless Appliances as a pair. Use the `no` form of the command to set up Wireless Appliances in stand-alone mode.

```
pair A.B.C.D primary | secondary
```

Parameters

<i>A.B.C.D</i>	Specifies the IP address of the peer Wireless Appliance in the availability pair.
primary secondary	Specifies if the Wireless Appliance is the primary or secondary controller in the pair.

Examples

```
EWC.extremenetworks.com:availability# pair 123.321.24.54 primary
```

pairip

Use the `pairip` command to specify the backup of the Wireless Appliance's IP address.

```
pairip A.B.C.D
```

Parameters

<i>A.B.C.D</i>	Specifies the IP address of the peer Wireless Appliance in the availability pair.
----------------	---

Examples

The following example sets an IP address for the backup Wireless Appliance:

```
EWC.extremenetworks.com:availability# pairip 123.321.24.54
```

pairrole

Use the `pairrole` command to designate the Wireless Appliance as the primary connection point for availability Link Exchange or as the secondary point.

When a Wireless Appliance is set as the secondary connection point, Wireless AP registration requests will be set to pending until the other Wireless Appliance is set up as the primary connection point.

```
pairrole primary | secondary
```

Parameters

primary	Assigns the primary connection point role.
secondary	Assigns the secondary connection point role.

Examples

The following example sets the current Wireless Appliance to be the primary connection point:

```
EWC.extremenetworks.com:availability# pairrole primary
```

fast_failover

Use the `fast_failover` command to enable fast failover of the Wireless APs to the secondary controller in 'availability' mode. Use the `no` form of the command to disable the fast failover feature.

fast_failover | no fast_failover

Parameters

None

Examples

```
EWC.extremenetworks.com:availability# fast_failover
```

link_timeout

Use the `link_timeout` command to specify the time period in which the link failure between the Wireless APs and the primary controller in 'availability' mode would be detected.

link_timeout *seconds*

Parameters

<i>seconds</i>	Specifies time period in seconds before link failure is detected. Valid values are 2 to 30 seconds.
----------------	---

Examples

The following example sets the time for link failure detection to 10 seconds:

```
EWC.extremenetworks.com:availability# link_timeout 10
```

sync-config

Use the `sync-config` command to enable or disable synchronization of the configuration elements.

sync-config **enable|disable**

Parameters

enable	Enable synchronization of the configuration elements.
disable	Disable synchronization of the configuration elements.

Example

The following example enables the synchronization of the configuration elements:

```
EWC.extremenetworks.com:availability# sync-config enable
```

sync-mu

Use the `sync-mu` command to enable or disable synchronization of the Guest Portal MU user accounts.

sync-mu | no sync-mu

Parameters

None.

Example

The following example enables the synchronization of the MU accounts:

```
EWC.extremenetworks.com:availability# sync-mu
```

backup

The `backup` command is deprecated. See [export](#) on page 36.

no backup

The `no backup` command is deprecated. See [no export](#) on page 37.

copy

Use the `copy` command to transfer files between the Wireless Appliance and an external server.

Available filenames and platform information can be retrieved by invoking the respective `show` commands. For more information, see [show](#) on page 47.

```

copy ap_certreq server / user / dir / file
copy apup server / user / dir / file / platform
copy cdrs server / user / dir / cdr_dir/file
copy configuration to-local | to-flash | to-remote | server / user / dir / ftp
password / scp password | from-local file | #file | from-flash file | #file |
from-remote | server / user / dir / file / ftp password / scp password
copy export server / user / dir / file | scp | scp password
copy floor-plan to-local | from-local | server / user / dir / file | ftp /
ftp_password | scp | scp password | show
copy import server / user / dir / file | scp | scp password
copy tcpdump server / user / dir / file | #file
copy tech_support server / user / dir / file | scp | scp password
copy upgrade server / user / dir / file | flash | scp | scp password

```

Parameters

<code>server</code>	Specifies the IP address of the FTP or SCP server. The IP address can be either IPv4 <code>A.B.C.D</code> or IPv6 <code>A:B:C:D:E:F:G:H</code> format.
<code>user</code>	Specifies the user name of an account on the FTP or SCP server.
<code>dir</code>	Specifies the name of a directory on the FTP or SCP server.
<code>file</code>	Specifies the name of a file on the Wireless Appliance.
<code>platform</code>	Specifies the platform of the Wireless AP.
<code>cdr_dir/file</code>	Specifies the location of a file on the Wireless Appliance.
<code>#file</code>	The sequence in which the files are listed in the corresponding list. For more information, see list on page 234.
<code>scp</code>	Sets the file transfer protocol to SCP rather than the default setting of FTP.

<i>scp password</i>	The scp password to use with scp for the ssh connection.
<i>ftp password</i>	The ftp password to use with ftp.
to-local	Specifies the local drive as the location the configuration is copied to
to-flash	Specifies the flash drive as the location the configuration is copied to
to-remote	Specifies the configuration is copied to the specified device or server
from-local	Specifies the configuration to be copied is located on the local drive
from-flash	Specifies the configuration to be copied is located on the flash drive
from-remote	Specifies the configuration to be copied is located on the specified remote device or server
flash	This option is available only when a flash device is plugged in
floor-plan show	Displays a list of all locally-stored floor plans

Examples

The following example copies the certificate request (.csr) file for a Wireless AP:

```
EWC.extremenetworks.com# copy ap_certreq 192.168.1.131 jdoe /jdoe/
OrlandoAP.csr
```

The following command copies the Call Detail Records from the Wireless Appliance onto the specified server location:

```
EWC.extremenetworks.com.com# copy cdrs 192.168.3.108 test mycdr 20110824wed/
20110824173358.dat
Please input password:
Attempting to upload file using ftp
SUCCESS: Upload completed.
```

The following command copies an upgrade image for the C25 platform from a server to the Wireless Appliance:

```
EWC.extremenetworks.com# copy apup 192.168.16.21 test new/ap/ C25-0x.xx.xx.
000x.img C25
Please input password:
Attempting to download file using ftp ...
SUCCESS: FTP Download completed.
EWC.extremenetworks.com#
```

The following command copies the Wireless Appliance's upgrade image from a specific FTP server location onto the Wireless Appliance:

```
EWC.extremenetworks.com# copy upgrade 192.168.16.21 test new/ac/rpm/
build07.41.03.0003 AC-MV-07.41.03.0003-1.rue
Please input password:
Attempting to download file using ftp ...
SUCCESS: FTP Download completed.
EWC.extremenetworks.com#
```


The following example copies the upgrade file to the flash device, mounted on the Wireless Appliance, from a specific FTP server:

```
EWC.extremenetworks.com# copy upgrade 192.168.16.21 test new/ac/rpm/  
build07.41.03.0003 AC-MV-07.41.03.0003-1.rue flash  
Please input password:  
Attempting to download file using ftp ...  
SUCCESS: FTP Download completed.  
EWC.extremenetworks.com#
```

In the following example, the CLI command states that the upgrade file will be downloaded from the SCP server to the flash card:

```
EWC.extremenetworks.com# copy upgrade 192.168.4.10 test system/images AC-  
MV-08.21.01.2222-1.rue flash scp TestPassword
```

In the following example, the CLI command states that the upgrade file will be downloaded from the SCP server to the Wireless Appliance local drive:

```
EWC.extremenetworks.com# copy upgrade 192.168.4.10 test system/images AC-  
MV-08.21.01.2222-1.rue scp TestPassword
```

The following example copies the TCPDump file to the FTP server:

```
EWC.extremenetworks.com# copy tcpdump 192.168.4.10 mnj /TCPDump/April_2008  
mgmt_traffic_capture.cap 1
```

The following example copies the fsh_1.zip configuration file located in the backup directory for user tester with password SECRET on the remote FTP server 132.152.1.3 to the local drive:

```
EWC.extremenetworks.com# copy configuration to-local from-remote 132.152.1.3  
tester backup fsh_1.zip ftp SECRET
```

The following example copies the my_conf.zip export file located on a flash drive to bak_dir directory of the remote SCP server 132.152.1.3 for user tester with password SECRET:

```
EWC.extremenetworks.com# copy configuration to-remote 132.152.1.3 tester  
bak_dir scp SECRET from-flash my_conf.zip
```

The following example copies the local export file with index 2 to a flash drive:

```
EWC.extremenetworks.com# copy configuration to-flash from-local 2
```

The following example lists all locally-stored floor plans:

```
EWC.extremenetworks.com# copy floor-plan show  
Locally stored floor-plan files:  
1. 1.fxml  
2. 10.fxml  
3. 101.fxml  
4. 12.fxml  
5. 12_export.fxml
```

host-attributes

Move to the host-attributes context from the root context to configure host attributes on the Wireless Appliance.

The following commands are available in the host-attributes context:

- `hostname` on page 34
- `domain` on page 34
- `dns` on page 35

hostname

Use the `hostname` command to configure a hostname for the controller.

After you have run the `hostname` command, run the `apply` command to implement the changes.

hostname *name* | *none*

Parameters

<i>name</i>	Specifies the hostname of the controller.
<i>none</i>	Removes the configured hostname.

Examples

The following example specifies that the host name of the controller should be EWC123.

```
EWC.extremenetworks.com:host-attributes# hostname EWC123
EWC.extremenetworks.com:host-attributes# apply
```

domain

Use the `domain` command to configure the domain name for the controller.

After you have run the `domain` command, run the `apply` command to implement the changes.

domain *domain name* | **none**

Parameters

<i>domain name</i>	Specifies the domain name of the controller.
none	Removes the configured domain name.

Examples

The following example specifies what the domain name of the controller:

```
EWC.extremenetworks.com:host-attributes# domain extremenetworks.com
EWC.extremenetworks.com:host-attributes# apply
```

dns

Use the `dns` command at the host-attributes context to move into DNS server configuration context.

The following commands are available in the host-attributes:dns context:

- `dns` on page 35
- `move` on page 35

dns

Use the `dns` command in the host-attributes:dns context to configure DNS servers for the controller. You can configure up to three DNS servers to resolve RADIUS server host names to their corresponding IP addresses. Use the `no` form of the command to remove a DNS server configuration.

After you have run the `dns` command, run the `apply` command to implement the changes.

```
dns 1-3 ip address no dns 1-3 ip address
```

Parameters

1-3	Specifies the position of the DNS server in the DNS servers list.
<i>ip address</i>	Specifies the IP address of the DNS server. The IP address can be either IPv4 <i>A.B.C.D</i> or IPv6 <i>A:B:C:D:E:F:G:H</i> format.

Examples

The following example defines a DNS server, with a 192.1.1.3 IP address, as the first DNS server:

```
EWC.extremenetworks.com:host-attributes:dns# dns 1 192.1.1.3
```

move

Use the `move` command in the dns context to reposition DNS servers in the DNS server list.

After you have run the `move` command, run the `apply` command to implement the changes.

```
move orig_index | new_index
```

Parameters

<i>orig_index</i>	Specifies the current position of the DNS server that you want to reposition.
<i>new_index</i>	Specifies the new position of the DNS server that you want to reposition.

Examples

The following example displays the current DNS server configuration:

```
EWC.extremenetworks.com:host-attributes:dns# show
dns 1 192.1.1.3
dns 2 192.1.2.3
dns 3 192.1.3.3
```

To move the DNS sever 192.1.3.3 into the first position on the DNS servers list, use the following command:

```
host-attributes:dns# move 3 1
```

The following displays the results of the previous `move` command:

```
EWC.extremenetworks.com:host-attributes:dns# show
dns 1 192.1.3.3
dns 2 192.1.1.3
dns 3 192.1.2.3
```

export

Use the `export` command to export the controller's configuration, CDRs, logs and audit information, or all of them in a .zip file to either the local or flash drive. During the export process, the .zip file containing the controller's data is zipped. The exported file displays .zip extension. If you want to upload the controller's data to the FTP or SCP server, you must use the `copy configuration` command. For more information, see [copy](#) on page 31.

export configuration | cdrs | all | logs | audit | local | flash

Parameters

configuration	Exports the controller's configuration.
cdrs	Exports the controller's CDRs.
all	Exports all of the following: controller's configuration, CDRs, logs, audit information.
logs	Exports the controller's logs.
audit	Exports the controller's audit information.
local	Exports the specified data to the local drive.
flash	Exports the specified data to the flash drive.

Examples

The following command exports the controller's existing configuration in a .zip file:

```
EWC.extremenetworks.com# export configuration
Filename (lab-91-f.16082010.110525):
Comment:
Please wait...
CLI Export start: Mon Aug 16 11:05:33 2010
CLI Export end: Mon Aug 16 11:05:37 2010
Creating lab-91-f.16082010.110525...
Backup/Export complete.
```

The following example exports the controller's CDRs:

```
EWC.extremenetworks.com# export cdrs
Filename (lab-91-f.16082010.110544):
```

```

Comment:
Please wait...
Creating lab-91-f.16082010.110544...
Backup/Export complete.

```

The following example exports the controller's logs:

```

EWC.extremenetworks.com# export logs
Filename (lab-91-f.16082010.110548):
Comment:
Please wait...
Creating lab-91-f.16082010.110548...
Backup/Export complete.

```

The following example exports the controller's audit information:

```

EWC.extremenetworks.com# export audit
Filename (lab-91-f.16082010.110554):
Comment:
Please wait...
Creating lab-91-f.16082010.110554...
Backup/Export complete.

```

The following example exports all of the following: Configuration, CDRs, logs, audit information:

```

EWC.extremenetworks.com# export all
Filename (lab-91-f.16082010.110654):
Comment:
Please wait...
CLI Export start: Mon Aug 16 11:06:59 2010
CLI Export end: Mon Aug 16 11:07:03 2010
Creating lab-91-f.16082010.110654...
Backup/Export complete.
EWC.extremenetworks.com#

```

no export

Use the `no export` command to remove the specified export file from the local or flash drive.

```
no export filename / number
```

Parameters

<i>filename</i>	Specifies the file name of the export file to remove. If the export file is located on a flash drive, the string "(flash)" must be suffixed to the end of the specified file name.
<i>number</i>	Specifies the index number of the export file on the list to remove.

Example

The following command removes the list index 2 file from the export list:

```

EWC.extremenetworks.com# no export 2
EWC.extremenetworks.com#

```

The following command removes the `export_lab213_V4R1.7.10_NAMO_ENT.zip` export file from the export list:

```
EWC.extremenetworks.com# no export export_lab213_V4R1.7.10_NAMO_ENT.zip
EWC.extremenetworks.com#
```

flash

Use the `flash` command to mount or dismount the flash device on the Wireless Appliance.

flash mount | unmount

Parameters

mount	Specifies to mount the flash device.
unmount	Specifies to dismount the flash device.

Examples

The following example mounts the flash device on the Wireless Appliance:

```
EWC.extremenetworks.com# flash mount
```

The following example dismounts the flash device from the Wireless Appliance:

```
EWC.extremenetworks.com# flash unmount
```

no flash

Use the `no flash` command to delete files on a flash device. The `no flash` command is under the root context.

no flash file name

Example

The following example deletes the files from the flash device:

```
EWC.extremenetworks.com# no flash lab-91-f.16082010.110525
Successfully deleted file lab-91-f.16082010.110525 from flash
```

healthpoll

Use the `healthpoll` command to enable or disable the poll timer.

healthpoll enable | disable

Parameters

enable	Enables the poll timer.
disable	Disables the poll timer.

Example

The following command enables the poll timer:

```
EWC.extremenetworks.com# healthpoll enable
EWC.extremenetworks.com# show healthpoll
healthpoll enable
```

import

Use the `import` command to import the controller's configuration from a file that was earlier exported from a previous platform or an old software release. If you want to import the controller's data from a remote FTP or SCP server, you must use the `copy configuration` command. For more information, see `copy` on page 31. Use the `no import` command to remove the specified file from the local or flash drive.

```
[no] import filename | number
```

Parameters

<i>filename</i>	The name of the .zip or .cli file that contains the controller's configuration. If the export file is located on a flash drive, the string "(flash)" must be suffixed to the end of the specified file name.
<i>number</i>	Specifies the index number of the import file. You can use the <code>show import</code> command to find the restore file's index number.

Examples

The following command imports the controller's configuration from a 'zipped' .zip file that was exported from the previous platform or from the older software:

```
EWC.extremenetworks.com# import lab-213-g.11042008.141154.zip
```

The following command removes the controller's import configuration, CDRS, logs, audit information file:

```
EWC.extremenetworks.com# no import lab-213-g.11042008.141154.zip
```

key

Move to the `key`: context to configure license key information for the Wireless Appliance.

The `key` context has the following commands:

- `activate` on page 40

- [ecap](#) on page 40

activate

Use the `activate` command to apply a license key on the Wireless Appliance. The `activate` command is accessible from the key context of the CLI.

activate *activation-key*

Parameters

<i>activation-key</i>	Specifies the license key to be applied on the Wireless Appliance. The license key format is: AAAAAAA-11111111-11111111-11111111-11111111.
-----------------------	--

Example

The following example applies a license key on the Wireless Appliance:

```
EWC.extremenetworks.com:key# activate
ABCDEF-12345678-22345678-32345678-42345678
```

ecap

Use the `ecap` command to apply a capacity enhancement license key on the Wireless Appliance. The `ecap` command is accessible from the key context of the CLI.

ecap *ecap-key*

Parameters

<i>ecap-key</i>	<p>Specifies the capacity enhancement license key to be applied on the Wireless Appliance. The capacity enhancement license key format for C5110/C4110 is CAPCTL-11111111-11111111-11111111-11111111.</p> <p>For the C25/V2110 platforms, the capacity enhancement license key formats are:</p> <ul style="list-style-type: none"> • CAPC20-11111111-11111111-11111111-11111111 • CAP001-11111111-11111111-11111111-11111111 <p>For the C5210 platform, the capacity enhancement license key formats are:</p> <ul style="list-style-type: none"> • CAPCTL-11111111-11111111-11111111-11111111 • CAPCTL-11111111-11111111-11111111-11111111 • CAP100-11111111-11111111-11111111-11111111 <p>For Radar In Service Scans, the capacity enhancement license key format is:</p> <ul style="list-style-type: none"> • RADCAP<i>nnn</i>-<i>xxxxxxxx</i>-<i>xxxxxxxx</i>-<i>xxxxxxxx</i>-<i>xxxxxxxx</i> • <i>nnn</i> is the capacity increment • <i>x</i> is an upper case alpha-numeric character. <p>Examples:</p> <ul style="list-style-type: none"> • RADCAP100-ABCD1234-7G8V9XYT-MVB1G7XA-QVR4UXDT • RADCAP001-ABCD1235-7G8V9XYT-MVB1G7XA-QVR4UXTD
-----------------	--

Usage

Capacity enhancement license keys specify a predetermined capacity for enhancement feature application. Capacity enhancement license keys include Radar (In Service Scan) capacity licenses as well as AP capacity licenses.

For details about Radar capacity licenses and their use, see the Radar chapter in the *Wireless User Guide*.

Example

The following example applies a capacity enhancement license key on the Wireless Appliance:

```
EWC.extremenetworks.com# ecap CAPCTL-12345678-22345678-32345678-42345678
```

The following example applies a Radar capacity enhancement license key on the Wireless Appliance:

```
EWC.extremenetworks.com# ecap RADCAP001-ABCD1235-7G8V9XYT-MVB1G7XA-QVR4UXTD
```

lanset

Use the `lanset` command to define the port speed — the data transmission rate of an output/input channel. The `lanset` command is available at the root context of the admin account type.

```
lanset lanN|admin autoneg_off|autoneg_on 10|100|any full|half
```

Syntax

Parameters

<code>lanN</code>	Specifies the data port. N can range from 1 to 4, depending on the controller model.
<code>admin</code>	Admin Port.
<code>autoneg_on</code>	Allows PHY (Physical Layer) to auto-negotiate the port speed and the duplex mode.
<code>autoneg_off</code>	Disallows PHY to auto-negotiate the port speed and the duplex mode.
<code>10</code>	Sets the port speed to 10 Mbps.
<code>100</code>	Sets the port speed to 100 Mbps.
<code>any</code>	Allows the PHY to negotiate the port speed from any of the three options — 10, 100 or 1000 Mbps — and the duplex mode from any of the two option options — half-duplex or full-duplex.
<code>full</code>	Allows the PHY to operate in full duplex mode.
<code>half</code>	Allows the PHY to operate in half-duplex mode.

The following example sets the port speed to 100 Mbps, full duplex mode, and disables auto-negotiation for the admin port:

```
EWC.extremenetworks.com# lanset admin autoneg_off 100 full
```

The following example enables auto-negotiation for any port speed and either duplex mode for the admin port:

```
EWC.extremenetworks.com# lanset admin autoneg_on any
```

In the case of Data Ports, the `lanset` command supports multiple options with auto-negotiation enabled. The following example disables auto-negotiation and sets the port speed to 100 Mbps in full duplex mode for data port 1:

```
EWC.extremenetworks.com# lanset lan1 autoneg_off 100 full
```

loglevel

Use the `loglevel` command to set the log level for the Wireless Appliance or the Wireless APs. The optional `stationlog`, `send2wm`, and `send_station_trap` parameters support station session streaming logs.

```
loglevel ac 1|2|3|4 stationlog enable|disable send_station_trap enable|disable  
send2wm enable|disable ap 1|2|3|4
```

Parameters

ac	Sets the log level of the Wireless Appliance.
ap	Sets the log level of the Wireless APs.
1	Indicates Critical severity level.
2	Indicates Major severity level.
3	Indicates Minor severity level.
4	Indicates Informational severity level.
stationlog	Enables or disables station session event reporting on the controller station events log.
send_station_trap	Enables or disables station event forwarding as SNMP traps.
send2wm	Enables or disables sending station session events to the Wireless Manager.

Examples

The following example sets the Wireless Appliance's log level to Minor:

```
EWC.extremenetworks.com# loglevel ac 3  
Successfully set ac log level to Minor (3)
```

The following example sets the Wireless Appliance log level to Information and enables station event reporting on the the controller station log, but doesn't enable station event forwarding to Wireless Manager:

```
EWC.extremenetworks.com# loglevel ac 4 stationlog enable send2wm disable
```

The following example sets the AP's log level to Information:

```
EWC.extremenetworks.com# loglevel ap 4
```

ping

Use the `ping` command to ping an IP address. The ping command accepts an optional parameter that specifies the source ip address to be used by the command. If this optional source is provided, ping uses the IP address of the specified interface as the source IP address.

```
ping source-interface name name | number id ip address
```

Parameters

source-interface name <i>name</i> number id	Specifies the address of the source interface you want to send pings from, either by interface name or ID.
<i>IP Address</i>	Specifies the IP address you want to ping. The IP address can be either IPv4 (A.B.C.D) or IPv6 (A:B:C:D:E:F:G:H) format.

Usage

You can identify the source IP using its interface name or, for short, the identifier returned by the `show topology 13` command. Interface name is the name of any topology with L3 configuration (Physical, Admin, B@AC or Routed).

Examples

The following example pings an IP address:

```
EWC.extremenetworks.com# ping 192.168.1.32
PING 192.168.1.32 (192.168.1.32) from 192.168.1.38 : 56(84) bytes of data.
64 bytes from 192.168.1.32: icmp_seq=1 ttl=64 time=0.423 ms
64 bytes from 192.168.1.32: icmp_seq=2 ttl=64 time=0.218 ms
64 bytes from 192.168.1.32: icmp_seq=3 ttl=64 time=0.204 ms
--- 192.168.1.32 ping statistics ---
3 packets transmitted, 3 received, 0% loss, time 2013ms
rtt min/avg/max/mdev = 0.204/0.281/0.423/0.101 ms
```

The following example first uses the `show topology 13` command to obtain interface names for use with ping as source addresses. Then, the following command pings an IP address using the IP address of interface name "esa1" (as determined with the `show topology 13` command) as the source address:

```
EWC.extremenetworks.com# show topology 13
Name                               Mode                               L3:IP
1:Admin                             admin
```

```

192.168.4.37
2:esa0          physical      10.0.0.1
3:esal          Physical     10.0.1.1
4:Extreme-37Topology b@ac        10.10.1.1

```

```

EWC.extremenetworks.com# ping source-interface name esal 192.168.4.37
PING 192.168.4.37 (192.168.4.37) from 10.0.1.1 : 56(84) bytes of data.
64 bytes from 192.168.4.37: icmp_seq=1 ttl=64 time=0.042 ms
64 bytes from 192.168.4.37: icmp_seq=2 ttl=64 time=0.037 ms
64 bytes from 192.168.4.37: icmp_seq=3 ttl=64 time=0.039 ms

--- 192.168.4.37 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.037/0.039/0.042/0.005 ms

```

radtest

Use the `radtest` command to test the RADIUS server's connectivity and configuration. RADIUS servers with captive portal (CP) and EAP authentication can be tested for connectivity.

Captive Portal Syntax

```
radtest vns_name | username | password
```

EAP Syntax

```
radtest vns_name | username
```

Parameters (CP and EAP)

<i>vns_name</i>	Specifies the VNS assignment ID of the virtual interface (WLAN Service) configured on the controller.
<i>username</i>	Specifies a username.
<i>password</i>	Specifies a password.

Examples

The following example tests the radius server on CNL-7-CP:

```

EWC.extremenetworks.com# radtest CNL-7-CP chap106 xyz789
Sending Captive portal authentication request to Radius Server for user
chap106, with password xyz789, on vns_name CNL-7-CP.
Please wait while all configured Radius Servers on this VNS are attempted as
needed ...
Test Completed.
The Radius Server has successfully authenticated the user chap106 with
password xyz789 and VNS CNL-7-CP.

```

radtest_mba

Use the `radtest_mba` command to test RADIUS servers used by the Wireless Appliance for Mac-based authorization.

```
radtest_mba vns_name | MAC Address | ap_bss_mac_addr | ap_eth_mac_addr
```

Parameters

<i>vns_name</i>	Specifies the VNS assignment ID of the virtual interface (WLAN Service) configured on the controller.
<i>MAC Address</i>	Specifies a MAC address.
<i>ap_bss_mac_addr</i>	Specifies the Wireless AP's Basic Service Set Identifier (BSSID).
<i>ap_eth_mac_addr</i>	Specifies the Wireless AP's ethernet MAC address.

Examples

The following example tests the RADIUS server on CNL-206-CPWEP:

```
EWC.extremenetworks.com# radtest_mba CNL-206-CPWEP 00:0E:35:CA:D1:96
Sending MAC-based authorization request to Radius Server for mac_str 00:0E:
35:CA:D1:96 on vns_name CNL-206-CPWEP with bss_mac DE:AD:DE:AD:DE:AD and
eth_mac DE:AD:DE:AD:DE:AD.
Please wait while all configured Radius Servers on this VNS are attempted as
needed ...
Test Completed.
```

reset

Use the `reset` command to reset configuration settings on the Wireless Appliance to their factory.

```
reset license | mgmt
```

Parameters

license	Removes the installed license.
mgmt	Resets the management port configuration.

Examples

The following example resets all configuration settings on the Wireless Appliance except for the management port configuration. You are prompted to confirm if you want to continue to reset the Wireless Appliance:

```
EWC.extremenetworks.com# reset
WARNING: Resetting will clear all configuration except for the management
port configuration. It will disconnect any clients currently using the
system. Following the reset, the system will be rebooted.
Do you wish to continue? (y/n)
```

The following example resets all configuration settings on the Wireless Appliance including the management port configuration. You are prompted to confirm if you want to continue to reset the Wireless Appliance:

```
EWC.extremenetworks.com# reset mgmt
WARNING: Resetting management will clear all configuration including the
management port configuration. It will disconnect any clients currently using
the system. Following the reset, the system will be rebooted.
Do you wish to continue? (y/n)
```

The following example removes installed licenses and resets all configuration settings on the Wireless Appliance including the management port configuration. You are prompted to confirm if you want to continue to reset the Wireless Appliance:

```
EWC.extremenetworks.com# reset license WARNING: Resetting the license will
clear all configuration and permanently delete any
installed licenses. It will
disconnect any clients currently using the system.
Following the reset, the
system will be rebooted. Activation key string :
XXXXXXXX-XXXXXXXX-XXXXXXXX-XXXXXXXX-XXXXXXXX Capacity
Enhancement Option
Keys: Radar License Keys: Do you wish to continue?
(y/n) n
Reset license cancelled by user request.
```

restart

Use the `restart` command to restart individual processes on the Wireless Appliance.

Use the `show system_state process` command to list the current processes on the Active Controller. For more information, see [show system_state](#) on page 79.

```
restart process_id | process_name
```

Parameters

<i>process_id</i>	Specifies the index number of the process.
<i>process_name</i>	Specifies the process name.

Example

The following command restarts the LLC Handler process by referring to its index number:

```
EWC.extremenetworks.com# restart 1094
LLC Handler process being restarted.
```

restore

The `restore` command is deprecated. See [import](#) on page 39.

secureconnection

Move to the `secureconnection` context to configure the shared secret between a Wireless Appliance and NetSight Wireless Manager.

The `secureconnection` context has the following commands:

- [secret](#) on page 47
- [weak-ciphers](#) on page 47

secret

Use the `secret` command to configure a shared secret for a Wireless Appliance and NetSight Wireless Manager. Use the `no` command to disable the shared secret. The `secret` command is available from the `secureconnection` context of the CLI.

```
secret A.B.C.D secret_string no secret
```

Parameters

<i>A.B.C.D</i>	Specifies the NetSight Wireless Manager's IP address.
<i>secret_string</i>	Specifies the shared secret string (16 to 232 characters).

Example

```
EWC.extremenetworks.com:secureconnection# secret 200.200.200.200
1234567890123456
```

weak-ciphers

Use the `weak-ciphers` command to enable/disable weak ciphers for a Wireless Appliance and NetSight Wireless Manager. The `weak-ciphers` command is available from the `secureconnection` context of the CLI.

```
weak-ciphers enable | disable
```

Parameters

enable disable	Enables or disables weak ciphers.
-------------------------	-----------------------------------

Example

```
EWC.extremenetworks.com:secureconnection# weak-ciphers enable
```

show

The CLI is equipped with `show` commands, which are used to display properties and configurations of component features on the Wireless Appliance. These `show` commands are accessible from the root context of the CLI.

- [show ac version](#) on page 49
- [show active-user](#) on page 49

- [show- antennas](#) on page 132
- [show ap \(AP Configuration\)](#) on page 49
- [show ap_certificate](#) on page 54
- [show ap_certreq](#) on page 55
- [show ap_inventory](#) on page 55
- [show apup](#) on page 57
- [show audits](#) on page 58
- [show availability](#) on page 58
- [show bootrom](#)
- [show cdrs](#) on page 58
- [show clients aserial](#) on page 60
- [show clients vns](#) on page 60
- [show run-config](#) on page 61
- [show dns](#) on page 61
- [show export](#) on page 61
- [show flash](#) on page 62
- [show healthpoll](#) on page 63
- [show import](#) on page 63
- [show import_status](#) on page 64
- [show key](#) on page 64
- [show l2ports](#) on page 65
- [show lanset](#) on page 65
- [show log](#) on page 66
- [show loglevel](#) on page 68
- [show ospf](#) on page 69
- [show policy](#) on page 70
- [show role](#) on page 70
- [show wlans](#) on page 71
- [show report](#) on page 71
- [show routes](#) on page 74
- [show schedule_backup](#) on page 75
- [show schedule_upgrade](#) on page 75
- [show snmp](#) on page 75
- [show stats](#) on page 76
- [show syslog](#) on page 78
- [show system_state](#) on page 79
- [show tech_support](#) on page 81
- [show time](#) on page 81
- [show time-config](#) on page 81
- [show time-config](#) on page 81
- [show topology](#) on page 82
- [show traffic_capture](#) on page 83
- [show upgrade](#) on page 83

- [show upgrade_backup_dest](#) on page 84
- [show upgrade_history](#) on page 84
- [show upgrade_image_src](#) on page 84
- [show users](#) on page 85
- [show vnsmode](#) on page 85
- [show vnsmode radius](#) on page 86
- [show web](#) on page 86

show ac version

Use the `show ac version` command to display the software version, software build, and hardware platform versions of the Wireless Appliance.

show ac version

Parameters

None

Examples

The following example displays the software version, software build and hardware platform version of the Wireless Appliance:

```
EWC.extremenetworks.com# show ac version
Software version: 9.01
Software build: 09.01.01.0xxx
Product Name: C5210
```

show active-user

Use this command to display the currently logged in user.

show active-user

Parameters

None.

Examples

```
EWC.extremenetworks.com# show active-user
User: admin
```

show ap (AP Configuration)

Use the `show ap` command to show the configuration information of Wireless APs connected to the Wireless Appliance.

```
show ap [access | registration | version | load-groups | (defaults (config|
3935FCC|ap37xx|ap38xx|ap3801)) | (ap_serial [clients | static_config | config |
radio1 | radio2 | version | professional_antenna])]
```

Use `ap37xx` to modify `ap37xx` and `W78xC` ap defaults settings.

Parameters

access	Displays the status of the Wireless APs.
registration	Displays the registration information.
version	Displays the software version installed on Wireless APs.
load-groups	Displays the configured load groups.
defaults	Displays the Dynamic Radio Frequency management settings.
config	Displays the configured values of the Wireless AP.
Specific model number that depends on the license of the controller. For example, 3935FCC 3935FCC 3935ROW 3965FCC 3965ROW	Displays the configured values of the Wireless APs. This can be any of the following models with the specific regulatory domain license: <ul style="list-style-type: none"> • 3935FCC • 3935ROW • 3965FCC • 3965ROW
ap37xx	Displays the configured values of the 37xx access point.
ap38xx	Displays the configured values of the 38xx access point.
ap3801	Displays the configured values of the 3801 access point.
<i>ap_serial</i>	Specifies the serial number of a specific Wireless AP.
clients	Displays the clients connected to the Wireless AP.
static_config	Displays the static configuration values.
config	Displays the configured values for the Wireless AP.
radio1	Displays the Wireless AP's radio 1 settings.
radio2	Displays the Wireless AP's radio 2 settings.
version	Displays the software version and hardware type of the Wireless AP.
professional_antenna	Displays the professional_antenna settings.

Examples

The following example displays the serial number, name, and platform of connected Wireless APs:

```
EWC.extremenetworks.com# show ap
serial 000000VPC1553827 W788C_06 W788C-2-RJ45
serial 0000141600020802 3865e_13 AP3865e
serial 12341770905A0000 3705i_01 AP3705i
serial 12343567905A0000 3705i_02 AP3705i
serial 13140663595A0000 3710i_03 AP3710i
serial 13440720085E0000 3715i_04-05 AP3715i-1
serial 1404009608410000 3825e_16-17 AP3825e
serial 1404013908410000 3825i_09-10 AP3825i
serial 14160231085A0000 3825e_11-12 AP3825e
serial 1450451508410000 3801i_07 AP3801i
serial 1525D10061100000 3935e-ROW_14-15 AP3935e-ROW
serial 1541D20040490000 3935i-ROW_18 AP3935i-ROW
```

```
serial 1544Y-1001600000 3935i-ROW_19 AP3935i-ROW
serial 2014180500000012 3805e_08 AP3805e
```

The following example displays the registration status of the Wireless APs:

```
EWC.extremenetworks.com# show ap access
0122003880188015 LOCAL APPROVED
0409920201204003 LOCAL APPROVED
12343502905A0000 LOCAL APPROVED ACTIVE
1306032659480000 LOCAL APPROVED ACTIVE
```

The following example displays the registration information:

```
EWC.extremenetworks.com# show ap registration
security on
dinterval 10
dretry 2
Cluster encryption: enable
Cluster inter AP roam: enable
Cluster shared secret: *****
```

The following example displays standard ap defaults information:

```
EWC.extremenetworks.com# show ap defaults 3935FCC
ssh enabled
poll_timeout 15
no client_session
no persistent
no bcast_disassoc
country United States
no lldp
led-mode normal
lbs-status enabled
secure-tunnel disable
ipmcast-assembly disabled
balanced-power enabled
```

The following example displays the clients connected to the Wireless AP with the serial 0409920201204003:

```
EWC.extremenetworks.com# show ap 0409920201204003 clients
```

Client User	IP Roam	Client MAC	Protoc ol	Radi o	BSS MAC	SSID	Auth	Time
		00:40:96:AB:61:58	g	2	00:0F:B B:09:F6 :A2	CNL-220-14-3-ssid	Priv EAP/WPA	0:21:14
Total 1								

```
show ap clients output, continued:
```

Policy Drop	Topolo DL	RSS Lost	Avg. (dBm)	Bytes Sent/Receive	Packets Sent/Received	UL Drop Rate	DL Drop Rate	DL
Buffer	gy	Retrie	(Mbps)			Packet	Packet	

Packet	s		Sent/	d	d	s/	s/
s/	Packet		Recvd			Bytes	Bytes
Bytes	s/						
Bytes							
CNL-220-0/0	CNL-0/0	-25	54.0/	1212/	297250/	0/0	0/0
14-3-default	220-14-3		54.0	2047	279660		

The following example displays the static configuration values of the Wireless AP:

```
EWC.extremenetworks.com# show ap 0409920201204003 static_config
Static IP Address: 10.205.0.11
Static Netmask:    255.255.255.0
Static Gateway:    10.205.0.2
AC IP: 10.205.0.1
AC Order: 1
```

The following example displays the configuration information of the Wireless AP with the serial number 111111111139351

```
EWC.extremenetworks.com# show ap 111111111139351 config
AP Serial Number: 111111111139351
AP host name: AP3935i-111111111139351
AP Name: 3935i
Description:
Active # of clients: 0
AP software version: 10.01.01.0123
Status: approved
role : ap
Home: local
DHCP IP address: 0.0.0.0
DHCP NetMask: 0.0.0.0
DHCP Gateway: 0.0.0.0
Hardware Type: Wireless AP3935i-FCC Internal
Wired MAC address: 00:00:00:00:00:00
```

The following example displays the Wireless AP's (3935FCC) radio 1 settings:

```
EWC.extremenetworks.com# show ap 111111111139351 radio1
dtim 5
beaconp 100
nonUnicastQuota 100
rts 2346
frag 2346
domain fjdkfj.jfadkl
tx_max_power 10 dBm
radio mode anac
no atpc
minbrate 6
n_chlwidth auto
current channel None
last requested channel 40: (5180,[5200],5220,5240)
n_guardinterval short
```

```

n_pmode auto
n_ptype cts only
n_pbthreshold 50
no n_aggr_msdu
n_aggr_mpdu
n_aggr_mpdu_max 1048575
n_aggr_mpdu_max_subframes 30
n_addba_support
probe-suppression disable
admin-mode on
ldpc enable
stbc enable
txbf mu_mimo
optimized-mcast disable
mcast-adaptable disable
mcast2ucast disabled
current_power: 0
dcs mode monitor
channel_plan all-non-dfs
noise_threshold -80
occupancy_threshold 100
update_period 5

```

The following example displays the Wireless AP's (3935FCC) radio 2 setting:

```

EWC.extremenetworks.com# show ap 1111111111139351 radio2
dtim 5
beaconp 100
nonUnicastQuota 100
rts 2346
frag 2346
domain MyDomain
preamble long
tx_max_power 13 dBm
pmode auto
prate 11
ptype cts only
radio mode bgn
no atpc
minbrate 1
n_chlwidth auto
current channel None
last requested channel Auto
n_guardinterval short
n_pmode auto
n_ptype cts only
n_pbthreshold 50
no n_aggr_msdu
n_aggr_mpdu
n_aggr_mpdu_max 65535
n_aggr_mpdu_max_subframes 30
no n_addba_support
probe-suppression disable
admin-mode on
ldpc enable
stbc enable
optimized-mcast disable
mcast-adaptable disable

```

```

mcast2ucast disabled
current_power: 0
dcs mode monitor
channel_plan auto
noise_threshold -80
occupancy_threshold 100
update_period 5
interference-wait-time 10

interference-event-type none

```

The following example displays the software version and hardware type for the Wireless AP:

```

EWC.extremenetworks.com# show ap 111111111139351 version
Software version: 10.01.01.0123
Hardware Type: Wireless AP3935i-FCC Internal

```

The following example displays the software version installed on all Wireless APs:

```

EWC.extremenetworks.com# show ap version
Serial: 111111111139351          Version: 10.01.01.0123
Serial: 111111111138251          Version: 10.01.01.0123
Serial: 13310619085D0000         Version: 10.01.01.0123
Serial: 111111111137152          Version: 10.01.01.0123

```

The following example displays the load groups:

```

EWC.extremenetworks.com# show ap load-groups
Load Groups:
Name: CNL_201_Radio-001          Type : radio
Name: CNL_201_Client_Balancing-002 Type : client
Name: CNL_201_Radio-008          Type : radio
Name: Radio-001                  Type : radio
Name: CNL_201_Client_Balancing-001 Type : client

```

show ap_certificate

Use the `show ap_certificate` command to displays the Wireless AP's current certificate credentials.

```
show ap_certificate ap_serial
```

Parameters

<i>ap_serial</i>	Specifies Wireless AP's serial number.
------------------	--

Examples

```

EWC.extremenetworks.com# show ap_certificate 0409920201204043
User: 0409920201204043
Password: *****
ap_serial: 0409920201204043
Certificate serial number: 51F5F66D000000000238
Issued on: Sat May 26 10:45:19 2015
Expire on: Sat Feb 21 18:25:02 2017
Issued by: CN=Seasametechtrial, DC=com, DC=extremenetworks, DC=techtrial

```

```
Full distinguished name: CN=0409920201203801
Subject alternative name:
```

show ap_certreq

Use the `show ap_certreq` command to display the available certificate signing request for the 802.1x EAP-TLS (Proxy mode) configuration.

show ap_certreq

Parameters

None

Examples

```
EWC.extremenetworks.com# show ap_certreq
1: 0409920201203894.CSR
```

show ap_inventory

A report of Wireless APs connected to the Wireless Appliance can be displayed. This includes information about the Wireless AP's hardware, software, and connection status.

Use the `show ap_inventory` command to display a report of the Wireless APs with a pending or approved status on the Wireless Appliance.

show ap_inventory

Parameters

None

Examples

The following example displays the Wireless APs connected to the Wireless Appliance:

```
EWC.extremenetworks.com# show ap_inventory
Name:                0002000007515340
Serial:              0002000007515340
Desc:
Status:              approved
Software:            09.21.01.0179
Hardware:            Wireless AP3765i Internal
Wired MAC:           00:0E:8C:8F:E5:B1
Poll Timeout:        15
Poll Interval:        3
Persistent:          off
Broadcast Dissoc:    off
Client Session Maintain:enabled
Broadcast
Assn:                DHCP
IP Address:           10.208.2.244
Netmask:             255.255.255.0
Gateway:             10.208.2.2
AC Search List:      10.208.2.67
```

```

Radio Settings          Radio a      Radio b/g

802.11a                 on          -
802.11b                 _          on
802.11g                 _          on
802.11n                 off         on
DTIM Period            5          5
Beacon Period          100        100
RTS/CTS Threshold      2346       2346
Frag. Threshold        2346       2346
Channel                 5500       2452
Power Level             23         10
ATPC                    disabled   disabled
TX Power Adjust         0          0
TX Min Power            5          5
TX Max Power            23         10
ATT                     2          1
Max Operational Rate    54         54
Preamble                -          Long
N Channel Width         -          40
N Channel Bonding       -
N Guard Interval        -          Long

BSS:MAC (radio a)
20:B3:99:E1:79:40

20:B3:99:E1:79:41

BSS:MAC (radio bg)
20:B3:99:E1:79:48
20:B3:99:E1:79:49

BSS:SSID (radio a)
SSID: ACTT-208
SSID: cnlcc1404010108410000
SSID: cnl208-rt

BSS:SSID (radio bg)
SSID: ACTT-208
SSID: cnl208-rt
--

```

show app (Application Group)

Use the `show app` command to show the application visibility group configuration.

The group names are pre-defined standard Extreme Application Analytics™ signature groups. The group names are case-sensitive.

```
show app [apptype (built-in | custom | all)] [group group_name]
```


Parameters

apptype	Specifies the application type. Possible values: <ul style="list-style-type: none"> • built-in • custom • all
group <i>group_name</i>	Displays applications within the specified group.

Usage

We recommend using the group parameter. Using the apptype all parameter without the group can result in over 2000 applications. Group names are case sensitive. You can run this command from the root or from the vnsmode:custom-app context.

Example

The following example shows all applications of type built-in from group p2p.

```
EWC.extremenetworks.com show app apptype built-in group p2p
```

The following example shows all applications from group p2p regardless of type.

```
EWC.extremenetworks.com show app group p2p
```

Related Links

[custom-app-list](#) on page 248

show apup

Use the `show apup` command to display all available upgrade images for Wireless APs on the Wireless Appliance by order of platform type.

```
show apup platform
```

Parameters

<i>platform</i>	Specifies the platform of the Wireless AP
-----------------	---

Examples

The following example displays the upgrade images currently available for the Wireless APs:

```
EWC.extremenetworks.com# show apup
AP3705i
1: AP3705-10.01.01.0123.img
AP3710
1: AP3710-10.01.01.0123.img
AP3715
1: AP3715-10.01.01.0123.img
AP3765
1: W78XC-2-10.01.01.0123.img
AP3767
1: W78XC-2-10.01.01.0123.img
AP3801
1: AP3801-10.01.01.0123.img
```

```

AP3805
1: AP3805-10.01.01.0123.img
AP3825
1: AP3825-10.01.01.0123.img
AP3865
1: AP3825-10.01.01.0123.img
AP3935
1: AP3935-10.01.01.0123.img
W78xC
1: W78XC-2-10.01.01.0123.img
W78xC SFP
1: W78XC-2-10.01.01.0123.img

```

The following example displays the upgrade images available for the AP3935 platform only:

```

EWC.extremenetworks.com# show apup AP3935
1: AP3935-10.01.01.0123.img

```

show audits

The `show audits` command has been deprecated.

show availability

Use the `show availability` command to display availability settings for the Wireless Appliance.

show availability

Parameters

None

Examples

The following example displays availability settings for the Wireless Appliance:

```

EWC.extremenetworks.com# show availability
pair paired
pairrole secondary
pairip 192.168.4.207
fast_failover enabled
link_timeout 2
sync-mu disabled

```

show backup

The `show backup` command has been deprecated. See [show export](#) on page 61.

show cdrs

Use the `show cdrs` command to display a directory listing of the user's call detail records. Use the parameters to display the contents of the records.

```
show cdrs dir | filename 1-9600
```

Parameters

<i>dir</i>	Specifies the name of the directory you want to view.
<i>filename</i>	Specifies the name of the file you want to view.
1-9600	Specifies an item number from the file name list.

Examples

The following example lists the folders containing the call detail records:

```
EWC.extremenetworks.com# show cdrs
20050921wed
20050922thu
20050923fri
20050929thu
20050930fri
20051103thu
```

The following example lists the file names within folder 20050921wed:

```
EWC.extremenetworks.com# show cdrs 20050921wed
1: 20050921194016.dat
2: 20050921204353.dat
3: 20050921212300.dat
4: 20050921212431.dat
5: 20050921213022.dat
6: 20050921213053.dat
```

The following example selects a record by file name and displays its contents:

```
EWC.extremenetworks.com# show cdrs 20050921wed 20050921194016.dat
-----
Acct-Session-Id = 4331ed220001
User-Name = david@lab.webdomain.com
Filter-Id = Default
Acct-Interim-Interval = 1800
Session-Timeout = 0
Class = 0x5a59 670 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Acct-Status-Type = 2
Acct-Delay-Time = 108287
Acct-Authentic = 1
Framed-IP-Address = 0.0.0.0
Connect-Info = 802.11a
NAS-Port-Type = Wireless-802.11
Called-Station-ID = 00:50:C2:23:A0:59
Calling-Station-ID = 00:0E:35:CA:EC:4E
Siemens-AP-Serial = 0122003880188006
Siemens-AP-Name = 0122003880188006
Siemens-VNS-Name = zone_qua
Siemens-SSID = lab7_zone
Acct-Session-Time = 574
Acct-Output-Packets = 54
Acct-Input-Packets = 558
Acct-Output-Octets = 9814
```

```

Acct-Input-Octets = 64865
Acct-Terminate-Cause = 6
Authenticated_time = Sep 21 2005 19:30:42
Disassociation_time = Dec 31 1969 19:00:00

```

Optionally, the same record could be viewed by specifying its number on the filename list instead of by its filename, as follows:

```
EWC.extremenetworks.com# show cdrs 20050921wed 1
```

show clients apserial

Use the `show clients apserial` command to display all clients connected to a specified Wireless AP.

Use `show ap` to list the serial numbers of existing Wireless APs. For more information, see [show ap \(AP Configuration\)](#) on page 49.

```
show clients apserial ap_serial
```

Parameters

<i>ap_serial</i>	Specifies the serial number of an Wireless AP.
------------------	--

Examples

The following example lists the clients connected to the Wireless AP with the serial number 0001000418800008:

```

EWC.extremenetworks.com# show clients apserial 0001000418800008
Client IP Client MAC User Time Conn. BSS MAC SSID
Authentication Privacy Filter Protocol Pkts Sent Pkts Recvd Bytes Sent Bytes
Recvd
172.16.50.250 0:40:96:AB:61:58 - 00:04:00 00:0F:BB:09:F6:A2 CNL-103-CPx Ext
CP WPA-PSK Global a 6 48 883 4937
Total
6 48 883 4937

```

show clients vns

Use the `show clients vns` command to display all clients connected to a specified VNS.

Use `show vnsmode` to list the VNS names used on the Wireless Appliance. For more information, see [show vnsmode](#) on page 85.

```
show clients vns vns_name
```

Parameters

<i>vns_name</i>	Specifies the name of a Virtual Network Service on the Wireless Appliance.
-----------------	--

Examples

The following example lists the clients connected to the VNS using the name CNL-205-CPn:

```
EWC.extremenetworks.com# show clients vns CNL-205-CPn
```

Client	Client	User	Time	BSS	SSID	Authen	Pri	Fil	Proto
Pkts	Pkts	Bytes	Bytes						
IP	MAC		Conn.	MAC		tica	vacy	ter	col
Sent	Recvd	Sent	Recvd						
172.1	00:40:	-	00:00:	00:0F	CNL-	Ext	WPA-	Global	a
6	48	883	4937						
6.50.	96:AB:		40	:BB:	103-	CP	PSK		
250	61:58			09:	CPx				
				F6:A2					
Total									
6	48	883	4937						

show run-config

Use the `show run-config` to display the system's current running configuration commands.

```
show run-config
```

Parameters

None

show dns

Use the `show dns` command to display the DNS configuration.

```
show dns 1-3
```

Parameters

1-3	Specifies the position of the DNS server in the DNS servers list.
-----	---

Examples

```
EWC.extremenetworks.com# show dns 1
dns 1 192.1.1.3
```

show export

Use the `show export` command to display a list of available export files, or the details about the specific file. During the export process, the text files, containing the controller's configuration, cdrs, logs, audit are zipped for which the files display .zip extension. The configuration text files are displayed with .cli extension.

```
show export filename | number
```

Parameters

<i>filename</i>	Specifies the file name of an export file on the list. If the export file is located on a flash drive, the string "(flash)" must be suffixed to the end of the specified file name.
<i>number</i>	Specifies the index number of an export file on the list.

Examples

The following example displays all the exported text files that contain controller's configuration, cdrs, logs, audit, or all of them:

```
EWC.extremenetworks.com# show export
1: test-lab6.04102014.174541.zip
2: test-lab6.04102014.174554.zip
3: test-lab6.04102014.174608.zip
4: test-lab6.04102014.174619.zip
```

The following example displays the details associated with the export file stored on flash:

```
EWC.extremenetworks.com# show export last_bak.zip(flash)
Comment="Time for another backup"
Backup type="all"
Backup creation date="Tue Jan 14 17:29:49 2014"
Backup/Export saved from software version="C5210-09.01.01.0186"
```

show flash

Use the `show flash` command to display whether the flash device is mounted or not.

show flash status | sysinfo | list

Parameters

status	Displays whether the flash device is mounted or not.
sysinfo	Displays the memory usage information of the flash device.
list	Displays all the files on the flash device.

Usage

The `show flash` command is applicable only to the Wireless Appliances that support flash devices.

Examples

The following example displays that the flash device is mounted:

```
EWC.extremenetworks.com# show flash status
flash mounted
```

The following example displays the following memory usage information of the flash device:

- Size – Total capacity of the flash device.
- Used – Space used so far.

- Available – Space available for use.
- Use % – Space used in percentage.

```
EWC.extremenetworks.com# show flash sysinfo
Size      Used      Available  Use %
3.9G      32k       3.9G      1%
```

The following example displays the list of files that are saved on the flash device:

```
EWC.extremenetworks.com# show flash list
AC-MV-gxs-V5R3.10007.0-1.tar
gxs-V5R3.10007.0-1-rescue.tgz
```

show healthpoll

Use the `show healthpoll` command to display the current Health Poll Checking setting.

show healthpoll

Parameters

None

Example

The following example displays the current Health Poll Checking setting:

```
EWC.extremenetworks.com# show healthpoll
healthpoll enable
```

show import

Use the `show import` command to display all the imported files that contained the controller's configuration.

show import

Parameters

None.

Example

The following example displays all the imported files that contain the controller's configuration, cdrs, logs, audit:

```
EWC.extremenetworks.com# show import
1: Test_lab213_V5R3.10007-avail.zip
2: export_lab213_V4R1.7.10_NAMO_ENT.zip
3: lab-213-g.11042008.140940.zip
4: lab-213-g.11042008.141154.zip
5: lab-213-g.11042008.141200.zip
6: lab-213-g.webdomain.com.07032008.144403.zip
```

show import_status

Use the `show import_status` command to display the import status of the text file, containing the controller's configuration.

show import_status

Parameters

None

Examples

The following example displays the import status of the text file, containing the controller's configuration:

```
EWC.extremenetworks.com# show import_status
Import is in progress .....
Current status is 60%
```

The following example displays the import status when the import of the text file is not running:

```
EWC.extremenetworks.com# show import_status
Import process is not started
```

show key

Use the `show key` command to display the current product registration and capacity enhancement key information.

show key

Parameters

None

Examples

The following example displays the current product registration key settings:

```
EWC.extremenetworks.com# show key
Locking ID : 00-0C-29-C2-C7-1A
Regulatory Domain: FCC
Product Name: V2110 Medium
License mode: Lone
Number of Unused AP licenses: 4
Number of Licensed APs: 8
Number of Licensed APs(Foreign): 0
Number of Licensed APs(Total): 8
Number of Unused Radar licenses: 2
Number of Licensed APs for Radar: 2
Number of Licensed APs for Radar(Foreign): 0
Number of Licensed APs for Radar(Total): 2

Activation key string : PRDKVFCC-XXXXXXXX-XXXXXXXX-XXXXXXXX-XXXXXXXX

Capacity Enhancement Option Keys:
```


If there is an active Radar capacity enhancement key installed, the following example lines display:

```
Radar License Keys:
Capacity Enhancement Option Keys(foreign):
- CAP001-4GF7N297-RP14XZC6-KCCK6FZO-6A267BZS
- CAP001-X2AQQA8R-682K788X-QPP7LG9H-Q9BHQ50R
- CAPC20-IAGUNJZV-NB8K3DZV-UF96LJFN-R25H4DYZ
- CAPC20-IG24VZ5L-UDZQ7FY7-4CGOXB84-XGDK78JH

Radar License Keys(foreign):
- RADCAP025-OJ0N3AY3-OG5OSGAU-7BCRUCBH-O91VXDD7
```

show l2ports

Use the `show l2ports` command to display the properties of the Layer 2 ports.

show l2ports

Parameters

None

Examples

The following example displays the Layer 2 ports of a C25 Controller:

```
EWC.extremenetworks.com# show l2ports
Status  Enable  Port  MAC  Untagged Vlan  Tagged Vlan
UP      enable  esa0  00:25:90:30:F2:DC  10
UP      enable  esa1  00:25:90:30:F2:DD
DOWN    enable  lag1  00:25:90:30:F2:DD
UP      enable  admin 00:1B:21:82:A0:AA
```

show lanset

Use the `show lanset` command to display the ports' speed — the data transmission rate of an output/input channel on each port.

show lanset

Parameters

None

Examples

The following example displays the lanset settings of a C25 Controller:

```
EWC.extremenetworks.com# show lanset
Port name:          admin
Port Auto Negotiation: On
Port Speed:         Any
Port Duplex:        Both
Port Name:          lan1
Port Auto Negotiation: On
Port Speed:         Any
Port Duplex:        Both
```

```

Port Name:          lan2
Port Auto Negotiation: On
Port Speed:         Any
Port Duplex:        Both

```

show log

Use the `show log` command to display logs and reports for the Wireless Appliance.

```
show log log_name | first | last | number
```

Parameters

<i>log_name</i>	The log that you want to view: <ul style="list-style-type: none"> ospf-neighbor ospf-linkstate dhcp ntp ac (critical major minor info all) ap <ap_serial> (critical major minor info all) mu_access.log upgradeLog.txt auditRecords.log upgrade.log configChanges.log login.log station
first	Indicates that the first records in the log will be displayed.
last	Indicates that the last records in the log will be displayed.
<i>number</i>	Specifies the number of logs to display from the file.

Examples

The following example displays the first two records from the auditRecords log file:

```

EWC.extremenetworks.com# show log auditRecords.log first 2
 5516324453019803260admin
CLI_controller          general          key configuration
changed: activate TRDKNAM-NCF47ABS-I1BVRP9U-SGDKVBFR-NFBQ6ZJQ,
 5516324457314024504admin
CLI_system_management  general          downloading
import file from server 192.168.3.108

```

The following example displays the last five DHCP log messages:

```

EWC.extremenetworks.com# show log dhcp last 5
Timestamp      DHCP Message
Sep 13 20:33:14  dhcpd: DHCPACK to 172.21.177.21 (00:11:95:ec:a7:c0) via
esa9
Sep 13 20:34:53  dhcpd: DHCPINFORM from 172.21.177.21 via esa9
Sep 13 20:34:53  dhcpd: DHCPACK to 172.21.177.21 (00:11:95:ec:a7:c0) via
esa9

```

```
Sep 13 20:34:56   dhcpd: DHCPINFORM from 172.21.177.21 via esa9
Sep 13 20:34:56   dhcpd: DHCPACK to 172.21.177.21 (00:11:95:ec:a7:c0) via
esa9
```

The following example displays log entries from OSPF neighbors:

```
EWC.extremenetworks.com# show log ospf-neighbor
Neighbor RouterID   Router Priority   State   IP           Interface
192.168.12.7       1                Full/DR 10.91.0.2   esa0:10.91.0.1
```

The following example displays the log entries for the OSPF linkstate database:

```
EWC.extremenetworks.com# show log ospf-linkstate
Router LSA (Type 1):
Link ID           Advertising Router   Age      Sequence No   Checksum
Link Count
192.168.4.202    192.168.4.202      1460    0x80000085   0x8f18      3
```

The following example displays the log entries for upgradeLog.txt:

```
EWC.extremenetworks.com# show log upgradeLog.txt
OS-7_31_0-7
Wed Mar 19 14:21:48 EDT 2008 OS-5_1_8-1
Installing rpm of version V5R1.10034.0 on Wed Mar 19 14:21:53 EDT 2008
Tue Mar 10 12:39:04 EDT 2009 OS-5_3_17-1
Installing rpm of version V5R3.10034.0 on Tue Mar 10 12:39:11 EDT 2009
Mon Jun 1 10:52:53 EDT 2009 OS-6_0_19-1
Installing rpm of version V6R0.10019.0 on Mon Jun 1 10:52:59 EDT 2009
Thu Aug 20 14:47:27 EDT 2009 OS-6_1_8-1
Installing rpm of version V6R1.10029.0 on Thu Aug 20 14:47:39 EDT 2009
Installing rpm of version V6R1.10602.0 on Mon Sep 13 05:11:30 EDT 2010
Installing rpm of version 07.41.01.0122T on Mon Sep 13 05:31:02 EDT 2010
EWC.extremenetworks.com#
```

The following example displays the log entries for upgrade.log:

```
EWC.extremenetworks.com# show log upgrade.log
Sep 13 05:30:47 EDT 2010 From: V6R1.10602.0 To: 07.41.01.0122T
Sep 13 05:30:47 EDT 2010 C25 Upgrading From Release 6_1
Sep 13 05:35:05 EDT 2010 Successfully imported license
Sep 13 05:35:21 EDT 2010 Successfully Restored the Configuration
Sep 13 05:35:22 EDT 2010 Successfully Performed Netsight Import
EWC.extremenetworks.com#
```

The following example displays the log entries for configChanges.log:

```
EWC.extremenetworks.com# show log configChanges.log
CLI Import/EWC.extremenetworks.com: start: Tue Sep 14 00:27:57 2010
CLI Import/EWC.extremenetworks.com: end: Tue Sep 14 00:28:16 2010
EWC.extremenetworks.com#
```

The following example displays the station log entries:

```
EWC.extremenetworks.com# show log station
Msg: 06/14/13 06:58:34 EventType[De-registration]
MAC[00:24:D7:23:89:4C] BSSID[00:0F:BB:09:EC:E9]           Details:
VNS[CNL-91-0-6] Cause[Idle timeout]
```

```

Msg: 06/14/13 05:49:48 EventType[State Change] MAC[00:24:D7:23:89:4C]
IP[172.21.176.54] BSSID[00:0F:BB:09:EC:E9] SSID[CNL-91-0-6-
ssid] User[tester1]
Msg: 06/14/13 05:49:45 EventType[Authentication]
MAC[00:24:D7:23:89:4C] AP[0500006072051204] BSSID[00:0F:BB:
09:EC:E9] SSID[CNL-91-0-6-ssid]User[tester1] Details:
VNS[CNL-91-0-6] AppliedRole[CNL-91-0-6-default]
Msg: 06/14/13 05:49:45 EventType[State Change] MAC[00:24:D7:23:89:4C]
BSSID[00:0F:BB:09:EC:E9] Details: VNS[CNL-91-0-6] Auth[valid]
Msg: 06/14/13 05:49:44 EventType[State Change] MAC[00:24:D7:23:89:4C]
BSSID[00:0F:BB:09:EC:E9] Details: VNS[CNL-91-0-6] Auth[invalid]
Msg: 06/14/13 05:49:44 EventType[MBA Accepted] MAC[00:24:D7:23:89:4C]
AP[0500006072051204] BSSID[00:0F:BB:09:EC:E9] SSID[CNL-91-0-6-
ssid] Details: VNS[CNL-91-0-6] AppliedRole[CNL-91-0-6-default]
Msg: 06/14/13 05:49:44 EventType[Registration] MAC[00:24:D7:23:89:4C]
AP[0500006072051204] BSSID[00:0F:BB:09:EC:E9] SSID[CNL-91-0-6-
ssid] Details: Radio[2]

```

show loglevel

Use the `show loglevel` command to display the system log level of the Wireless Appliance or the Wireless AP.

```
show loglevel ac | ap
```

Parameters

ac	Displays the log level of the Wireless Appliance.
ap	Displays the log level of the Wireless AP.

Examples

The following displays the system log level of both the Wireless Appliance and the Wireless AP:

```

EWC.extremenetworks.com# show loglevel
AC Log level: Major (2)
AP Log level: Critical (1)
Report station session events on controller: enable
Forward station session events as traps: disable
Send station session events to NetSight: enable

```

The following displays the system log level of the Wireless Appliance only:

```

EWC.extremenetworks.com# show loglevel ac
AC Log level: Major (2)

```

The following displays the system log level of the Wireless AP only:

```

EWC.extremenetworks.com# show loglevel ap
AP Log level: Critical (1)

```

show ospf

Use the `show ospf` command to display the system's Open Shortest Path First (OSPF) interfaces and configuration.

show ospf interface | neighbors | config | database

Parameters

interface	Displays the details of all current OSPF interfaces.
neighbors	Displays the OSPF neighbors with which the Wireless Appliance has adjacency.
config	Displays the OSPF configuration details.
database	Displays the OSPF linkstate database.

Examples

The following example displays the details of all OSPF interfaces:

```
EWC.extremenetworks.com# show ospf interface
OSPF Interface #0:
  Port Name           :esa0
  OSPF Status         :Enabled
  OSPF authentication :None
  Link Cost           :10
  Hello Interval      :10
  Dead Interval       :40
  Retransmit Interval :5
  Transmit Delay      :1
```

The following example displays the details of all OSPF neighbors:

```
EWC.extremenetworks.com# show ospf neighbors
Neighbor ID  Router ID      Priority  State      IP Address  Interface
1            192.168.4.3   1        Full/DR    10.209.0.2
esa0:10.209.0.1
```

The following example displays all OSPF configuration data:

```
EWC.extremenetworks.com# show ospf config
OSPF Area           :0.0.0.5
OSPF Area Type      :default
OSPF Router ID      :
OSPF Protocol Status :enable
```

The following example displays OSPF information from a database:

```
EWC.extremenetworks.com# show ospf database
Router LSA (Type 1):
Link ID          Advertising Router  Age      Sequence No  Checksum  Link
Count
10.203.1.2       10.203.1.2         1745    0x800001c3  0xae1f   17
10.206.0.1       10.206.0.1         1525    0x8000009d  0x782e   3
Network LSA (Type 2):
Link ID          Advertising Router  Age      Sequence No  Checksum
10.109.0.2       192.168.4.3        334     0x800000a8  0x781d
```

```

10.203.0.2    192.168.4.3          334    0x80000713    0xb73a
Network Summary LSA (Type 3):
Link ID      Advertising Router   Age     Sequence No    Checksum    Route
10.2.0.0     192.168.4.3         76     0x80000080    0xd36a
10.2.0.0/24
10.2.0.0     192.168.4.9         969    0x8000007f    0xb187
10.2.0.0/24
ASBR Summary LSA (Type 4):
Link ID      Advertising Router   Age     Sequence No    Checksum
10.203.1.2   192.168.4.3         1324   0x8000002b    0xd1f4
10.203.1.2   192.168.4.9         970    0x8000002b    0xa31e
AS-External LSA (Type 5):
Link ID      Advertising Router   Age     Sequence No    Checksum
Route
0.0.0.0     192.1.5.115         806    0x80000030    0x160a
0.0.0.0/0
10.22.1.0   192.168.3.2         585    0x800006f1    0x30e9
10.22.1.0/24

```

show policy

Use the `show policy` command to display configuration information for all policies configured on the Wireless Appliance.

show policy

Examples

The following example displays configuration information about all configured policies:

```

EWC.extremenetworks.com# show policy
Policy Name  Topology          Ingress rate  Egress rate  Mode  Filter
defined
              profile          profile
open         Seg1_Routed       no-change     no-change     routed Yes
unAuth       Seg2_Routed       no-change     no-change     routed Yes
Auth         Seg2_Routed       no-change     no-change     routed Yes
BAC          Bridged at AP     no-change     no-change     b@ap  Yes
              untagged

```

show role

Use the `show role` command to display the current roles for this system.

show role

Parameters

None

Examples

The following displays the current roles for this system:

```

EWC.extremenetworks.com# show role
Role name    Topology          Class of Service  Mode  Filter

```

```

defined
CNL-218-0-0-default          CNL-218-0-0    Authenticated CoS
routed      Yes
CNL-218-0-0-non-authenticated CNL-218-0-0    Non-Authenticated CoS
routed      Yes
CNL-218-0-1-default          CNL-218-0-1    no-change
routed      Yes
CNL-218-0-1-non-authenticated CNL-218-0-1    no-change
routed      Yes
CNL-218-0-2-default          CNL-218-0-2    no-change
b@ac        Yes

```

show wlans

Use the `show wlans` command to display a list of all WLAN Services configured on the Wireless Appliance.

show wlans

Examples

The following example displays information about all configured WLAN Services:

```

EWC.extremenetworks.com# show wlans

Name           Service      Enabled   SSID      Privacy   Auth Mode
              Type
Lab12-open     std          enabled   Lab12-    none      disabled
              open
Lab12-INT_CP   std          enabled   Lab12-    none      internal
              INT_CP    none      disabled
Lab12-1        std          enabled   Lab12-1   none      disabled
top-routed     std          enabled   aaaa      none      disabled
Lab12-EXT_CP   std          enabled   Lab12-    none      external
              EXT_CP

```

show report

Use the `show report` command to display a list of all activity reports on the Wireless Appliance, or detailed information within an individual report.

show report *report_name*

Parameters

<i>report_name</i>	Specifies the report name from the list of activity reports.
--------------------	--

Examples

The following example displays a list of activity reports available on the Wireless Appliance:

```
EWC.extremenetworks.com# show report
reports:
active_clients
active_clients_by_vns
active_clients_by_wireless_apserial
active_wireless_aps
active_wireless_load_groups
admission_control_wireless_aps
ap_availability
clients-home-controller

clients_by_home
external_connection
mesh_wds_wlan_wireless_ap_stats
mobility_tunnel_matrix
policy_filter_stats
radius_stats
remotable_vns_information
remote_states
topology_filter_stats
topology_stats
wired_ap_stats <ap-serial-number>
wireless_ap_stats
wireless_controller_port_statistics
```

The following example displays information contained within the external_connection report:

```
EWC.extremenetworks.com# show report external_connection
Connection Security Level
192.168.1.10 Open
192.168.3.25 Private
```

The following example displays information contained within the active_wireless_aps report:

```
EWC.extremenetworks.com# show report active_wireless_aps
name: 0409920201201319
serial: 0409920201201319
AP IP: 10.7.0.54
Num Clients: 0
Home: LOCAL
Packets sent: 0
Packet Received: 0
Bytes Sent: 0
Bytes Received: 0
802.11b/g Channel: 1 Power: 0
802.11a Channel: 1 Power: 0
```

The following example displays clients connected to the home Wireless Appliance:

```
EWC.extremenetworks.com# show report clients_by_home
ac_ip 10.109.0.1
ac_ixp_addr 10.109.0.1
ac_desc C20-37
```



```

mu_ip 172.22.214.30
mu_mac 00:03:7F:BF:16:9F
mu_user
home ip 10.109.0.1
Tunnel with 10.109.0.4 Disconnected
Tunnel with 10.209.0.1 Disconnected
ac_ip 10.109.0.4
ac_ixp_addr 10.109.0.4
ac_desc controller
Tunnel with 10.209.0.1 Disconnected
Tunnel with 10.109.0.1 Disconnected
ac_ip 10.209.0.1
ac_ixp_addr 10.209.0.1
ac_desc EWC
Tunnel with 10.109.0.4 Disconnected
Tunnel with 10.109.0.1 Disconnected

```

The following example displays client connected to foreign EWC:

```

EWC.extremenetworks.com# show report clients_by_foreign_EWC
ac_ip 10.109.0.1
ac_ixp_addr 10.109.0.1
ac_desc C20-37
mu_ip 172.22.215.27
mu_mac 00:14:6C:F6:A4:4E
mu_user wzhu
home ip 10.109.0.1
Tunnel with 10.209.2.1 Connected
Tunnel with 10.109.1.4 Connected
Tunnel with 10.109.0.5 Connected
Tunnel with 10.209.0.3 Connected
ac_ip 10.109.1.4
ac_ixp_addr 10.109.1.4
ac_desc EWC
Tunnel with 10.209.2.1 Connected
Tunnel with 10.109.0.1 Connected
Tunnel with 10.109.0.5 Connected
Tunnel with 10.209.0.3 Connected
ac_ip 10.209.0.3
ac_ixp_addr 10.209.0.3
ac_desc EWC
Tunnel with 10.109.0.1 Connected
Tunnel with 10.109.0.5 Connected
Tunnel with 10.109.1.4 Connected
Tunnel with 10.209.2.1 Connected
ac_ip 10.209.2.1
ac_ixp_addr 10.209.2.1
ac_desc EWC
Tunnel with 10.109.1.4 Connected
Tunnel with 10.109.0.1 Connected
Tunnel with 10.109.0.5 Connected
Tunnel with 10.209.0.3 Connected
ac_ip 10.109.0.5
ac_ixp_addr 10.109.0.5
ac_desc EWC
Tunnel with 10.209.2.1 Connected
Tunnel with 10.109.1.4 Connected
Tunnel with 10.109.0.1 Connected

```

```
Tunnel with 10.209.0.3 Connected
EWC.extremenetworks.com#
```

The following example displays a nearby AP status report for AP 0000141600040802 radio1:

```
EWC.extremenetworks.com# show report nearby_ap_stats 0000141600040802 radio1
```

show restore

The `show restore` command is deprecated. See [show import](#) on page 63.

show routes

Use the `show routes` command to display the routing table or static routes of the Wireless Appliance.

show routes all | static

Parameters

all	Displays the routing table.
static	Displays the static routes.

Examples

The following example displays the routing table:

```
EWC.extremenetworks.com# show routes all
Dest Addr          Netmask          Gateway          Interface
RouteType         Status
0.0.0.0            0.0.0.0          10.7.0.2         esa0
Static            Active
10.7.0.0           255.255.255.0    None             esa0
Connected         Active
10.7.1.0           255.255.255.0    None             esa1
Connected         Active
127.0.0.0          255.0.0.0        None             lo             Kernel
Inactive
127.0.0.0          255.0.0.0        None             lo
Connected         Active
136.157.233.128    255.255.255.128  192.168.1.1     eth0
Kernel            Active
172.16.113.0       255.255.255.0    None             esa2
Connected         Active
172.16.114.0       255.255.255.0    None             esa3
Connected         Active
172.16.117.0       255.255.255.128  None             esa5
Connected         Active
172.16.117.128    255.255.255.128  None             esa6
Connected         Active
172.16.118.0       255.255.255.192  None             esa7
Connected         Active
172.16.118.64     255.255.255.192  None             esa8
Connected         Active
172.16.118.128    255.255.255.192  None             esa9
Connected         Active
```

```

172.16.118.192      255.255.255.192   None           esa4
Connected        Active
172.16.125.0       255.255.255.0     None           esa10
Connected        Active

```

The following example displays the static routes on the Wireless Appliance:

```

EWC.extremenetworks.com# show routes static
RouteID   Dest Addr   Netmask   Next Hop   Interface   OverrideDynamic
1         0.0.0.0     0.0.0.0   10.7.0.2   1           on

```

show schedule_backup

Use the `show schedule_backup` command to display the current scheduled backup settings.

show schedule_backup

Parameters

None

Examples

```

EWC.extremenetworks.com# show schedule_backup
protocol ftp
server 192.168.4.81
user admin
password *****
dir /home/user/destdir
type all
freq daily everyday
starttime 02:00
destination remote

```

show schedule_upgrade

Use `show schedule_upgrade` command to display the current scheduled upgrade settings.

show schedule_upgrade

Parameters

None

Examples

```

EWC.extremenetworks.com# show schedule_upgrade
schld_upgrd 10:01:01:02 local AC-MV-07.41.03.0003-1.rue
upgrade_backup remote 192.168.4.121 test abc123 /tmp/v53 L103-
C25-07.41.03.0003-rescue-user.tgz

```

show snmp

Use the `show snmp` command to display the SNMP settings for the Wireless Appliance.

show snmp*Parameters*

None

Examples

The following example displays the SNMP settings for the Wireless Appliance:

```
EWC.extremenetworks.com# show snmp
SNMP v1/v2
contact Bill Smith
location lab-91
rcommunity public
rwcommunity private
context
severity 4 (informational)
port 162
publish-ap enable
trap-manager-v1v2 1 136.157.233.176
trap-manager-v1v2 2 192.168.3.108
no SNMPv3 trap1 destination
no SNMPv3 trap2 destination
```

show stats

Use show stats to display throughput related statistics for the Wireless APs and for the Wireless Appliance interfaces.

Use show ap to list the serial numbers of existing Wireless APs. For more information, see [show ap \(AP Configuration\)](#) on page 49.

```
show stats ap | ap_serial | wired | wireless | radio1 | radio2 | interface |
interface_name
```

Parameters

ap	Displays properties of an Wireless AP.
<i>ap_serial</i>	Specifies the serial number of an Wireless AP.
wired	Displays the hardwired connection.
wireless	Displays the wireless connection.
radio1	Displays radio1 statistics.
radio2	Displays radio2 statistics.
interface	Displays properties of a port on the Wireless Appliance.
<i>interface_name</i>	Specifies the name of a port on the Wireless Appliance.

Examples

The following example displays statistics for the Wireless AP0001000418800008:

```
EWC.extremenetworks.com# show stats ap 0001000418800008
Serial:          0409920201203917
IP Address:     10.222.0.126
Clients:        1
Home:           local
Session start:  2008-06-18 19:30:50
Uptime:         9878.13333333 min
Packets Sent:   419350
Packets Received: 936371
Bytes Sent:     110108177
Bytes Received: 428278710
Protection Mode: on
802.11b/g Ch/Tx: 2462 /15
802.11a Ch/Tx:  5200 /16
```

The following example displays the statistics for the same Wireless AP over its wired connection:

```
EWC.extremenetworks.com# show stats ap 0001000418800008 wired
IP Address:     10.222.0.126
Status:         approved
Statistics      Receive      Transmit
Discarded Packets 1661         0
Total Errors      0             0
Unicast Packets   645614       419231
Multicast Packets 201404       3
Broadcast Packets 90139        488
Total Packets     0             419722
Total Bytes       428661221    110236012
```

The following example displays the statistics for Wireless AP 0500006072051204 over the radio1 wireless connection:

```
EWC.extremenetworks.com# show stats ap 0500006072051204 wireless radio1
Mode: a
MAC Address: 00:0F:BB:09:EC:E0
MAC Address: 00:0F:BB:09:EC:E1
MAC Address: 00:0F:BB:09:EC:E2
MAC Address: 00:0F:BB:09:EC:E3
MAC Address: 00:0F:BB:09:EC:E4
SSID: CNL-91-0-0-ssid
SSID: CNL-91-0-1-ssid
SSID: CNL-91-0-2-ssid
SSID: CNL-91-0-3-ssid
SSID: CNL-91-WDS-ssid
Operational Max Rate: 54
Channel: 157:5785MHz
Current Power Level(dBm): 0
IP Address:     10.91.0.50
Status:         approved
There are no active clients on this radio
There are 1 WDS Children.
Statistics      Received      Transmitted
Discarded Packets 1             1
```

Errors	82519	1	
Unicast Packets	0	46605	
Multicast Packets	0	0	
Broadcast Packets	0	0	
Total Successful Packets	0	46605	
Total Successful Bytes	727933	6815737	
Statistics			802.11 MIB Values
WEP ICV Error Count			0
WEP Excluded Count			0
Retry Count			0
Multiple Retry Count			0
RTS Success Count			0
RTS Failure Count			0
ACK Failure Count			609
Frame Duplicate Count			1
Transmitted Fragment Count			5312
Multicast Transmitted Frame Count			0
Failed Count			1
Received Fragment Count			46605
Multicast Received Frame Count			0
FCS Error Count			124944
WEP Undecryptable Count			0
Deauthentications Due to CAC			0
DCS Channel Utilization by Adjacent AP's [%] - Average			n/a
DCS Channel Utilization by Adjacent AP's [%] - Maximum			n/a
DCS Tx Channel Utilization [%] - Average			n/a
DCS Tx Channel Utilization [%] - Maximum			n/a
DCS Rx Channel Utilization [%] - Average			n/a
DCS Rx Channel Utilization [%] - Maximum			n/a
DCS Noise [dBm] - Average			n/a
DCS Noise [dBm] - Maximum			n/a

The following example displays the statistics for the interface esa0:

```
EWC.extremenetworks.com# show stats interface esa0
Frames Transmitted:      466898
Frames Received:        673553
Octets Transmitted:     105750978
Octets Received:       131981692
Multicast Frames Transmitted:  11
Multicast Frames Received:    1419
Broadcast Frames Transmitted: 2852
Broadcast Frames Received:   1197
Pause Frames Transmitted:    0
Pause Frames Received:      0
Frame Check Sequence Error:  0
Frame Too Long Errors:     0
```

show syslog

Use the `show syslog` command to display system log levels.

show syslog

Parameters

None

Examples

The following example displays the current system log levels:

```
EWC.extremenetworks.com# show syslog
syslogip 1 192.168.3.106 enable
syslogip 2 192.168.4.129 enable
syslogip 3 192.168.4.200 enable
svcmsg
audmsg
stationevent enabled
facility application 0
facility service 4
facility audit 6
facility station 1
```

show system_state

Use the `show system_state` command to display the Wireless Appliance's system information.

```
show system_state process | cpu | memory | disk | mgmt | uptime | info |
manufacturing
```

Parameters

process	Displays the current CPU and memory usage of system processes.
cpu	Displays the amount of CPU usage.
memory	Displays the amount of memory being used on the system.
disk	Displays the hard-disk usage by folder.
mgmt	Displays the system management settings.
uptime	Displays the amount of time the system has been running continuously.
info	Displays the information on various processes run by the system.
manufacturing	Displays hardware information about the controller.

Examples

The following example displays the current processes running on the system:

```
EWC.extremenetworks.com# show system_state process
PID      Process Name      State      % CPU      % Mem
1123     VN Manager        S          0.0        0.9
8010     NSM Server        S          0.0        0.6
16527    Config Manager    S          0.0        1.6
1425     CLI               S          0.0        3.5
-        OSPF Server       inactive   -          -
-        Remote INS       inactive   -          -
15891    Langley           S          0.0        0.5
1111     RU Manager        S          0.0        0.9
15893    SNMP Agent        S          0.0        0.5
-        RF Data Collector inactive   -          -
23758    Radius Client     S          0.0        0.5
960     Stats Server      S          0.0        0.6
16566    Security Manager  S          0.0        0.9
```

```

656      Event Server          S          0.0      1.4
548      Startup Manager       S          0.0      0.5
1131     RU Session Manager     S          0.0      0.5
974      Host Services Manager S          0.0      2.3
1117     Radius Accounting       S          0.0      0.4
-        DHCP                  inactive   -         -
990      Test Client            S          0.0      0.4
1129     LLC Handler             S          0.0      0.6

```

The following example displays the CPU usage on the system:

```

EWC.extremenetworks.com# show system_state cpu
CPU states: 1.5% user, 1.5% system, 0.0% nice, 6.8% idle

```

The following example displays the memory usage on the system:

```

EWC.extremenetworks.com# show system_state memory
Mem: 247372K av, 235516K used, 11856K free, 0K shrd, 67528K buff
Swap: 1028120K av, 6368K used, 1021752K free 85756K
cached

```

The following example displays the hard disk usage (C25 platform):

```

EWC.extremenetworks.com# show system_state disk
Partition  Total Space  Used  Available  Use %
root       27193624    381960 25992592   2%
home       2040016     32840 1986696    2%
cdr         2032048     32812 1978756    2%
logs        1528032     33180 1479512    3%
reports     1522032     32812 1473880    3%
trace       1531008     32812 1482856    3%
tmp         131072      32     131040    1%

```

The following example displays the system management settings:

```

EWC.extremenetworks.com# show system_state mgmt
Software version: 9.xx
Software build: 09.xx.0x.0xxx
Product Name: C25
Hostname: EWC
Domain: extremenetworks.com
IP Address: 192.168.33.333
Subnet Mask: 255.255.255.0
Mgmt Gateway: 192.168.22.2
Static IPv6 Address: fd66:2280:2669:ffff::102 64
Static IPv6 Gateway: fd66:2280:2669:ffff::105
Dynamic IPv6 Address:
1: fd66:2280:2669:ffff:021b:21ff:feb0:899a 64
2: fd66:2280:2669:0000:021b:21ff:feb0:899a 64
3: fe80:0000:0000:0000:021b:21ff:feb0:899a 64
4: fe80:0000:0000:0000:0230:48ff:fe77:a94a (gw)
Primary DNS: fd66:2280:2669::f
Secondary DNS: 192.168.33.332
Time Zone: America/Montreal
Country: CA

```


The following example displays system uptime:

```
EWC.extremenetworks.com# show system_state uptime
System uptime: 6 days, 1:49
```

show tech_support

Use the `show tech_support` command to display a list of technical support files available on the system.

Use `tech_support` to generate technical support files. For more information, see [tech_support](#) on page 87.

show tech_support

Parameters

None

Examples

The following example displays the available technical support files:

```
EWC.extremenetworks.com# show tech_support
1: tech-ac.tar.gz
2: tech-all.tar.gz
3: tech-ap.tar.gz
4: tech-log.tar.gz
```

show time

Use the `show time` command to display the system time.

show time

Parameters

None

Examples

The following example displays the system time and time server settings:

```
EWC.extremenetworks.com# show time
Fri Mar 14 11:49:24 EDT 2014
```

show time-config

Use the `show time-config` command to display the system time and time server settings.

show time-config

Parameters

None

Examples

The following example displays the system time and time server settings:

```
EWC.extremenetworks.com# show time-config
ntp: internal ntp server
ntpip 1 192.168.4.84
ntpip 2 192.168.4.89
ntpip 3 200.200.200.200
tz America/Montreal
```

show topology

Use the `show topology` command to display the IDs and names of IP interfaces.

show topology 13

Parameters

13	Displays only topologies with an L3 configuration. The topologies are listed by index number.
-----------	---

Usage

You can identify an IP using its interface name or, for short, the identifier returned by the `show topology 13` command. Interface name is the name of any topology with L3 configuration (Physical, Admin, B@AC or Routed).

Examples

The following example displays the output of the `show topology` command when run without additional parameters:

```
EWC.extremenetworks.com# show topology

Name                               Mode           L2:VlanId,port           L3:IP,GW,DHCP

Admin                               admin          N/A,Admin
192.168.4.37,192.168.4.11,N/A

esa0                                physical      545,esa0
10.109.0.1,10.0.0.2,none

esa1                                physical      -1,esa1
10.0.1.1,10.0.1.2,none

Bridged at AP untagged             b@ap          -1,N/A
Extreme-37Topology                 b@ac          647,esa0
10.209.2.37,0.0.0.0,none
777                                 b@ac          777,esa-1
649                                 b@ac          649,esa-1
650                                 b@ac          650,esa0

Topology global info:
Internal VLAN ID: 1
Multicast support:
disabled
```

The following example uses the `show topology 13` command to obtain interface information for use with the ping or traceroute commands:

```
EWC.extremenetworks.com# show topology 13
```

Name	Mode	L3:IP
1:Admin	physical	192.168.4.37
2:esa0	physical	10.0.0.1
3:esa1	physical	10.0.1.1
4:Extreme-37Topology	b@ac	10.10.1.1
5:CNL-209-AAA:engineering	routed	172.22.2.1

show traffic_capture

Use the `show traffic_capture` command to display the status of traffic capture.

show traffic_capture

Parameters

None

Examples

The following is the example of the status display when the traffic capture is running:

```
EWC.extremenetworks.com# show traffic_capture
Interface:
Size: 1000(MB).
Filename: mgmt_traffic_dump.cap
Destination: local
Capture Status: stopped
Traffic Capture Files:
  1:mgmt_traffic_dump.cap
```

show upgrade

Use the `show upgrade` command to display all of the software upgrade images available on the Wireless Appliance.

Files located on an external flash device have (flash) next to them. In the above example, the file AC-MV-07.41.03.0003-1.rue (flash) is located on the flash device.

show upgrade

Parameters

None

Examples

The following example displays the upgrade images on the Wireless Appliance:

```
EWC.extremenetworks.com# show upgrade
1: AC-MV-07.41.03.0003-1.rue (flash)
```

show upgrade_backup_dest

Use the `show upgrade_backup_dest` command to display the settings of FTP server where the controller's existing image is backed up.

```
show upgrade_backup_dest
```

Parameters

None

Examples

```
EWC.extremenetworks.com# show upgrade_backup_dest
upgrade_backup_dest 192.168.4.181 admin abc123 / backupClone.tgz
```

show upgrade_history

Use the `show upgrade_history` command to display the software upgrade history.

```
show upgrade_history
```

Parameters

None

Examples

```
EWC.extremenetworks.com# show upgrade_history
Date      Type      Version
Thu Feb 24 11:41:00 EST 2011    Upgraded      07.41.01.0150
Tue Jan 11 10:36:44 EST 2011    Installed     07.41.01.0100T
Tue Jan 11 10:36:27 EST 2011    Installed     OS-7_41_0-7
```

show upgrade_image_src

Use `show upgrade_image_src` command to display the settings of FTP server where the controller's new image is located.

```
show upgrade_image_src
```

Parameters

None

Examples

```
EWC.extremenetworks.com# show upgrade_image_src
upgrade_image_src 192.168.4.10 admin abc123 /rpms AC-MV-07.41.03.0003-1.gxs
```

show users

Use the `show users` command to display the user and administrator accounts defined on the Wireless Appliance.

show users*Parameters*

None

Examples

The following example displays the users defined on the Wireless Appliance:

```
EWC.extremenetworks.com# show users
ID      Privilege
admin   admin
test    admin
```

show vnsmode

Use the `show vnsmode` command to display all VNS information for every VNS on the Wireless Appliance.

show vnsmode*Parameters*

None

Examples

The following example displays a list of every VNS currently on the Wireless Appliance:

```
EWC.extremenetworks.com# show vnsmode
```

VNS Topology	Enabled Mode	WLAN Service	Authentication	Privacy	Default Policy
Lab12-open	enabled	Lab12-open	disabled	none	open
Seg1_Routed	routed				
Lab12-INT_CP	enabled	Lab12-	internal	none	UnAuth
Seg2_Routed	routed				
testvns	enabled	Lab12-1	disabled	none	Auth
Seg2_Routed	routed				
3PAP	disabled	3PAP	disabled	none	3PAP
esa2	physical				

show vnsmode radius

Use the `show vnsmode radius` command to display configured RADIUS server information for the Wireless Appliance.

show vnsmode radius

Parameters

None

Examples

The following example displays a list of every RADIUS server currently known by the Wireless Appliance:

```
EWC.extremenetworks.com# show vnsmode radius
Strict: disable
Radius MAC format:1.XXXXXXXXXXXXX
```

Name	IP address	Protocol	Retries	Timeout
Ports	Priority		(Auth:Acct)	(Auth:Acct)
(Auth:Acct)	(Auth:Acct)			
IAS	192.0.1.202	PAP	3:3	5:5
1812:1813	4:4			
Lab	134.14.12.23	PAP	3:3	5:5
1812:1813	1:1			
test-radius	10.10.10.10	PAP	3:3	5:5
1812:1813	5:5			

show web

Use the `show web` command to display the web timeout time (in minutes) – the time after which the web session will time out.

show web

Parameters

None

Examples

The web timeout time is displayed in hh:mm format. In the following example, the web timeout time is 1 hour:

```
EWC.extremenetworks.com# show web
timeout 1:00
no showvns
guestportal-admin-timeout 0:01
```

shutdown

Use the `shutdown` command to stop or reboot the Wireless Appliance.

shutdown **halt** | **reboot**

Parameters

halt	Stop the Wireless Appliance.
reboot	Reboots the Wireless Appliance.

Examples

The following example reboots the Wireless Appliance:

```
EWC.extremenetworks.com# shutdown reboot
```

tech_support

Use the `tech_support` command to create compressed technical support files containing system information. Use the `no` form of the command to delete them.

Use `show tech_support` to display a list of technical support files created on the system. For more information, see [show tech_support](#) on page 81.

```
tech_support ap | nostats | ac | log | all | nostats | lite | filename no  
tech_support | filename | number
```

Parameters

ap	Collects Wireless AP information.
ac	Collects Wireless Appliance information.
log	Collects log information.
all	Collects Wireless AP, Wireless Appliance, and log information.
lite	Creates a smaller technical support file that can be used for a controller Health Check review. The lite support file includes: <ul style="list-style-type: none"> • Log file messages • Error messages • AP alarms • Controller CLI configuration • Upgrade log information • auditRecords_readable.log
<i>filename</i>	Specifies the file name.
<i>number</i>	Specifies the how listed number the file appears.
nostats	This parameter can be used with [tech_support ap] and [tech_support all]. If the [nostats] option is specified, the technical support file will not have any traffic statistic information.

Usage

Issue the `tech_support` command to gather information about the AP, information about the controller, or information about both the AP and the controller. The `tech_support lite` command creates a smaller file that can be used for a controller Health Check Review.

Examples

The following example creates a tech support file for Wireless AP, Wireless Appliance, and log information, which is assigned a default file name. A comment to identify the file is also added:

```
EWC.extremenetworks.com# tech_support all
Filename (tech_support.06122005.135027):
Comment: Technical support information for MrUser12
Please wait...
Creating tech_support.06122005.135027...
Executing AP commands...
.....
Executing AC commands...
.....
.....
Executing LOG commands...
Tech_support backup complete.
```

The following example deletes a tech support file by name:

```
EWC.extremenetworks.com# no tech_support tech_ap.tar.gz
Successfully deleted file tech_ap.tar.gz
```

The following example creates a lite tech support file that can be used for a controller Health Check Review.

```
EWC.extremenetworks.com# tech_support lite 052716
Please wait...
CLI Export start: Fri May 27 12:03:05 2016
CLI Export end: Fri May 27 12:03:08 2016
Creating 052716...
Executing LOG commands...
Tech_support backup complete.
```

traceroute

Use the `traceroute` command to perform a traceroute to a specified IP address. Optionally, you can specify the source interface.

```
traceroute source-interface | name | number id | IP Address
```

Parameters

source-interface	Keyword indicating that a source interface will be specified.
<i>name</i>	Identifies the source interface by name. The names are platform specific. You can use the <code>show topology</code> command to display a list of interfaces.

<i>number id</i>	Identifies the source interface by number. The numbers are platform specific.
<i>IP Address</i>	Specifies an IP address. The IP address can be either IPv4 <i>A.B.C.D</i> or IPv6 <i>A:B:C:D:E:F:G:H</i> format.

Examples

The following example performs a traceroute to a specified IP Address:

```
EWC.extremenetworks.com# traceroute 68.142.226.40
traceroute to 68.142.226.40 (68.142.226.40), 30 hops max, 38 byte packets
 1 192.168.1.1 (192.168.1.1) 0.801 ms 0.749 ms 0.729 ms
 2 67.69.27.57 (67.69.27.57) 1.898 ms 1.909 ms 1.894 ms
 3 64.230.194.178 (64.230.194.178) 9.660 ms 14.352 ms 11.032 ms
 4 64.230.233.81 (64.230.233.81) 9.666 ms 10.382 ms 9.307 ms
 5 64.230.222.21 (64.230.222.21) 10.266 ms 10.114 ms 10.300 ms
 6 206.108.107.230 (206.108.107.230) 10.169 ms 9.392 ms 10.494 ms
 7 209.58.25.69 (209.58.25.69) 10.458 ms 9.367 ms 10.942 ms
 8 216.6.57.33 (216.6.57.33) 28.928 ms 29.757 ms 30.315 ms
 9 216.6.57.42 (216.6.57.42) 36.011 ms 35.677 ms 34.488 ms
10 63.243.149.110 (63.243.149.110) 38.094 ms 33.761 ms 35.160 ms
11 216.115.96.189 (216.115.96.189) 34.285 ms 216.115.96.173
   (216.115.96.173) 40.339 ms 216.115.96.193 (216.115.96.193) 34.594 ms
12 206.190.33.95 (206.190.33.95) 36.994 ms 206.190.33.93 (206.190.33.93)
   36.402 ms 206.190.33.89 (206.190.33.89) 32.584 ms
13 68.142.226.40 (68.142.226.40) 36.595 ms 35.023 ms 35.818 ms
```

The following example performs a traceroute, specifying the source interface by number:

```
EWC.extremenetworks.com# traceroute source-interface number 2 192.168.3.12
traceroute to 192.168.3.12 (192.168.3.12) from 10.1.0.1, 30 hops max, 38 byte
pa
ckets
 1 ac_esa_port_0 (10.1.0.1) 3001.190 ms !H 3000.825 ms !H 3000.581 ms !H
```

upgrade ac

Use the `upgrade ac` command to upgrade the controller software. The `upgrade ac` command is accessible from the root context of the CLI.

```
upgrade ac filename | number | ftp | bckto local | bckto ftp | bckto flash
filename
```

Parameters

<i>filename</i>	Specifies the file name of the new image.
<i>number</i>	Specifies an ordinal image number returned by the <code>show upgrade</code> command
<i>ftp</i>	Specifies ftp server on which the upgrade image is uploaded. This ftp server is set by <code>upgrade_image_src</code> command.
bckto local	Backs up the existing operating system of the controller to the local drive. The <code>bckto local</code> command is supported only on the platforms that support local storage.

bckto ftp	Backs up the existing operating system of the controller to the remote FTP server. The FTP server is set by the <code>upgrade_backup_dest</code> command.
bckto flash filename	Backs up the existing operating system of the controller to the external flash.

- If you use the `bckto ftp` option in the syntax, you must first set the settings of the ftp server, where the existing os image will be backed up, by running the `upgrade_backup_dest` command. For more information, see [upgrade_backup_dest](#) on page 91.
- If you use the `ftp` option in the syntax, you must first specify the details of the ftp server, where the new image is located, by running the `upgrade_image_src` command. For more information, see [upgrade_image_src](#) on page 92.
- If you use the `ftp` and `bckto ftp` options in the syntax, you must first set the settings of the ftp server, where the existing os image will be backed up, by running the `upgrade_backup_dest` command, and then specify the details of the ftp server, where the new image is located, by running the `upgrade_image_src` command. For more information, see [upgrade_backup_dest](#) on page 91, and [upgrade_image_src](#) on page 92.

Examples

In the following example, the .pfe image file for the C25 was downloaded prior to running the upgrade command:

```
EWC.extremenetworks.com# upgrade ac AC-MV-07.41.03.0003-1.rue
```

In the following example, the .rue image file for the C5210 was downloaded prior to running the upgrade command, and the existing os image is backed up to a remote ftp server:

```
EWC.extremenetworks.com# upgrade ac AC-MV-09.12.01.0067-1.rue bckto ftp
```

In the following example, the upgrade image is downloaded from the remote ftp server:

```
EWC.extremenetworks.com# upgrade ac ftp
```

In the following example, the upgrade image is downloaded from the remote ftp server and the existing image of the os is backed up to the remote ftp server:

```
EWC.extremenetworks.com# upgrade ac ftp bckto ftp
```

In the following example, the upgrade image is downloaded from the remote ftp server, and the existing image of the os backed up to the flash device:

```
EWC.extremenetworks.com# upgrade ac ftp bckto flash backupfile-rescue-user.tgz
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
:: Access Controller Software          ::
:: Application Upgrade / Downgrade    ::
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
WARNING: Upgrading the controller will disconnect any clients currently using
the system. Following the upgrade, the system will be rebooted.
Do you wish to continue? (y/n) Y
```

upgrade apup

Use the `upgrade apup` command to upgrade the software of the Wireless AP. The `upgrade apup` command is accessible from the root context of the CLI.

```
upgrade apup platform | filename | number ap ap_serial# ap_serial# ... ap_serial#
```

Parameters

<i>platform</i>	Specifies the platform of the Wireless AP.
<i>filename</i>	Specifies the file name of the new image.
<i>number</i>	Specifies an ordinal image number returned by the <code>show apup</code> command.
<i>ap_serial#</i>	Specifies the serial number of the Wireless AP.

Example

The following example upgrades a Wireless AP:

```
EWC.extremenetworks.com# upgrade apup AP3705 1 ap 0122003999382
```



Caution

Upgrading an AP disconnects any clients currently using the AP. Following the upgrade, the AP reboots.

upgrade_backup_dest

Use the `upgrade_backup_dest` command to backup the controller's existing software image on the remote ftp server.

```
upgrade_backup_dest server | user | password | dir | file
```

Parameters

<i>server</i>	The FTP server where the backup image will be created.
<i>user</i>	The user name to access the FTP server.
<i>password</i>	The password to access the FTP server.
<i>dir</i>	The directory where the new software image is located.
<i>file</i>	The file name that you want to assign to the backup image.

Example

The following example backs up the controller's existing software image on the remote ftp server:

```
EWC.extremenetworks.com# upgrade_backup_dest 192.168.4.181 administrator  
abc123 /backup backupFile-rescue-user.tgz
```

upgrade_image_src

Use the `upgrade_image_src` command to locate the new software image on the remote server.

```
upgrade_image_src server | user | password | dir | file
```

Parameters

<i>server</i>	The FTP server on which the new software image is located.
<i>user</i>	The user name to access the FTP server.
<i>password</i>	The password to access the FTP server
<i>dir</i>	The directory where the new software image is located.
<i>file</i>	The file name of the software image.

Example

The following example locates the new software image on the remote server:

```
EWC.extremenetworks.com# upgrade_image_src 192.168.4.10  
test abc123 /ac/rpm/build09.12.01.0067 AC-MV-09.12.01.0067-1.txe
```

5 ap Commands

ap Context
Radio Commands
DCS Commands
logs
maintain_cycle

This chapter describes commands required to manage the basic functions of the Wireless APs on the system. The commands in this chapter are under the ap context of the CLI.

All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

There are many configurable parameters pertaining to wireless access points. Some commands are common to all AP contexts and some apply only to specific AP contexts. To avoid repetition and confusion, this chapter on AP configuration is organized into the following sections:

- [ap Context](#) on page 93

Lists and describes commands available in the ap: context. The ap: context is the highest-level context for AP configuration. Commands for configuration of specific AP models (such as 11n or 37xx) are located in the [defaults:](#) context, and commands for configuration of individual APs (by serial number) are located in the [<serial>:](#) context.

- [Radio Commands](#) on page 140

Radio commands, which are common to all APs (but vary from one AP type to another, and from Radio1 to Radio2) are listed and described in the [Radio Commands](#) on page 140 section.

- [DCS Commands](#) on page 158

DCS commands, all of which are common to some radio command contexts, are in the [DCS Commands](#) on page 158 section.

- [Serial Commands](#)

Serial commands, in the ap <serial>: context, are commands for configuring a specific Wireless AP (by serial number).

ap Context

The following commands are at the highest (first) level of the ap context:

- [access](#) on page 94
- [blacklist](#) on page 95 — See for commands in the ap:blacklist context.
- [defaults](#) on page 97 — See for commands in the ap:defaults context.
- [load-groups](#) on page 103 — See for commands in the ap:load-groups context.

- [lpm-override](#) on page 111
- [logs](#) on page 163 — See for commands in the `ap:logs` context.
- [logout](#) on page 23
- [maintenance](#) on page 111 — See for commands in the `ap:maintenance` context.
- [registration](#) on page 112 — See for commands in the `ap:registration` context.
- [remove](#) on page 114
- [search](#) on page 115
- [serial](#) on page 115
- `<serial>` on page 116 — See [Serial Commands](#) for commands in the `ap:<serial>` context.

access

Use the `access` command to modify the registration status of Wireless APs on the system. The `access` command is accessible from the `ap` context of the CLI.

```
access ap_serial release | pending | approved | reboot | foreign |
```

If rehoming is enabled, the command to change a local AP to a Foreign AP is:

```
access ap_serial foreign
```

The command to change a foreign AP to a Local AP is:

```
access ap_serial approved
```

Parameters

<code>ap_serial</code>	The serial number of the Wireless AP.
release pending approved reboot foreign	The administrative options for the Wireless AP.

Usage

Rehoming is enabled if availability is enabled between two V9.01 and higher controllers. Both Controllers need to be in the same regulatory domain. APs in WDS/MESH configurations cannot be rehomed. APs in load groups will be removed from the load group if they are rehomed.

Examples

The following example modifies the status of a Wireless AP to pending:

```
EWC.extremenetworks.com:ap# access 0409920201204003 pending
```

The following example reboots the Wireless AP:

```
EWC.extremenetworks.com:ap# access 0500008043050355 reboot
Rebooting selected AP may result in a localized service interruption. Are you
sure you want to continue(yes/no)?
(yes/no):yes
```

blacklist

The `blacklist` command moves you into the blacklist context, which contains commands to configure a MAC address list. If the MAC address list mode is black, the MAC addresses on the list identify clients that are not allowed to associate with the AP (a “blacklist”). If the MAC list mode is white, only the clients identified by the MAC addresses on the list are allowed to associate with the AP (a “whitelist”). The `blacklist` command is accessible from the `ap` context of the CLI.

The following commands are available in the `ap:blacklist` context:

- `export` on page 95
- `import` on page 95
- `mac` on page 96
- `mac-list-mode` on page 96

export

Use the `export` command to export the current MAC address list to a file. The `export` command is accessible from the `ap:blacklist` context of the CLI.

```
export server | user | dir | file
```

Parameters

<i>server</i>	Specifies the IP address of the server.
<i>user</i>	Specifies the username of an account on the server.
<i>dir</i>	Specifies the directory containing the file.
<i>file</i>	Specifies the file name.

Examples

The following example exports the MAC address list to a file on a server:

```
EWC.extremenetworks.com:ap:blacklist# export 192.168.1.6 mgrey /mgrey/home
MAClist.txt
Please input password:
Attempting to upload file...
```

import

Use the `import` command to import a list of MAC addresses for the MAC address list from a file. The `import` command is accessible from the `ap:blacklist` context of the CLI.

```
import server | user | dir | file
```

Parameters

<i>server</i>	Specifies the IP address of the server.
<i>user</i>	Specifies the username of an account on the server.
<i>dir</i>	Specifies the directory containing the file.
<i>file</i>	Specifies the file name.

Examples

The following example imports a MAC address list file from a server:

```
EWC.extremenetworks.com:ap:blacklist# import 192.168.1.3 jdoe /jdoe/home
MAClist.txt
Please input password:
Attempting to download file...
```

mac

Use the `mac` command to add a new MAC address, an IAB (Individual Address Block), or an OUI (Organizationally Unique ID) to the MAC address list. Use the `no` form of the command to remove an address from the MAC address list. The `mac` command is accessible from the `ap:blacklist` context of the CLI.

mac *MAC Address* | *mask no mac MAC Address* | *mask*

Parameters

<i>MAC Address</i>	Specifies the MAC address to be added to the MAC address list.
<i>mask</i>	The mask is expressed in number of bits used. <ul style="list-style-type: none"> • a fully qualified MAC address has a mask value of 48 • an OUI has a mask value of 24 • an IAB has a mask value of 36

Examples

The following example adds a MAC address to the MAC address list:

```
EWC.extremenetworks.com:ap:blacklist# mac 43:0D:37:5C:8A:12
EWC.extremenetworks.com:ap:blacklist# show
mac-list-mode black
43:0D:37:5C:8A:12
```

The following example adds an OUI from a MAC address to the MAC address list:

```
EWC.extremenetworks.com.com:ap:blacklist# mac 22:22:22 24
```

The following example adds an IAB from a MAC address to the MAC address list:

```
EWC.extremenetworks.com:ap:blacklist# mac FF:FF:FF:FF:F 36
```

mac-list-mode

Use this command to set the mode of the MAC address list. If the MAC address list mode is `black`, the MAC addresses on the list identify clients that are not allowed to associate with the AP (a “blacklist”). If the MAC list mode is `white`, only the clients identified by the MAC addresses on the list are allowed to associate with the AP (a “whitelist”).

mac-list-mode *black* | *white*

Parameters

<i>black</i>	Sets the MAC address list as a blacklist, denying clients on the list access to the AP. This is the default.
<i>white</i>	Sets the MAC address list as a whitelist, allowing only clients on the list access to the AP.

Usage

If you change the mode from blacklist to whitelist, all existing MAC addresses on the list will be erased. Use the `show` command to list the current mode and entries in the MAC address list.

Examples

This example shows the system prompt printed when changing from black mode to white mode:

```
EWC.extremenetworks.com:ap:blacklist# mac-list-mode white
Change address list from whitelist to blacklist or vice versa will erase all
existing address. Are you sure to do it?
(yes/no):no
```

mac-list-sync-mode

Use this command to synchronize the blacklist and whitelist between two controllers configured in availability.

mac-list-sync-mode enable | disable

Parameters

enable	Enables mac-list-sync-mode, which synchronizes MAC addresses between controllers configured as blacklisted or whitelisted.
disable	Disables mac-list-sync-mode, so that blacklisted or whitelisted MAC addresses are not synchronized between controllers.

Examples

This example enables the `mac-list-sync-mode`:

```
EWC.extremenetworks.com:ap:blacklist# mac-list-sync-mode enable
```

defaults

The `defaults` command moves you into the defaults context, which contains commands to configure the Wireless AP's default settings. The `defaults` command is accessible from the `ap` context of the CLI.

As the Wireless APs discover and register with the controller, they inherit the properties of the default Wireless AP setting. Since these defaults must apply to multiple AP platforms, they consist only of values that are supported on all platforms. To apply options individually to an AP, you can modify the default Wireless AP settings on that AP either via the Wireless Assistant GUI or the CLI <serial> context.

The following commands are available in the `ap:defaults` context:

- [ap37xx](#) on page 98 — See for commands in the `ap:defaults:ap37xx` context.
- [ap38xx](#) on page 98 — See `ap38xx` for commands in the `ap:defaults:ap38xx` context.

- [ap3801](#) — See [ap3801](#) for commands in the `ap:defaults:ap3801` context.
- [3935FCC](#) on page 99 — See [ap3935FCC](#) for commands in the `ap:defaults:ap3935FCC` context.
- [3935ROW](#) on page 100— See [ap3935ROW](#) for commands in the `ap:defaults:ap3935ROW` context.
- [3965FCC](#) on page 100— See [ap3965FCC](#) for commands in the `ap:defaults:ap3965FCC` context.
- [3965ROW](#) on page 101— See [ap3965ROW](#) for commands in the `ap:defaults:ap3965ROW` context.
- [assign](#) on page 101 — See [assign](#) for commands in the `ap:defaults:` context.
- [learnac](#) on page 102
- [aclist](#) on page 118
- [move](#) on page 103

ap37xx

The `ap37xx` command moves you into context `ap37xx`, which is an AP default profile context for AP37xx serial APs. The `ap37xx` command is accessible from the `ap:defaults` context of the CLI.

The following commands are available in the `ap:defaults:ap37xx` context:

- [balanced-power](#) on page 120
- [bcast_disassoc](#) on page 120
- [client_session](#) on page 121
- [country](#) on page 121
- [ipmcast-assembly](#) on page 122
- [lbs-status](#) on page 122
- [led-mode](#) on page 123
- [lldp](#) on page 123
- [persistent](#) on page 125
- [poll_timeout](#) on page 126
- [radio1](#) on page 132 — See [Radio Commands](#) on page 140 for commands in the `radio1` contexts.
- [radio2](#) on page 133 — See [Radio Commands](#) on page 140 for commands in the `radio2` contexts.
- [secure-tunnel](#) on page 135
- [secure-tunnel-lifetime](#) on page 135
- [ssh](#) on page 137
- [show](#) on page 136

ap38xx

The `ap38xx` command moves you into context `ap38xx`, which is an AP default profile context for AP38xx serial APs. The `ap38xx` command is accessible from the `ap:defaults` context of the CLI.

The following commands are available in the `ap:defaults:ap38xx` context:

- [balanced-power](#) on page 120
- [bcast_disassoc](#) on page 120
- [client_session](#) on page 121
- [country](#) on page 121
- [ipmcast-assembly](#) on page 122
- [lbs-status](#) on page 122

- [led-mode](#) on page 123
- [lldp](#) on page 123
- [persistent](#) on page 125
- [poll_timeout](#) on page 126
- [radio1](#) on page 132 — See [Radio Commands](#) on page 140 for commands in the radio1 contexts.
- [radio2](#) on page 133 — See [Radio Commands](#) on page 140 for commands in the radio2 contexts.
- [secure-tunnel](#) on page 135 — This command is not available on the AP3805 model.
- [secure-tunnel-lifetime](#) on page 135
- [ssh](#) on page 137
- [show](#) on page 136

ap3801

The `ap3801` command moves you into context `ap3801`, which is an AP default profile context for AP3801 serial APs. The `ap3801` command is accessible from the `ap:defaults` context of the CLI.

The following commands are available in the `ap:defaults:ap3801` context:

- [balanced-power](#) on page 120
- [bcast_disassoc](#) on page 120
- [client_session](#) on page 121
- [country](#) on page 121
- [ipmcast-assembly](#) on page 122
- [lbs-status](#) on page 122
- [led-mode](#) on page 123
- [lldp](#) on page 123
- [persistent](#) on page 125
- [poll_timeout](#) on page 126
- [radio1](#) on page 132 — See [Radio Commands](#) on page 140 for commands in the radio1 contexts.
- [radio2](#) on page 133 — See [Radio Commands](#) on page 140 for commands in the radio2 contexts.
- [secure-tunnel](#) on page 135
- [secure-tunnel-lifetime](#) on page 135
- [ssh](#) on page 137
- [show](#) on page 136

3935FCC

The `ap3935FCC` command moves you into context `ap3935FCC`, which is an AP default profile context for ap3935FCC serial APs. The `ap3935FCC` command is accessible from the `ap:defaults` context of the CLI.

The following commands are available in the `ap:defaults:ap3935FCC` context:

- [balanced-power](#) on page 120
- [bcast_disassoc](#) on page 120
- [client_session](#) on page 121
- [country](#) on page 121

- [ipmcast-assembly](#) on page 122
- [lbs-status](#) on page 122
- [led-mode](#) on page 123
- [lldp](#) on page 123
- [persistent](#) on page 125
- [poll_timeout](#) on page 126
- [radio1](#) on page 132 — See [Radio Commands](#) on page 140 for commands in the radio1 contexts.
- [radio2](#) on page 133 — See [Radio Commands](#) on page 140 for commands in the radio2 contexts.
- [secure-tunnel](#) on page 135
- [ssh](#) on page 137
- [show](#) on page 136

3935ROW

The `ap3935ROW` command moves you into context `ap3935ROW`, which is an AP default profile context for `ap3935ROW` serial APs. The `ap3935ROW` command is accessible from the `ap:defaults` context of the CLI.

The following commands are available in the `ap:defaults:ap3935ROW` context:

- [balanced-power](#) on page 120
- [bcast_disassoc](#) on page 120
- [client_session](#) on page 121
- [country](#) on page 121
- [ipmcast-assembly](#) on page 122
- [lbs-status](#) on page 122
- [led-mode](#) on page 123
- [lldp](#) on page 123
- [persistent](#) on page 125
- [poll_timeout](#) on page 126
- [radio1](#) on page 132 — See [Radio Commands](#) on page 140 for commands in the radio1 contexts.
- [radio2](#) on page 133 — See [Radio Commands](#) on page 140 for commands in the radio2 contexts.
- [secure-tunnel](#) on page 135
- [ssh](#) on page 137
- [show](#) on page 136

3965FCC

The `ap3965FCC` command moves you into context `ap3965FCC`, which is an AP default profile context for `ap3965FCC` serial APs. The `ap3965FCC` command is accessible from the `ap:defaults` context of the CLI.

The following commands are available in the `ap:defaults:ap3965FCC` context:

- [balanced-power](#) on page 120
- [bcast_disassoc](#) on page 120
- [client_session](#) on page 121

- [country](#) on page 121
- [ipmcast-assembly](#) on page 122
- [lbs-status](#) on page 122
- [led-mode](#) on page 123
- [lldp](#) on page 123
- [persistent](#) on page 125
- [poll_timeout](#) on page 126
- [radio1](#) on page 132 — See [Radio Commands](#) on page 140 for commands in the radio1 contexts.
- [radio2](#) on page 133 — See [Radio Commands](#) on page 140 for commands in the radio2 contexts.
- [secure-tunnel](#) on page 135
- [ssh](#) on page 137
- [show](#) on page 136

3965ROW

The `ap3965ROW` command moves you into context `ap3965ROW`, which is an AP default profile context for `ap3965ROW` serial APs. The `ap3965ROW` command is accessible from the `ap:defaults` context of the CLI.

The following commands are available in the `ap:defaults:ap3965ROW` context:

- [balanced-power](#) on page 120
- [bcast_disassoc](#) on page 120
- [client_session](#) on page 121
- [country](#) on page 121
- [ipmcast-assembly](#) on page 122
- [lbs-status](#) on page 122
- [led-mode](#) on page 123
- [lldp](#) on page 123
- [persistent](#) on page 125
- [poll_timeout](#) on page 126
- [radio1](#) on page 132 — See [Radio Commands](#) on page 140 for commands in the radio1 contexts.
- [radio2](#) on page 133 — See [Radio Commands](#) on page 140 for commands in the radio2 contexts.
- [secure-tunnel](#) on page 135
- [ssh](#) on page 137
- [show](#) on page 136

assign

The `assign` command refers to context `assign`, which contains the `wlans-list` and `wlan-foreign-ap` commands. The `assign` command is accessible from the `ap:defaults` context of the CLI.

The following commands are available in the `ap:defaults:assign` context:

- [wlans-list](#) on page 102
- [wlan-foreign-ap](#) on page 102

wlans-list

Use the `wlans-list` command to assign Radio 1 and Radio 2 of APs to specific WLAN Services. Use the `no` command to remove radio assignment from specific WLAN Services. The `wlans-list` command is accessible from the `ap:defaults` context of the CLI.

After you run the `wlans-list` command, run the `apply` command to implement the changes in radio assignments.

```
wlans-list wlans-name | radio1 | radio2 no wlans-list wlans-name | radio1 | radio2
```

Parameters

<i>wlans-name</i>	The name of the WLAN service.
radio1	5GHz radio.
radio2	2.4GHz radio.

Examples

The following example assigns Radio 1 to CNL-209 WLANS:

```
EWC.extremenetworks.com:ap:defaults:assign# wlans-list CNL-209 radio1
```

wlan-foreign-ap

Use the `wlan-foreign-ap` command to enable the application of default WLAN assignments to foreign APs. The `wlans-list` command is accessible from the `ap:defaults:` context of the CLI.

```
wlan-foreign-ap enable | disable
```

Parameters

enable	Specifies that default WLAN assignments are applied to foreign APs.
disable	Specifies that default WLAN assignments are not applied to foreign APs.

Examples

The following example enables the application of default WLAN assignments to foreign APs:

```
EWC.extremenetworks.com:ap:defaults:# wlan-foreign-ap enable
```

learnac

Use the `learnac` command to allow the Wireless AP to provide its own EWC Search List. Use `no` form of the command to disable this feature. The `learnac` command is accessible from the `ap:defaults` context of the CLI.

If you disallow the Wireless AP from providing its own EWC Search List, you should specify the controller's static IP address by running the `ac1ist` command. For more information, see [ac1ist](#) on page 118. If you disallow the Wireless AP from providing its own EWC Search List and do not specify the controller's static IP address, the Wireless AP uses the SLP to discover the controller.

After you run the `learnac` command, run the `apply` command to implement the changes.

```
learnac no learnac
```

Parameters

None

Examples

The following example allows each Wireless AP to provide its own EWC Search List:

```
EWC.extremenetworks.com:ap:defaults# learnac
```

move

Use the `move` command to change the rank of Wireless Appliances on the Wireless Appliance list. The `move` command is accessible from the `ap:<serial>` context of the CLI. It is also available from `ap:defaults` if `learnac` is disabled (no `learnac`) in that context.

```
move aclist rank1 + | - rank2
```

Parameters

<code>rank1</code>	Specifies the rank of the listed item to be moved
<code>+ -</code>	Move rank one position above or below the rank2 item
<code>rank2</code>	Specifies the rank of the second item

Example

```
EWC.extremenetworks.com:ap:0500008043050212# move aclist 3 + 2
```

load-groups

The `load-groups` command moves you to the load-groups context, which contains commands to configure Wireless AP load balancing groups. The `load-groups` command is accessible from the `ap` context of the CLI.

The following commands are available in the `ap:load-groups` context:

- [create](#) on page 103
- [delete](#) on page 105
- [<named-load-group>](#) on page 105 — See for commands in the `ap:load-groups:<named-load-group>` context.
- [show](#) on page 110

create

Use the `create` command to create a load group with a specified type. After creating a load group, assign a radio and a WLAN to the load group. See [assign-radio](#) on page 106 and [assign-wlan](#) on page 106.

The `create` command is accessible from the `ap:load-groups` context of the CLI.

```
create load group name | radio | client
```

Parameters

<i>load group name</i>	The name of the load group. Load group names can be up to 32 characters long.
radio	Specifies that this load group will perform band preference steering and load control.
client	Specifies that this load group will perform client load balancing between radios. Default is client balancing.

Usage

A radio type load group can perform band preference steering and load control. Band preference steering is a mechanism to move 11a-capable clients to the 11a radio on the AP, relieving congestion on the 11g radio. No balancing is done between the 11a and 11g radios. Load control allows you to configure the maximum number of clients allowed per radio on the AP. Load control is disabled by default. A radio load group executes band preference steering and/or load control across the radios on each AP in the group. Each AP balances in isolation from the other APs, but all APs in the group have the same configuration related to band preference and load control.

A client type of load group performs load balancing based on the number of clients across all APs in the group and only for the WLANs assigned to the group. This is different from load control in the radio type group — load control APs make decisions in isolation from each other.

The number of load groups you can create is dependent on the controller you are configuring.

Table 6: Load Groups Supported on an ExtremeWireless Appliance

Controller	Maximum Number of Load Groups
C25	8
C35	8
C4110	32
C5110	64
C5210	64
V2110	64

Each load group can contain up to 32 Wireless APs. For information about assigning a Wireless AP to a load group, see [assign-radio](#) on page 106.

Examples

The following example creates a load group, which will be the default client balancing type named loadgroup1:

```
EWC.extremenetworks.com:ap:load-groups# create loadgroup1
EWC.extremenetworks.com:ap:load-groups# show loadgroup1
Load Group ID: loadgroup1
Group Type: client
WLAN Assignment:
Radio Assignment:
Radio1  Radio2  AP Name
          0500008043050236
```


delete

Use the `delete` command to remove a load group.

The `delete` command is accessible from the `ap:load-groups` context of the CLI.

delete *load group name*

Parameters

<i>load group name</i>	The load group being deleted.
------------------------	-------------------------------

Examples

The following example deletes the load group named `loadgroup2`:

```
EWC.extremenetworks.com:ap:load-groups# delete loadgroup2
```

<named-load-group>

The `<named-load-group>` command, where `<named-load-group>` refers to the name of a given load group, moves you into the `ap:load-groups:<named-load-group>` context, which contains commands to configure the settings of the specified individual load group.

The following commands are available in the `ap:load-groups:<named-load-group>` context. The commands available to you depend on the type of load group you are configuring, either radio or client (see [create](#) on page 103).

- [assign-ap](#) on page 105
- [assign-radio](#) on page 106
- [assign-wlan](#) on page 106
- [bandpreference](#) on page 107
- [name](#) on page 107
- [radio-load](#) on page 108
- [radio1-loadcontrol](#) on page 108
- [radio2-loadcontrol](#) on page 109
- [radio1-strictlimit](#) on page 109
- [radio2-strictlimit](#) on page 110
- [show](#) on page 110

assign-ap

Use this command to add or remove the AP radios from the named radio type load group. The `assign-ap` command is accessible from the `ap:load-groups:<named-load-group>` context of the CLI, for load groups of type radio.

assign-ap **add** | **delete** | *ap-name*

Parameters

add delete	Add or remove the specified AP radio from the load group.
<i>ap-name</i>	Specifies the AP.

Usage

If the specified AP is already assigned to a load group, a new assignment removes the original radio assignment. You are prompted to confirm the new assignment.

Examples

This example adds a Wireless AP named AP3935FCC to named radio load group “radiogroup1”:

```
EWC.extremenetworks.com:ap:load-groups:radiogroup1# assign-ap add AP3935FCC
```

assign-radio

Use the `assign-radio` command to assign AP radios to the named client load group. You can also use this command to unassign the AP radios from the named client load group. The `assign-radio` command is accessible from the `ap:load-groups:<named-load-group>` context of the CLI, for groups of type client.

assign-radio add | delete *ap-name* **radio1 | radio2 | both**

Parameters

add delete	Use add to assign a Wireless AP's radios to a load group. Use delete to unassign radios from a load group.
<i>ap-name</i>	The name of the Wireless AP.
radio1 radio2 both	The radios that you want to assign or unassign.

If you assign radios that are currently assigned to another load group, the radios will automatically be removed from the other load group.

Example

The following example assigns both radios of a Wireless AP named AP3935FCC to the client load group named clientgroup1:

```
EWC.extremenetworks.com:ap:load-groups:clientgroup1# assign-radio add
AP3935FCC both
```

assign-wlan

Use the `assign-wlan` command to assign a WLAN service to both types of load groups. You can also use this command to unassign a WLAN service from a load group. The `assign-wlan` command is accessible from the `ap:load-groups:<named-load-group>` context of the CLI, for both types of load groups.

assign-wlan add | delete *WLAN name*

Parameters

add delete	Use add to assign a WLAN service to a load group. Use delete to unassign a WLAN service from a load group.
<i>WLAN name</i>	The name of the WLAN service.

Assign a WLAN service to the load group. Assigning a WLAN service to the load group also assigns the WLAN service to the load group's Wireless APs.

Examples

The following example assigns the WLAN service named Lab45-WPA to the client load group named clientgroup1:

```
EWC.extremenetworks.com:ap:load-groups:clientgroup1# assign-wlan add Lab45-WPA
```

bandpreference

Use this command to enable or disable the band preference feature for all APs in a radio type load group. The `bandpreference` command is accessible from the `ap:load-groups:<named-load-group>` context of the CLI, for the radio type of load group.

bandpreference enable | disable

Parameters

enable	Enable band preference steering.
disable	Disable band preference steering. The default condition is disabled.

Examples

This example enables band preference steering for the radio load group named radiogroup1:

```
EWC.extremenetworks.com:ap:load-groups:radiogroup1# bandpreference enable
```

name

Use the `name` command to change the name of a load group. The `name` command is accessible from the `ap:load-groups:<named-load-group>` context of the CLI, for both types of load groups.

name *load group name*

Parameters

<i>load group name</i>	The new name of the load group.
------------------------	---------------------------------

Usage

After you change the name of the load group and apply the change (with the `apply` command), the `ap:load-groups:<named-load-group>` context retains the previous name of the load group. To change the `ap:load-groups:<named-load-group>` context to the new name of the load group, you exit the context and then enter the `ap:load-groups:<named-load-group>` context using the new name.

Example

The following example changes the name of loadgroup1 to lg_lab:

```
EWC.extremenetworks.com:ap:load-groups:loadgroup1# name lg_lab
EWC.extremenetworks.com:load-groups:loadgroup1# apply
EWC.extremenetworks.com:load-groups:loadgroup1# exit
EWC.extremenetworks.com:load-groups# ?
Available commands are:
create                Create load group
delete                Delete load group
end                   Return to the base mode
```

```

exit                Return to the previous mode if not in the
base mode
lg_lab             Configure details for load group lg_lab
logout            Exit the shell
show
EWC.extremenetworks.com:ap:load-groups# lg_lab
EWC.extremenetworks.com:load-groups:lg_lab#

```

radio-load

Use this command to configure the maximum number of clients for each radio when the radio load control feature is enabled. The `radio-load` command is accessible from the `ap:load-groups:<named-load-group>` context of the CLI, for the radio type of load group.

radio-load radio1 | radio2 max-clients

Parameters

radio1 radio2	Specifies the radio being configured.
<i>max-clients</i>	Specifies the maximum number of clients for the specified radio. Can be an integer between 5 and 60.

Usage

For access to this command, the `radioN-loadcontrol` command must be enabled.

Examples

This example enables load control per radio for load group named `radiogroup1`, then specifies the maximum number of clients for radio 1 and radio 2:

```

EWC.extremenetworks.com:ap:load-groups:radiogroup1# loadcontrol enable
EWC.extremenetworks.com:ap:load-groups:radiogroup1# radio-load radio1 40
EWC.extremenetworks.com:ap:load-groups:radiogroup1# radio-load radio2 50

```

radio1-loadcontrol

Use the `radio1-loadcontrol` command to enable or disable load control (soft load limits) on Radio1 only. The `radio1-loadcontrol` command is accessible from the `ap:load-groups:<named-loadgroup>` context.

Radio Load Control activates only when the number of clients on the radio reaches the configured limit, and does not disconnect any clients already connected. This is the default and preferred mode of load control. Load control can be enabled on one radio and disabled on the other. Members of a WLAN load control group are assigned to both radios and cannot be load controlled individually.

radio1-loadcontrol enable | disable

Parameters

enable disable	Enables or disables the load control function on Radio1.
-------------------------	--

Usage

For access to this command, the load group must be defined as a radio type load group.

Example

The following example enables load control on Radio1:

```
EWC.extremenetworks.com:ap:load-groups:radiogroup1# radio1-loadcontrol enable
```

radio2-loadcontrol

Use the `radio2-loadcontrol` command to enable or disable load control (soft load limits) on Radio2 only. The `radio2-loadcontrol` command is accessible from the `ap:load-groups:<named-loadgroup>` context.

Radio Load Control activates only when the number of clients on the radio reaches the configured limit, and does not disconnect any clients already connected. This is the default and preferred mode of load control. Load control can be enabled on one radio and disabled on the other. Members of a WLAN load control group are assigned to both radios and cannot be load controlled individually.

radio2-loadcontrol enable | disable

Parameters

enable disable	Enables or disables the load control function on Radio2.
-------------------------	--

Usage

For access to this command, the load group must be defined as a radio type load group.

Example

The following example disables load control on Radio2:

```
EWC.extremenetworks.com:ap:load-groups:radiogroup1# radio2-loadcontrol disable
```

radio1-strictlimit

Use the `radio1-strictlimit` command to enable or disable strict enforcement of hard load limits on Radio1 when Radio Load Control is active. When strict limit is enabled, any clients in excess of the configured limits on the radio are immediately disconnected. The `radio1-strictlimit` command is accessible from the `ap:load-groups:<named-loadgroup>` context.

radio1-strictlimit enable | disable

Parameters

enable disable	Enables or disables the strict enforcement of load limits on Radio1.
-------------------------	--

Usage

Radio Load Control must be enabled for this radio before this command can take effect.

Example

The following example enables strict load limiting on Radio1:

```
EWC.extremenetworks.com:ap:load-groups:radiogroup1# radio1-strictlimit enable
```

radio2-strictlimit

Use the `radio2-strictlimit` command to enable or disable strict enforcement of load limits on Radio2 when Radio Load Control is active. When `strictlimit` is enabled, any clients in excess of the configured limits on the radio are immediately disconnected. The `radio2-strictlimit` command is accessible from the `ap:load-groups:<named-loadgroup>` context.

radio2-strictlimit enable | disable

Parameters

enable disable	Enables or disables the strict enforcement of load limits on Radio2.
-------------------------	--

Usage

Radio Load Control must be enabled for this radio before this command can take effect.

Example

The following example disables strict load limiting on Radio2:

```
EWC.extremenetworks.com:ap:load-groups:radiogroup1# radio2-strictlimit disable
```

show

Use the `show` command to display information about the load group. The `show` command is accessible from the `ap:load-groups:<named-load-group>` context of the CLI, for both types of load groups.

show

Parameters

None.

Examples

The following example displays information for the radio type load group `radiogroup1`:

```
EWC.extremenetworks.com:ap:load-groups:radiogroup1# show
Load Group ID: radiogroup1
Group Type: radio
WLAN Assignment:
WLAN Name Assigned
aaaa          x
Band Preference: disable
Load Control: disable
Maximum clients for radio1/radio2: 112/112
Radio Assignment:
Radio1 Radio2 AP Name
                0500008043050236
```

show

Use the `show` command to display a list of the load groups configured on the Wireless Appliance. The `show` command is accessible from the `ap:load-groups` context of the CLI.

show

Parameters

None.

Examples

The following example displays the load groups:

```
EWC.extremenetworks.com:ap:load-groups# show
Load Groups:
Name: loadgroup1   Type: radio
Name: loadgroup2   Type: client
```

lpm-override

Use the `lpm-override` command to configure Low Power Mode Override.

lpm-override enable | disable

Parameters

enable	Enable Low Power Mode Override.
disable	Disable Low Power Mode Override. The default configuration for the 39xx APs is disabled.

Usage

Enable `lpm-override` to have AP *always* operate in 4x4 mode regardless of what was negotiated with the Switch PoE. When this option is disabled, the AP operates in 2x2 or 4x4 depending on what was negotiated with the Switch PoE using the 2-event classification.

- AP sends Power Status element with "Power Mode" set to 0 when "Low Power Mode Override" is enabled.
- AP sends Critical Log "entering Low Power mode" only if negotiated .af with Switch PoE and "Low Power Mode Override" is disabled. Otherwise, Critical Log is not sent.
- Controller "Network Health" shows only APs that have "Power Mode" bit in the Power Status set to 1. The default configuration for the 39xx APs is disabled.

Examples

```
EWC.extremenetworks.com:ap# lpm-override enable
```

maintenance

The `maintenance` command moves to the maintenance context from which you can upgrade the Wireless AP's software image. The `upgrd` on page 111 command is available from the maintenance context.

upgrd

Use the `upgrd` command to upgrade the Wireless AP's software image. The `upgrd` command is accessible from the `ap:maintenance` context of the CLI.

After you run the `upgrd` command to upgrade the Wireless AP's software image, run the `apply` command.

upgrd default | control

Parameters

default	Specifies default upgrade. As part of the default upgrade process, when the Wireless AP registers with the controller, the AP's firmware version is verified. If it does not match with the value as defined for the default image, the AP is requested to upgrade to the default image.
control	Specifies controlled upgrade. The controlled upgrade allows you to individually select and control the state of a Wireless AP image upgrade. For example, you can specify which Wireless AP to upgrade, the upgrade schedule, and how to upgrade.

Examples

The following example specifies default upgrade:

```
EWC.extremenetworks.com:ap:maintenance# upgrd default
```

The following example specifies controlled upgrade:

```
EWC.extremenetworks.com:ap:maintenance# upgrd control
```

registration

The `registration` command refers to context `ap:registration`, which describes commands to configure registration options for connected Wireless APs.

The `registration` command is accessible from the `ap` context of the CLI.

The following commands are available in the `ap:registration` context:

- [cluster-encryption](#) on page 112
- [cluster-shared-secret](#) on page 113
- [dinterval](#) on page 113
- [dretry](#) on page 113
- [security](#) on page 114
- [sshpasswd](#) on page 114

cluster-encryption

Use the `cluster-encryption` command to enable or disable the encryption for the cluster shared secret. The `cluster-encryption` command is accessible from the `ap:registration` context of the CLI.

cluster-encryption enable | disable

Parameters

enable disable	Enables or disables the encryption for the cluster shared secret.
-------------------------	---

Examples

The following example enables the encryption for the cluster shared secret:

```
EWC.extremenetworks.com:ap:registration# cluster-encryption enable
```

cluster-shared-secret

Use the `cluster-shared-secret` command to configure the cluster shared secret. The `cluster-shared-secret` command is accessible from the `ap:registration` context of the CLI.

cluster-shared-secret *string*

Parameters

<i>string</i>	The cluster shared secret, which can be 8-63 characters long.
---------------	---

Examples

The following example sets the cluster shared secret to “sharedsecret”:

```
EWC.extremenetworks.com:ap:registration# cluster-shared-secret sharedsecret
```

dinterval

Use the `dinterval` command to set the time delay between registration attempts. The Wireless AP will wait for a predetermined amount of time between attempts to register with the Wireless Appliance. The `dinterval` command is accessible from the `ap:registration` context of the CLI.

dinterval 1-10

Parameters

1-10	Specifies the amount of time in seconds between attempts to register with the Wireless Appliance.
------	---

Examples

The following example sets the time interval between registration attempts to 6 seconds:

```
EWC.extremenetworks.com:ap:registration# dinterval 6
```

dretry

Use the `dretry` command to set the number of retry attempts for the Wireless AP registration process. The Wireless AP will make a specified number of attempts to register its serial number with the Wireless Appliance following a registration failure. The `dretry` command is accessible from the `ap:registration` context of the CLI.

dretry *number*

Parameters

<i>number</i>	Specifies the number of retry attempts for the Wireless AP registration process. Valid entries are integers from 1 - 255.
---------------	---

Examples

The following example sets the number of registration retry attempts to 4:

```
EWC.extremenetworks.com:ap:registration# dretry 4
```

security

Use the `security` command to allow only approved Wireless APs to connect to the Wireless Appliance. Use the `no` form of the command to allow all Wireless APs to connect to it. The `security` command is accessible from the `ap:registration` context of the CLI.

Wireless APs without connection approval are put into a pending state, and an administrator has to manually approve those connections.

```
security no security
```

Parameters

None

Examples

The following example allows only approved Wireless APs to connect to the Wireless Appliance:

```
EWC.extremenetworks.com:ap:registration# security
```

sshpasswd

Use the `sshpasswd` command to reset the ssh password. Use the `no` command to disable the ssh password. The `sshpasswd` command is accessible from the `ap:registration` context of the CLI.

```
sshpasswd password no sshpasswd
```

Parameters

<i>password</i>	Specifies the ssh password. The password must be between 5 and 30 alphanumeric characters.
-----------------	--

Examples

```
EWC.extremenetworks.com:ap:registration# sshpasswd mynewpassword
```

remove

Use the `remove` command to remove a client from the Wireless AP. The `remove` command is accessible from the `ap` context of the CLI.

```
remove client mac MAC | mip MIP
```

Parameters

mac	Indicates that a MAC address will be specified.
<i>MAC</i>	Specifies the MAC address.

mip	Indicates that an IP address will be specified.
<i>MIP</i>	Specifies the IP address.

Examples

The following example removes a client from the Wireless AP by specifying its MAC address:

```
EWC.extremenetworks.com:ap# remove client mac 00:12:F0:81:A4:62
```

The following example removes a client from the Wireless AP by specifying its IP address:

```
EWC.extremenetworks.com:ap# remove client mip 172.28.209.251
```

search

Use the `search` command to search for a client on the Wireless AP by specifying its MAC address, IP Address, or User ID. The `search` command is accessible from the `ap` context of the CLI.

search mmac *MAC Address* | **mip** *IP Address* | **muser** *string*

Parameters

mmac	Indicates that MAC address will be specified.
<i>MAC Address</i>	Specifies the MAC address.
mip	Indicates that an IP address will be specified.
<i>MIP</i>	Specifies the IP address.
muser	Indicates that a User ID will be specified.
<i>string</i>	Specifies the User ID.

Examples

The following example searches for a client on the Wireless AP by its MAC address:

```
EWC.extremenetworks.com:ap# search mmac 00:12:F0:81:A4:62
00:12:F0:81:A4:62 172.28.209.251 mschap
```

The following example searches for a client on the Wireless AP by its IP Address:

```
EWC.extremenetworks.com:ap# search mip 172.28.209.251
00:12:F0:81:A4:62 172.28.209.251 mschap
```

The following example searches for a client on the Wireless AP by specifying its User ID:

```
CNL205:ap# search muser mschap
00:12:F0:81:A4:62 172.28.209.251 mschap
```

serial

Use the `serial` command to add a Wireless AP to the Wireless Appliance. The `serial` command is accessible from the `ap` context of the CLI.

serial *ap serial number | name | hardware type | ap role | description*

Parameters

<i>ap serial number</i>	Specifies the serial number of the Wireless AP.
<i>name</i>	Specifies a unique ID for the Wireless AP.
<i>hardware type</i>	Specifies the hardware type of the Wireless AP.
<i>ap role</i>	Specifies the role of the Wireless AP.
<i>description</i>	Specifies a descriptive word for the Wireless AP.

Examples

The following example adds a Wireless AP to the Wireless Appliance:

```
EWC.extremenetworks.com:ap# serial 0409920201203751 Orlandoe_4_P2 AP3765i ap
```

<serial>

The `<serial>` command, where `<serial>` refers to the serial number of a Wireless AP, moves you into the `<serial>` context, which contains commands to configure attributes for a specific Wireless AP. The `<serial>` command is accessible from the `ap` context of the CLI.

The following commands are available in the `ap:<serial>` context:

Available commands depend on the AP hardware type and prerequisite settings. For example, you must configure `secure-tunnel` before you can configure `secure-tunnel-lifetime`.

- [802_1x](#) on page 117 — See for commands in the `ap:<serial>:802_1x` context.
- [aclist](#) on page 118
- [ap_env](#) on page 119
- [apip](#) on page 119
- [balanced-power](#) on page 120
- [bcast_disassoc](#) on page 120
- [bgway](#) on page 120
- [client_session](#) on page 121
- [country](#) on page 121
- [desc](#) on page 121
- [ipmcast-assembly](#) on page 122
- [lcp](#) on page 122
- [lbs-status](#) on page 122
- [led-mode](#) on page 123
- [lldp](#) on page 123
- [location](#) on page 124
- [move](#) on page 103
- [name](#) on page 125
- [persistent](#) on page 125
- [poll_timeout](#) on page 126

- [port-setting](#) on page 126
- [professional_antenna](#) on page 127
- [radio1](#) on page 132 — See [Radio Commands](#) on page 140 for commands in the radio1 contexts.
- [radio2](#) on page 133 — See [Radio Commands](#) on page 140 for commands in the radio2 contexts.
- [real_capture](#) on page 134
- [secure-tunnel](#) on page 135
- [secure-tunnel-lifetime](#) on page 135
- [show](#) on page 136
- [ssh](#) on page 137
- [tunnel-mtu](#) on page 138
- [usedhcp](#) on page 138
- [vlanid](#) on page 138
- [wlan](#) on page 139
- [zone](#) on page 139

802_1x

The `802_1x` command refers to 802_1x context that describes commands to configure 802.1x authentication for a Wireless AP. The `802_1x` command is accessible from the `ap:<serial>` context of the CLI.

The following commands are available in the `ap:<serial>:802_1x` context:

- [eap](#) on page 117
- [gen_certreq](#) on page 118
- [peap](#) on page 118

eap

Use the `eap` command to download and set the certificate from the FTP server as part of the 802.1x EAP-TLS authentication configuration process. You can use the `eap` command for EAP Proxy mode as well as EAP Pass-through mode. The `eap` command is accessible from the `ap:<serial>:802_1x` context of the CLI.

```
eap server user dir file [secret]
```

Parameters

<i>server</i>	IP address of the FTP server from where the certificate is downloaded.
<i>user</i>	User name for accessing the FTP server.
<i>dir</i>	The directory where the certificate is stored on the FTP server.
<i>file</i>	The file name of the certificate.
<i>secret</i>	The password for encrypting the private key. This parameter is optional.

Example

```
EWC.extremenetworks.com:ap:0409920201203751 AP:802_1x# eap 192.168.4.88 admin
certificates ap3765.pfx abc123
```

gen_certreq

Use the `gen_certreq` command to generate a certificate signing request as part of the 802.1x EAP-TLS (proxy mode) authentication configuration. The `gen_certreq` command is accessible from the `ap:<serial>:802_1x` context of the CLI.

```
gen_certreq cn [(location country state city) (organization name unit) (email
email_addr) (key-size 1024 | 2048)]
```

Parameters

<i>cn</i>	Common name that you want to assign to the Wireless AP.
location	Keyword indicating that the next three parameters specify the location where the Wireless AP is operating.
<i>country</i>	The name of the country where the AP is located. You must use the two-letter ISO abbreviation for the country.
<i>state</i>	The name of the state or province where the AP is located
<i>city</i>	The name of the city where the AP is located
organization	Keyword indicating that the next two parameters specify the name of the organization to which the AP belongs.
<i>name, unit</i>	Organization name, Organizational Unit name to which the AP belongs.
email <i>email_addr</i>	The email address of the organization to which the AP belongs
key-size	Specifies that the certificate supports key size. Valid key size values are 1024 or 2048.

Example

```
EWC.extremenetworks.com:ap:0409920201203751 AP:802_1x# gen_certreq
shopfloor_aps location CA Ontario Mississauga organization mnj_Ware_House
Service email me@email.com key-size 2048
```

peap

Use the `peap` command to set PEAP (Protected Extensible Authentication Protocol) authentication. Use the `no` command to delete the PEAP authentication credentials from the Wireless AP. The `peap` command is accessible from the `ap:<serial>:802_1x` context of the CLI.

```
peap user password
no peap
```

Parameters

None

Examples

```
EWC.extremenetworks.com:ap:0409920201203751 AP:802_1x# peap admin abc123
```

aclist

Use the `aclist` command to statically configure the IP addresses of Wireless Appliances for discovery. Use the `no` form of the command to remove any IPs either by address or by rank. IP addresses removed from the Wireless Appliance list are replaced in rank by the next listed IP address. Use the `show` function

to list the added Wireless Appliance IPs by rank. The `aclist` command is accessible from the `ap:<serial>` context of the CLI. It is also available from `ap:defaults` if `learnac` is disabled (`no learnac`) in that context.

```
aclist IP Address
no aclist rank | IP Address
```

Parameters

<i>IP Address</i>	Specifies the IP address of the Wireless Appliance
<i>rank</i>	Specifies the rank number of the listed Wireless Appliance

Examples

The following example adds three IP addresses to the Wireless Appliance list:

```
EWC.extremenetworks.com:ap:0409920201204003# aclist 6.178.34.54
EWC.extremenetworks.com:ap:0409920201204003# aclist 81.30.6.312
EWC.extremenetworks.com:ap:0409920201204003# aclist 167.232.92.39
```

The following example removes an entry from the Wireless Appliance list by IP address:

```
EWC.extremenetworks.com:ap:0409920201204003# no aclist 167.232.92.39
```

The following example removes an entry from the Wireless Appliance list by rank:

```
EWC.extremenetworks.com:ap:0409920201204003# no aclist 1
```

ap_env

Use the `ap_env` command to configure the environment of the Wireless AP – indoor or outdoor. The `ap_env` command is accessible from the `ap:<serial>` context of the CLI.

```
ap_env (indoor | outdoor)
```

Parameters

(indoor outdoor)	Specifies the environment of the Wireless AP – indoor or outdoor.
---------------------------	---

Examples

The following example sets the environment of the AP to outdoor:

```
EWC.extremenetworks.com:ap:0409920201202222# ap_env outdoor
```

apip

Use the `apip` command when statically configuring a Wireless AP. In order to statically configure a Wireless AP, you must first run the `no usedhcp` command. The `apip` command is accessible from the `ap:<serial>` context of the CLI.

```
apip IP Address netmask
[no] apip xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx
```

Parameters

<i>IP Address</i>	IP address of the Wireless AP
<i>netmask</i>	Netmask of the of the Wireless AP

Example

```
EWC.extremenetworks.com:ap:7000001222222222 apip 10.205.3.131 255.255.255.0
```

balanced-power

Use the `balanced-power` command to simplify the power settings so that they apply to all channels in the channel list.

balanced-power enable | disable

Parameters

enable	Power settings apply to all channels in the channel list.
disable	Power settings do not apply to all channels in the channel list.

Examples

```
EWC.extremenetworks.com:ap:defaults:3935FCC# balanced-power enable
```

bcast_disassoc

Use the `bcast_disassoc` command to enable the Wireless AP to use broadcast disassociation when disconnecting all clients, instead of disassociating each client one by one. Use the `no` form of the command to disable the feature. The `bcast_disassoc` command is accessible from all `ap:` contexts of the CLI.

After you run the `bcast_disassoc` command, run the `apply` command to implement the change in broadcast disassociation.

```
bcast_disassoc no bcast_disassoc
```

Parameters

None

Examples

The following disassociates clients from the Wireless AP:

```
EWC.extremenetworks.com:ap:defaults:ap3935FCC# bcast_disassoc
```

bgway

Use the `bgway` command when statically configuring a Wireless AP. In order to statically configure a Wireless AP, you must first run the `no usedhcp` command. The `bgway` command is accessible from the `ap:<serial>` context of the CLI.

```
bgway xxx.xxx.xxx.xxx
```


Parameters

<code>xxx.xxx.xxx.xxx</code>	Specifies the default gateway of the network.
------------------------------	---

Example

```
EWC.extremenetworks.com:ap:70000122222222# bgway 10.205.3.2
```

client_session

Use the `client_session` command to enable users to maintain client sessions in the event of a poll failure. Use the `no` form of the command to disable the feature. The `client_session` command is accessible from the `ap:<serial>` and all `ap:defaults` contexts of the CLI.

After you run the `client_session` command, run the `apply` command to implement the change in client session.

```
client_session no client_session
```

Parameters

None

Examples

The following example enables user client sessions:

```
EWC.extremenetworks.com:ap:defaults:3935FCC# client_session
```

country

Use the `country` command to specify the country the Wireless AP resides in. The `country` command is accessible from the `ap:<serial>` and all `ap:defaults` contexts of the CLI.

After you run the `country` command, run the `apply` command to implement the change in country.

```
country country_name
```

Parameters

<code>country_name</code>	Specifies the name of the country
---------------------------	-----------------------------------

Example

The following example sets the name of the country to United States:

```
EWC.extremenetworks.com:ap:defaults:ap3935FCC# country United States
```

desc

Use the `desc` command to change the description of the Wireless AP. The `desc` command is accessible from the `ap:<serial>` context of the CLI.

```
desc new_description
```

Parameters

<i>new_description</i>	Specifies a description of the Wireless AP.
------------------------	---

Example

The following example provides a description for a Wireless AP

```
EWC.extremenetworks.com:ap:0500008043050212# desc This Access Point belongs
to the Blue Office
```

ipmcast-assembly

Use the `ipmcast-assembly` command to enable or disable AP IP multicast assembly. IP multicast assembly is accessible from the `ap:<serial>` and all `ap:defaults` contexts of the CLI.

ipmcast-assembly enable | disable

Parameters

enable	Enables IP multicast assembly for the current AP context
disable	Disables IP multicast assembly for the current AP context

Example

The following example enables IP multicast assembly for AP 1313254259510000:

```
EWC.extremenetworks.com:ap:1313254259510000#ipmcast-assembly enable
```

lACP

Use the `lACP` command to enable or disable LAGs on an AP. The `lACP` command is accessible from the `ap:<serial>` context of the CLI.

lACP enable | disable

Parameters

enable	Enables the LACP LAG feature on the AP3825i, AP3825e, and the AP3865e.
disable	Disables the LACP LAG feature on the AP3825i, AP3825e, and the AP3865e.

Example

The following example enables LAGs on AP ap:1111111111113825:

```
EWC.extremenetworks.com:ap:1111111111113825# lACP
```

lbs-status

Use the `lbs-status` command to enable or disable the collection of location-based (AeroScout or Ekahau) tags for any AP. The `lbs-status` command is accessible from the `ap:<serial>` and all `ap:defaults` contexts of the CLI.

lbs-status enable | disable

Parameters

enable disable	Enable or disable the collection of location-based tags for the APs.
--------------------------------	--

Examples

The following example enables the collection of AeroScout or Ekahau tags for the 802.11n APs:

```
EWC.extremenetworks.com:ap:defaults:ap3935FCC# lbs-status enable
```

led-mode

Use the `led-mode` command to configure the behavior of the LEDs on the Wireless AP. The `led-mode` command is accessible from the `ap:<serial>` and all `ap:defaults` contexts of the CLI.

led-mode identify | normal | off | wds-signal

Parameters

identify	All LEDs blink simultaneously approximately two to four times every second. Note: This parameter is only available in the <code><serial></code> context.
normal	Identifies the AP status at all times while the AP is powered on.
off	Displays fault patterns only. LEDs do not light when the AP is fault free and the discovery is complete.
wds-signal	Indicates the WDS signal strength as a bar graph. This setting helps to align external antennas in WDS deployments by correlating the WDS link RSS with the LED pattern. Use this setting only if the AP is participating in a Mesh or WDS network. Note: This parameter is only available in the <code><serial></code> context.

Usage

Only options `normal` and `off` are allowed in the `ap:defaults` contexts.

Examples

The following example turns off LED activity:

```
EWC.extremenetworks.com:ap:defaults:ap3935FCC# led-mode off
```

The following example configures the LED mode to indicate WDS signal strength:

```
EWC.extremenetworks.com:ap:0409920201202222# led-mode wds-signal
```

lldp

Use the `lldp` command to enable the broadcast of the LLDP protocol by a Wireless AP. Use the `no` form of the command to disable LLDP. The `lldp` command is accessible from the `ap:<serial>` and all `ap:defaults` contexts of the CLI.

lldp Announcement Interval Announcement Delay | no lldp

Parameters

<i>Announcement Interval</i>	Specifies the scheduled frequency, measured in seconds, in which the Wireless AP advertises its information by sending a new LLDP packet. Range is 5 to 32768.
<i>Announcement Delay</i>	Specifies the delay, measured in seconds, between successive LLDP frame transmissions that is initiated by a value/status change in the LLDP local systems MIB. Range is 1 to 1/4 x Announcement Interval value.

Examples

The following example enables LLDP for the default Wireless AP configuration with an announcement interval of 30 seconds, and an announcement delay of 2:

```
EWC.extremenetworks.com:ap:defaults:3935FCC# lldp 30 2
```

If SNMP is enabled to publish on the Wireless Appliance and you enable LLDP, the following message is displayed:

```
WARNING: SNMP is set to publish. How Do you wish to continue?
(C) Cancel
(P) Proceed
(O) Disable SNMP publishing and proceed
```

Type one of the following:

- C - Cancels the LLDP configuration and returns to the AP context.
- P - Enables LLDP and maintains SNMP running
- O - Enables LLDP and disables SNMP publishing

location

Use the `location` command to set the location string for the specified AP. The `location` command is accessible from the `ap:<serial>` context of the CLI.

location *location* | **no location**

Parameters

<i>location</i>	Assign an existing location or a new location
no location	Remove the location

Usage

This command supports the use of Unicode (UTF-8) strings. If the location string includes more than one word, you must enclose the string in double quotation marks.

Example

The following example sets the location for the Wireless AP as "2nd floor south":

```
EWC.extremenetworks.com:ap:0500008043050236# location "2nd floor south"
EWC.extremenetworks.com:ap:0500008043050236# apply
EWC.extremenetworks.com:ap:0500008043050236# show
host_name AP3801-0500008043050236
```

```
name 0500008043050236
desc
Location: 2nd floor south
```

move

Use the `move` command to change the rank of Wireless Appliances on the Wireless Appliance list. The `move` command is accessible from the `ap:<serial>` context of the CLI. It is also available from `ap:defaults` if `learnac` is disabled (no `learnac`) in that context.

```
move aclist rank1 + | - rank2
```

Parameters

<i>rank1</i>	Specifies the rank of the listed item to be moved
+ -	Move rank one position above or below the rank2 item
<i>rank2</i>	Specifies the rank of the second item

Example

```
EWC.extremenetworks.com:ap:0500008043050212# move aclist 3 + 2
```

name

Use the `name` command to assign or change the name of the Wireless AP. The `name` command is accessible from the `ap:<serial>` context of the CLI.

```
name newname
```

Parameters

<i>newname</i>	Specifies the new name of the Wireless AP
----------------	---

Example

The following example sets the name of the Wireless AP:

```
EWC.extremenetworks.com:ap:0500008043050212# name HomeAP1
```

persistent

Use the `persistent` command to enable the radio service to be restarted even in the absence of the controller. Use the `no` form of the command to disable the feature. The `persistent` command is accessible from the `ap:<serial>` and all `ap:defaults` contexts of the CLI.

```
persistent no | persistent
```

Parameters

None

Usage

Enable this feature (if using a bridged at AP VNS) to ensure the Wireless AP's radios continue providing service if the Wireless AP's connection to the controller is lost. If this feature is enabled, it allows the Wireless AP to start a bridged at AP VNS even in the absence of a wireless controller.

After you run the `persistent` command, run the `apply` command to implement the change in mode persistence value.

Example

The following example enables service persistence:

```
EWC.extremenetworks.com:ap:defaults:3935FCC# persistent
```

poll_timeout

Use the `poll_timeout` command to set the amount of time the Wireless AP waits for a response from the Wireless Appliance before rebooting. The `poll_timeout` command is accessible from the `ap:<serial>` and all `ap:defaults` contexts of the CLI.

After you run the `poll_timeout` command, run the `apply` command to implement the change in poll timeout value.

poll_timeout *value*

Parameters

<i>value</i>	Specifies the amount of time, in seconds, to wait for a response from the Wireless Appliance before rebooting. The range for <code>poll_timeout</code> value is from 3 to 600 unless the controller is in an availability pair without fast failover enabled.
--------------	---

Example

The following example sets the poll timeout to 20 seconds:

```
EWC.extremenetworks.com:ap:defaults:ap3801# poll_timeout 20
```

port-setting

Use the `port-setting` command to set the duplex mode and speed of the AP's Ethernet port. The `port-setting` command is accessible from the `ap:<serial>` context of the CLI.

port-setting **auto** | ((**half** | **full**) (**10** | **100**))

Parameters

auto	Auto negotiate speed and duplex mode
half full	Half or full duplex mode
10 100	10Mbps or 100Mbps Ethernet

Example

The following example sets the Ethernet port on the AP to auto:

```
EWC.extremenetworks.com:ap:0500008043050212# port-setting auto
```

professional_antenna

The `professional_antenna` command moves you into the professional-antenna context, which contains commands to configure professional antenna attributes. The `professional_antenna` command is accessible from the `ap:<serial>` context of the CLI.

**Note**

The `professional_antenna` command is available for APs with external antennas.

The following professional antenna configuration commands are available in the `ap:<serial>:professional_antenna` context for AP37xx and AP38xx APs:

- `leftantenna-radio1` on page 127
- `leftantenna-radio2` on page 128
- `middleantenna-radio1` on page 128
- `middleantenna-radio2` on page 129
- `rightantenna-radio1` on page 129
- `rightantenna-radio2` on page 130
- `show- antennas` on page 132

leftantenna-radio1

Use the `leftantenna-radio1` command to select an antenna supported by the Wireless AP. This command is accessible from the `<serial>` context of the CLI if the AP supports configuration of a left radio1 antenna. For AP models that support the Professional Install feature, `leftantenna-radio1` is accessible from the `ap:<serial>:professional_antenna#` context. To display a list of the available antenna models, enter the command without arguments.

The antenna commands available are dependent on the AP type.

leftantenna-radio1 *antenna_model*

Parameters

<i>antenna_model</i>	Model name of an antenna supported by the Wireless AP.
----------------------	--

Examples

This example lists the valid antenna models that can be entered with this command, then executes the command with an appropriate model number:

```
EWC.extremenetworks.com:ap:0500010032150135 leftantenna-radio1
Usage: leftantenna-radio1 <antenna_model>
antenna_model:
<list of valid antenna models>
WS-AO-2S03360 G 3.5 dBi Omni
No Antenna
EWC.extremenetworks.com:ap:0500010032150135 leftantenna-radio1 WS-AO-2S03360
G 3.5 dBi Omni
```

This example removes a configured left radio1 antenna:

```
EWC.extremenetworks.com:ap:0500010032150135# leftantenna-radio1 No Antenna
```

leftantenna-radio2

Use the `leftantenna-radio2` command to select an antenna supported by the Wireless AP. Enter the command without arguments to list the available antenna models. The `leftantenna-radio2` command is accessible from the `ap:<serial>` context of the CLI if the AP supports configuration of a left antenna radio2. For AP models that support the Professional Install feature, `leftantenna-radio2` is accessible from the `ap:<serial>:professional_antenna` context.

The antenna commands available are dependent on the AP type.

leftantenna-radio2 *antenna_model*

Parameters

<i>antenna_model</i>	Model name of an antenna supported by the Wireless AP.
----------------------	--

Examples

This example lists the valid antenna models that can be entered with this command, then executes the command with an appropriate model number:

```
EWC.extremenetworks.com:ap:0500010032150135# leftantenna-radio2
Usage: leftantenna-radio2 <antenna_model>
antenna_model:
<list of valid antenna models>
No Antenna
WS-AO-2S03360 G 3.5 dBi Omni
EWC.extremenetworks.com:ap:0500010032150135# leftantenna-radio2 WS-AO-2S03360
G 3.5 dBi Omni
```

This example removes a configured left radio2 antenna:

```
EWC.extremenetworks.com:ap:0500010032150135# leftantenna-radio2 No Antenna
```

middleantenna-radio1

Use the `middleantenna-radio1` command to select an antenna supported by the Wireless AP. This command is accessible from the `<serial>` context of the CLI if the AP supports configuration of a middle antenna. For AP models that support the Professional Install feature, `middleantenna-radio1` is accessible from the `ap:<serial>:professional_antenna#` context. To display a list of the available antenna models, enter the command without arguments.

The antenna commands available are dependent on the AP type.

middleantenna-radio1 *antenna_model*

Parameters

<i>antenna_model</i>	Model name of an antenna supported by the Wireless AP.
----------------------	--

Examples

This example lists the valid antenna models that can be entered with this command, then executes the command with an appropriate model number:

```
EWC.extremenetworks.com:ap:0500010032150135# middleantenna-radio1
Usage: middleantenna-radio1 <antenna_model>
antenna_model:
<list of valid antenna models>
WS-ANT02 AG 4dBi Omni Factory
No Antenna
EWC.extremenetworks.com:ap:0500010032150135 middleantenna-radio1 WS-ANT02 AG
4dBi Omni Factory
```

This example removes a configured middle antenna for radio1:

```
EWC.extremenetworks.com:ap:0500010032150135# middleantenna-radio1 No Antenna
```

middleantenna-radio2

Use the `middleantenna-radio2` command to select an antenna supported by the Wireless AP. This command is accessible from the `<serial>` context of the CLI if the AP supports configuration of a right antenna. For AP models that support the Professional Install feature, `middleantenna-radio2` is accessible from the `ap:<serial>:professional_antenna#` context. To display a list of the available antenna models, enter the command without arguments.

The antenna commands available are dependent on the AP type.

middleantenna-radio2 *antenna_model*

Parameters

<i>antenna_model</i>	Model name of an antenna supported by the Wireless AP.
----------------------	--

Examples

This example lists the valid antenna models that can be entered with this command, then executes the command with an appropriate model number:

```
EWC.extremenetworks.com:ap:0500010032150135# middleantenna-radio2
Usage: middleantenna-radio2 <antenna_model>
antenna_model:
<list of valid antenna models>
WS-ANT01 AG 4dBi Omni Factory
No Antenna
EWC.extremenetworks.com:ap:0500010032150135# middleantenna-radio2 WS-ANT01 AG
4dBi Omni Factory
```

This example removes a configured middle antenna for radio2:

```
EWC.extremenetworks.com:ap:0500010032150135# middleantenna-radio2 No Antenna
```

rightantenna-radio1

Use the `rightantenna-radio1` command to select an antenna supported by the Wireless AP. This command is accessible from the `<serial>` context of the CLI if the AP supports configuration of a right radio1 antenna. For AP models that support the Professional Install feature, `rightantenna-radio1` is

accessible from the `ap:<serial>:professional_antenna#` context. To display a list of the available antenna models, enter the command without arguments.

The antenna commands available are dependent on the AP type.

rightantenna-radio1 *antenna_model*

Parameters

<i>antenna_model</i>	Model name of an antenna supported by the Wireless AP.
----------------------	--

Examples

This example lists the valid antenna models that can be entered with this command, then executes the command with an appropriate model number:

```
EWC.extremenetworks.com:ap:0500010032150135# rightantenna-radio1
Usage: rightantenna-radio1 <antenna_model>
antenna_model:
<list of valid antenna models>
WS-AO-2S03360 G 3.5 dBi Omni
No Antenna
EWC.extremenetworks.com:ap:0500010032150135# rightantenna-radio1 WS-
AO-2S03360 G 3.5 dBi Omni
```

This example removes a configured right radio1 antenna:

```
EWC.extremenetworks.com:ap:0500010032150135# rightantenna-radio1 No Antenna
```

rightantenna-radio2

Use the `rightantenna-radio2` command to select an antenna supported by the Wireless AP. This command is accessible from the `<serial>` context of the CLI if the AP supports configuration of a right radio2 antenna. For AP models that support the Professional Install feature, `rightantenna-radio2` is accessible from the `ap:<serial>:professional_antenna#` context. Enter the command without arguments to list the available antenna models.

The antenna commands available are dependent on the AP type.

rightantenna-radio2 *antenna_model*

Parameters

<i>antenna_model</i>	Model name of an antenna supported by the Wireless AP.
----------------------	--

Examples

This example lists the valid antenna models that can be entered with this command, then executes the command with an appropriate model number:

```
EWC.extremenetworks.com:ap:0500010032150135# rightantenna-radio2
Usage: rightantenna-radio2 <antenna_model>
antenna_model:
<list of valid antenna models>
No Antenna
WS-AO-2S03360 G 3.5 dBi Omni
```

```
EWC.extremenetworks.com:ap:0500010032150135# rightantenna-radio2 WS-
AO-2S03360 G 3.5 dBi Omni
```

This example removes a configured right radio2 antenna:

```
EWC.extremenetworks.com:ap:0500010032150135# rightantenna-radio2 No Antenna
```

3935e ports

Use the following port commands for the AP 3935e to select an antenna port. These commands are accessible from the <serial> context of the CLI. For AP models that support the Professional Install feature, these commands are accessible from the ap:<serial>;professional_antenna# context. To display a list of the available antenna models, enter a command without arguments.

- port1-radio1 <antenna_model>
- port1-radio2 <antenna_model>
- port2-radio1 <antenna_model>
- port2-radio2 <antenna_model>
- port3-radio1 <antenna_model>
- port3-radio2 <antenna_model>
- port4-radio1 <antenna_model>
- port4-radio2 <antenna_model>

```
port1-radio1 antenna_model
```

Parameters

<i>antenna_model</i>	Model name of an antenna supported by the Wireless AP.
----------------------	--

Examples

This example lists the valid antenna models that can be entered with this command, then executes the command with an appropriate model number:

```
EWC.extremenetworks.com ap:3935e000R100on00:professional_antenna# port1-radio1
Error : There is no selected antenna model.
Usage: port1-radio1 <antenna_model>
antenna_model:
<list of valid antenna models>
WS-ANT-5DIP-4 Dipole
WS-AI-DQ05120 5dBi 120deg Sector
WS-AI-DQ04360 4dBi Omni
WS-AI-DE10055 10/6dbi 55deg Sector
WS-AI-DE07025 6.5/5dbi 25deg Sector
WS-AI-5Q05025 5.5dbi 25deg Sector
WS-AI-5Q04060 5dbi 60deg Sector
No Antenna
EWC.extremenetworks.comap:3935e000R100on00:professional_antenna# port1-radio1
WS-ANT-5DIP-4
```

This example removes a configured port1 radio1 antenna:

```
EWC.extremenetworks.com:ap:3935e000R100on00:professional_antenna# port1-
radio1 No Antenna
```

show- antennas

Use the `show` command in the `professional_antenna` context to display the antenna configuration for the selected AP.

show

Parameters

There are no parameters.

Examples

The following example lists the antenna configuration for the AP 37xx.

```
EWC.extremenetworks.com:ap:111111111137152:professional_antenna# show
Professional Antenna Install:
```

Antenna	Type
Radio 1 Left Antenna Type	PRO-AI-DT05120 AG 5dBi 120deg 3f
Radio 1 Middle Antenna Type	No Antenna
Radio 1 Right Antenna Type	No Antenna
Radio 2 Left Antenna Type	PRO-AI-DT05120 AG 5dBi 120deg 3f
Radio 2 Middle Antenna Type	No Antenna
Radio 2 Right Antenna Type	No Antenna

Refer to [user](#) on page 223 for descriptions of the values in the various columns of this output.

radio1

The `radio1` command refers to the `radio1` context, which contains commands to configure Radio 1 on each Wireless AP. The `radio1` command is accessible from the `ap:<serial>` and all `ap:defaults` contexts of the CLI; `radio` command options differ depending on the AP type and radio mode.

- [admin-mode](#) on page 141
- [antsel](#) on page 141
- [atpc](#) on page 142
- [att](#) on page 142
- [beaconp](#) on page 143
- [ch](#) on page 143
- [dcs](#) on page 144 — See [DCS Commands](#) on page 158 for commands in the `dcs` context.
- [domain](#) on page 144
- [dtim](#) on page 144
- [force-disassociate](#) on page 145
- [frag](#) on page 145
- [ldpc](#) on page 146
- [max-distance](#) on page 146
- [mcast-adaptable](#) on page 146
- [mcast2ucast](#) on page 147
- [minbrate](#) on page 147
- [mode](#) on page 148

- [n_addba_support](#) on page 149
- [n_aggr_mpdu](#) on page 149
- [n_aggr_mpdu_max](#) on page 150
- [n_aggr_mpdu_max_subframes](#) on page 150
- [n_aggr_msdu](#) on page 150
- [n_chlwidth](#) on page 151
- [n_guardinterval](#) on page 151
- [n_pbthreshold](#) on page 152
- [n_pmode](#) on page 152
- [n_ptype](#) on page 152
- [nonUnicastQuota](#) on page 153
- [optimized-mcast](#) on page 153
- [pmode](#) on page 153
- [prate](#) on page 154
- [preamble](#) on page 154
- [probe-suppression](#) on page 155
- [ptype](#) on page 155
- [rss-threshold](#) on page 155
- [rts](#) on page 156
- [stbc](#) on page 156
- [tx_adjust_power](#) on page 157
- [txbf](#) on page 157
- [tx_max_power](#) on page 158
- [tx_min_power](#) on page 158

radio2

The `radio2` command refers to the radio2 context, which contains commands to configure Radio 2 on each Wireless AP. The `radio2` command is accessible from the `ap:<serial>` and all `ap:defaults` contexts of the CLI; `radio` command options differ depending on the AP type and radio mode.

- [admin-mode](#) on page 141
- [antssel](#) on page 141
- [atpc](#) on page 142
- [att](#) on page 142
- [beaconp](#) on page 143
- [ch](#) on page 143
- [dcs](#) on page 144 — See [DCS Commands](#) on page 158 for commands in the dcs context.
- [domain](#) on page 144
- [dtim](#) on page 144
- [force-disassociate](#) on page 145
- [frag](#) on page 145
- [ldpc](#) on page 146
- [max-distance](#) on page 146
- [mcast-adaptable](#) on page 146

- [mcast2ucast](#) on page 147
- [minbrate](#) on page 147
- [mode](#) on page 148
- [n_addba_support](#) on page 149
- [n_aggr_mpdu](#) on page 149
- [n_aggr_mpdu_max](#) on page 150
- [n_aggr_mpdu_max_subframes](#) on page 150
- [n_aggr_msdu](#) on page 150
- [n_chlwidth](#) on page 151
- [n_guardinterval](#) on page 151
- [n_pbthreshold](#) on page 152
- [n_pmode](#) on page 152
- [n_ptype](#) on page 152
- [nonUnicastQuota](#) on page 153
- [optimized-mcast](#) on page 153
- [pmode](#) on page 153
- [prate](#) on page 154
- [preamble](#) on page 154
- [probe-suppression](#) on page 155
- [ptype](#) on page 155
- [rss-threshold](#) on page 155
- [rts](#) on page 156
- [stbc](#) on page 156
- [tx_adjust_power](#) on page 157
- [txbf](#) on page 157
- [tx_max_power](#) on page 158
- [tx_min_power](#) on page 158

real_capture

Use the `real_capture` command to monitor beacons, association requests, probe responses, and data packets on the radio 1, radio 2, or ethernet of all APs. The `real_capture` command is meant to be used in conjunction with Wireshark tool to analyze traffic on the ap and is available from the `ap:<serial>` context of all APs.

```
real_capture start | stop time eth0 | wifi0 | wifi1
```

Parameters

start	Begins monitoring the traffic on the ap.
stop	Stops monitoring the traffic on the ap.
<i>time</i>	The amount of time (in minutes) the ap monitors traffic. Valid entries are 0-3600.
eth0	Monitors the ethernet connection.

wifi0	Monitors the radio1 connection.
wifi1	Monitors the radio2 connection.

Example

The following example monitors traffic on radio1 of AP ap:0500008043050236 for 30 minutes:

```
EWC.extremenetworks.com:ap:0500008043050236# real_capture start 30 wifi0
```

secure-tunnel

Use the `secure-tunnel` command to enable or disable a secure tunnel on this site. The `secure-tunnel` command is accessible from the `ap:<serial>` and all `ap:defaults` contexts of the CLI.

secure-tunnel disable | control | data | debug

Parameters

disable	Disables a secure tunnel between this AP and the controller.
control	Enables a secure tunnel by encrypting control traffic between the AP and the controller.
data	Enables a secure tunnel by encrypting control and data traffic between the AP and the controller.
debug	Enables tunnel in debug mode, which preserves keys without encryption.

Usage

If enabling a secure tunnel, specify the type of traffic this tunnel will encrypt and carry: control traffic, or control and data traffic. Secure tunneling can also be used for debug mode (keys are preserved without encryption).



Note

For some AP models, the data option is not available.

Example

The following example enables a secure tunnel that encrypts control and data traffic on AP37xxs:

```
EWC.extremenetworks.com:ap:defaults:ap37xx# secure-tunnel data
```

secure-tunnel-lifetime

Use the `secure-tunnel-lifetime` command to enable or configure the lifetime (the number of hours the tunnel remains enabled) of this tunnel. The `secure-tunnel-lifetime` command is accessible from the `ap:<serial>` and all `ap:defaults` contexts of the CLI.

secure-tunnel-lifetime hours

Parameters

<i>hours</i>	Specifies the number of hours the tunnel will remain enabled.
--------------	---

Usage

The `secure-tunnel` command must be enabled before the `secure-tunnel-lifetime` command can be run. The default is 0 hours, indicating the tunnel remains enabled until it is manually disabled. Valid entries are 0, or any number between 24-3600. When this value expires, the tunnel becomes disabled. Use the `secure-tunnel disable` command to terminate a tunnel.

Example

The following example enables a secure tunnel for 24 hours:

```
EWC.extremenetworks.com:ap:defaults:ap37xx# secure-tunnel-lifetime 24
```

show

Use the `show` command to display AP information. The `show` command is accessible from the `ap:<serial>`, all `ap:defaults:` contexts and professional-antenna contexts of the CLI.

show**Parameters**

None

Examples

The following example displays 3935FCC AP information:

```
EWC.extremenetworks.com:ap:defaults:3935FCC# showssh enabled
poll_timeout 15
no client_session
no persistent
no bcast_disassoc
country United States
no lldp
led-mode normal
lbs-status enabled
secure-tunnel disable
ipmcast-assembly disabled
balanced-power enabled
```

The following example displays ap37xx information:

```
EWC.extremenetworks.com:ap:defaults:ap37xx# show
ssh enabled
poll_timeout 22
client_session
persistent
bcast_disassoc
country Ireland
no lldp
led-mode normal
lbs-status enabled
secure-tunnel disable
ipmcast-assembly disabled
```


The following example displays information for the <serial> AP:

```
EWC.extremenetworks.com:ap:0500008043050236# show
host_name AP3620-0500008043050236
name 0500008043050236
desc
Location:
role ap
ap_env indoor
usedhcp
poll_timeout 15
client_session
no persistent
no bcast_disassoc
no vlanid
country United States
led-mode normal
wlan test both
lbs-status enabled
port-setting auto
tunnel-mtu 1500
ssh enabled
antennaleft No Antenna
antennamiddle No Antenna
antennaright No Antenna
```

The following example displays the load groups:

```
EWC.extremenetworks.com:ap:load-groups# show
Load Groups:
loadgroup1
loadgroup2
```

The following example displays the contents of the professional-antenna context:

```
EWC.extremenetworks.com:ap:1313254259510000:professional_antenna# show
Professional Antenna Install:
Antenna                               Type
Radio 1 Left Antenna Type             No Antenna
Radio 1 Middle Antenna Type           PRO-AI-DT05120 AG 5dBi 120deg 3f
Radio 1 Right Antenna Type            PRO-AI-DX02360 AG 2dBi Omni
Radio 2 Left Antenna Type              PRO-AI-DX02360 AG 2dBi Omni
Radio 2 Middle Antenna Type            PRO-AI-DX02360 AG 2dBi Omni
Radio 2 Right Antenna Type             PRO-AI-DX07025 AG 7dBi 27/30deg
```

ssh

Use the `ssh` command to enable or disable SSH.

The `ssh` command is accessible from the `ap:<serial>` and all `ap:defaults` contexts of the CLI.

ssh enable | disable

Parameters

enable disable	Enables or disables SSH on the specified AP.
-------------------------	--

Usage

By default, SSH is enabled. If you disable SSH, you can still retrieve AP traces from the controller through SFTP.

Example

The following command disables SSH on AP 0500008043050236:

```
EWC.extremenetworks.com:ap:0500008043050236# ssh disable
```

tunnel-mtu

Use the `tunnel-mtu` command to set the static MTU value. The `tunnel-mtu` command is accessible from the `ap:<serial>` context of the CLI.

```
tunnel-mtu 600-1500
```

Parameters

<code>600-1500</code>	Specifies the static MTU size in bytes. The default is 1500 bytes. Some controllers allow you to enable jumbo frames, in which case the range increases to 600-1800.
-----------------------	--

Usage

The wireless software enforces the static MTU size if it cannot discover the MTU size. Set the MTU size to allow the source to reduce the packet size and avoid the need to fragment data packets in the tunnel.

Example

The following command sets the MTU tunnel size to 1300 bytes:

```
EWC.extremenetworks.com:ap:0500008043050236# tunnel-mtu 1300
```

usedhcp

Use the `usedhcp` command to enable DHCP. Use the `no` form of the command to statically configure a Wireless AP. The `usedhcp` command is accessible from the `ap:<serial>` context of the CLI.

```
usedhcp  
no usedhcp
```

Parameters

None

Example

The following example enables DHCP on the Wireless Appliance:

```
EWC.extremenetworks.com:ap:0122003880188015# usedhcp
```

vlanid

Use `vlanid` to assign a VLAN tag to the subnet carrying the Wireless AP's management traffic. The `vlanid` command is accessible from the `ap:<serial>` context of the CLI.

```
vlanid 1-4094
```

Parameters

<code>1-4094</code>	Specifies the ID tag for the VLAN
---------------------	-----------------------------------

Example

The following example assigns the subnet a VLAN tag:

```
EWC.extremenetworks.com:ap:0122003880188015# vlanid 4
```

wlan

Use the `wlan` command to assign one or both of the AP's radios to the specified WLAN service. You can also use this command to unassign the AP's radios from the specified WLAN service. The `wlan` command is accessible from the `ap:<serial>` context of the CLI.

```
wlan wlan name ( radio1 | radio2 | both | none )
```

Parameters

<code>wlan name</code>	The WLAN service to which you want to assign the AP's radios or from which you want to unassign the AP's radios.
<code>radio1 radio2 both none</code>	Specifies the radios that you want to assign to the WLAN service. Use none to unassign the radios from the WLAN service.

Example

The following example assigns radio 2 of AP 0500008043050355 to the WLAN service named CNL-91-0-1:

```
EWC.extremenetworks.com:ap:0500008043050355# wlan CNL-91-0-1 radio2
EWC.extremenetworks.com:ap:0500008043050355# show
host_name AP3935-0500008043050355
name AP3935 internal
desc
usedhcp
poll_timeout 15
client_session
no persistent
no bcast_disassoc
no vlanid
country Germany
led-mode normal
wlan CNL-91-0-1 radio2
```

zone

Use the `zone` command to create a policy zone for the named Wireless AP. The command is accessible from the `ap:<serial>` context of the CLI.

```
zone name
```

Parameters

<code>zone name</code>	Specifies the name for the policy zone you are assigning to this AP.
------------------------	--

Examples

The following example sets the policy zone for AP 0500008043050212 to “Newbury”:

```
EWC.extremenetworks.com:ap:0500008043050212# zone Newbury
EWC.extremenetworks.com:ap:0500008043050212# show
Policy Zone: Newbury
SW Version: 08.11.01.0055
Hardware Type: Wireless AP3935 External
Tunnel Type: unsecured
Wired MAC Address: 00:0F:C8:F0:1B:3C
Home: LOCAL
Static IP Address: 10.201.0.172
Status: APPROVED
Port#:
```

Radio Commands

The commands in this section are common to multiple radio1 and radio2 commands in all the ap:defaults and ap:<serial> contexts.

- [admin-mode](#) on page 141
- [antssel](#) on page 141
- [atpc](#) on page 142
- [att](#) on page 142
- [beaconp](#) on page 143
- [ch](#) on page 143
- [dcs](#) on page 144 — See [DCS Commands](#) on page 158 for commands in the ap:<serial>:radio1:dcs context.
- [domain](#) on page 144
- [dtim](#) on page 144
- [force-disassociate](#) on page 145
- [frag](#) on page 145
- [ldpc](#) on page 146
- [max-distance](#) on page 146
- [mcast-adaptable](#) on page 146
- [mcast2ucast](#) on page 147
- [minbrate](#) on page 147
- [mode](#) on page 148
- [n_addba_support](#) on page 149
- [n_aggr_mpdu](#) on page 149
- [n_aggr_mpdu_max](#) on page 150
- [n_aggr_mpdu_max_subframes](#) on page 150
- [n_aggr_msdu](#) on page 150
- [n_chlwidth](#) on page 151
- [n_guardinterval](#) on page 151
- [n_pbthreshold](#) on page 152
- [n_pmode](#) on page 152

- [n_ptype](#) on page 152
- [nonUnicastQuota](#) on page 153
- [optimized-mcast](#) on page 153
- [pmode](#) on page 153
- [prate](#) on page 154
- [preamble](#) on page 154
- [probe-suppression](#) on page 155
- [ptype](#) on page 155
- [rss-threshold](#) on page 155
- [rts](#) on page 156
- [stbc](#) on page 156
- [tx_adjust_power](#) on page 157
- [txbf](#) on page 157
- [tx_max_power](#) on page 158
- [tx_min_power](#) on page 158

admin-mode

Use this command to configure the administration status for the radio. The `admin-mode` command is accessible from all radio1 and radio2 contexts of the CLI.

admin-mode off | on

Parameters

off	Clear the administrative status.
on	Set the administrative status.

Example

```
EWC.extremenetworks.com:ap:defaults:3935FCC:radio2# admin-mode on
```

antse1

Use the `antse1` command to configure the antenna combination you want to use for the radio. The `antse1` command is accessible from the `ap:defaults: ap37xx`, and `ap38xx` as well as `ap:<serial>` CLI contexts for all 37xx, and 38xx APs, except for ap3705, ap3801, and ap3805.

After you run the `antse1` command, run the `apply` command to implement the change.

antse1 left | left-middle | left-middle-right

Parameters

left	Specifies the use of the left antenna on the AP.
left-middle	Specifies the use of the left-middle antenna combination on the AP.
left-middle-right	Specifies the use of the left-middle-right antenna combination on the AP.

Usage

The antenna options available depend on the type of AP and the radio. We support: left, left/middle, and left/middle/right on many APs. This is not supported on the AP39xx.

Example

The following example depicts Radio 2 of the Wireless AP37xx AP configured to use the left-middle-right antenna combination:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio2# antsel left-middle-right
```

atpc

Use the `atpc` command to enable Auto Tx Power Ctrl (ATPC). Use the `no` form of the command to disable the ATPC feature. The `atpc` command is accessible from all `radio1` and `radio2` contexts of the CLI.

After you run the `atpc` command, run the `apply` command to implement the change.

```
atpc no | atpc [maintain_power]
```

Parameters

maintain_power	When you disable ATPC, you can elect to maintain using the current Tx power setting ATPC had established.
-----------------------	---

Example

The following example disables `atpc` on Radio 1:

```
EWC.extremenetworks.com:ap:defaults:ap3801:radio1# no atpc maintain_power
```

att

Use this command to configure the attenuation for this radio context. The `att` command is accessible only from `ap:<serial>:radio1` and `ap:<serial>:radio2` contexts for APs with external antennas.

```
att att-value
```

Parameters

<i>att-value</i>	Specifies a radio attenuation value between 0 - 30
------------------	--

Example

This example sets the attenuation value to 10 for the AP 0409920201204003 `radio2` context:

```
EWC.extremenetworks.com:ap:0409920201204003:radio2# att 10
EWC.extremenetworks.com:ap:0409920201204003:radio2# apply
```

beaconp

Use the `beaconp` command to set time units between beacon transmissions. The `beaconp` command is accessible from all radio contexts of the CLI.

After you run the `beaconp` command, run the `apply` command to implement the change.

```
beaconp 50-1000
```

Parameters

<code>50-1000</code>	Specifies the number of time units (milliseconds) between beacon transmissions.
----------------------	---

Example

The following example sets the time between successive beacons to 70 ms on Radio 2:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio2# beaconp 70
```

ch

Use the `ch` command to set a fixed channel for this radio. The `ch` command is accessible from the `ap:<serial>`: radio contexts of the CLI.

```
ch channel number
```

Parameters

<code>channel number</code>	<p>Specifies the number of the channel this radio uses. Possible channel ranges are:</p> <ul style="list-style-type: none"> • 2.4GHz radio: 1-14 • 5 GHz radio: 36-165 <p>Actual channels available depend on AP type, controller license, country, antenna settings, AP environment, and radio mode. It is advisable to set the channel to Auto and allow the controller to ensure the best overall wireless coverage for the environment.</p>
-----------------------------	---

Example

The following example sets the channel to 40 on Radio 1:

```
EWC.extremenetworks.com:ap:<serial>:radio1# ch 40
```

The following example checks available channels and then sets the channel to Auto on Radio 1:

```
EWC.extremenetworks.com:ap:1313254259510000:radio1# ch
Usage: ch (Auto|36|40|44|48|52|56|60|64|100|104|108|112|149|153|157|161)
Auto
36: ([5180],5200,5220,5240):13.5dBm
40: (5180,[5200],5220,5240):13.5dBm
44: (5180,5200,[5220],5240):13.5dBm
48: (5180,5200,5220,[5240]):13.5dBm
52: ([5260],5280,5300,5320):15.5dBm
56: (5260,[5280],5300,5320):15.5dBm
60: (5260,5280,[5300],5320):15.5dBm
```

```

64: (5260,5280,5300,[5320]):15.5dBm
100: ([5500],5520,5540,5560):15.5dBm
104: (5500,[5520],5540,5560):15.5dBm
108: (5500,5520,[5540],5560):15.5dBm
112: (5500,5520,5540,[5560]):15.5dBm
149: ([5745],5765,5785,5805):21.5dBm
153: (5745,[5765],5785,5805):21.5dBm
157: (5745,5765,[5785],5805):21.5dBm
161: (5745,5765,5785,[5805]):21.5dBm
EWC.extremenetworks.com:ap:<serial>:radio1# ch Auto

```

dcS

The `dcS` command refers to the `dcS` context, which contains commands to configure the Dynamic Channel Selection (DCS) feature. The `dcS` command is accessible from all radio contexts of the CLI.

The `dcS` commands are described in the [DCS Commands](#) on page 158.

DCS commands do not require being followed with an `apply` command.

The following commands (or a subset of these) are available in the various `dcS` contexts:

- [channel_plan](#) on page 159
- [mode](#) on page 160
- [noise_threshold](#) on page 161
- [occupancy_threshold](#) on page 161
- [radio_channels](#) on page 161
- [update_period](#) on page 162

domain

Use the `domain` command to identify a group of APs that cooperate in managing RF channels and transmission power levels. The `domain` command is accessible from all radio contexts of the CLI.

domain *domain_name*

Parameters

<i>domain_name</i>	Specifies the group name of APs that cooperate in managing RF channels. The maximum length of the domain string is 16 characters.
--------------------	---

Example

The following example assigns the name `test` to the group of APs that cooperate in managing RF channels and transmission power levels:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio2# domain test
```

dtim

Use the `dtim` command to set the Delivery Traffic Indication Message (DTIM) period. The `dtim` command is accessible from all radio contexts of the CLI.

dtim *value*

Parameters

<i>value</i>	Specifies the DTIM period in beacon intervals. The range for the dtim value is from 1 to 255 beacon intervals.
--------------	--

Example

The following example sets the Delivery Traffic Indication Message period to 2 beacons:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio2# dtim 2
```

force-disassociate

Use the `force-disassociate` command to enable or disable force disassociate on an AP radio. The `force-disassociate` command is accessible from all default contexts: and from `ap <serial> radio` contexts when probe-suppression is enabled.

force-disassociate **enable** | **disable**

Parameters

disable enable	Enables or disables force disassociate for this radio context.
--------------------------------	--

Usage

Probe-suppression is useful in dense deployments (such as stadiums) where a large number of APs may be operating in close proximity. It permits the administrator to configure smaller cells. Thus clients only attempt to associate with the AP that is closest and has the strongest signal. This removes much of the overhead, permitting better performance of the network.

If `force-disassociate` is enabled, clients who move away from their AP, from one cell to another, find it easier to roam to a new AP.

Example

The following example enables force disassociate on radio 1 of AP 111111111113705:

```
EWC.extremenetworks.com:ap:111111111113705:radio1# force-disassociate enable
```

frag

Use the `frag` command to set the fragmentation threshold, which is the maximum size of a packet or data unit that can be delivered. Any data above this threshold is fragmented into packets that are less than or equal to this limit. The `frag` command is accessible from all `radio1` and `radio2` contexts of the CLI.

frag *value*

Parameters

<i>value</i>	Specifies the maximum size, measured in bytes, of any packet fragment for delivery. The value range is 256 to 2346.
--------------	---

Example

The following example sets the fragmentation threshold to 1500:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio2# frag 1500
```

ldpc

Use the `ldpc` command to enable or disable 11n advanced LDPC feature on the radio of this context. The `ldpc` command is accessible from all `ap:defaults: radio` contexts and `ap:<serial>:radio` contexts of the CLI.

ldpc enable | disable

Parameters

enable	Enables LDPC on this radio.
disable	Disables LDPC on this radio.

Example

The following example enables LDPC on Radio 2:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio2# ldpc enable
```

max-distance

Use the `max-distance` command to set the maximum link distance, in meters, between APs that participate in a WDS. This value ensures that the acknowledgement of communication between APs does not exceed the timeout value predefined by the 802.11 standard. If the link distance between APs is greater than the default value of 100 meters, configure the maximum distance up to 15,000 meters so that the software increases the timeout value proportionally with the distance between APs. The `max-distance` command is accessible from most radio contexts of the CLI.

Do not change the default setting for any radio that is not participating in a Mesh or WDS.

max-distance value

Parameters

value	Specifies the maximum distance between APs in meters. The default is 100 meters. You can enter a value from 100 to 15000 meters.
--------------	--

Example

The following example sets the maximum distance between APs to 1500 meters:

```
EWC.extremenetworks.com:ap:defaults:ap3801:radio2# max-distance 1500
```

mcast-adaptable

Use the `mcast-adaptable` command to enable or disable an adaptable rate for multicasts. The `mcast-adaptable` command is accessible from all `ap:defaults: radio` contexts of the CLI.

mcast-adaptable enable | disable

Parameters

enable	Enables the adaptable multicast rate on this radio.
disable	Disables the adaptable multicast rate on this radio

Example

The following example enables adaptable multicast rate on radio1:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio1# mcast-adaptable enable
```

mcast2ucast

Use the `mcast2ucast` command to configure multicast to unicast delivery. The `mcast2ucast` command is accessible from `radio1` and `radio2` contexts of the CLI.

mcast2ucast (disabled | auto)

Parameters

auto	Multicast to unicast delivery is automatic on this radio.
disabled	Multicast to unicast delivery is disabled on this radio.

Example

The following example makes multicast to unicast delivery automatic on radio1:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio1# mcast2ucast auto
```

minbrate

Use this command to configure the minimum basic data rate for radio 2. The `minbrate` command is accessible from all radio contexts of the CLI.

minbrate min-rate

Parameters

Valid values for `min-rate` depend on the radio mode:

Radio Mode	Minimum Basic Rates
a	6 12 24
ac-strict	6 12 24 MCS0,1 MCS1,1 MCS2,1 MCS3,1 MCS4,1 MCS5,1 MCS6,1 MCS7,1
an	6 12 24
anac	6 12 24
b	1 2 5.5 11
g	6 12 24

Radio Mode	Minimum Basic Rates
gn	6 12 24
n-strict	6 12 24 MCS0 - MCS7
bg	1 2 5.5 11
bgn	1 2 5.5 11

Usage

The minimum basic rate must be lower than or equal to the configured maximum basic data rate and maximum data rate that clients can operate at while associated with the AP.

Example

This example sets the mode for radio 2 to g, then sets the minimum basic data rate to 12 Mbps:

```
EWC.extremenetworks.com:ap:defaults:ap3801:radio2# mode g
EWC.extremenetworks.com:ap:defaults:ap3801:radio2# minbrate 12
```

mode

Use the `mode` command to set the radio options for the radio context. The `mode` command is accessible from all radio contexts of the CLI. Depending on the radio mode you select, some of the radio settings may not be available for configuration.

Syntax: (ap37xx, radio1)

mode a | an | n-strict

Syntax: (ap37xx, radio2)

mode b | g | gn | n-strict | bg | bgn

Syntax: (ap38xx, ap3801, ap3935, ap3965 radio1)

mode anac | ac-strict

Syntax: (ap38xx, ap3801, ap3935, ap3965 radio2)

mode bg | gn | bgn | n-strict

Parameters

a	Enables only 802.11a mode.
ac-strict	Enables the 802.11ac strict mode.
an	Enables both the 802.11a mode and the 802.11n mode.
anac	Enables the 802.11ac mode as well as supporting 802.11a and 802.11n modes.
b	Enables the 802.11b-only mode. If enabled, the AP uses only 11b (CCK) rates with all associated clients.
g	Enables the 802.11g-only mode. The AP uses 11g-only (OFDM) rates with all associated clients.

gn	Enables both the 802.11g mode and the 802.11n mode of Radio 2. If selected, the AP uses 11n and 11g-specific (OFDM) rates with all of the associated clients. The AP does not transmit or receive 11b rates.
n-strict	Enables the 802.11n-strict mode. If selected, the AP uses 11n and (optionally) 11a or 11g rates with all of the associated clients, depending on the radio. The AP does not transmit or receive 11b rates.
bg	Enables both the 802.11g mode and the 802.11b mode. If enabled, the AP uses 11b (CCK) and 11g-specific (OFDM) rates with all of the associated clients. The AP does not transmit or receive 11n rates.
bgn	Enables b/g/n modes. If enabled, the AP uses all available 11b, 11g, and 11n rates.

Examples

The following example enables 802.11ac as well as supporting 802.11a and 802.11n modes of Radio 1:

```
EWC.extremenetworks.com:ap:defaults:ap38xx:radio1# mode anac
```

The following example enables only the 802.11ac strict mode of Radio 1:

```
EWC.extremenetworks.com:ap:defaults:ap38xx:radio1# mode ac-strict
```

n_addba_support

Use the `n_addba_support` command to enable the ADDBA support. Use the `no` command to disable the feature. The `n_addba_support` command is accessible from all radio contexts of the CLI.

```
n_addba_support
no n_addba_support
```

Parameters

None

Example

The following example enables the ADDBA support:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio2# n_addba_support
```

n_aggr_mpdu

Use the `n_aggr_mpdu` command to enable the use of aggregate MPDUs. Use the `no` command to disable this feature. The `n_aggr_mpdu` command is accessible from all radio contexts of the CLI.

```
n_aggr_mpdu
no n_aggr_mpdu
```

Parameters

None

Example

The following example disables MPDU:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio2# no n_aggr_mpdu
```

n_aggr_mpdu_max

Use the `n_aggr_mpdu_max` command to specify the maximum length of the aggregate MPDU. The `n_aggr_mpdu_max` is accessible from all radio contexts of the CLI.

n_aggr_mpdu_max *value*

Parameters

<i>value</i>	The maximum size in bytes for an aggregate MPDU. The range of values allowed is 1024 to 65535. When the radio mode is anac or ac-strict, the range of values allowed is 1024 to 1048575.
--------------	--

Example

The following example sets the maximum length of the aggregate MPDU to 5000 bytes:

```
EWC.extremenetworks.com:ap:defaults:ap3801:radio2# n_aggr_mpdu_max 5000
```

n_aggr_mpdu_max_subframes

Use the `n_aggr_mpdu_max_subframes` command to specify the maximum number of subframes that may be contained in an aggregate MPDU. The `n_aggr_mpdu_max_subframes` command is accessible from all radio contexts of the CLI.

n_aggr_mpdu_max_subframes *2-64*

Parameters

<i>2-64</i>	The maximum number of subframes allowed in an aggregate MPDU. The range of values is from 2 to 64.
-------------	--

Example

The following example sets the maximum number of subframes to 50:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio2# n_aggr_mpdu_max_subframes
50
```

n_aggr_msdu

Use the `n_aggr_msdu` command to enable the use of aggregate MSDUs. Use the `no` command to disable the use of aggregate MSDUs. The `n_aggr_msdu` command is accessible from all radio contexts of the CLI.

n_aggr_msdu
no n_aggr_msdu

Parameters

None

Example

The following example disables the aggregate MSDU:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio2# no n_aggr_msdu
```

n_chlwidth

Use the `n_chlwidth` command to specify the 11n or 11ac channel width – 20 MHz, 40 MHz, 80 MHz, or Auto. This command is accessible from all radio contexts of the CLI.

n_chlwidth (20 | 40 | 80 | auto)

Parameters

20	Specifies the channel width as 20 MHz
40	Specifies the channel width as 40 MHz
80	Specifies the channel width as 80 MHz (802.11ac radios only)
auto	Specifies that the AP automatically selects the channel width depending upon how busy the extension channel is. The extension channel threshold is set via the <code>n_pbthreshold</code> command.

Example

The following example sets the channel width to 40 MHz:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio2# n_chlwidth 40
```

n_guardinterval

Use the `n_guardinterval` command to specify the guard interval – short or long. The `n_guardinterval` command is accessible from all radio contexts of the CLI.

n_guardinterval short | long

Parameters

short	Specifies a short guard interval
long	Specifies a short guard interval

Example

The following example sets the long guard interval:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio2# n_guardinterval long
```

n_pbthreshold

Use the `n_pbthreshold` command to specify the extension channel threshold. This value is used to determine which channel width to use when the `n_chlwidth` is set to `auto`.

n_pbthreshold 0-100

Parameters

0-100	Specifies the extension channel threshold value as a percentage.
-------	--

Usage

This command is not available for AP38xx radio 1 and AP39xx both radios.

Example

The following example sets the extension channel threshold value to 60 per cent:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio2# n_pbthreshold 60
```

n_pmode

Use the `n_pmode` command to enable the protection on the primary channel. The `n_pmode` command is accessible from all radio contexts of the CLI.

n_pmode none | always | auto

Parameters

none	Specifies that <code>n_pmode</code> is not enabled.
always	Specifies that <code>n_pmode</code> is always enabled.
auto	Specifies that the <code>n_pmode</code> is auto selected.

Example

The following example enables the protection mode with the `always` option:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio2# n_pmode always
```

n_ptype

Use the `n_ptype` command to specify the 40 MHz protection type – whether CTS, RTS or none. The `n_ptype` command is accessible from all radio contexts of the CLI.

n_ptype { cts only | rts cts }

Parameters

cts only	Specifies Clear to Send (CTS) protection type.
rts cts	Specifies Receive to Send (RTS) / Clear to Send (CTS) protection type.

Example

The following example sets the clear to send (CTS) protection type:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio2# n_ptype cts only
```

nonUnicastQuota

Use the `nonUnicastQuota` command to specify the maximum percentage of time that the AP transmits non-unicast packets (broadcast and multicast traffic) for each configured Beacon period. For each non-unicast packet transmitted, the system calculates the airtime used by each packet and drops all packets that exceed the maximum percentage. By restricting non-unicast traffic, you limit the impact of broadcasts and multicasts on overall system performance. The `nonUnicastQuota` command is accessible from all `ap: radio` contexts of the CLI.

nonUnicastQuota *value*

Parameters

value	Specifies the maximum non-unicast traffic percentage allowed. Valid values are 10-100.
--------------	--

Example

The following example sets the maximum non-unicast traffic percentage to 50%:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio2# nonUnicastQuota 50
```

optimized-mcast

Use the `optimized-mcast` command to enable or disable the optimized-multicast feature. The `optimized-mcast` command is accessible from all `radio` contexts of the CLI.

optimized-mcast **enable** | **disable**

Parameters

enable	Enables the optimized multicast feature on this radio.
disable	Disables the optimized multicast feature on this radio

Example

The following example enables optimized multicast on radio1:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio1# optimized-mcast enable
```

pmode

Use the `pmode` command to configure the Protection Mode, which will protect 802.11g client transmissions from interruption by 802.11b clients. The `pmode` command is accessible from all `ap: radio2` contexts of the CLI.

Use `none` only if the Wireless AP will NOT be servicing 802.11b clients, and there are no 802.11b clients or Wireless APs sharing the same air space.

`pmode (none | auto | always)`

Parameters

none	Deactivates Protection Mode
auto	Indicates that Protection Mode will be used only when 802.11b clients or Wireless APs are detected
always	Indicates that Protection Mode will remain active at all times

Example

The following example configures the Wireless AP to use Protection Mode at all times:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio2# pmode always
```

prate

Use the `prate` command to adjust the Protection Rate. The `prate` command is accessible from all `ap: radio2` contexts of the CLI when radio mode includes 'g' (e.g. g, b/g, b/g/n, or n-strict).

`prate (1 | 2 | 5.5 | 11)`

Parameters

1 2 5.5 11	Specifies the Protection Rate in Mbps
-------------------------	---------------------------------------

Example

The following example adjusts the Protection Rate to 5.5 Mbps:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio2# prate 5.5
```

preamble

Use the `preamble` command to set the preamble type. The `preamble` command is accessible from all `ap: radio2` contexts of the CLI when the mode includes 'b' (for example, b/g/n).

`preamble (short | long)`

Parameters

short	Specifies short preambles
long	Specifies long preambles

Example

The following example enables the long option for the preamble type:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio2# preamble long
```

probe-suppression

Use the `probe-suppression` command to enable or disable probe suppression on an AP radio. You can also optionally set the RSS threshold and enable or disable force disassociate. The `probe-suppression` command is accessible from all radio contexts of the CLI.

probe-suppression **disable** | **enable**

Parameters

disable enable	Enables or disables probe suppression for this radio context.
--------------------------------	---

Usage

Probe-suppression is useful in dense deployments (such as stadiums) where a large number of APs may be operating in close proximity. It permits the administrator to configure smaller cells. Thus clients only attempt to associate with the AP that is closest and has the strongest signal. This removes much of the overhead, permitting better performance of the network.

Example

The following example enables probe suppression on radio 1 of AP 111111111113705:

```
EWC.extremenetworks.com:ap:111111111113705:radio1# probe-suppression enable
```

ptype

Use the `ptype` command to select the Protection Type. The `ptype` command is accessible from all `ap:radio2` contexts of the CLI.

ptype (**cts only** | **rts cts**)

Parameters

cts only	Specifies the Clear to Send (CTS) type.
rts cts	Specifies the Request to Send (RTS) and Clear to Send (CTS) types

Example

The following example sets the protection type to CTS:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio2# ptype cts only
```

rss-threshold

Use the `rss-threshold` command to set the RSS threshold on an AP radio. The `rss-threshold` command is accessible from all radio contexts of the CLI when probe-suppression is enabled.

rss-threshold *dBm*

Parameters

<i>dBm</i>	Specifies the RSS-threshold in dBm.Defaults to -90 if probe suppression is enabled. Supported values are -50 to -100 dBm.
------------	---

Usage

Probe-suppression is useful in dense deployments (such as stadiums) where a large number of APs may be operating in close proximity. It permits the administrator to configure smaller cells. Thus clients only attempt to associate with the AP that is closest and has the strongest signal. This removes much of the overhead, permitting better performance of the network.

Configuring `rss-threshold` allows the administrator to control the size of the cells. A higher `rss-threshold` equates to a smaller cell size. A lower `rss-threshold` equates to a larger cell size.

Example

The following example sets the RSS threshold on radio 1 of AP 111111111113705 to -80 dBm:

```
EWC.extremenetworks.com:ap:111111111113705:radio1# rss-threshold -80
```

rts

Use the `rts` command to specify the size of the Request to Send (RTS) threshold. The `rts` command is accessible from all radio contexts of the CLI.

rts value

Parameters

value	Specifies the Request to Send packet size threshold. The value for the <code>rts</code> value is 256 to 2346.
--------------	---

Example

The following example sets the RTS packet size to 256:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio2# rts 256
```

stbc

Use the `stbc` command to enable or disable the 11n advanced STBC feature. The `stbc` command is accessible from all radio contexts of the CLI.

stbc enable | disable

Parameters

enable	Enables the 11n advanced STBC feature.
disable	Disables the 11n advanced STBC feature

Usage

- `n` must be enabled in radio mode.
- When STBC is enabled, antenna selection must be left-middle-right.

Example

The following example enables STBC on radio1:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio1# stbc enable
```

tx_adjust_power

Use the `tx_adjust_power` command to specify an offset to the Tx power level, which is used to adjust the ATPC power levels from the calculated value. The `tx_adjust_power` command is accessible from most `ap:defaults:ap_type:radioX` contexts of the CLI.

tx_adjust_power *value*

Parameters

<i>value</i>	Specifies the value in dB.
--------------	----------------------------

Example

The following example sets the Tx power adjust level to 0 dB:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio1# tx_adjust_power 0
```

txbf

Use the `txbf` command to enable or disable the 11n advanced TXBF feature. The `txbf` command is accessible from the `ap:defaults:` context and the `ap:<serial>` radio contexts for the following AP models:

- ap37xx
- ap38xx (radio 2)
- ap3801
- ap3935 (FCC and ROW, radio 1)
- ap3965 (FCC and ROW, radio 1)

The available parameters depend on the AP type and the radio.

txbf enable | **disable** or **txbf mu_mimo enable** | **disable** for AP3935 and AP3965 on Radio 1.

Usage

When TXBF is enabled, antenna selection must be left-middle-right.

Parameters

enable	Enables the 11n advanced TXBF feature.
disable	Disables the 11n advanced TXBF feature
mu_mimo	Sets TxBF to MU-MIMO.

Example

The following example enables TXBF on radio1:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio1# txbf enable
```

tx_max_power

Use the `tx_max_power` command to set the maximum Tx power level. The `tx_max_power` command is accessible from all ap: radio contexts of the CLI.

tx_max_power *value*

Parameters

<i>value</i>	Specifies the maximum Tx power level.
--------------	---------------------------------------

Example

The following example sets the maximum Tx power level to 18 dBm:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio2#tx_max_power 18
```

tx_min_power

Use the `tx_min_power` command to specify the minimum Tx power level. The `tx_min_power` command is accessible from all radio contexts of the CLI. The `tx_min_power` is available only when Auto Tx Power Ctrl (ATPC) is enabled.

tx_min_power *value*

Parameters

<i>value</i>	Specifies the value in dBm.
--------------	-----------------------------

Example

The following example specifies the minimum Tx power level to 8 dBm:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio1# tx_min_power 8
```

DCS Commands

The commands in this section are common to radio1 and radio2 dcs commands in various contexts. For example, navigate to the dcs context from the ap context as follows:

```
ap <serial> radio1 dcs
```

The following commands are variously available in the radio1 and radio2 dcs contexts:

- [channel_plan](#) on page 159
- [interference-event-type](#) on page 160
- [interference-wait-time](#) on page 160
- [mode](#) on page 160

- [noise_threshold](#) on page 161
- [occupancy_threshold](#) on page 161
- [radio_channels](#) on page 161
- [update_period](#) on page 162

Commands entered in the dcs context do not need to be followed by "apply" in order for them to take effect.

channel_plan

Use the `channel_plan` command to customize the channel plan for the Wireless AP's Radio 1. The `channel_plan` command is accessible from all radio dcs contexts of the CLI.

The parameters available in the `channel_plan` command are determined by the setting of the `mode` command in the same radio context.

Syntax: `<ap_type> and <serial> radio1`

channel_plan all-non-dfs | all | channel[, channel]

Parameters

all-non-dfs	Radio 1 uses all non-DFS channels.
all	Radio 1 uses all channels
channel[, channel]	Radio 1 uses the channels that are listed, separated by commas.

Syntax: `(<ap_type> and <serial> radio2)`

channel_plan auto | 3-channel | 4-channel | channel[, channel]

Parameters

auto	Radio 2 uses 3 channels for countries supporting 11 channels and 4 channels for countries supporting 13 channels.
3-channel	Radio 2 uses 3 channels.
4-channel	Radio 2 uses 4 channels.
channel [,channel]	Radio 2 uses the channels that are listed, separated by commas.

Examples

The following example shows the channel plan for Radio 1 is configured to include all non-DFS channels:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio1:dcs# channel_plan all-non-dfs
```

The following example shows that the channel plan for radio 1 is customized to include channels 1, 2 and 3:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio2:dcs# channel_plan 1, 2, 3
```

interference-event-type

This command is only available on radio 2. Event types must be values from a bluetooth, microwave, cordless phone, constant wave, and/or video bridge.

interference-event-type (**none** | *type1* [, *type2*])

Parameters

none	Set the event type to none.
<i>type1</i> [, <i>type2</i>]	Specifies one or more event types from bluetooth, microwave, cordless phone, constant wave, and/or video bridge sources.

The following example sets the interference event type to none:

```
C5110-NAM.10.100.3.1:ap:defaults:ap37xx:radio2:dcs# interference-event-type none
```

interference-wait-time

The interference wait time must be an integer between 10 and 120 seconds. This command is available on radio 2.

interference-wait-time *10-120*

Parameters

<i>10-120</i>	Specifies the interference wait time interval.
---------------	--

The following example sets the interference wait time to 10 seconds:

```
C5110-NAM.10.100.3.1:ap:defaults:ap37xx:radio2:dcs# interference-wait-time 10
```

mode

Use the `mode` command to set the DCS mode. The `mode` command is accessible from all `ap: radio dcs` contexts of the CLI.

In monitor mode, DCS generates an alarm, but does not change the channel, even if the noise and interference levels on the current channel exceed their thresholds. In active mode, generates an alarm and changes the channel if the noise and interference levels on the current channel exceed their thresholds.

mode **monitor** | **active**

Parameters

monitor	Monitors the noise and interference on the current channel
active	Enables DCS

Example

The following example sets DCS to active mode:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio1:dcs# mode active
```

noise_threshold

Use the `noise_threshold` command to set the DCS noise threshold. The `noise_threshold` command is accessible from all radio dcs contexts of the CLI.

noise_threshold *threshold*

Parameters

<i>threshold</i>	Specifies the DCS noise threshold in dB. The DCS noise threshold must be in the -95 to -50 range. ACS will scan for a new operating channel for the Wireless AP if the threshold is exceeded.
------------------	---

Example

The following example sets the noise threshold to -50 dB:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio1:dcs# noise_threshold -50
```

occupancy_threshold

Use the `occupancy_threshold` command to set the DCS Channel Occupancy Threshold. The `occupancy_threshold` command is accessible from all radio dcs contexts of the CLI.

occupancy_threshold *threshold*

Parameters

<i>threshold</i>	Specifies the DCS Occupancy Threshold as a percentage. The DCS Occupancy Threshold must be in the 10 to 100 range.
------------------	--

Example

The following example sets the DCS Channel Occupancy Threshold to 10 per cent:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio1:dcs# occupancy_threshold 10
```

radio_channels

Use the `radio_channels` command to display the list of available radio channels for auto channel selection (ACS). The `radio_channels` command is accessible from all dcs contexts of the CLI.

radio_channels

Parameters

None

Examples

```
EWC.extremenetworks.com:ap:defaults:3935FCC:radio2:dcs# radio_channels
```

```
Available radio channels:
```

```
1: 2412 MHz
2: 2417 MHz
3: 2422 MHz
4: 2427 MHz
5: 2432 MHz
6: 2437 MHz
7: 2442 MHz
8: 2447 MHz
9: 2452 MHz
10: 2457 MHz
11: 2462 MHz
```

```
EWC.extremenetworks.com:ap:defaults:3935FCC:radio1:dcs# radio_channels
```

```
Available radio channels:
```

```
36: 5180 MHz
40: 5200 MHz
44: 5220 MHz
48: 5240 MHz
52: 5260 MHz
56: 5280 MHz
60: 5300 MHz
64: 5320 MHz
100: 5500 MHz
104: 5520 MHz
108: 5540 MHz
112: 5560 MHz
116: 5580 MHz
120: 5600 MHz
124: 5620 MHz
128: 5640 MHz
132: 5660 MHz
136: 5680 MHz
140: 5700 MHz
149: 5745 MHz
153: 5765 MHz
157: 5785 MHz
161: 5805 MHz
165: 5825 MHz
```

update_period

Use the `update_period` command to set the DCS update period, during which the Wireless AP averages the DCS noise threshold and DCS channel occupancy threshold measurements. If either one of these thresholds is exceeded, the Wireless AP triggers ACS. The `update_period` command is accessible from all radio dcs contexts of the CLI.

```
update_period period
```

Parameters

<i>period</i>	Specifies the time period, measured in minutes, during which the Wireless AP averages the DCS noise threshold and DCS channel occupancy threshold measurements. If either one of these thresholds is exceeded, then the Wireless AP triggers ACS. Range is 1 to 15 minutes, or 0 to disable.
---------------	--

Example

The following example sets the DCS update period to 12 minutes:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio1:dcs# update_period 12
```

The following example disables the DCS update period:

```
EWC.extremenetworks.com:ap:defaults:ap37xx:radio1:dcs# update_period 0
```

logs

The following commands are at the highest (first) level of the logs context:

- [aplist](#) on page 163
- [collection](#) on page 164
- [destination](#) on page 209
- [frequency](#) on page 164

aplist

Use the `aplist` command to add or remove APs to and from the logs collection list.

After you run the `aplist` command, run the `apply` command to implement the change.

```
aplist [(add|delete)] serial[, serial]*
```

Parameters

add delete	Add or delete the (following) APs from the logs collection list. If you omit these options, by default all APs in the scan profile are replaced with the APs listed in this command.
<i>serial[, serial]*</i>	Specifies the Wireless AP by their serial numbers that are to be added to the log collection list. They can be added or deleted individually, or listed as a comma and space separated list.

Usage

Use the add or delete option add or remove APs to/from the logs collection list. You can replace the APs listed in the collection list by omitting the add or delete option, and listing the APs you want.

Example

The following example adds a Wireless AP with a serial number:

```
EWC.extremenetworks.com:ap:logs# aplist [(add|delete)] <serial[ serial]*>
```

collection

Use the `collection` command to enable/disable an AP log collection.

After you run the `collection` command, run the `apply` command to implement the change.

collection [(enable|disable)]

Parameters

enable disable	Enable/disable AP log collection.
-------------------------	-----------------------------------

Usage

Use the `enable` or `disable` option to enable or disable log collection.

Example

The following example enables/disables an AP log collection:

```
EWC.extremenetworks.comap:logs# collection enable|disable
```

destination

Use the `destination` command to set the AP log destination.

destination (local | flash | remote)

Parameters

local	Save the log file on a local drive
flash	Save the log file on a flash drive
remote	Upload the log file onto a remote server

Examples

```
EWC.extremenetworks.com:ap:logs# destination local
```

frequency

Use the `frequency` command to configure collection frequency per day.

frequency (1|2|4|6)

Parameters

1	Configures log collection once per day.
2	Configures log collection twice per day.
4	Configures log collection four times per day.
6	Configures log collection six times per day.

Example

```
EWC.extremenetworks.com:ap:logs# frequency 1
```

maintain_cycle

The following commands are at the highest (first) level of the AP Maintain context. The Maintain Cycle context makes use of several common commands as well.

- [duration](#) on page 165
- [freq](#) on page 166
- [platform](#) on page 165
- [show](#) on page 24
- [starttime](#) on page 211

duration

Use the `duration` command to configure maintenance cycle duration in hours.

After you run the `duration` command, run the `apply` command to implement the change.

duration [1-6]

Parameters

1-6	Number of hours for the maintenance cycle.
-----	--

Usage

Use the `duration` command to configure the duration of the maintenance cycle.

Example

The following example specifies the duration of the maintenance cycle:

```
EWC.extremenetworks.com:maintain_cycle# duration 1
```

platform

Use the `platform` command to specify the platform where the maintenance cycle is run.

After you run the `platform` command, run the `apply` command to implement the change.

platform [no | <platform> [, <platform> , . . . , <platform>]]

Parameters

no	Removes all configured platforms.
platforms	Identifies one or more platforms to be maintained.

Usage

Use the platform command to specify the platform for the maintenance cycle.

Supported platforms: AP3705, AP3710, AP3715, AP3765, AP3767, AP3801, AP3805, AP3825, AP3865, AP3935, AP3965, APVMAP, W78XC, W78XCSFP



Note

The platform list may vary on controllers with different regulation license.

Example

The following example specifies the platform of the maintenance cycle:

```
EWC.extremenetworks.com: maintain_cycle# platform AP3935
```

The following example adds three platforms:

```
EWC.extremenetworks.com:maintain_cycle# platform AP3767,AP3801,AP3805
EWC.extremenetworks.com:maintain_cycle# show
Frequency: daily weekend
Platform: AP3767,AP3801,AP3805
Start Time: 00:00
Duration: 3
```

The following example removes all configured platforms:

```
EWC.extremenetworks.com:maintain_cycle# platform no
EWC.extremenetworks.com:maintain_cycle# show
Frequency: daily weekend
Platform:Start Time: 00:00
Duration: 3
```

freq

Use the `freq` command to configure maintenance cycle frequency.

```
freq ((daily everyday|weekday|weekend) | (weekly
<Sunday,Monday,Tuesday,Wednesday,Thursday,Friday,Saturday>) | (monthly week of
month, (Sunday|Monday|Tuesday|Wednesday|Thursday|Friday|Saturday)) | never)
```

Parameters

daily	Specify a value to run the daily maintenance. Possible values for daily are: everyday, weekday, weekend.
weekly	Specify a day of the week to run the weekly maintenance.
monthly <i>week of month</i>	Specify a week to run the monthly maintenance and the day of the week to start the cycle. <hr/> Numeric value to represent the week of a month. Valid values are 1-4. For example, maintain_cycle# freq monthly 1,Tuesday
never	Do not run the maintenance cycle.

Example

The following example configures the maintenance cycle to run weekly on Sunday.

```
EWC.extremenetworks.com::maintain_cycle# freq weekly sunday
```

The following example configures the maintenance cycle to run on the first week of the month, starting on Tuesday.

```
EWC.extremenetworks.com::maintain_cycle# # freq monthly 1,Tuesday
```

6 I2ports Commands

```
esaN
jumbo-frames
portN
show
<named-LAG-port>
```

This section describes commands to enable and disable ports on the Wireless Appliance. These commands are located in the I2ports context of the CLI. L2 port configuration is performed within a named topology context. See [I2](#) on page 391 for L2 port configuration information.

All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the I2ports context:

- [esaN](#) on page 168
- [jumbo-frames](#) on page 168
- [portN](#) on page 169
- [show](#) on page 170
- [<named-LAG-port>](#) on page 170 — See for commands in the I2ports:<named-LAG-port> context.

esaN

The `esaN` command moves you into the context I2ports:esaN (where variable N refers to the physical data port number). This context contains the port command which enables or disables ports. This command is available on the following controllers: C25, V2110, C5110 and C5210. See [port](#) on page 169 for information on enabling and disabling a port in this context.

jumbo-frames

Use the `jumbo-frames` command to enable or disable jumbo frames on all Layer 2 ports on the controller. The jumbo frames feature allows for frames greater than 1500 bytes (maximum MTU frame size).

```
jumbo-frames enable | disable
```

Parameters

enable	Enables jumbo frames on all controller Layer 2 ports.
disable	Disables jumbo frames on all controller Layer 2 ports.

Usage

The standard Ethernet frame MTU for untagged packets is 1518 bytes including the 18 Ethernet header bytes. The standard Ethernet frame MTU for tagged packets is 1522 bytes.

Enabling jumbo frame support, the maximum frame size is 1818 bytes, including 18 Ethernet header bytes for untagged packets and 1822 bytes, including 22 Ethernet header bytes for tagged packets.

Jumbo frame size between the standard frame MTU and the jumbo frame size is not administratively configurable and is hard set to the stated values.

Example

The following example enables jumbo frame support for the l2ports# context:

```
EWC.extremenetworks.com# l2ports
EWC.extremenetworks.com:l2ports# jumbo-frames enable
EWC.extremenetworks.com:l2ports#
```

portN

The `portN` command moves you into the context l2ports:portN (where variable N refers to the physical data port number). This context contains the port command which enables or disables ports. This command is available on the C4110 platform. See [port](#) on page 169 for information on enabling and disabling a port in this context.

port

Use the `port` command to enable or disable the port from within the appropriate port context for your platform:

- l2ports:esaN# is available on the C25, V2110, C5110 and C5210 controllers. See [esaN](#) on page 168.
- l2ports:portN# is available on the C4110 controller. See [portN](#) on page 169.

port enable | disable

Parameters

enable	Enables the port for this context.
disable	Disables the port for this context.

Examples

The following example enables the ESA1 port in an l2ports:esa1# context:

```
EWC.extremenetworks.com# l2ports
EWC.extremenetworks.com:l2ports# esa1
EWC.extremenetworks.com:l2ports:esa1# port enable
EWC.extremenetworks.com:l2ports:esa1# apply
EWC.extremenetworks.com:l2ports:esa1# show
Port: enable
EWC.extremenetworks.com:l2ports:esa1#
```

show

Use the `show` command in the I2ports context to display port information for the Wireless Appliance.

show

Parameters

None

Examples

The following example displays port information for the Wireless Appliance:

```
EWC.extremenetworks.com# l2ports
EWC.extremenetworks.com:l2ports# show
Status   Enable  Port   MAC                Untagged Vlan  Tagged Vlan
UP       enable  esa0   00:21:9B:98:B7:07  30              4,5,3,7,8,211
UP       enable  esa1   00:1B:21:40:58:D0  4093
UP       enable  esa2   00:1B:21:3B:EF:02  4089
DOWN    enable  lag1   00:1B:21:40:58:D0  30              4,5,3,7,8,211
UP       enable  admin  00:21:9B:98:B7:05
```

The VLAN Service field specifies the VLAN IDs set on bridged at controller topologies for the specific physical port (in this case esa0).

<named-LAG-port>

The `<named-LAG-port>` command, where `<named-LAG-port>` is the name of a given link aggregation (LAG) port, moves you into the `I2ports:<named-LAG-port>` context, which contains commands to configure the settings of the specified individual LAG port.

The following commands are available in the `I2ports:<named-LAG-port>` context.

- [lag-member](#) on page 170
- [port](#) on page 171

lag-member

Use the `lag-member` command to attach or detach an L2 port to or from the link aggregation. The `lag-member` command is accessible from the `I2ports:<named-LAG-port>` context.

lag-member add | delete *L2 port name*

Parameters

add	Attaches the specified port to the link aggregation.
delete	Detaches the specified port from the link aggregation.
<i>L2 port name</i>	Specifies the layer 2 port being added or deleted.

Examples

The following example attaches the esal port in an l2ports:lag1# context:

```

EWC.extremenetworks.com# l2ports
EWC.extremenetworks.com:l2ports# lag1
EWC.extremenetworks.com:l2ports:lag1# lag-member add esal
EWC.extremenetworks.com:l2ports:lag1# apply
EWC.extremenetworks.com:l2ports:lag1# show
LAG members: esal
EWC.extremenetworks.com:l2ports:lag1#

```

port

Use the `port` command to enable or disable the port administration status of the layer 2 port in this context. The `port` command is accessible from the l2ports:<named-LAG-port> context.

port enable | disable

Parameters

enable	Enables the administration status for the port for this context.
disable	Disables the administration status for the port for this context.

Examples

The following example enables the administration status of lag-member ports in an l2ports:lag1# context:

```

EWC.extremenetworks.com# l2ports
EWC.extremenetworks.com:l2ports# lag1
EWC.extremenetworks.com:l2ports:lag1# port enable
EWC.extremenetworks.com:l2ports:lag1# apply
EWC.extremenetworks.com:l2ports:lag1# show
Admin: enable
EWC.extremenetworks.com:l2ports:lag1#

```

7 ip Commands

route ospf

This section describes the commands with options to configure routing information. These options can be found within the ip context of the CLI.

All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the ip context:

- [route](#) on page 172
- [ospf](#) on page 173 — See for commands in the ip:ospf context.

route

Use the `route` command to add routing information. Use the `no` forms of the command to disable the information.

Use `show routes` to display the routing table. For more information, see [show routes](#) on page 74.

```
route IP Address /netmask gateway [ float | nofloat ]  
route IP Address netmask gateway [ float | nofloat ]  
route default gateway [ float | nofloat ]  
no route IP Address  
no route default  
no route routeId
```

Parameters

<i>IP Address</i>	Specifies the destination IP address
<i>netmask</i>	Specifies the subnet mask
<i>/netmask</i>	Specifies the subnet mask in CIDR format
<i>gateway</i>	Specifies the gateway
float	Does not override Open Shortest Path First (OSPF) learned route
nofloat	Overrides OSPF learned route
<i>routeId</i>	Specifies index number of route on the routing table

Examples

The following example adds an IP address to the routing table, specifying the netmask in CIDR format and disallowing OSPF overrides:

```
EWC.extremenetworks.com:ip# route 1.1.2.1/24 10.7.0.3 nofloat
```

The following example adds an IP address to the routing table, specifying the netmask as an IP address and allowing OSPF overrides:

```
EWC.extremenetworks.com:ip# route 1.1.2.1 255.255.255.0 10.7.0.3 float
```

The following example configures the default route:

```
EWC.extremenetworks.com:ip# route default 10.7.0.3
```

The following example removes an IP address from the routing table:

```
EWC.extremenetworks.com:ip# no route 1.1.2.1
```

The following example removes the default route from the routing table:

```
EWC.extremenetworks.com:ip# no route default
```

The following example removes an IP address from the routing table by its index number:

```
EWC.extremenetworks.com:ip# no route 12
```

ospf

The `ospf` command is associated with the context `ip:ospf`, which contains commands to configure global settings for the Open Shortest Path First (OSPF) protocol on a network.

The following commands are available in the `ip:ospf` context.

- [area](#) on page 173
- [areatype](#) on page 174
- [routerid](#) on page 174
- [status](#) on page 174
- [ospfinterface](#) on page 175 — See for commands in the `ip:ospf:ospfinterface` context. If `ospfinterface` does not appear in the `ip:ospf` context command list, use the `status` command to enable OSPF.

area

Use the `area` command to define the area identification of the OSPF interface.

```
area area_id
```

Parameters

<code>area_id</code>	Specifies an integer or an IP address defining the OSPF area
----------------------	--

Examples

The following example sets the OSPF area to Area 0:

```
EWC.extremenetworks.com:ip:ospf# area 0.0.0.0
```

areatype

Use the `areatype` command to select the type of Open Shortest Path First (OSPF) protocol area to be used on the Wireless Appliance.

areatype (**default** | **stub** | **nssa**)

Parameters

default	Selects the Normal OSPF area
stub	Selects the Stub area
nssa	Selects the “Not So Stubby” area

Examples

The following example sets the OSPF area type to a Stub area:

```
EWC.extremenetworks.com:ip:ospf# areatype stub
```

routerid

Use the `routerid` command to identify the IP address of the router originating Open Shortest Path First (OSPF) packets.

routerid *IP Address*

Parameters

<i>IP Address</i>	Specifies the IP address of the router originating OSPF packets
-------------------	---

Examples

The following example sets the routerid to 1.1.1.1:

```
EWC.extremenetworks.com:ip:ospf# routerid 1.1.1.1
```

status

Use the `status` command to enable or disable the Open Shortest Path First (OSPF) protocol on the Wireless Appliance.

status (**enable** | **disable**)

Parameters

enable	Indicates that the OSPF will be enabled
disable	Indicates that the OSPF will be disabled

Examples

The following example enables OSPF on the Wireless Appliance

```
EWC.extremenetworks.com:ip:ospf# status enable
```

ospfinterface

The `ospfinterface` command moves you to the context `ip:ospf:ospfinterface`, which contains commands to configure Open Shortest Path First (OSPF) protocol options for a port of the Wireless Appliance. The `ospfinterface` command supports the specifying of an `esaN` interface, where `N` is a number from 0 - 3.

The `ospfinterface` command is accessible from within the `ip:ospf` context. If the `ospfinterface` command does not appear on the `ip:ospf` context command list, you must use the `status` command to enable OSPF.

The following commands are available in the `ip:ospf:ospfinterface` context.

- [add-ospf-interface](#) on page 175
- [delete-ospf-interface](#) on page 175

add-ospf-interface

Use the `add-ospf-interface` command to create a `<named-ospfinterface>`. The `add-ospf-interface` command is available from the `ip:ospf:ospfinterface` context of the CLI.

The `add-ospf-interface` command is available to the physical topology and the `b@ac` topology with the layer 3 interface configured. The `ospf` interface name must be created as a physical or `b@ac` topology in the topology context before you execute this command.

```
add-ospf-interface ospf interface name
```

Parameters

<i>ospf interface name</i>	Specifies the name for the new ospf interface. The name must already be created as a physical or b@ac topology in the topology context.
----------------------------	---

Examples

The following adds an `ospfinterface` with the name `top1`:

```
EWC.extremenetworks.com:ip:ospf:ospfinterface# add-ospf-interface top1
```

delete-ospf-interface

Use the `delete-ospf-interface` command to delete an OSPF interface object. The `delete` command is accessible from the `ospfinterface` context of the CLI.

delete-ospf-interface *ospf interface name*

Parameters

<i>ospf interface name</i>	Specifies the name of the OSPF interface to delete. The name must already be created as a physical or b@ac topology in the topology context.
----------------------------	--

Examples

The following deletes an ospfinterface with the name you specify:

```
EWC.extremenetworks.com:ip:ospf:ospfinterface# delete-ospf-interface top1
```

<named-ospfinterface>

The <named-ospfinterface> command, where <named-ospfinterface> refers to the name of a given ospfinterface, moves you into the ospfinterface:<named-ospfinterface> context, which contains commands to configure the settings of the specified individual ospfinterface.

The following commands are available in the ip:ospf:ospfinterface:<named-ospfinterface> context.

- [authkey](#) on page 176
- [authtype](#) on page 177
- [deadinterval](#) on page 177
- [hellointerval](#) on page 177
- [linkcost](#) on page 177
- [retransmitinterval](#) on page 178
- [status](#) on page 178
- [transmitdelay](#) on page 178

authkey

Use the `authkey` command to set the password used for authentication. Use the `no` form of the command to clear the password.

Authentication must be configured to use a password before this command can be used. For more information, see [authtype](#) on page 177.

```
authkey password
no authkey
```

Parameters

<i>password</i>	Specifies the password used for authentication
-----------------	--

Examples

The following example sets an authentication password:

```
EWC.extremenetworks.com:ip:ospf:ospfinterface:top1# authkey hello123
```


authype

Use the `authype` command to indicate whether the authentication will require a password or not.

authype (**none** | **password**)

Parameters

none	Indicates that no password is required
password	Indicates that authentication will require a password

Examples

The following example configures authentication to require a password:

```
EWC.extremenetworks.com:ip:ospf:ospfinterface:top1# authype password
```

deadinterval

Use the `deadinterval` command to set the amount of time the OSPF protocol will wait for a response before assuming peer devices are unreachable.

deadinterval 1-65535

Parameters

1-65535	Specifies the time interval (in seconds) the OSPF protocol will wait for a response
---------	---

Examples

The following example sets the time to wait for a packet response to 300 seconds:

```
EWC.extremenetworks.com:ip:ospf:ospfinterface:top1# deadinterval 300
```

hellointerval

Use the `hellointerval` command to specify the time interval between the transmission of OSPF Hello packets to devices on the network.

hellointerval 1-65535

Parameters

1-65535	Specifies a time interval in seconds
---------	--------------------------------------

Examples

The following example sets the time interval between outgoing packets to 10 seconds:

```
EWC.extremenetworks.com:ip:ospf:ospfinterface:top1# hellointerval 10
```

linkcost

Use the `linkcost` command to assign a Link Cost to the port.

linkcost 1-65535

Parameters

<code>1-65535</code>	Specifies a numerical value
----------------------	-----------------------------

Examples

The following example sets the Link Cost of the port to 10:

```
EWC.extremenetworks.com:ip:ospf:ospfinterface:top1# linkcost 10
```

retransmitinterval

Use the `retransmitinterval` command to set the amount of time the port waits before it attempts to retransmit outgoing packets

```
retransmitinterval 1-65535
```

Parameters

<code>1-65535</code>	Specifies the time interval in seconds
----------------------	--

Examples

The following example sets the retransmission time interval to five seconds:

```
EWC.extremenetworks.com:ip:ospf:ospfinterface:top1# retransmitinterval 5
```

status

Use the `status` command to enable or disable OSPF advertising on the port.

```
status ( enable | disable )
```

Parameters

enable	Indicates that OSPF advertising will be enabled
disable	Indicates that OSPF advertising will be disabled

Examples

The following example enables OSPF advertising on the port:

```
EWC.extremenetworks.com:ip:ospf:ospfinterface:top1# status enable
```

transmitdelay

Use the `transmitdelay` command to set the delay time before initiating transmission.

```
transmitdelay 1-65535
```

Parameters

<code>1-65535</code>	Specifies the amount of time in seconds
----------------------	---

Examples

The following example sets the delay time for transmission to one second:

```
EWC.extremenetworks.com:ip:ospf:ospfinterface:top1# transmitdelay 1
```

8 login Commands

apply
auth
auth-order
move
show

The `login` command refers to login context, which contains commands to configure the login authentication modes. The `login` command is accessible from the root context of the CLI.

All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The Wireless Appliance offers four login authentication options:

- Local authentication
- RADIUS-based authentication
- Local authentication first, then RADIUS-based authentication
- RADIUS-based authentication first, then local authentication

Local authentication is enabled by default. If the administrator chooses to use the RADIUS-based login, all password policy enforcement is delegated to the RADIUS server, and the account management features on the CLI are disabled.

You must test the RADIUS server configuration before configuring a user profile (User ID and Password), and submitting it to the RADIUS server.

After you have switched to RADIUS-based login, you must use the RADIUS credentials to log on the Wireless Appliance.

The following commands are available in the login context.

- [apply](#) on page 180
- [auth](#) on page 181 — See for commands in the login:auth context.
- [auth-order](#) on page 183
- [move](#) on page 184
- [show](#) on page 185

apply

Use the `apply` command to save login configuration changes.

apply

Parameters

None

Examples

The following example saves login configuration changes:

```
EWC.extremenetworks.com:login# apply
```

auth

The `auth` command moves you into the `login:auth` context, which contains commands to configure the RADIUS server for RADIUS-based login.

The following commands are available in the `login:auth` context.

- `server` on page 181
- `primary` on page 181
- `authset` on page 182
- `move` on page 182
- `radtest_login` on page 183

server

Use the `server` command to select a RADIUS server. The `server` command is available from the `login:auth` context.

```
server ( # | name )
no server ( # | name )
```

Parameters

<code>#</code>	Specifies the index number of the RADIUS server to be used
<code>name</code>	Specifies the name of the RADIUS server to be used

Examples

The following example selects a radius server by name:

```
EWC.extremenetworks.com:login:auth# server rad2
```

primary

Use the `primary` command to set the RADIUS server as the primary server for authentication. Use the `no` form of the command to disable it. The `primary` command is available from the `login:auth` context.

```
primary server_name
no primary server_name
```

Parameters

<i>server_name</i>	Specifies the name of the server
--------------------	----------------------------------

Examples

The following example sets the primary authentication server:

```
EWC.extremenetworks.com:login:auth# primary FreeRadius70
```

authset

Use the `authset` command to set authentication server information. The `authset` command is available from the `login:auth` context.

```
authset server_name port retry_value time_out nas_ip nas_string PAP | CHAP | MS-CHAP | MS-CHAP2
```

Parameters

<i>server_name</i>	Specifies a valid RADIUS server name
<i>port</i>	Specifies the RADIUS server port
<i>retry_value</i>	Specifies the number of times to attempt to access the RADIUS server
<i>time_out</i>	Specifies the time in seconds to wait for a response from the RADIUS server before trying again
<i>NAS_IP</i>	Specifies the NAS IP address
<i>nas_string</i>	Specifies the Network Access Server (NAS) Identifier
PAP CHAP MS-CHAP MS-CHAP2	Specifies the Authentication Protocol

Examples

The following example specifies the authentication server information:

```
EWC.extremenetworks.com:login:auth# authset Radius 1812 3 5 192.168.4.112 NAS MS-CHAP
```

move

Use the `move` command to change the order of the RADIUS server in the list of RADIUS servers. The `move` command is available from the `login:auth` context.

```
move #1 { + | - } #2
```

Parameters

<i>#1</i>	Specifies Server # 1 in the list of RADIUS servers
{+}	Specifies to move the RADIUS server up in order
{-}	Specifies to move the RADIUS server down in order
<i>#2</i>	Specifies Server # 2 in the list of RADIUS servers

Examples

The following example moves the Server # 1 to second in order in the list of RADIUS servers:

```
EWC.extremenetworks.com:login:auth# move 2 - 1
```

radtest_login

Use the `radtest_login` command to check the RADIUS server's configuration. The `radtest_login` command is available from the `login:auth` context.

```
radtest_login user name password
```

Parameters

<code>user name</code>	User Name required to log on the controller
<code>password</code>	Password required to log on the controller

Examples

The following example tests the RADIUS server's configuration:

```
EWC.extremenetworks.com:login:auth# radtest_login admin abc123
==> called pam_start (1)
got success
==> called pam_authenticate
got: 'Success'
RETURN VALUE: 0 resp.code: 0
Test Result: Success
```

auth-order

Use the `auth-order` command to add an authentication mode to the end of the ordered list of authentication modes. You can also delete an authentication mode from the ordered list.

```
auth-order add | delete radius | local
```

Parameters

<code>add delete</code>	Specifies whether an authentication mode is to be added to or deleted from the ordered list.
<code>radius local</code>	Specifies authentication mode to be added or deleted

Usage

- You must configure the RADIUS server before you can add RADIUS-based authentication to the list. To do this, use the `auth` commands. See [auth](#) on page 181.
- You cannot add duplicate authentication modes to the list.

- The authentication order list must contain at least one authentication mode. You cannot delete an authentication mode if it is the only mode in the list.
- To change the order of authentication modes in the list, use the `move` command. See [move](#) on page 184

Examples

The following example sets the login authentication to RADIUS-based mode:

```
EWC.extremenetworks.com:login# auth-order add radius
EWC.extremenetworks.com:login# auth-order delete local
Changing login mode will cause CLI to terminate. Do you want to proceed? y|
[n]:y
*****
  Login mode has changed. CLI will terminate in 5 seconds!
*****
```

The following example sets the login authentication to the combination of local authentication first, then RADIUS-based authentication:

```
EWC.extremenetworks.com:login# show
1 authentication method: local
EWC.extremenetworks.com:login# auth-order add radius
EWC.extremenetworks.com:login# show
1 authentication method: local
2 authentication method: radius
```

move

Use the `move` command to change the order of authentication modes in the authentication mode ordered list.

```
move order order
```

Parameters

<code>order</code>	Specifies the current priority of the authentication mode.
--------------------	--

Usage

Use the `show` command to view the priorities of the authentication modes. See [show](#) on page 185.

Examples

The following example changes the authentication mode order from local, RADIUS to RADIUS, local:

```
EWC.extremenetworks.com:login# show
1 authentication method: local
2 authentication method: radius
EWC.extremenetworks.com:login# move 2 1
EWC.extremenetworks.com:login# show
1 authentication method: radius
```



```
2 authentication method: local
EWC.extremenetworks.com:login# apply
Changing login mode will cause CLI to terminate. Do you want to proceed? [y|
n]:y
*****
Login mode has changed. CLI will terminate in 5 seconds!
*****
```

show

Use the `show` command to display the currently configured authentication modes and their priorities.

show

Parameters

None

Examples

```
EWC.extremenetworks.com:login# show
1 authentication method: local
```

9 Radar Commands

mitigator Context Common Scan /Profile Commands



Note

The ExtremeWireless Appliance uses a software module called Radar to scan for rogue Access Points, DoS attacks, and other potential network intrusion events.

Radar provides: a radio frequency (RF) scanning task that runs on Wireless APs, an RF Data Collector (RFDC) to receive and manage RF scan messages sent by Wireless APs, and an Analysis Engine to process data from RFDCs generated by APs managed locally by the controller and also those from other controllers. The Analysis Engine participates with Radar in generating historical reports and reporting active threats. APs participating in In-service scanning must be added to in-service scan profiles, so they can be processed and managed by the Radar WIDS-WIPS system (see the *ExtremeWireless User Guide* for detailed information about Radar).

Guardian APs must be added to Guardian scan profiles. (That is any AP except the 3705.)

This chapter describes the commands that enable and configure the Radar options for the controller. These commands are located in the mitigator context of the CLI.

All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

mitigator Context

The following commands are available at the highest (first) level of the mitigator context:

- [analysis](#) on page 186
- [scprof](#) on page 187 — See [scprof](#) on page 187 for commands in the mitigator:scprof context.
- [gsprof](#) on page 188 — See [gsprof](#) on page 188 for commands in the mitigator:gsprof context.
- [maintenance](#) on page 190 — See [maintenance](#) on page 190 for commands in the mitigator:maintenance context.

For In-service and Guardian scan profile configuration commands, see [Common Scan /Profile Commands](#) on page 193.

analysis

Use the `analysis` command to enable the Analysis Engine. Use the `no` form of the command to disable it. The `analysis` command is accessible from the mitigator context of the CLI.

After you enable or disable the Analysis Engine, run the `apply` command to implement the changes.

```
analysis
no analysis
```

Parameters

None

Example

The following command enables the Analysis Engine:

```
EWC.extremenetworks.com:mitigator# analysis
EWC.extremenetworks.com:mitigator# apply
```

scprof

The `scprof` command moves you to the `scprof` context, which contains commands to create and delete scan profiles. Scan profiles define In-service scans for AP37xx and AP38xx series APs. The `scprof` command is accessible from the mitigator context of the CLI.

For Out-of-Service scanning of AP37xx and AP38xx series APs in scan groups, see the command.

InService profile can do Rogue AP scanning as well. Rogue scanning can be enabled after Security scan has been enabled.

The following commands are available in the `mitigator:scprof` context:

- [create](#) on page 187
- [delete](#) on page 187

create

Use the `create` command to create a scan profile. The `create` command is accessible from the `mitigator:scprof` context of the CLI.

```
create scan profile name
```

Parameters

<i>scan profile name</i>	Name for a new scan profile
--------------------------	-----------------------------

Example

The following example creates a scan profile named `scp_name`:

```
EWC.extremenetworks.com:mitigator:scprof# create scp_name
```

delete

Use the `delete` command to delete a scan profile. The `delete` command is accessible from the `mitigator:scprof` context of the CLI.

```
delete scan profile name
```

Parameters

<i>scan profile name</i>	Name of the scan profile to be deleted
--------------------------	--

Example

The following example deletes a scan profile named `scp_name`:

```
EWC.extremenetworks.com:mitigator:scprof# delete scp_name
```

<named scan profile>

Move to the <named scan profile> context, which contains commands to modify the attributes for a specified scan profile. The parameter <named scan profile> refers to the scan profile's name.

The <named scan profile> command is accessible from the `mitigator:scprof` context of the CLI.

The following commands are available in the `mitigator:scprof:<named scan profile>` context:

- [adhoc](#) on page 193
- [aplist](#) on page 194
- [blacklist-timer](#) on page 195
- [dosa](#) on page 197
- [drop-faf](#) on page 197
- [external-friendly](#) on page 198
- [external-honeypot](#) on page 198
- [internal-honeypot](#) on page 198
- [adhoc](#) on page 193
- [name](#) on page 199
- [spoofed-ap](#) on page 201
- [show](#) on page 201

gsprof

The `gsprof` command moves you to the `gsprof` context, which contains commands to create and delete guardian scan profiles. Guardian scan profiles define and configure Guardian APs. Guardian APs are dedicated to performing Radar (WIDS-WIPS) threat detection and countermeasures. The `gsprof` command is accessible from the `mitigator` context of the CLI.

For a complete description of Identify Guardian APs, profiles, and functions, see the *Wireless User Guide*.

The following commands are available in the `mitigator:gsprof` context:

- [create](#) on page 189
- [delete](#) on page 189
- [end](#) on page 21
- [exit](#) on page 22
- [logout](#) on page 23

- [show](#) on page 201
- [<named guardian scan profile>](#) on page 189 — See for commands in the `mitigator:gsprof:<named guardian scan profile>` context.

create

Use the `create` command to create a guardian scan profile. The `create` command is accessible from the `mitigator:gsprof` context of the CLI.

create *guardian scan profile name*

Parameters

<i>guardian scan profile name</i>	Name for a new guardian scan profile
-----------------------------------	--------------------------------------

Example

The following example creates a guardian scan profile named `ffguard_name`:

```
EWC.extremenetworks.com:mitigator:gsprof# create ffguard_name
```

delete

Use the `delete` command to delete a guardian scan profile. The `delete` command is accessible from the `mitigator:gsprof` context of the CLI.

delete *guardian scan profile name*

Parameters

<i>guardian scan profile name</i>	Name of the guardian scan profile to be deleted
-----------------------------------	---

Example

The following example deletes a guardian scan profile named `ffguard_name`:

```
EWC.extremenetworks.com:mitigator:gsprof# delete ffguard_name
```

<named guardian scan profile>

Move to the `<named guardian scan profile>` context, which contains commands to modify the attributes for a specified guardian scan profile. The parameter `<named guardian scan profile>` refers to the guardian scan profile's name.

The `<named guardian scan profile>` command is accessible from the `mitigator:gsprof` context of the CLI.

The following commands are available in the `mitigator:gsprof:<named guardian scan profile>` context:

- [adhoc](#) on page 193
- [aplist](#) on page 194
- [blacklist-timer](#) on page 195
- [dosa](#) on page 197
- [drop-faf](#) on page 197
- [external-friendly](#) on page 198

- [external-honeypot](#) on page 198
- [internal-honeypot](#) on page 198
- [adhoc](#) on page 193
- [name](#) on page 199
- [spoofed-ap](#) on page 201
- [show](#) on page 201

maintenance

The `maintenance` command moves you to the maintenance context, which contains commands to configure various security states for APs, and reclassify the security status of APs. The `maintenance` command is accessible from the mitigator context of the CLI.

The following commands are available in the `mitigator:maintenance` context:

- [authorized-ap](#) on page 190
- [friendly-ap](#) on page 191
- [prohibited-ap](#) on page 191
- [reclassify](#) on page 192
- [show](#) on page 192

authorized-ap

Use the `authorized-ap` command to add, update, or remove an authorized AP. APs are identified in this context by their BSSID (Basic Service Set ID), which is the same as their MAC address. The `authorized-ap` command is accessible from the `mitigator:maintenance` context of the CLI.

After you run the `authorized-ap` command, run the `apply` command to implement the change.

```
authorized-ap (bssid [desc string]) | (bssid delete)
```

Parameters

<i>bssid</i>	The MAC address of the AP.
desc <i>string</i>	An optional alphanumeric character string describing the AP.
delete	Removes the AP identified from BSSID from authorized status.

Example

The following example adds `testap1` by its BSSID: `11:11:22:22:33:33` as an authorized AP:

```
EWC.extremenetworks.com:mitigator:maintenance# authorized-ap
11:11:22:22:33:33 desc testap1
EWC.extremenetworks.com:mitigator:maintenance# apply
```

The following example deletes the AP with BSSID: `11:11:22:22:33:33` from authorized status:

```
EWC.extremenetworks.com:mitigator:maintenance# authorized-ap
11:11:22:22:33:33 delete
EWC.extremenetworks.com:mitigator:maintenance# apply
```

friendly-ap

Use the `friendly-ap` command to add, update, or remove a friendly AP. APs are identified in this context by their BSSID (Basic Service Set ID), which is the same as their MAC address. The `friendly-ap` command is accessible from the `mitigator:maintenance` context of the CLI.

After you run the `friendly-ap` command, run the `apply` command to implement the change.

```
friendly-ap (bssid [ssid string] [desc string]) | (bssid delete)
```

Parameters

<i>bssid</i>	The MAC address of the AP.
<i>ssid string</i>	An optional alphanumeric character string identifying the subsystem (SSID).
<i>desc string</i>	An optional alphanumeric character string describing the AP.
delete	Removes the AP identified by the BSSID from friendly AP status.

Example

The following example adds friendly AP “testing” by its BSSID: 11:11:22:22:33:33 on channel 5:

```
EWC.extremenetworks.com:mitigator:maintenance# friendly-ap 11:11:22:22:33:33
ssid testing channel 5 desc testing
EWC.extremenetworks.com:mitigator:maintenance# apply
```

The following example deletes an AP with BSSID: 11:11:22:22:33:33 from friendly status:

```
EWC.extremenetworks.com:mitigator:maintenance# friendly-ap 11:11:22:22:33:33
delete
EWC.extremenetworks.com:mitigator:maintenance# apply
```

prohibited-ap

Use the `prohibited-ap` command to add, update, or remove an AP from prohibited status. APs are identified in this context by their BSSID (Basic Service Set ID), which is the same as their MAC address. The `prohibited-ap` command is accessible from the `mitigator:maintenance` context of the CLI.

After you run the `prohibited-ap` command, run the `apply` command to implement the change.

```
prohibited-ap (bssid [desc string] [category string]) | (bssid delete)
```

Parameters

<i>bssid</i>	The MAC address of the AP.
<i>desc string</i>	An optional alphanumeric character string describing the AP.
<i>category string</i>	The optional category defines the reason the AP is prohibited. Valid values are: <code>prohibitedap</code> , <code>internalhoneypot</code> , and <code>externalhoneypot</code>
delete	Removes the AP identified by the BSSID from prohibited AP status.

Example

The following example makes testap1 with BSSID: 11:11:22:22:33:33 prohibited due to the prohibitedap category:

```
EWC.extremenetworks.com:mitigator:maintenance# prohibited-ap
11:11:22:22:33:33 desc testap1 category prohibitedap
EWC.extremenetworks.com:mitigator:maintenance# apply
```

The following example removes the AP with BSSID: 11:11:22:22:33:33 from prohibited status:

```
EWC.extremenetworks.com:mitigator:maintenance# prohibited-ap
11:11:22:22:33:33 delete
EWC.extremenetworks.com:mitigator:maintenance# apply
```

reclassify

Use the `reclassify` command to modify the state of one or more APs. APs are identified in this context by their BSSID (Basic Service Set ID), which is the same as their MAC address. The `reclassify` command is accessible from the `mitigator:maintenance` context of the CLI.

Not every reclassification is possible in any given circumstance: only the allowed transitions, as seen in the GUI. (For instance, Prohibited can be reclassified to Friendly, but not to Authorized)

After you run the `reclassify` command, run the `apply` command to implement the change.

reclassify *bssid* [, *bssid*] (**authorized**|**friendly**|**prohibited**)

Parameters

<i>bssid</i> [, <i>bssid</i>]	The MAC address of the AP. Multiple APs can be added as a comma-separated list.
authorized friendly prohibited	Specifies the classification of the specified AP(s).

Example

The following example reclassifies the APs with BSSID: 11:11:22:22:33:33 and 11:11:22:22:33:34 as authorized:

```
EWC.extremenetworks.com:mitigator:maintenance# reclassify 11:11:22:22:33:33,
11:11:22:22:33:34 authorized
EWC.extremenetworks.com:mitigator:maintenance# apply
```

show

Use the `show` command to display security states of APs managed on this controller. This `show` command is accessible from the `mitigator:maintenance` context of the CLI.

show [**authorized**|**friendly**|**prohibited**|**unclassified**]

Parameters

authorized friendly prohibited unclassified	Specifies the classification of APs you want to display. No classification means all four categories are displayed.
---	---

Example

The following example displays the authorized APs on the controller:

```
EWC.extremenetworks.com:mitigator# show authorized
```

The following example displays APs of all status categories on the controller:

```
EWC.extremenetworks.com:mitigator# show
```

Common Scan /Profile Commands

The commands in this section are common to the configuration of In-service scan profiles and Guardian scan profiles. Every profile must be configured in its own context: `scprof <named scan profile>` on page 188 or `gsprof <named guardian scan profile>` on page 189.

- [adhoc](#) on page 193
- [aplist](#) on page 194
- [blacklist-timer](#) on page 195
- [dosa](#) on page 197
- [drop-faf](#) on page 197
- [external-friendly](#) on page 198
- [external-honeypot](#) on page 198
- [internal-honeypot](#) on page 198
- [name](#) on page 199
- [port](#) on page 199
- [rogue](#) on page 200
- [rogue-prevent](#) on page 200
- [spoofed-ap](#) on page 201
- [show](#) on page 201

adhoc

Use the `adhoc` command to enable or disable removal of network access from clients in adhoc mode. The `adhoc` command is accessible from the `mitigator:scprof:<named scan profile>` context and the `mitigator:gsprof:<named guardian scan profile>` context of the CLI.

After you run the `adhoc` command, run the `apply` command to implement the change.

```
adhoc (enable | disable)
```

Parameters

enable	Enables removal of adhoc clients on this profile from network access
disable	Disables removal of adhoc clients on this profile from network access

Example

The following example enables ad hoc client removal:

```
EWC.extremenetworks.com:mitigator:scprof:scp_name# adhoc enable
EWC.extremenetworks.com:mitigator:scprof:scp_name# apply
```

aplist

Use the `aplist` command to modify the list of the Wireless APs that are part of the scan profile. Use the `no` form of the command to delete the Wireless APs from the list. The `aplist` command is accessible from the `mitigator:scprof:<named scan profile>` context, and the `mitigator:gsprof:<named guardian scan profile>` context of the CLI.

After you run the `aplist` command, run the `apply` command to implement the change.

```
aplist [(add|delete)] serial[, serial]*
```

Parameters

add delete	Add or delete the (following) APs from the scan profile. If you omit these options, by default all APs in the scan profile are replaced with the APs listed in this command.
<i>serial[, serial]*</i>	Specifies the Wireless AP by their serial numbers that are to be added to the scan profile. They can be added or deleted individually, or listed as a comma and space separated list.

Usage

Use the `add` or `delete` option to make changes to an existing scan profile AP list. You can replace the APs listed in the scan profile by omitting the `add` or `delete` option, and listing the APs you want.

Example

The following example adds a Wireless AP with the serial number 500006072051354 to the scan profile:

```
EWC.extremenetworks.com:mitigator:scprof:scp_name# aplist add 500006072051354
EWC.extremenetworks.com:mitigator:scprof:scp_name# apply
```

The following example deletes a Wireless AP with the serial number 500006072051354 from the scan profile:

```
EWC.extremenetworks.com:mitigator:scprof:scp_name# aplist delete
500006072051354
EWC.extremenetworks.com:mitigator:scprof:scp_name# apply
```

The following example replaces the Wireless APs in the scan profile with those with the following serial numbers: 500006072051354, 500005380080168, and 0500006072051427:

```
EWC.extremenetworks.com:mitigator:scprof:scp_name# aplist 500006072051354,
0500006072051427, 500005380080168
EWC.extremenetworks.com:mitigator:scprof:scp_name# apply
```

blacklist-timer

Use the `blacklist-timer` command to configure the maximum amount of time a device can be blacklisted. The `blacklist-timer` command is accessible from the `mitigator:scprof:<named scan profile>` context and the `mitigator:gsprof:<named guardian scan profile>` context of the CLI.

The `blacklist-timer` command takes effect after `dosa` (which removes network access from clients originating DoS attacks) is enabled.

After you run the `blacklist-timer` command, run the `apply` command to implement the change.

```
blacklist-timer 900-86400
```

Parameters

<code>900-86400</code>	The maximum amount of time, in seconds, a device can be blacklisted. Valid values are not less than 900, or greater than 86400 seconds.
------------------------	---

Example

The following example configures blacklisting of a device to a maximum of 2000 seconds:

```
EWC.extremenetworks.com:mitigator:scprof:scp_name# blacklist-timer 2000
EWC.extremenetworks.com:mitigator:scprof:scp_name# apply
```

channels

Use the `channels` command to modify the channel list of the scan profile. The `channels` command is accessible from the `mitigator:gsprof:<named guardian scan profile>` context of the CLI.

After you run the `channels` command, run the `apply` command to implement the change.

```
channels all | none | channel[, channel]
```

Parameters

all	Specifies that all channels be added to the scan profile list.
none	Specifies that no channels be listed in the scan profile.
<code>channel[, channel]</code>	Specifies the channel(s) by number that are to be added to the scan profile. They can be added individually, or listed as a comma separated list.

Usage

To delete some channels from the list, specify `none`, then if necessary re-add the ones you want scanned.

Example

The following example adds all channels to the scan profile:

```
EWC.extremenetworks.com:mitigator:scprof:scp_name# channels all
EWC.extremenetworks.com:mitigator:scprof:scp_name# apply
```

The following example deletes all channels from the scan profile:

```
EWC.extremenetworks.com:mitigator:scprof:scp_name# channels none
EWC.extremenetworks.com:mitigator:scprof:scp_name# apply
```

The following example adds channels 1, 3, and 9 to the scan profile:

```
EWC.extremenetworks.com:mitigator:scprof:scp_name# channels 1,3,9
EWC.extremenetworks.com:mitigator:scprof:scp_name# apply
```

classification

Use the `classification` command to enable or disable interference classification on this profile. The `classification` command is accessible from the `mitigator:scprof:<named scan profile>` context and the `mitigator:gsprof:<named guardian scan profile>` context of the CLI.

After you run the `classification` command, run the `apply` command to implement the change.

classification (enable | disable)

Parameters

enable	Enables interference classification on this profile
disable	Disables interference classification on this profile

Example

The following example enables classification:

```
EWC.extremenetworks.com:mitigator:scprof:scp_name# classification enable
EWC.extremenetworks.com:mitigator:scprof:scp_name# apply
```

concurrent-number

Use the `concurrent-number` command to configure the maximum number of channels on which a Guardian AP can concurrently launch countermeasures. The `concurrent-number` command is accessible from the `mitigator:gsprof:<named guardian scan profile>` context of the CLI.

After you run the `concurrent-number` command, run the `apply` command to implement the change.

concurrent-number 1-4

Parameters

1-4	The maximum number of channels on which countermeasures can be concurrently launched. Valid values are not less than one, or greater than 4.
------------	--

Usage

This command can be applied on any AP, except AP3705. An AP can concurrently launch countermeasures on all channels it is scanning. As more countermeasures are applied and the number of channels to which they are applied increases, the frequency of countermeasures being applied will decrease.

Example

The following example enables countermeasures on two concurrent channels:

```
EWC.extremenetworks.com:mitigator:gsprof:scp_name# concurrent-number 2
EWC.extremenetworks.com:mitigator:gsprof:scp_name# apply
```

dosa

Use the `dosa` command to enable or disable removal of network access from clients originating DoS attacks. The `dosa` command is accessible from the `mitigator:scprof:<named scan profile>` context and the `mitigator:gsprof:<named guardian scan profile>` context of the CLI.

After you run the `dosa` command, run the `apply` command to implement the change.

dosa (enable | disable)

Parameters

enable	Enables removal of clients originating DoS attacks from network access
disable	Disables removal of clients originating DoS attacks from network access

Example

The following example enables DoS attack client removal:

```
EWC.extremenetworks.com:mitigator:scprof:scp_name# dosa enable
EWC.extremenetworks.com:mitigator:scprof:scp_name# apply
```

drop-faf

Use the `drop-faf` command to enable or disable dropping frames in a controlled manner during a flood attack. The `drop-faf` command is accessible from the `mitigator:scprof:<named scan profile>` context and the `mitigator:gsprof:<named guardian scan profile>` context of the CLI.

After you run the `drop-faf` command, run the `apply` command to implement the change.

drop-faf (enable | disable)

Parameters

enable	Enables dropping of frames during a flood attack
disable	Disables dropping of frames, even during a flood attack

Example

The following example enables frame dropping:

```
EWC.extremenetworks.com:mitigator:scprof:scp_name# drop-faf enable
EWC.extremenetworks.com:mitigator:scprof:scp_name# apply
```

external-friendly

Use the `external-friendly` command to enable or disable prevention of authorized stations from roaming to external friendly APs. The `external-friendly` command is accessible from the `mitigator:scprof:<named scan profile>` context and the `mitigator:gsprof:<named guardian scan profile>` context of the CLI.

After you run the `external-friendly` command, run the `apply` command to implement the change.

external-friendly (**enable** | **disable**)

Parameters

enable	Enables prevention of authorized stations from roaming to external APs.
disable	Disables prevention of roaming to external APs.

Example

The following example enables prevention of roaming to external APs:

```
EWC.extremenetworks.com:mitigator:scprof:scp_name# external-friendly enable
EWC.extremenetworks.com:mitigator:scprof:scp_name# apply
```

external-honeypot

Use the `external-honeypot` command to enable or disable prevention of authorized stations from roaming to external honeypot APs. The `external-honeypot` command is accessible from the `mitigator:scprof:<named scan profile>` context and the `mitigator:gsprof:<named guardian scan profile>` context of the CLI.

After you run the `external-honeypot` command, run the `apply` command to implement the change.

external-honeypot (**enable** | **disable**)

Parameters

enable	Enables prevention of authorized stations from roaming to external honeypot APs.
disable	Disables prevention of roaming to external honeypot APs.

Example

The following example enables prevention of roaming to external honeypot APs:

```
EWC.extremenetworks.com:mitigator:scprof:scp_name# external-honeypot enable
EWC.extremenetworks.com:mitigator:scprof:scp_name# apply
```

internal-honeypot

Use the `internal-honeypot` command to enable or disable the preventing of any station from using an internal honeypot AP. The `internal-honeypot` command is accessible from the `mitigator:scprof:<named scan profile>` context and the `mitigator:gsprof:<named guardian scan profile>` context of the CLI.

After you run the `internal-honeypot` command, run the `apply` command to implement the change.

internal-honeypot (**enable** | **disable**)

Parameters

enable	Enables prevention of any station from roaming to an internal honeypot AP.
disable	Disables prevention of any station from roaming to an internal honeypot AP.

Example

The following example enables prevention of roaming to internal honeypot APs:

```
EWC.extremenetworks.com:mitigator:scprof:scp_name# internal-honeypot enable
EWC.extremenetworks.com:mitigator:scprof:scp_name# apply
```

name

Use the `name` command to modify the name of this scan profile. The `name` command is accessible from the `mitigator:scprof:<named scan profile>` context and the `mitigator:gsprof:<named guardian scan profile>` context of the CLI.

After you run the `name` command, run the `apply` command to implement the change.

name *profile name*

Parameters

<i>profile name</i>	Specifies a profile name in alphanumeric characters.
---------------------	--

Example

The following example renames the `scp_name` scan profile to `test22`:

```
EWC.extremenetworks.com:mitigator:scprof:scp_name# name test22
EWC.extremenetworks.com:mitigator:scprof:scp_name# apply
EWC.extremenetworks.com:mitigator:scprof:test22#
```

port

Use the `port` command to configure the port number used for rogue detection on the AP. The `port` command is accessible from the `mitigator:scprof:<named scan profile>` context of the CLI and the `mitigator:gsprof:<named guardian scan profile>` context of the CLI. (Guardian also scans for Rogues.)

The `port` command is only available if security scan is enabled.

port *port-number*

Parameters

<i>port-number</i>	Specifies the number of the port used for rogue detection on the AP. Valid port numbers are 1-32768.
--------------------	--

Example

The following example specifies port 1538 as the port used for rogue detection on the AP for the scp_name scan profile in-service:

```
EWC.extremenetworks.com:mitigator:scprof:in-service# port 1538
EWC.extremenetworks.com:mitigator:scprof:in-service#
```

rogue

Use the `rogue` command to enable or disable rogue detection for this scan profile. The `rogue` command is accessible from the `mitigator:scprof:<named scan profile>` context of the CLI.

The `rogue` command is only available if security scan is enabled (see [security-scan](#) on page 201).

rogue enable | disable

Parameters

enable	Enables rogue detection for this scan profile.
disable	Disables rogue detection for this scan profile.

Example

The following example enables rogue detection for the scp_name scan profile in-service:

```
EWC.extremenetworks.com:mitigator:scprof:in-service# rogue enable
EWC.extremenetworks.com:mitigator:scprof:in-service#
```

rogue-prevent

Use the `rogue-prevent` command to enable or disable the prevention of any station from using a rogue AP. The `rogue-prevent` command is accessible from the `mitigator:scprof:<named scan profile>` context of the CLI.

rogue-prevent enable | disable

Parameters

enable	Enables the prevention of any station from using a rogue AP.
disable	Disables the prevention of any station from using a rogue AP.

Example

The following example enables prevention of any station from using a rogue AP for the scp_name scan profile in-service:

```
EWC.extremenetworks.com:mitigator:scprof:in-service# rogue-prevent enable
EWC.extremenetworks.com:mitigator:scprof:in-service#
```


security-scan

Use the `security-scan` command to enable or disable security scans. The `security-scan` command is accessible from the `mitigator:scprof:<named scan profile>` context and the `mitigator:gsprof:<named guardian scan profile>` context of the CLI.

After you run the `security-scan` command, run the `apply` command to implement the change.

security-scan (enable | disable)

Parameters

enable	Enables security scans for rogue APs.
disable	Disables security scans for rogue APs.

Example

The following example enables security scans:

```
EWC.extremenetworks.com:mitigator:scprof:scp_name# security-scan enable
EWC.extremenetworks.com:mitigator:scprof:scp_name# apply
```

spoofed-ap

Use the `spoofed-ap` command to enable or disable prevention of any station using a spoofed AP. The `spoofed-ap` command is accessible from the `mitigator:scprof:<named scan profile>` context and the `mitigator:gsprof:<named guardian scan profile>` context of the CLI.

After you run the `spoofed-ap` command, run the `apply` command to implement the change.

spoofed-ap (enable | disable)

Parameters

enable	Enables prevention of access to a spoofed AP.
disable	Disables prevention of access to spoofed APs.

Example

The following example enables prevention of access to spoofed APs:

```
EWC.extremenetworks.com:mitigator:scprof:scp_name# spoofed-ap enable
EWC.extremenetworks.com:mitigator:scprof:scp_name# apply
```

show

Use the `show` command to display the settings for the scan profile. This `show` command is accessible from the `mitigator:scprof:<named scan profile>` context and the `mitigator:gsprof:<named guardian scan profile>` context of the CLI.

show

Parameters

None

Example

The following example displays the scan profile scp_name's settings:

```
EWC.extremenetworks.com:mitigator:scprof:scp_name# show
Profile Name: scp_name
Security Scan: enable
Interference Classification: disable
External Honeypot: disable
External Friendly: enable
Internal Honeypot: disable
Spoofed AP: disable
Drop Frames FAF: disable
Adhoc mode removal: disable
DoS attacks removal: enable
Blacklisting timer: 900
Concurrent Channel Number: 1
channels 1,3,5
aplist
1000005380080166
```

10 mobility Commands

backupmanagerip
mrole
mport
mheartbeat
slpreg
agent
secmode
mdismethod
mmanagerip

Multiple Wireless Appliances on a network can share and exchange client session information, which enables a wireless device to roam between Wireless APs on different Wireless Appliances without service interruption.

This section describes the commands required to configure the Mobility options for the Wireless Appliance. These commands are located in the mobility context of the CLI.

All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, exit and re-enter the context so that the database is synchronized with the latest change.

The following commands are available in the mobility context:

- [backupmanagerip](#) on page 203
- [mrole](#) on page 204
- [mport](#) on page 204
- [mheartbeat](#) on page 205
- [slpreg](#) on page 205
- [agent](#) on page 205
- [secmode](#) on page 206
- [mdismethod](#) on page 206
- [mmanagerip](#) on page 207

backupmanagerip

Use the `backupmanagerip` command to configure an IP address for the backup manager in the mobility zone. The role of the Wireless Appliance must be set to Agent before this option becomes available (see [mrole](#) on page 204 for more information).

backupmanagerip *IP Address*

Parameters

<i>IP Address</i>	Specifies the IP address of the network backup manager
-------------------	--

Examples

The following example sets the backup manager IP address:

```
EWC.extremenetworks.com:mobility# backupmanagerip 195.160.1.40
```

mrole

Use the `mrole` command to set the role of the Wireless Appliance.

```
mrole ( none | manager | agent )
```

Parameters

none	Removes role designations from the controller
manager	Sets the role of the Wireless Appliance to Manager
agent	Sets the role of the Wireless Appliance to Agent

Examples

The following example sets the role of the Wireless Appliance as a Mobility Agent:

```
EWC.extremenetworks.com:mobility# mrole agent
```

mport

Use the `mport` command to select the port to be used by the Mobility feature.

```
mport esaX
```

Parameters

<i>esaX</i>	Specifies the ESA port, where X refers to the port number
-------------	---

Examples

The following example selects the `esa3` port:

```
EWC.extremenetworks.com:mobility# mport esa3
```

mheartbeat

The Wireless Appliance that has the VNManager designation sends regular Heartbeat messages containing information regarding wireless device session changes to the VNAgents, and waits for an update message to come back.

Use the `mheartbeat` command to set the time interval (in seconds) for the connection establishment response between the Mobility Agent and the Mobility Manager.

mheartbeat *value*

Parameters

<i>value</i>	Specifies the interval time in seconds between outgoing heartbeats
--------------	--

Examples

The following example sets the outgoing heartbeats to occur at 5 second intervals:

```
EWC.extremenetworks.com:mobility# mheartbeat 5
```

slpreg

Use the `slpreg` command to enable SLP registration. Use the `no` form of the command to disable it.

slpreg
no **slpreg**

Parameters

None

Examples

The following example enables SLP registration:

```
EWC.extremenetworks.com:mobility# slpreg
```

agent

Use the `agent` command to add, remove, or approve an agent on the network by its IP address when the current controller serves as a mobility manager.

The role of the Wireless Appliance must be set to Manager before this option becomes available. For more information, see [mrole](#) on page 204.

agent (**add** | **remove** | **approve** | **backupMgr**) *IP Address*

Parameters

add	Adds an agent to the network
remove	Removes an agent from the network
approve	Approves an agent on the network
backupMgr	Specifies the agent at the IP address as the network backup manager
<i>IP Address</i>	Specifies the IP address of the agent

Examples

The following example adds an agent to the network:

```
EWC.extremenetworks.com:mobility# agent add 10.0.0.1
```

The following example removes an agent from the network:

```
EWC.extremenetworks.com:mobility# agent remove 10.0.2.4
```

The following example approves an agent on the network:

```
EWC.extremenetworks.com:mobility# agent approve 10.0.0.1
```

The following example specifies 10.0.0.1 as backup manager agent on the network:

```
EWC.extremenetworks.com:mobility# agent backupmgr 10.0.0.1
```

secmode

Use the `secmode` command to set the Security Mode to allow only approved Agents to connect to the manager, or allow all agents to connect.

secmode (**approved**|**none**)

Parameters

approved	Allows only approved agents to connect to the manager
none	Allows all agents to connect to the manager

Examples

The following example configures the security mode to have no restrictions, allowing all agents to connect to the manager:

```
EWC.extremenetworks.com:mobility# secmode none
```

mdismethod

Use the `mdismethod` command to locate the Mobility Manager on the network.

mdismethod (**slpd**|**static**)

Parameters

slpd	Uses the Service Location Protocol (SLP) Discovery method
static	Uses a statically configured IP address for detection

Examples

The following example uses the SLP discovery method:

```
EWC.extremenetworks.com# mdismethod slpd
```

mmanagerip

Use the `mmanagerip` to specify the IP address of the Mobility Manager. The role of the Wireless Appliance must be set to Agent before this option becomes available. For more information, see [backupmanagerip](#) on page 203.

mmanagerip *IP Address*

Parameters

<i>IP Address</i>	Specifies the IP address of the VN Manager
-------------------	--

Examples

The following example changes the IP address of the Mobility Manager:

```
EWC.extremenetworks.com:mobility# mmanagerip 195.160.1.39
```

11 `schedule_backup` Commands

`destination`
`dir`
`freq`
`password`
`protocol`
`server`
`starttime`
`type`
`user`

This section describes commands for scheduling the backup of the following information:

- Software configurations
- CDRs
- Logs
- Audit Report

This section describes commands which manage scheduling options for the backup of data locally or to an FTP or SCP address. The `destination` command setting specifies the destination where the export file is saved to. These commands are located in the `schedule_backup` context of the CLI.

All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

After running the `schedule_backup` commands, you must run the `apply` command to implement the changes.

The following commands are available in the `schedule_backup` context:

- [destination](#) on page 209
- [dir](#) on page 209
- [freq](#) on page 209
- [password](#) on page 210
- [protocol](#) on page 211
- [server](#) on page 211
- [starttime](#) on page 211
- [type](#) on page 212
- [user](#) on page 212

destination

Use the `destination` command to specify where the backup file is saved to.

destination (**local** | **flash** | **remote**)

Parameters

local	Save the backup file on a local drive
flash	Save the backup file on a flash drive
remote	Upload the backup file onto a remote server

Examples

Examples

The following example specifies local drive as a destination for the backup file:

```
EWC.extremenetworks.com:schedule_backup# destination local
```

dir

Use the `dir` command to specify a directory to contain backup data on the FTP or SCP server.

`dir path`

Parameters

<i>path</i>	Specifies the directory path
-------------	------------------------------

Examples

The following example specifies the directory path for backup data:

```
EWC.extremenetworks.com:schedule_backup# dir /home/user/destdir
```

freq

Use the `freq` command to specify the frequency of software backups.

freq (**daily** | **everyday** | **weekday**) | (**weekly** **0,1,2,3,4,5,6**) | (**monthly** *date*) | **never**

Parameters

daily	Indicates that backups will occur on a daily basis
everyday	Configures backup to occur every day of the week

weekday	Configures backup to occur from Monday to Friday only
weekly	Indicates that backups will occur on weekly basis
0	Configures backup scheduling to occur on Sunday
1	Configures backup scheduling to occur on Monday
2	Configures backup scheduling to occur on Tuesday
3	Configures backup scheduling to occur on Wednesday
4	Configures backup scheduling to occur on Thursday
5	Configures backup scheduling to occur on Friday
6	Configures backup scheduling to occur on Saturday
monthly	Indicates that backups will occur on a monthly basis
<i>date</i>	Specifies a calendar day
never	Indicates that backups will not occur

Examples

The following example sets the software backups to occur from Monday to Friday:

```
EWC.extremenetworks.com:schedule_backup# freq daily weekday
```

The following example sets the software backups to occur every Tuesday and Thursday:

```
EWC.extremenetworks.com:schedule_backup# freq weekly 2,4
```

The following example sets the software backups to occur on the 15th day of every month:

```
EWC.extremenetworks.com:schedule_backup# freq monthly 15
```

The following example disables all backup scheduling:

```
EWC.extremenetworks.com:schedule_backup# freq never
```

password

Use the `password` command to specify the password of the user name on the FTP or SCP server.

The user name must be specified using the `user` command. For more information, see [user](#) on page 212.

password *string*

Parameters

<i>string</i>	Specifies a password for a user on the FTP or SCP server
---------------	--

Examples

The following command specifies a password for the user on the server:

```
EWC.extremenetworks.com:schedule_backup# password rYm239sJ
```

protocol

Use the `protocol` command to specify the appropriate protocol to use when communicating with the destination server.

```
protocol [ftp|scp]
```

Parameters

ftp	Specifies the FTP protocol
scp	Specifies the SCP protocol

Examples

The following example sets the protocol to SCP:

```
EWC.extremenetworks.com:schedule_backup# protocol scp
```

server

Use the `server` command to specify the IP address of the destination server for backup data.

```
server IP Address
```

Parameters

<i>IP Address</i>	Specifies the IP address of the FTP or SCP server. The IP address can be either IPv4 (A.B.C.D) or IPv6 (A:B:C:D:E:F:G:H) format.
-------------------	--

Examples

The following example sets the IP address of the server receiving backup data:

```
EWC.extremenetworks.com:schedule_backup# server 192.168.1.17
```

starttime

Use the `starttime` command to specify the time of day to start a scheduled backup. The scheduled task time must be set to daily, weekly, or monthly before the start time can be specified. For more information, see [freq](#) on page 209.

```
starttime HH:mm
```

Parameters

<i>HH</i>	Specifies the hour (in a 24 hour clock format) to start a scheduled backup
<i>mm</i>	Specifies the minute to start scheduled backup

Examples

The following example sets the start time of a scheduled backup to 1:16 PM:

```
EWC.extremenetworks.com:schedule_backup# starttime 13:16
```

type

Use the `type` command to indicate the data types to backup.

```
type ( configuration | cdrs | all | logs | audit )
```

Parameters

configuration	Indicates that configuration files will be backed up
cdrs	Indicates that call detail records will be backed up
all	Indicates that all configuration, call detail records, log files, audit files, and rogue files will be backed up
logs	Indicates that log files will be backed up
audit	Indicates that audit files will be backed up

Examples

The following example indicates that audit files are to be backed up:

```
EWC.extremenetworks.com:schedule_backup# type audit
```

user

Use the `user` command to specify the user name of an account on the FTP or SCP server.

Syntax

```
user id
```

Parameters

<i>id</i>	Specifies a user name
-----------	-----------------------

Examples

The following example specifies a username for the server:

```
EWC.extremenetworks.com:schedule_backup# user admin
```

12 schedule_upgrade Commands

schld_upgrd upgrade_backup

Use the `schedule_upgrade` context to access the commands for scheduling an upgrade and back up of the controller's software. The `schedule_upgrade` context is accessible from the root context of the CLI.

`schedule_upgrade` is not the command. It is the context. You must be in the `schedule_upgrade` context to access the commands for scheduling the upgrade and backup of the controller's software. The commands for scheduling the upgrade and back up of the controller's image are provided in the following sections.

All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the `schedule_upgrade` context:

- `schld_upgrd` on page 214
- `upgrade_backup` on page 215

schld_upgrd

Use the `schld_upgrd` command to schedule a local or remote upgrade of the Wireless Appliance's software. Use the `no` form of the command to delete the scheduled upgrade. This command is accessible from the `schedule_upgrade` context.

Before you schedule a local upgrade, download the upgrade image to the controller.

```
[no] schld_upgrd MM:DD:hh:mm (local image_name) |(remote server user password dir image_name)
```

Parameters

<i>MM</i>	Month on which the upgrade will be carried out
<i>DD</i>	The date on which the upgrade will be carried out
<i>hh:mm</i>	The time (in 24-hour format) at which the upgrade will be carried out
local	Specifies that the new software will be downloaded locally from the Wireless Appliance
<i>image_name</i>	The new software's file name
remote	Specifies that the new software will be downloaded from the remote FTP server
<i>server</i>	The remote FTP server where the image file is located

<i>user</i>	The user name to access the FTP server
<i>password</i>	The password to access the FTP server
<i>dir</i>	The path to the directory where the new software is stored on the FTP server
<i>image name</i>	The new software's file name

Examples

If you want to delete the existing local upgrade schedule, add `no` before the local upgrade syntax as shown in the following example:

```
EWC.extremenetworks.com:schedule_upgrade# no schld_upgrd
```

The following example schedules a local upgrade:

```
EWC.extremenetworks.com:schedule_upgrade# schld_upgrd 06:01:12:00 local AC-
MV-07.41.03.0003-1.rue
```

The following example schedules a remote upgrade:

```
EWC.extremenetworks.com:schedule_upgrade# schld_upgrd 06:01:12:00 remote
192.168.4.10 test abc123 /ac/rpm/build07.41.03.0003 AC-MV-07.41.03.0003-1.rue
```

If you want to delete the existing remote upgrade schedule, add `no` before the remote upgrade syntax as shown in the following example:

```
EWC.extremenetworks.com: schedule_upgrade# no schld_upgrd
```

upgrade_backup

Use the `upgrade_backup` command to create a rescue backup of the existing software of the Wireless Appliance on the remote FTP server. Use the `no` form of the command to delete the remote rescue backup.

The `upgrade_backup` command is accessible from the `schedule_upgrade` context.

```
upgrade_backup (local|flash|remote server user password dir file)
no upgrade_backup
```

Parameters

upgrade_backup	Specifies to backup the existing software of the Wireless Appliance before initiating the upgrade process
flash <i>filename</i>	Specifies that the backup image of the existing software of the Wireless Appliance is to be saved on the flash card. This option is only available if an external flash card has been mounted on the controller. Backup file name can optionally be provided, but it must end with "-rescue-user.tgz".

local	Specifies that the backup image of the existing software of the Wireless Appliance is to be saved locally.
remote	Specifies that the backup image of the existing software of the Wireless Appliance is to be created on the remote FTP server
<i>server</i>	The FTP server where the backup image will be created
<i>user</i>	The user name to access the FTP server
<i>password</i>	The password to access the FTP server
<i>dir</i>	The directory where the backup image will be created on the FTP server
<i>file</i>	The file name that you want to assign to the backup image. Filename must end with "-rescue-user.tgz".

Examples

In the following example, the backup image is created on the ftp server:

```
EWC.extremenetworks.com:schedule_upgrade# upgrade_backup remote 192.168.4.181
admin abc123/ myDir/ backup-rescue-user.tgz
```

In the following example, the backup image is created on the external flash:

```
EWC.extremenetworks.com:schedule_upgrade# upgrade_backup flash backupToFlash-
rescue-user.tgz
```

The following example deletes the upgrade backup:

```
EWC.extremenetworks.com:schedule_upgrade# no upgrade_backup
```


13 snmp Commands

contact
context
enable
engine-id
location
port
publish-ap
rcommunity
rwcommunity
severity
show
trap-manager-v1v2
trap-manager-v3
user

The Wireless Appliance supports the Simple Network Management Protocol (SNMP) for retrieving statistics and configuration information.

This section describes commands which manage SNMP settings for the Wireless Appliance. These commands are located in the `snmp` context of the CLI.

All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the `snmp` context:

- [contact](#) on page 218
- [context](#) on page 218
- [enable](#) on page 218
- [engine-id](#) on page 219
- [location](#) on page 219
- [severity](#) on page 221
- [trap-manager-v1v2](#) on page 222
- [trap-manager-v3](#) on page 223
- [user](#) on page 223
- [show](#) on page 222
- [rwcommunity](#) on page 221
- [port](#) on page 220
- [publish-ap](#) on page 220
- [show](#) on page 222

contact

Use the `contact` command to identify the name of the SNMP administrator.

contact *string*

Parameters

<i>string</i>	Specifies the name of the person enabling SNMP traps on the system
---------------	--

Examples

The following example specifies a name to identify the SNMP administrator:

```
EWC.extremenetworks.com:snmp# contact Bill
```

context

Use the `context` command to add an SNMPv3 context.

context *string*

Parameters

<i>string</i>	Specifies the context name
---------------	----------------------------

Examples

The following example specifies the SNMPv3 context:

```
EWC.extremenetworks.com:snmp# context context1
```

enable

Use the `enable` command to enable and configure SNMP.

enable (**none**|**v1v2**|**v3**) [*contact location rcommunity rwcommunity* (**1**|**2**|**3**|**4**|**5**)
1-65535]

Parameters

none	Disables SNMP
(v1v2 v3)	Enables either SNMPv1/V2 or SNMPv3
<i>contact</i>	Specifies the name of the SNMP administrator
<i>location</i>	Specifies a description for the location of the SNMP administration machine
<i>rcommunity</i>	Specifies a name for the read-only network management community

<i>rwcommunity</i>	Specifies a name for the read-write network management community
1	Forwards the SNMP trap with the Critical severity level
2	Forwards the SNMP trap with the Major severity level
3	Forwards the SNMP trap with the Minor severity level
4	Forwards the SNMP trap with the Informational severity level
5	Forwards the SNMP trap with the Trace severity level
<i>1-65555</i>	Specifies the destination port for the SNMP traps

Example

The following example enables SNMPv3:

```
EWC.extremenetworks.com:snmp# enable v3
```

engine-id

Use the `engine-id` command to configure the SNMPv3 engine ID for the Wireless Appliance running the SNMP agent.

```
engine-id string [auto-gen]
```

Parameters

<i>string</i>	Specifies the SNMPv3 engine ID for the Wireless Appliance running the SNMP agent. The string must be from 5 to 32 characters in length when auto-gen is not selected, and from 1 to 27 characters when auto-gen is selected.
auto-gen	Automatically generates the SNMPv3 engine ID from the manually entered string.

Examples

The following example specifies the SNMPv3 engine ID of the SNMP agent. Note that resetting the engine-id will reset all users:

```
EWC.extremenetworks.com:snmp# engine-id aaaaaaa
All users will be reset.
(yes/no):no
Warning : Operation to update engine ID cancelled.
```

location

Use the `location` command to enter a descriptive string indicating the physical location of the Wireless Appliance running the SNMP agent.

```
location string
```

Parameters

<i>string</i>	Specifies the location Wireless Appliance running the SNMP agent
---------------	--

Examples

The following example specifies the location of the SNMP agent:

```
EWC.extremenetworks.com:snmp# location Blue Office - Second Floor
```

port

Use the `port` command to specify the destination port for the SNMP traps.

port *value*

Parameters

<i>value</i>	Specifies the trap port of the SNMP manager. The value can range from 1 to 65535.
--------------	---

Examples

The following example sets the trap port of the SNMP manager to 163:

```
EWC.extremenetworks.com:snmp# port 163
```

publish-ap

Use the `publish-ap` command to enable or disable SNMP publishing of the access point as an interface to the Wireless Appliance.

publish-ap (**enable** | **disable**)

Parameters

enable disable	Enables or disables publishing of the access point as an interface to the controller.
--------------------------------	---

Examples

The following example enables SNMP publishing:

```
EWC.extremenetworks.com:snmp# publish-ap enable
```

If you attempt to enable SNMP publish when LLDP is enabled on one or more APs, you will get the following warning:

```
WARNING: LLDP is enabled for some Wireless APs. Would you like to continue?
(C) Cancel
```

- (P) Proceed
- (O) Disable LLDP and proceed

Type one of the following:

- C - Cancels the SNMP configuration and returns to the AP context.
- P - Enables SNMP publishing and maintains LLDP enabled
- O - Enables SNMP and disables LLDP

rcommunity

Use the `rcommunity` command to set the name of the read-only community.

rcommunity *string*

Parameters

<i>string</i>	Specifies the name used for the read-only community
---------------	---

The following example sets the name of the read-only community:

```
EWC.extremenetworks.com:snmp# rcommunity public
```

rwcommunity

Use the `rwcommunity` command to specify the name of the read-write community. This community allows the modification of stored data on the administrative system.

rwcommunity *string*

Parameters

<i>string</i>	Specifies the name used for the read-write community
---------------	--

Examples

The following example sets the name of the read-write community:

```
EWC.extremenetworks.com:snmp# rwcommunity private
```

severity

Use the `severity` command to configure the Wireless Appliance to send SNMP traps of the specified severity level.

severity (1|2|3|4|5)

Parameters

1	Forwards the SNMP trap with the Critical severity level
2	Forwards the SNMP trap with the Major severity level
3	Forwards the SNMP trap with the Minor severity level
4	Forwards the SNMP trap with the Informational severity level
5	Forwards the SNMP trap with the Trace severity level

Example

The following example forwards traps having the Critical level of severity:

```
EWC.extremenetworks.com.com:snmp# severity 2
```

show

Use the `show` command in the SNMP context to display all SNMP configuration information or just information about configured SNMPv3 users.

```
show [user]
```

Parameters

user	Display only configured users.
-------------	--------------------------------

Examples

The following example lists only the SNMPv3 users, when in the SNMP context:

```
EWC.extremenetworks.com:snmp# show user
User      Authentication  ProtocolAuth  ProtocolPriv  Enabled
test1    noauthnopriv    none          none          False
```

Refer to [user](#) on page 223 for descriptions of the values in the various columns of this output.

trap-manager-v1v2

Use the `trap-manager-v1v2` command to identify either the primary or secondary machine monitoring SNMPv1/v2 traps by IP address.

```
trap-manager-v1v2 1|2 (IP Address | delete)
```

Parameters

1 2	Identifies the primary or secondary machine monitoring SNMPv1/v2 traps
<i>IP Address</i>	Specifies the IP address of the machine monitoring SNMPv1/v2 traps. The IP address can be either IPv4 (A.B.C.D) or IPv6 (A:B:C:D:E:F:G:H) format.
delete	Delete the specified trap manager.

Examples

The following example specifies the IP address of the primary machine monitoring SNMPv1/v2 traps:

```
EWC.extremenetworks.com:snmp# trap-manager-v1v2 1 192.168.1.5
```

The following example deletes the secondary machine monitoring SNMPv1/v2 traps:

```
EWC.extremenetworks.com:snmp# trap-manager-v1v2 2 delete
```

trap-manager-v3

Use the `trap-manager-v3` command to identify either the primary or secondary machine monitoring SNMPv3 traps by IP address.

```
trap-manager-v3 (1|2) (IP address | delete)
```

Parameters

1 2	Identifies the primary or secondary machine monitoring SNMPv3 traps
<i>IP address</i>	Specifies the IP address of the machine monitoring SNMPv3 traps. The IP address can be either IPv4 (A.B.C.D) or IPv6 (A:B:C:D:E:F:G:H) format.
<i>delete</i>	Removes the SNMPv3 machine monitoring SNMPv3 traps

Examples

The following example specifies the IP address of the primary machine monitoring SNMPv3 traps and the SNMPv3 user “admin”:

```
EWC.extremenetworks.com:snmp# trap-manager-v3 1 192.168.1.5
```

The following example deletes the primary trap manager configured in the previous example:

```
EWC.extremenetworks.com:snmp# trap-manager-v3 1 delete
```

user

Use the `user` command to configure SNMP v3 users and security.

```
user username security (noAuthNoPriv | authNoPriv (md5|sha) authpassword |  
authPriv (md5|sha) authpassword des privpassword)  
user username disable|enable  
user username delete
```

Parameters

<i>username</i>	Specifies the SNMPv3 user to configure for use with SNMPv3 traps
security (noAuthNoPriv authNoPriv authPriv)	Specifies the security options to use with this SNMPv3 user (Noauthpriv, Authnopriv, or Authpriv)

md5 sha	Specifies the authentication protocol to use when security level is set to authNoPriv or authPriv.
<i>authpassword</i> des	Specifies the authentication password and the DES protocol to use when security level is set to authNoPriv or authPriv. DES must be used when the security level is set to authPriv.
<i>privpassword</i>	Specifies the privacy password to use when security level is set to authPriv.
enable disable	Enables or disables an existing user
delete	Deletes an existing user

Examples

The following example creates an SNMPv3 user named “test” with an authPriv security level using MD5, an authentication password of “tester1234” and a privacy password of “tester1234”:

```
EWC.extremenetworks.com# user test security authPriv md5 tester1234 des
test1234
```


14 syslog Commands

audmsg
facility
stationevents
svcmmsg
syslogip

This section describes commands to configure System Log settings on the Wireless Appliance. These commands are located in the `syslog` context of the CLI.

All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the `syslog` context:

- [audmsg](#) on page 225
- [facility](#) on page 226
- [stationevents](#) on page 226
- [svcmmsg](#) on page 227
- [syslogip](#) on page 227

audmsg

Use the `audmsg` command to enable service messages. Use the `no` form of the command to disable them.

```
audmsg  
no audmsg
```

Parameters

None

Example

The following example enables service messages on the Wireless Appliance:

```
EWC.extremenetworks.com:syslog# audmsg
```

facility

Use the `facility` command to send update application, service, audit, and station event log information to the syslog server. Application logs and service logs cannot use the same log level at the same time.

facility (**application**|**service**|**audit**|**station**) (0|1|3|4|5|6)

Parameters

application	Specifies that application logs are to be updated.
service	Specifies that service logs are to be updated.
audit	Specifies that audit logs are to be updated.
station	Specifies that station event logs are to be updated.
0	Sends the log with the Emergency severity level to the syslog server.
1	Sends the log with the Alert severity level to the syslog server.
3	Sends the log with the Error severity level to the syslog server.
4	Sends the log with the Warning severity level to the syslog server.
5	Sends the log with the Notice severity level to the syslog server.
6	Sends the log with the Info severity level to the syslog server.

Example

The following example sets the application log level 3 to be sent to the syslog server:

```
EWC.extremenetworks.com:syslog# facility application 3
Successfully updated application logs to 3.
```

The following example sets the station event log level 2 to be sent to the syslog server:

```
EWC.extremenetworks.com:syslog# facility station 2
Successfully updated station logs to 2.
```

stationevents

Use the `stationevents` command to turn on or off station event forwarding to the syslog server.

stationevents **enable**|**disable**

Parameters

enable	Enables station event logging.
disable	Disables station event logging.

Examples

The following example enables station event logging:

```
EWC.extremenetworks.com:syslog# stationevents enable
```

svcmsg

Use the `svcmsg` command to enable DHCP messages. Use the `no` form of the command to disable these and use log and traces messages only.

```
svcmsg
no svcmsg
```

Parameters

None

Examples

The following example enables service messages on the system:

```
EWC.extremenetworks.com:syslog# svcmsg
Successfully turned on service messages.
```

The following example disables service messages:

```
EWC.extremenetworks.com:syslog# no svcmsg
Successfully turned off service messages.
```

syslogip

Use the `syslogip` command to configure up to three syslog servers. Use the `no` form of the command to delete a server. Use `show syslog` to display system log levels. For more information, see [show syslog](#) on page 78.

```
syslogip # IP Address [enable|disable]
no syslogip
```

Parameters

#	Specifies the index number of the system log ID
<i>IP Address</i>	Specifies the IP address to be configured. The IP address can be either IPv4 (A.B.C.D) or IPv6 (A:B:C:D:E:F:G:H) format.
enable	Enables the server
disable	Disables the server

Examples

The following example specifies the IP address of a syslog server and enables it:

```
EWC.extremenetworks.com:syslog# syslogip 1 143.23.34.52 enable  
Successfully updated syslogip 1.
```

The following example deletes the syslog server:

```
EWC.extremenetworks.com:syslog# no syslogip 1  
Successfully removed syslogip 1.
```

15 time Commands

clock
date
ntp
ntpip
tz

Network elements on the Wireless Appliance can be synchronized to a universal clock in one of two ways:

- using the Wireless Appliance's own system time
- using the Network Time Protocol

The commands described in this section are used to select and configure these options, and are located in the time context of the CLI.

All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

After you run any of the `time` commands, run the `apply` command to implement the changes.

The following commands are available in the time context:

- [clock](#) on page 229
- [date](#) on page 230
- [ntp](#) on page 230
- [ntpip](#) on page 230
- [tz](#) on page 231

clock

Use the `clock` command to set the system time.

The Network Time Protocol must be disabled before this command can be used. For more information, see [ntp](#) on page 230.

After you run the `clock` command, run the `apply` command to implement the changes.

```
clock hh:mm
```

Parameters

<i>hh</i>	Specifies the current hour (in 24 hour clock format)
<i>mm</i>	Specifies the current minute

Example

The following example sets the system time to 12:01pm:

```
EWC.extremenetworks.com:time# clock 12:01
```

date

Use the `date` command to set the system date. The Network Time Protocol must be disabled before this command can be used. For more information, see [ntp](#) on page 230.

date *dd:mm:yyyy*

Parameters

<i>dd</i>	Specifies the day
<i>mm</i>	Specifies the month
<i>yyyy</i>	Specifies the year

Example

The following example sets the date to January 17, 2099:

```
EWC.extremenetworks.com# date 17:01:2099
```

ntp

Use the `ntp` command to use the Network Time Protocol (NTP). Use the `no` form of the command to disable it. If you want to use the external NTP Server, configure the NTP Server's IP address by running the `ntpip` command. For more information, see [ntpip](#) on page 230.

ntp [**2** | **3**]
(no) ntp [**1** | **2** | **3**]

Parameters

2	Specifies to use the external NTP Server to synchronize the network time
3	Specifies to use the internal NTP Server to synchronize the network time

Example

The following example specifies to use the internal NTP Server to synchronize the network time:

```
EWC.extremenetworks.com:time# ntp 3
```

ntpip

Use the `ntpip` command to configure the IP address of up to 3 standard NTP time servers. Use the `no` form of the command to remove an IP address by its index number.

```
ntpip (1|2|3) IP address|domain
no ntpip (1|2|3)
```

Parameters

1 2 3	Indicates the index number on the list of configured NTP time servers
<i>IP Address</i>	Specifies the IP address of an NTP time server. The IP address can be either IPv4 (A.B.C.D) or IPv6 (A:B:C:D:E:F:G:H) format.
<i>domain</i>	Specifies a domain for the NTP time server

Example

The following example configures the IP address of an NTP time server and assigns it an index value of 2:

```
EWC.extremenetworks.com:time# ntpip 2 192.168.4.89
```

tz

Use the `tz` command to set time zone information for the Wireless Appliance.

The Wireless Appliance reboots when the time zone is changed.

```
tz continent continent country country region region
```

Parameters

<i>continent</i>	Specifies the continent
<i>country</i>	Specifies the country
<i>region</i>	Specifies the region

Example

The following example sets the time zone information:

```
EWC.extremenetworks.com:time# tz continent america country united states
region new_york
```

16 traffic_capture Commands

file_name
size
interface
delete
list
start
stop
show
show interfaces

The `traffic_capture` command moves you to the `traffic_capture` context, which contains the commands to manage the TCPDump. The `traffic_capture` command is accessible from the root context of the CLI.

All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the `traffic_capture` context:

- [file_name](#) on page 232
- [size](#) on page 233
- [interface](#) on page 233
- [delete](#) on page 234
- [list](#) on page 234
- [start](#) on page 235
- [stop](#) on page 235
- [show](#) on page 235
- [show interfaces](#) on page 236

file_name

Use the `file_name` command to specify a file name for the TCPDump. If you do not assign any file name to the TCPDump, the CLI gives a default name `mgmt_traffic_dump.cap`. The CLI enforces `.cap` file extension to the TCPDump file. The `file_name` command is accessible from the `traffic_capture` context of the CLI.

file_name *fileName*

Parameters

<i>fileName</i>	Specifies the file name for the TCPDump
-----------------	---

Examples

The following example specifies the file name as TrafficCapture for the TCPDump:

```
EWC.extremenetworks.com:traffic_capture# file_name TrafficCapture
```

size

Use the `size` command to specify the file size of TCPDump file. The `size` command is accessible from the `traffic_capture` context of the CLI.

Refer to the Wireless Appliance Convergence Software Maintenance Guide for more information.

size *filesize*

Parameters

<i>filesize</i>	Specifies the file size of TCPDump file. File size can range from 10 MB (minimum) to a maximum of 1 GB.
-----------------	---

Example

The following example specifies the file size of the TCPDump file as 15MB:

```
EWC.extremenetworks.com:traffic_capture# size 15
```

interface

Use the `interface` command to specify the interface on which the exception traffic is to be captured.

interface *interfacename*

Parameters

<i>interfacename</i>	<p>The interface name on which the exception traffic is to be captured. You can choose any of the following interfaces:</p> <ul style="list-style-type: none"> • Management Port (eth0) • Physical esa ports • Defined VNS
----------------------	---

Example

The following example specifies the exception traffic to be captured on esa0:

```
EWC.extremenetworks.com:traffic_capture# interface esa0
```

delete

Use the `delete` command to delete the TCPDump file. The `delete` command is accessible from the `traffic_capture` context of the CLI.

To display the “TCPDump file capture” list, run the `list` command from the `traffic_capture` context of the CLI. For more information, see [list](#) on page 234.

delete # *from the capture file list*

Parameters

# <i>from the capture file list</i>	The sequence in which the files are listed in the capture file list
-------------------------------------	---

Example

The following example specifies the file #1 in the “TCPDump file capture” list to be deleted:

```
EWC.extremenetworks.com:traffic_capture# delete 1
```

list

Use the `list` command to display the “TCPDump file capture” list. The `list` command is accessible from the `traffic_capture` context of the CLI.

The files that are stored on the CF card have `flash` suffixed to their file names. For example, `mgmt_traffic_dump.cap (flash)`. The files that are stored on the local drive of the controller do not have anything suffixed to them.

You can save only one TCPDump file on the local drive.

list

Parameters

None

Example

The following example displays the list of TCPDump file capture:

```
EWC.extremenetworks.com:traffic_capture# list
Traffic Capture Files:
 1:mgmt_traffic_dump.cap
 2:mgmt_traffic_dump.cap (flash)
 3:mgmt_traffic_dump-01.cap (flash)
 4:mgmt_traffic_dump-02.cap (flash)
 5:dhcp-relay-01.cap (flash)
 6:third-party-01.cap (flash)
 7:mgmt_traffic_dump-03.cap (flash)
```

start

Use the `start` command to start capturing the exception traffic to and from the management plane. The capture includes the following:

- All traffic on the management port (eth0)
- Exception traffic for the physical esa ports and defined VNS

The `start` command is accessible from the `traffic_capture` context of the CLI.

start

Parameters

None

Example

The following example specifies to start capturing the exception traffic:

```
EWC.extremenetworks.com:traffic_capture# start
```

stop

Use the `stop` command to stop capturing the exception traffic to and from the management plane. The `stop` command is accessible from the `traffic_capture` context of the CLI.

stop

Parameters

None

Example

The following example specifies to stop capturing the exception traffic:

```
EWC.extremenetworks.com:traffic_capture# stop
```

show

Use the `show` command to display the configuration for capturing the exception traffic to and from the management plane. The `show` command is accessible from the `traffic_capture` context of the CLI.

show

Parameters

None

Example

The following example displays the configuration for capturing the exception traffic to and from the management plane:

```
EWC.extremenetworks.com:traffic_capture# show
Interface: esa2
Size: 30(MB).
Filename: mgmt_traffic_dump.cap
Destination: local
Capture Status: stopped
Traffic Capture Files:
    1:mgmt_traffic_dump.cap
```

show interfaces

Use the `show interfaces` command to display the physical and virtual ports for which the exception traffic can be captured. The `show interfaces` command is accessible from the `traffic_capture` context of the CLI.

```
show interfaces
```

Parameters

None

Example

The following example displays the physical and virtual ports for which the exception traffic can be captured:

```
EWC.extremenetworks.com:traffic_capture# show interfaces
eth0
esa0
esa1
esa2
esa3
CNL-208-202brAC
CNL-209-AAA
CNL-209-AAADyn
CNL-209-bri
CNL-209-briAC
CNL-209-briAC_AAA
```

17 users Commands

id
pwd

This section describes commands used to create and manage user accounts on the network. These commands are found within the users context of the CLI.

All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the users context:

- [id](#) on page 237
- [pwd](#) on page 238

id

Use the `id` command to create user or administrator accounts on the system. In conjunction with the `id` command, you must specify and confirm a password for the account. The password must be 8–24 alphanumeric characters long.

```
id userid admin|guestportal|readonly
```

Parameters

userid	Specifies a name for the account
admin	Sets account type to administrator
guestportal	Sets account type to guestportal administrator. A guest administrator user created using the guestportal user type can login to the system only via the GUI.
readonly	Sets account type to readonly

Examples

The following example creates the read-only user account “abby” on the system:

```
EWC.extremenetworks.com:users# id abby readonly
Please input password:
Please confirm password:
Successfully created user abby.
```

The following example creates the administrator account “fred” on the system:

```
EWC.extremenetworks.com:users# id fred admin
Please input password:
```

```
Please confirm password:  
Successfully created user fred.
```

The following example creates a guest administrator user account called “tester” on the system:

```
EWC.extremenetworks.com:users# id tester guestportal  
Please input password:  
Please confirm password:  
Successfully created user tester.
```

pwd

Use the `pwd` command to change the password for a specified account. The password must be 8-24 alphanumeric characters long.

```
pwd userid
```

Parameters

<i>userid</i>	Specifies the name of the account
---------------	-----------------------------------

Examples

The following example changes the password for the account named “fred”:

```
EWC.extremenetworks.com:users# pwd fred  
Please input new password:  
Please confirm new password:
```

18 VNS Commands (vnsmode)

```
adminctr
create
custom-app
das
default-role
delete
nac
netflow-mirror
radius
rateprofile
redirection-url-list
<named-VNS>
Common Filter Configuration Commands
```

This section describes commands used to define and configure Virtual Network Services (VNS) for the network. These commands are located in the `vnsmode` context of the CLI. Execute the `vnsmode` command at the root level to enter `vnsmode` context.

All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the `vnsmode` context:

- [adminctr](#) on page 240 — See for commands in the `vnsmode:adminctr` context.
- [create](#) on page 247
- [custom-app](#) on page 247
- [das](#) on page 249 — See for commands in the `vnsmode:das` context.
- [default-role](#) on page 249 — See for commands in the `vnsmode:default-role` context.
- [delete](#) on page 252
- [nac](#) on page 252 — See for commands in the `vnsmode:nac` context.
- [netflow-mirror](#) on page 254 — See for commands in the `vnsmode:netflow-mirror` context
- [radius](#) on page 255 — See for commands in the `vnsmode:radius` context.
- [rateprofile](#) on page 268 — See for commands in the `vnsmode:rateprofile` context.
- [redirection-url-list](#) on page 270
- [<named-VNS>](#) on page 271 — See for commands in the `vnsmode:<named-VNS>` context.
- [Common Filter Configuration Commands](#) on page 274

adminctr

Executing the `adminctr` command moves you into the `vnsmode:adminctr` context, in which you configure several global QoS (Quality of Service) settings. This context contains global admission control commands to configure flexible client access, egress filtering, and to control the amount of bandwidth for voice and video applications on Wireless APs.

The following commands are available in the `vnsmode:adminctr` context:

- [auto-login](#) on page 240
- [egress-filtering](#) on page 241
- [flex-client-access](#) on page 241
- [hybrid-policy](#) on page 242
- [max-video-assoc](#) on page 243
- [max-video-reassoc](#) on page 244
- [max-voice-assoc](#) on page 244
- [max-voice-reassoc](#) on page 245
- [policy-invalid-action](#) on page 245
- [rule-redirect](#) on page 245
- [tg-selection](#)
- [vlan-policy](#) on page 246

auto-login

Use the `auto-login` command to configure global client Auto-Login behavior. The `auto-login` command is accessible from the `vnsmode:adminctr` context of the CLI. Many devices such as those made by Apple implement an autologin feature that prompts the user to login as soon as the device detects the presence of a Captive Portal. These features sometimes cause problems for users who actually interact with the captive portal.

auto-login redirect | drop | hide

Parameters

redirect	Redirect detection messages to the Captive Portal. This option allows client autologin to detect the captive portal and prompt the user to login. This option may cause post-authentication redirection to fail.
drop	Drop detection messages.
hide	Hides the captive portal from Autologin detector. This is the default option. This option provides the most control over the captive portal experience.

Examples

The following example sets auto-login to drop detection messages:

```
EWC.extremenetworks.com:vnsmode:adminctr# auto-login drop
```


egress-filtering

Use the `egress-filtering` command to enable or disable egress filtering globally. The `egress-filtering` command is accessible from the `vnsmode::adminctr` context of the CLI.

egress-filtering on | off | wlan

Parameters

on	Enables global egress filtering. When egress filtering is enabled globally, it overrides individual wlan settings.
off	Disables global egress filtering. When egress filtering is disabled globally, it overrides individual wlan settings.
wlan	Enables egress filtering globally on the wlan. When this is enabled, individual wlan filtering settings override global settings.

Examples

The following example enables filtering on the wlan:

```
EWC.extremenetworks.com:vnsmode:adminctr# egress-filtering wlan
EWC.extremenetworks.com:vnsmode:adminctr# apply
EWC.extremenetworks.com:vnsmode:adminctr# show
Global Egress Filtering: wlan
```

flex-client-access

Use the `flex-client-access` command to configure flexible client access (FCA) to the wireless medium. FCA can be adjusted in multiple steps between packet fairness and airtime fairness using this command. This command is available in the `vnsmode:adminctr` context.

flex-client-access 100%-packet | mostly-packet | mixed | mostly-airtime | 100%-airtime

Parameters

100%-packet	Specifies 100% packet access to the wireless medium
mostly-packet	Specifies mostly packet access to the wireless medium
mixed	Specifies mixed access to the wireless medium
mostly-airtime	Specifies mostly airtime access to the wireless medium
100%-airtime	Specifies 100% airtime access to the wireless medium

Examples

The following example sets the FCA to 100% packet access:

```
EWC.extremenetworks.com:vnsmode:adminctr# flex-client-access 100%-packet
```

hybrid-policy

Use the `hybrid-policy` command to configure RFC 3580 options. This mode enables the controller to use both a VLAN ID in the tunnel attributes and a filter ID to select policy for a station. This command is available in the `vnsmode:adminctr` context.

hybrid-policy policy | vlan | combined

Parameters

policy	Specifies that the VLAN tunnel ID is ignored; use the topology assigned by the policy.
vlan	Specifies that the policy used for the station is based on the VLAN tunnel ID. The filter ID is ignored.
combined	Specifies that the policy identified in the filter ID and the topology associated with the VLAN tunnel ID are used.

Examples

The following example sets the hybrid policy to combined:

```
EWC.extremenetworks.com:vnsmode:adminctr# hybrid-policy combined
```

max-beffort-assoc

Use the `max-beffort-assoc` command to set the Maximum Best Effort (BE) BW for new streams in percent of total. The `max-beffort-assoc` command is accessible from the `vnsmode:adminctr` context of the CLI.

max-beffort-assoc 0 - 100

Parameters

0 - 100	Specifies the percentage configured for the Maximum Best Effort (BE) BW for new streams.
----------------	--

Examples

The following example sets the Maximum Best Effort (BE) BW for new streams to 50 percent:

```
EWC.extremenetworks.com:vnsmode:adminctr# max-beffort-assoc 50
```

max-beffort-reassoc

Use the `max-beffort-reassoc` command to set the Maximum Best Effort (BE) BW for roaming streams in percent of total. The `max-beffort-reassoc` command is accessible from the `vnsmode:adminctr` context of the CLI.

max-beffort-reassoc 0 - 100

Parameters

0 - 100	Specifies the percentage configured for the Maximum Best Effort (BE) BW for roaming streams.
----------------	--

Examples

The following example sets the Maximum Best Effort (BE) BW for roaming streams to 50 percent:

```
EWC.extremenetworks.com:vnsmode:adminctr# max-beffort-reassoc 50
```

max-bground-assoc

Use the `max-bground-assoc` command to set the Maximum Background (BK) BW for new streams in percent of total. The `max-bground-assoc` command is accessible from the `vnsmode:adminctr` context of the CLI.

```
max-bground-assoc 0 - 100
```

Parameters

<code>0 - 100</code>	Specifies the percentage configured for the Maximum Background (BK) BW for new streams.
----------------------	---

Examples

The following example sets the Maximum Background (BK) BW for new streams to 50 percent:

```
EWC.extremenetworks.com:vnsmode:adminctr# max-bground-assoc 50
```

max-bground-reassoc

Use the `max-bground-reassoc` command to set the Maximum Background (BK) BW for roaming streams in percent of total. The `max-bground-reassoc` command is accessible from the `vnsmode:adminctr` context of the CLI.

```
max-bground-reassoc 0 - 100
```

Parameters

<code>0 - 100</code>	Specifies the percentage configured for the Maximum Background (BK) BW for roaming streams.
----------------------	---

Examples

The following example sets the Maximum Background (BK) BW for roaming streams to 50 percent:

```
EWC.extremenetworks.com:vnsmode:adminctr# max-bground-reassoc 50
```

max-video-assoc

Use the `max-video-assoc` command to configure the maximum allowed overall bandwidth on an AP when an already associated client requests admission for a new video stream.

After you run the `max-video-assoc` command, run the `apply` command to implement the changes.

```
max-video-assoc 0-100
```

Parameters

<i>0-100</i>	Specifies the maximum allowable bandwidth as a percentage of total bandwidth.
--------------	---

Examples

The following example sets the maximum video bandwidth for new streams to 40% of total bandwidth:

```
EWC.extremenetworks.com:vnsmode:adminctr# max-video-assoc 40
```

max-video-reassoc

Use the `max-video-reassoc` command to set the maximum allowed overall bandwidth on the new AP when a client with an active video stream roams to a new AP and requests admission for the video stream.

After you run the `max-video-reassoc` command, run the `apply` command to implement the changes.

```
max-video-reassoc 0-100
```

Parameters

<i>0-100</i>	Specifies the maximum allowable bandwidth as a percentage of total bandwidth.
--------------	---

Examples

The following example sets the maximum video bandwidth for roaming streams to 60% of total bandwidth:

```
EWC.extremenetworks.com:vnsmode:adminctr# max-video-reassoc 60
```

max-voice-assoc

Use the `max_voice_assoc` command to set the maximum allowed overall bandwidth on an AP when an already associated client requests admission for a new voice stream.

After you run the `max-voice-assoc` command, run the `apply` command to implement the changes.

```
max-voice-assoc 0-100
```

Parameters

<i>0-100</i>	Specifies the maximum allowable bandwidth as a percentage of total bandwidth.
--------------	---

Example

The following example sets the maximum voice bandwidth for new streams to 60% of total bandwidth:

```
EWC.extremenetworks.com:vnsmode:adminctr# max-voice-assoc 60
```

max-voice-reassoc

Use the `max-voice-reassoc` command to set the maximum allowed overall bandwidth on the new AP when a client with an active voice stream roams to a new AP and requests admission for the voice stream.

After you run the `max-voice-reassoc` command, run the `apply` command to implement the changes.

max-voice-reassoc 0-100

Parameters

<code>0-100</code>	Specifies the maximum allowable bandwidth as a percentage of total bandwidth.
--------------------	---

Examples

The following example sets the maximum voice bandwidth for roaming streams to 80%:

```
EWC.extremenetworks.com:vnsmode:adminctr# max-voice-reassoc 80
```

policy-invalid-action

Use the `policy-invalid-action` command to configure the global invalid policy action. The `policy-invalid-action` command is accessible from the `vnsmode:adminctr` context of the CLI.

policy-invalid-action default | allow | deny

Parameters

default	Sets the global invalid policy action to the default.
allow	Sets the global invalid policy action to allow an invalid policy.
deny	Sets the global invalid policy action to deny an invalid policy.

Examples

The following example sets `policy-invalid-action` behavior to deny:

```
EWC.extremenetworks.com:vnsmode:adminctr# policy-invalid-action deny
```



rule-redirect

Use the `rule-redirect` command to enable or disable policy rule-based redirection. The `rule-redirect` command is accessible from within the `root: vnsmode:adminctr` context.

rule-redirect enable | disable

Parameters

enable	Enables policy rule-based redirection for ExtremeWireless versions prior to v10.11. Policy rule-based redirection is enabled for ExtremeWireless v10.11 by default. For installations coming from an upgrade, enable rule-redirect.
disable	Disables policy rule-based redirection. Policy rule-based redirection is enabled for ExtremeWireless v10.11 by default.

Usage

Enable rule-redirect from the adminctr context before issuing other redirection commands. When this command is enabled, the redirection URL list is available from the VNS screen. For ExtremeWireless v10.11 and later, rule-based redirection is enabled by default. Enable rule-based redirection in ExtremeWireless release versions prior to v10.11 using the `rule-redirect` command.

Examples

```
EWC.extremenetworks.com:vnsmode:adminctr# rule-redirect enable
```

```
EWC.extremenetworks.com:vnsmode:adminctr# apply
```

Exit adminctr and refresh vnsmode before issuing the redirection url commands.

Related Links

[redirection-url](#) on page 378

[redirection-url-list](#) on page 270

tg-selection

Use the `tg-selection` command to configure the topology group selection algorithm. The `tg-selection` command is accessible from the `vnsmode:adminctr` context of the CLI.

```
tg-selection (round-robin | mac | random | least)
```

Parameters

round-robin	Specifies that the round-robin topology group selection algorithm is used.
mac	Specifies that the mac topology group selection algorithm is used.
random	Specifies that the random topology group selection algorithm is used.
least	Specifies that the least topology group selection algorithm is used.

Examples

The following example sets the topology group selection algorithm to random:

```
EWC.extremenetworks.com:vnsmode:adminctr# tg-selection random
```

vlan-policy

Use the `vlan-policy` command to map a VLAN ID to a policy.

After you run the `vlan-policy` command, run the `apply` command to implement the changes.

```
vlan-policy (add|update vlan-id policy name) | (remove vlan-id)
```

Parameters

add update	Adds or updates the mapping of the specified <code>vlan-id</code> to the specified policy.
remove	Removes the <code>vlan-id</code> mapping from the policy.
<i>vlan-id</i>	Specifies a VLAN to map to or remove from the specified policy.
<i>policy name</i>	Specifies a policy to which a VLAN is mapped.

Examples

The following example updates the VLAN mapping (`vlan-id 102`) to the `test2` policy:

```
EWC.extremenetworks.com:vnsmode:adminctr# vlan-policy update 102 test2
```

create

Use the `create` command to create a new VNS. This command is available in the `vnsmode` context. After you create a VNS with this command, you can configure additional parameters in the `vnsmode:<named-VNS>` context. Refer to [<named-VNS>](#) on page 271 for more information.

After you run the `create` command, run the `apply` command to implement the changes.

```
create vns name wlans WLANS name pol role-name
```

Parameters

<i>vns name</i>	Specifies a name for this VNS
wlans <i>WLANS name</i>	Specifies a WLAN Service for this VNS
pol <i>role-name</i>	Specifies the non-authentication role for this VNS

Usage

When you create a VNS, if the referenced WLAN Service has a mode of:

- “std” then the referenced role must have a topology of mode “b@ap,” “b@ac,” or “routed”
- “3pap” then the referenced role must have a physical topology mode
- “wds” then the referenced role must have a null topology

Example

The following example creates a VNS named `testvns` and assigns it a WLAN Service named “EWC-1” and a role named “NonAuth”:

```
EWC.extremenetworks.com:vnsmode# create testvns wlans EWC-1 pol NonAuth
```



custom-app

Executing the `custom-app` command moves you into the `vnsmode:custom-app` context where you configure the custom-app-list.

Related Links

[custom-app-list](#) on page 248

custom-app-list

Use the `custom-app-list` command to configure a custom application list for ExtremeWireless application visibility. The custom application list includes the application name, group, and matching pattern. The `custom-app-list` command is accessible from within the root: `vnsmode: custom-app` context.

```
custom-app-list (add [group group name name app name pattern matching pattern]* |
delete [sequence id]* | [name]*)
```

Parameters

add	Add a custom application to the list of possible applications available for ExtremeWireless application visibility.
delete	Remove a custom application from the list of possible applications available for ExtremeWireless application visibility.
<i>group group name</i>	Indicates the name of the group name to which the custom application belongs. For more information, see Usage on page 248.
<i>name app name</i>	Indicates the name of the custom application.
<i>pattern matching pattern</i>	Indicates the matching pattern for the custom application. Pattern matching is an element of deep packet inspection used as part of network security.
<i>sequence id</i>	Identifies the sequence of the APP in the database.

Usage

The `custom-app-list` command is issued from the custom-app context.

The group names are pre-defined standard Extreme Application Analytics™ signature groups. The group names are case-sensitive.

To see a list of pre-defined group names, see [show app group](#).

Examples

```
EWC.extremenetworks.com:vnsmode:custom-app# custom-app-list add group
Advertising name Letv pattern letv.com
```

Related Links

[show app \(Application Group\)](#) on page 56

[custom-app](#) on page 247

das

Use the `das` command to configure DAS (Dynamic Authorization Server) settings. Executing the `das` command puts you in the `vnsmode:das` context where the following commands are available.

The following commands are available in the `vnsmode:das` context:

- `port` on page 249
- `replay_interval` on page 249

port

Use the `port` command to configure the DAS port. The `port` command is available from the `vnsmode:das` context.

```
port 1024-65535
```

Parameters

1024-65535	Specifies the DAS port.
------------	-------------------------

Examples

The following example sets the DAS port number to 3799:

```
EWC.extremenetworks.com:vnsmode:das# port 3799
```

replay_interval

Use the `replay_interval` command to configure the DAS replay interval, measured in seconds. The `replay_interval` command is available from the `vnsmode:das` context.

```
replay_interval 0-1000
```

Parameters

0-1000	Specifies the DAS replay interval, measured in seconds.
--------	---

Examples

The following example sets the DAS replay interval to 60 seconds:

```
EWC.extremenetworks.com:vnsmode:das# replay_interval 60
```

default-role

The `default-role` command moves you into the `vnsmode:default-role` context. The `default-role` replaces the former `default-policy` of previous releases. The `vnsmode:default-role` context provides commands for the configuration of the `default-role`.

The default-role definitions provide a placeholder for completion of incomplete (no-change) roles (policies) for the VNS being configured. Refer to [role Commands](#) on page 368 for a complete discussion of role commands.

The default-role specifies:

- A topology to use when a VNS is created using a role (non-auth role) that does not specify a topology. The default assigned topology is the Bridge Traffic Locally at AP topology.
- An inbound and outbound rate control profile. The default rate control profile is “Unlimited”.
- A set of filters. The default filter set is a single deny all rule.

After you complete configuration changes for the default-role, run the `apply` command before exiting the `vnsmode:default-role` context to implement the changes.

The following commands are available in the `vnsmode:default-role` context:

- [show](#) on page 250
- [sync](#) on page 250
- [topology-name](#) on page 251
- [acfilters](#) on page 251 — See for commands in the `vnsmode:default-role:acfilters` context.
- [apfilters](#) on page 252 — See for commands in the `vnsmode:default-role:apfilters` context.

show

Use the `show` command to display the default-role configuration information for the current `vnsmode:default-role` context. The `show` command is accessible from within the `vnsmode:default-role` context.

show

Parameters

None.

Examples

The following example displays the default-role configuration from within the `vnsmode:default-role` context:

```
EWC.extremenetworks.com:vnsmode:default-role# show
Assigned topology: Bridged at AP untagged
Ingress rate profile: Unlimited
Egress rate profile: Unlimited
Enable AP filtering: enable
Synchronize: disable
EWC.extremenetworks.com:vnsmode:default-role#
```

sync

Use the `sync` command to enable or disable automatic synchronization of the default-role across paired controllers. Refer to the *Wireless User Guide* for more information about synchronization of policies.

The `sync` command is accessible from within the `vnsmode:default-role` context.

sync {enable | disable}

Parameters

enable disable	Enables or disables synchronization of the default-role across controllers.
-------------------------	---

Examples

The following example enables the synchronization of the default-role across controllers:

```
EWC.extremenetworks.com:vnsmode:default-role# sync enable
EWC.extremenetworks.com:vnsmode:default-role# apply
EWC.extremenetworks.com:vnsmode:default-role# show
Assigned topology: Bridged at AP untagged
Ingress rate profile: Unlimited
Egress rate profile: Unlimited
Enable AP filtering: disable
Synchronize: enable
EWC.extremenetworks.com:vnsmode:default-role#
```

topology-name

Use the `topology-name` command to associate an already existing topology with a role. The `topology-name` command is accessible from the `vnsmode:default-role` context.

topology-name *topology*

Parameters

<i>topology</i>	Specifies the name of the topology to configure for this <code>vnsmode:default-role</code> context.
-----------------	---

Usage

Refer to [VNS Commands \(vnsmode\)](#) on page 239 for information on configuring topologies.

Examples

The following example configures the default-role with the `guestPortal` topology:

```
EWC.extremenetworks.com:vnsmode:default-role# topology-name guestPortal
EWC.extremenetworks.com:vnsmode:default-role# apply
EWC.extremenetworks.com:vnsmode:default-role# show
Assigned topology: guestPortal
Ingress rate profile: Unlimited
Egress rate profile: Unlimited
Enable AP filtering: disable
Synchronize: enable
EWC.extremenetworks.com:vnsmode:default-role#
```

acfilters

Use the `acfilters` command to enter the `vnsmode:default-role:acfilters` context for the configuring of default-role AC filters. The `acfilters` command is accessible from within the `vnsmode:default-role` context.

AC filter rules are applied at the controller. Default-role AC filter configuration is applied when no AC filters are configured for role applied at the controller. AC filtering is not available when the associated topology is configured for Bridge at AP. AC filtering is available when the associated topology is set to either Bridge at AC or Routed.

The following commands are available in the `vnsmode:default-role:acfilters` context:

- [create](#) on page 274
- [config](#) on page 278
- [delete](#) on page 280
- [move](#) on page 281

apfilters

Use the `apfilters` command to enter the `vnsmode:default-role:apfilters` context for the configuring of AP custom filters. AP custom filters are applied at the AP. Default-role AP custom filters are applied when no AP custom filters are configured for role applied at the AP. The `apfilters` command is accessible from the `vnsmode:default-role` context.

This command is not visible in the CLI if you execute the `apcustom disable` command.

The following commands are available in the `vnsmode:default-role:apfilters` context:

- [create](#) on page 274
- [config](#) on page 278
- [delete](#) on page 280
- [move](#) on page 281

delete

Use the `delete` command in `vnsmode` to delete an existing VNS.

```
delete VNS name
```

Parameters

<i>VNS name</i>	Specifies the VNS to delete.
-----------------	------------------------------

Examples

The following example deletes the VNS named `guestportal`:

```
EWC.extremenetworks.com:vnsmode:delete guestportal
```

nac

Executing the `nac` command moves you into the `vnsmode:nac` context, which contains the following commands to manage NAC configuration.

The following commands are available in the vnsmode:nac context:

- [create](#) on page 253
- [delete](#) on page 253
- [show](#) on page 254

create

Use the `create` command to create an NAC server configuration. The NAC server accepts DHCP messages. The `create` command is accessible from the vnsmode:nac context of the CLI. After you create an NAC server configuration, you can further configure it by entering the vnsmode:nac:<named-NAC-server> context. See [radius](#) on page 255.

create *name* *A.B.C.D*

Parameters

<i>name</i>	Specifies the name of the NAC server
<i>A.B.C.D</i>	Specifies the IP address of the NAC server

Usage

Up to three NAC server configurations can be created.

Examples

The following example creates and then displays the details of an NAC server configuration named test-nac-server with an IP address of 10.10.10.11:

```
EWC.extremenetworks.com:vnsmode:nac# create test-nac-server 10.10.10.11
EWC.extremenetworks.com:vnsmode:nac# test-nac-server
EWC.extremenetworks.com:vnsmode:nac:test-nac-server# show
```

delete

Use the `delete` command to delete an NAC server configuration. The `delete` command is accessible from the vnsmode:nac context of the CLI.

delete *NAC_server*

Parameters

<i>NAC_server</i>	Specifies the name of the NAC server to delete
-------------------	--

Examples

The following example deletes the NAC server named test-nac-server:

```
EWC.extremenetworks.com:vnsmode:nac# delete test-nac-server
```

show

Use the `show` command to display NAC server configuration information. The `show` command is accessible from the `vnsmode:nac` context of the CLI.

show [*NAC_server*]

Parameters

<i>NAC_server</i>	Specifies to display information about the specific NAC server
-------------------	--

Examples

The following example displays a list of NAC server configuration information:

```
EWC.extremenetworks.com:vnsmode:nac# show
NAC Name  IP Address
test1     192.168.3.11
```

netflow-mirror

The `netflow-mirror` command moves you into the `vnsmode:netflow-mirror` context, which contains commands to configure NetFlow Mirror. The `netflow-mirror` command is accessible from the `vnsmode` context of the CLI.

The following commands are available in the `vnsmode:netflow-mirror` context.

- [netflow-export-dest](#) on page 254
- [netflow-export-interval](#) on page 254
- [traffic-mirror-firstn](#) on page 255

netflow-export-dest

Use the `netflow-export-dest` command to configure the IP address that receives the NetFlow records. The `netflow-export-dest` command is accessible from the `vnsmode:netflow-mirror` context of the CLI.

netflow-export-dest *ip-address*

Parameters

<i>ip-address</i>	Specifies the IP address that receives the NetFlow records.
-------------------	---

Example

The following example sets the NetFlow export IP destination address to 1.1.1.1:

```
EWC.extremenetworks.com:vnsmode:netflow-mirror# netflow-export-dest 1.1.1.1
```

netflow-export-interval

Use the `netflow-export-interval` command to set the NetFlow export interval. The `netflow-export-interval` command is accessible from the `vnsmode:netflow-mirror` context of the CLI.

netflow-export-interval *seconds*

Parameters

<i>seconds</i>	Specifies the NetFlow export interval in seconds from 30 - 360. The default is 60 seconds.
----------------	--

Example

The following example sets the NetFlow export interval to 50 seconds:

```
EWC.extremenetworks.com:vnsmode:netflow-mirror# netflow-export-interval 50
```

traffic-mirror-firstn

Use the `traffic-mirror-firstn` command to configure the MirrorN first N packets. The `traffic-mirror-firstn` command is accessible from the `vnsmode:netflow-mirror` context of the CLI.

traffic-mirror-firstn *packets*

Parameters

<i>packets</i>	Specifies the MirrorN first N packets from 1 - 31. The default is 15 packets.
----------------	---

Example

The following example sets the MirrorN first N packets to 20 packets:

```
EWC.extremenetworks.com:vnsmode:netflow-mirror# traffic-mirror-firstn 20
```

traffic-mirror-l2port

Use the `traffic-mirror-l2port` command to set the traffic mirror L2 port. The `traffic-mirror-l2port` command is accessible from the `vnsmode:netflow-mirror` context of the CLI.

traffic-mirror-l2port (**none** | **esa0** | **esa1**)

Parameters

none esa0 esa1	Configures the L2 mirror port and the controller to none, esa0, or esa1.
---	--

Example

The following example sets the mirror L2 port to esa0:

```
EWC.extremenetworks.com:vnsmode:netflow-mirror# traffic-mirror-l2port esa0
```

radius

Executing the `radius` command moves you into the `vnsmode:radius` context, which contains the following commands to manage RADIUS server configuration. After you create a radius server configuration, you can further configure it by entering the `vnsmode:radius:<server-name>` context. See [<named_RADIUS_server>](#) on page 261.

The following commands are available in the vnsmode:radius context:

- [create](#) on page 256
- [defer-acct-start](#) on page 257
- [delay-client-msg](#) on page 257
- [delete](#) on page 257
- [include-service-type](#) on page 258
- [show](#) on page 258
- [radius-accounting](#) on page 259
- [radius-mac-format](#) on page 259
- [rename](#) on page 260
- [service-type-login](#) on page 260
- [strict](#) on page 261
- [usage-mode](#) on page 261
- [<named_RADIUS_server>](#) on page 261 — See for commands in the vnsmode:radius:<server-name> context.

create

Use the `create` command to create a RADIUS server configuration. The `create` command is accessible from the vnsmode:radius context of the CLI.

```
create name A.B.C.D secret
```

Parameters

<i>name</i>	Specifies the name of the RADIUS server
<i>A.B.C.D</i>	Specifies the IP address of the RADIUS server
<i>secret</i>	Specifies the shared secret for the RADIUS server

Examples

The following example creates and then displays the details of a RADIUS server configuration named test-radius-server with an IP address of 10.10.10.10 and a shared secret of “test”:

```
EWC.extremenetworks.com:vnsmode:radius# create test-radius-server 10.10.10.10
test
EWC.extremenetworks.com:vnsmode:radius# test-radius-server
EWC.extremenetworks.com:vnsmode:radius:test-radius-server# show
Authentication port: 1812
Accounting port: 1813
Authentication priority: 5
Accounting priority: 5
Authentication total number of tries: 3
Accounting total number of tries: 3
Authentication RADIUS request timeout: 5
Accounting RADIUS request timeout: 5
Interim accounting interval: 0
Default protocol: PAP
Shared secret: ****
Name: test-radius-server
```


defer-acct-start

Use the `defer-acct-start` command to enable or disable deferring sending the accounting start request until the client's IP address is known. The `defer-acct-start` command is accessible from the `vnsmode:radius` context of the CLI.

The global setting of Radius Accounting must be enabled prior to using this command. Defer accounting start is disabled by default.

defer-acct-start (**enable** | **disable**)

Parameters

enable	Enables the defer accounting start feature.
disable	Disables the defer accounting start feature.

Examples

The following example enables defer accounting start:

```
EWC.extremenetworks.com:vnsmode:radius# defer-acct-start enable
```

delay-client-msg

Use the `delay-client-msg` command to set the delay, in seconds, for the client message that displays if a topology change occurs during authentication. The `delay-client-msg` command is accessible from the `vnsmode:radius` context of the CLI.

delay-client-msg *1-60*

Parameters

<i>1-60</i>	The time, in seconds, that the client message displays if a topology change occurs during authentication.
-------------	---

Examples

The following example sets the delay to 40 seconds:

```
EWC.extremenetworks.com:vnsmode:radius# delay-client-msg 40
```

delete

Use the `delete` command to delete a RADIUS server configuration. The `delete` command is accessible from the `vnsmode:radius` context of the CLI.

delete *RADIUS_server*

Parameters

<i>RADIUS_server</i>	Specifies the name of the RADIUS server to delete
----------------------	---

Examples

The following example deletes the RADIUS server named test-radius-server:

```
EWC.extremenetworks.com:vnsmode:radius# delete test-radius-server
```

include-service-type

Use the `include-service-type` command to include or exclude the Service-Type attribute in the client Access-Request message. The `include-service-type` command is accessible from the `vnsmode:radius` context of the CLI.

include-service-type enable|disable

Parameters

enable	Include the Service-Type attribute in the client Access-Request message.
disable	Exclude the Service-Type attribute from the client Access-Request message.

Examples

```
EWC.extremenetworks.com:vnsmode:radius# include-service-type enable
```

show

Use the `show` command to display RADIUS server configuration information. The `show` command is accessible from the `vnsmode:radius` context of the CLI.

show [RADIUS_server]

Parameters

RADIUS_server	Specifies to display information about the specific RADIUS server
----------------------	---

Examples

The following example displays a list of RADIUS server configuration information:

```
EWC.extremenetworks.com:vnsmode:radius# show
Strict: disable
Radius MAC format: 1. XXXXXXXXXXXXX
Client Access-Request includes Service-Type Attribute: disable
Name      IP address  Protocol  Retries(Auth:Acct)  Timeout(Auth:Acct)
Ports(Auth:Acct)  Priority(Auth:Acct)
RADIUS_1  192.0.1.202  PAP       3:3                 5:5
1812:1813          1:1
```

The following example displays configuration information for the RADIUS server named "RADIUS_1":

```
EWC.extremenetworks.com:vnsmode:radius# show RADIUS_1
Authentication port: 1812
Accounting port: 1813
Authentication priority: 1
Accounting priority: 1
```

```

Authentication total number of tries: 3
Accounting total number of tries: 3
Authentication RADIUS request timeout: 5
Accounting RADIUS request timeout: 5
Interim accounting interval: 30
Default protocol: PAP
Shared secret: *****
Name: RADIUS_1
Radius IP: 192.0.1.202

```

radius-accounting

Use the `radius-accounting` command to enable or disable RADIUS accounting. The `radius-accounting` command is accessible from the `vnsmode:radius` context of the CLI.

radius-accounting (enable | disable)

Parameters

enable	Enables RADIUS accounting.
disable	Disables RADIUS accounting.

Examples

The following example enables RADIUS accounting:

```
EWC.extremenetworks.com:vnsmode:radius# radius-accounting enable
```

radius-mac-format

Use the `radius-mac-format` command to set the MAC address format to be exchanged with the RADIUS server. The `radius-mac-format` command is accessible from the `vnsmode:radius` context of the CLI.

After you run the `radius-mac-format` command, run the `apply` command to implement the changes.

radius-mac-format 1-12

Parameters

1	Specifies a MAC address format of XXXXXXXXXXXX for use with the RADIUS server
2	Specifies a MAC address format of XX:XX:XX:XX:XX:XX for use with the RADIUS server
3	Specifies a MAC address format of XX-XX-XX-XX-XX-XX for use with the RADIUS server
4	Specifies a MAC address format of XXXX.XXXX.XXXX for use with the RADIUS server
5	Specifies a MAC address format of XXXXXX-XXXXXX for use with the RADIUS server
6	Specifies a MAC address format of XX XX XX XX XX XX for use with the RADIUS server

7	Specifies a MAC address format of xxxxxxxxxxxx for use with the RADIUS server
8	Specifies a MAC address format of xx:xx:xx:xx:xx:xx for use with the RADIUS server
9	Specifies a MAC address format of xx-xx-xx-xx-xx-xx for use with the RADIUS server
10	Specifies a MAC address format of xxxx.xxxx.xxxx for use with the RADIUS server
11	Specifies a MAC address format of xxxxxx-xxxxxx for use with the RADIUS server
12	Specifies a MAC address format of xx xx xx xx xx xx for use with the RADIUS server

Examples

The following example sets the RADIUS MAC address format to XX:XX:XX:XX:XX:XX:

```
EWC.extremenetworks.com:vnsmode:radius# radius-mac-format 2
```

rename

Use the `rename` command to rename the RADIUS server. The `rename` command is accessible from the `vnsmode:radius` context of the CLI.

```
rename radius-name new-name radius-name
```

Parameters

<i>radius-name</i>	Specifies the existing name of the RADIUS server.
new-name	Identifies that the following characters are to be the new name for the RADIUS server.
<i>radius-name</i>	Specifies the new name of the RADIUS server.

Examples

The following example renames the RADIUS server ADV to IAV:

```
EWC.extremenetworks.com:vnsmode:radius# rename ADV new-name IAV
```

service-type-login

Use the `service-type-login` command to enable or disable setting the service type attribute to login. The `service-type-login` command is accessible from the `vnsmode:radius` context of the CLI.

```
service-type-login (enable | disable)
```

Parameters

enable	Enables the defer accounting start feature.
disable	Disables the defer accounting start feature.

Usage

This command allows you to optionally set the RADIUS Access-Request and Accounting-Request Service-Type attribute to Login. The default service type is Framed. Setting the Service-Type to Login

conflicts with the controller administrative RADIUS login since the administrative login also sets the Service-Type to Login. If administrative RADIUS login is enabled, Service-Type set to Login will be blocked and vice versa.

Examples

The following example enables service type to login:

```
EWC.extremenetworks.com:vnsmode:radius# service-type-login enable
```

strict

Use this command to enable or disable the ability to change RADIUS server settings per WLAN Service. This command is available from the vnsmode:radius context.

strict (**enable** | **disable**)

Parameters

enable	Enables changing RADIUS server settings per WLAN Service.
disable	Disables changing RADIUS server settings per WLAN Service.

Examples

This example disables changing RADIUS server settings per WLAN Service:

```
EWC.extremenetworks.com:vnsmode:radius# strict disable
```

usage-mode

Use this command to configure the RADIUS server usage mode. This command is available from the vnsmode:radius context.

usage-mode (**exclusive** | **primary-backup**)

Parameters

exclusive	Sets the RADIUS server usage mode to exclusive.
primary-backup	Sets the RADIUS server usage mode to primary-backup.

Examples

This example sets the RADIUS server usage mode to primary-backup:

```
EWC.extremenetworks.com:vnsmode:radius# usage-mode primary-backup
```

<named_RADIUS_server>

The <named_RADIUS_server> command, where <named_RADIUS_server> refers to the name of a given RADIUS server, is available in the vnsmode:radius context. When executed, it moves you into the vnsmode:radius:<named_RADIUS_server> context, which contains commands to configure the settings of the specified individual RADIUS server.

The following commands are available in the `vnsmode:radius:<named_RADIUS_server>` context:

- [acct-port](#) on page 262
- [acct-prio](#) on page 262
- [acct-retries](#) on page 263
- [acct-timeout](#) on page 263
- [auth-port](#) on page 263
- [auth-prio](#) on page 264
- [auth-retries](#) on page 264
- [auth-timeout](#) on page 264
- [fast-failover](#) on page 265
- [interim](#) on page 265
- [ip](#) on page 266
- [name](#) on page 266
- [polling-interval](#) on page 266
- [polling-mechanism](#) on page 267
- [protocol](#) on page 267
- [shared-secret](#) on page 267

acct-port

Use the `acct-port` command to set the port for RADIUS accounting. The `acct-port` command is accessible from the `vnsmode:radius:<named_RADIUS_server>` context of the CLI.

If you do not change the port with this command, the default port 1813 is used.

acct-port *0-65535*

Parameters

<i>0-65535</i>	Specifies the RADIUS accounting port
----------------	--------------------------------------

Example

The following example sets the RADIUS accounting port to 1646 for the RADIUS server named RAD1:

```
EWC.extremenetworks.com:vnsmode:radius:RAD1# acct-port 1646
```

acct-prio

Use the `acct-prio` command to set the priority for RADIUS accounting. The `acct-prio` command is accessible from the `vnsmode:radius:<named_RADIUS_server>` context of the CLI.

acct-prio *integer*

Parameters

<i>integer</i>	Specifies the RADIUS accounting priority. Possible values can be any integer 0 or greater.
----------------	--

Example

The following example sets the RADIUS accounting priority to 12 for the RADIUS server named RAD1:

```
EWC.extremenetworks.com:vnsmode:radius:RAD1# acct-prio 12
```

acct-retries

Use the `acct-retries` command to set the the total number of RADIUS accounting attempts. The `acct-retries` command is accessible from the `vnsmode:radius: <named_RADIUS_server>` context of the CLI.

acct-retries 1-32

Parameters

1-32	Specifies the total number of RADIUS accounting attempts.
------	---

Examples

The following example sets the number of RADIUS accounting retries to 5 for the RADIUS server named RAD1:

```
EWC.extremenetworks.com:vnsmode:radius:RAD1# acct-retries 5
```

acct-timeout

Use the `acct-timeout` command to set the timeout for RADIUS accounting. The `acct-timeout` command is accessible from the `vnsmode:radius:<named_RADIUS_server>` context of the CLI.

acct-timeout 1-360

Parameters

1-360	Specifies the RADIUS accounting timeout in seconds.
-------	---

Examples

The following example sets the RADIUS accounting timeout to 10 seconds for the RADIUS server named RAD1:

```
EWC.extremenetworks.com:vnsmode:radius:RAD1# acct-timeout 10
```

auth-port

Use the `auth-port` command to set the priority for RADIUS authentication. The `auth-port` command is accessible from the `vnsmode:radius:<named_RADIUS_server>` context of the CLI. If you do not change the authentication port number with this command, the controller uses the default port 1812.

auth-port 0-65535

Parameters

0-65535	Specifies the RADIUS authentication port.
---------	---

Examples

The following example sets the port for RADIUS authentication to port 1816 for the RADIUS server named RAD1:

```
EWC.extremenetworks.com:vnsmode:radius:RAD1# auth-port 1816
```

auth-prio

Use the `auth-prio` command to set the priority for RADIUS authentication. The `auth-prio` command is accessible from the `vnsmode:radius:<named_ RADIUS_server>` context of the CLI.

auth-prio *integer*

Parameters

<i>integer</i>	Specifies the RADIUS authentication priority. Possible values can be any integer 0 or greater.
----------------	--

Examples

The following example sets the RADIUS authentication priority to 5 for the RADIUS server named RAD1:

```
EWC.extremenetworks.com:vnsmode:radius:RAD1# auth-prio 5
```

auth-retries

Use the `auth-retries` command to set the the total number of RADIUS authentication attempts. The `auth-retries` command is accessible from the `vnsmode:radius: <named_ RADIUS_server>` context of the CLI.

auth-retries *1-32*

Parameters

<i>1-32</i>	Specifies the total number of RADIUS authentication attempts.
-------------	---

Examples

The following example sets the number of RADIUS authentication attempts to 5 for the RADIUS server named RAD1:

```
EWC.extremenetworks.com:vnsmode:radius:RAD1# auth-retries 5
```

auth-timeout

Use the `auth-timeout` command to set the timeout for RADIUS authentication. The `auth-timeout` command is accessible from the `vnsmode:radius:<named_ RADIUS_server>` context of the CLI.

auth-timeout *1-360*

Parameters

<i>1-360</i>	Specifies the RADIUS authentication timeout in seconds.
--------------	---

Examples

The following example sets the RADIUS authentication timeout to 10 seconds for the RADIUS server named RAD1:

```
EWC.extremenetworks.com:vnsmode:radius:RAD1# auth-timeout 10
```

fast-failover

Use the `fast-failover` command in the `vnsmode:<named-VNS>` context to enable or disable the sending of interim account records (to the RADIUS server) when a failover occurs and the session home moves to the availability partner.

After you run the `fast-failover` command, run the `apply` command to implement the changes.

fast-failover (**enable** | **disable**)

Parameters

enable	Enables the sending of interim account records to RADIUS for fast failover.
disable	Disables the sending of interim account records to RADIUS for fast failover.

Usage

This command is available only when this controller has been enabled for fast-failover (see the `wlans:<WLAN-service-name>:auth` RADIUS server configuration context [fast-failover](#) on page 306 command).

Examples

This example disables fast failover:

```
EWC.extremenetworks.com:vnsmode:VNS1# fast-failover disable
EWC.extremenetworks.com:vnsmode:VNS1# apply
```

interim

Use the `interim` command to set the RADIUS interim accounting interval. The `interim` command is accessible from the `vnsmode:radius:<named_RADIUS_server>` context of the CLI.

interim *0-360*

Parameters

<i>0-360</i>	Specifies the RADIUS interim accounting interval in seconds.
--------------	--

Examples

The following example sets the RADIUS interim accounting interval to 10 seconds for the RADIUS server named RAD1:

```
EWC.extremenetworks.com:vnsmode:radius:RAD1# interim 10
```

ip

Use the `ip` command to configure the RADIUS server's IP address or FQDN (Fully Qualified Domain Name). The `ip` command is accessible from the `vnsmode:radius:<named_RADIUS_server>` context of the CLI.

ip *A.B.C.D*

Parameters

<i>A.B.C.D</i>	Specifies the IP address of the RADIUS server in dotted decimal notation.
----------------	---

Examples

The following example sets the IP address of the IAS RADIUS server to 222.224.1.23:

```
EWC.extremenetworks.com:vnsmode:radius:RAD1# ip 222.224.1.23
```

name

Use the `name` command to modify the RADIUS server name. The `name` command is accessible from the `vnsmode:radius:<named_RADIUS_server>` context of the CLI.

name *new_RADIUS_server_name*

Parameters

<i>new_RADIUS_server_name</i>	Specifies the name of the RADIUS server.
-------------------------------	--

Examples

The following example renames the RADIUS server RAD1 to RAD2:

```
EWC.extremenetworks.com:vnsmode:radius:RAD1# name RAD2
EWC.extremenetworks.com:vnsmode:radius:RAD1# show name
Name: RAD2
```

polling-interval

Use this command to configure the RADIUS test request timeout. This command is available from the `vnsmode:radius:<named_RADIUS_server>` context.

polling-interval (*30 - 300*)

Parameters

none

Examples

This example sets the RADIUS server polling-interval to 43:

```
EWC.extremenetworks.com:vnsmode:radius:<named_RADIUS_server># polling-
interval 43
```

polling-mechanism

Use this command to configure the RADIUS server polling mechanism. This command is available from the vnsmode:radius:<RADIUS_server> context.

polling-mechanism (**actual-user** | **rfc5997**)

Parameters

actual-user	Sets the RADIUS server polling-mechanism to actual-user.
rfc5997	Sets the RADIUS server polling-mechanism to rfc5997.

Examples

This example sets the RADIUS server polling-mechanism to rfc5997:

```
EWC.extremenetworks.com:vnsmode:radius:<named_RADIUS_server># polling-
mechanism rfc5997
```

protocol

Use the `protocol` command to set the security protocol used with the RADIUS server. The `protocol` command is accessible from the vnsmode:radius: <named_RADIUS_server> context of the CLI.

protocol [**CHAP** | **MS-CHAP** | **MS-CHAP2** | **PAP**]

Parameters

CHAP MS-CHAP MS-CHAP2 PAP	Specifies the security protocol that is used between the RADIUS Server and the Wireless Appliance.
---	--

Examples

The following example sets the security protocol to PAP for the RADIUS server named RAD1:

```
EWC.extremenetworks.com:vnsmode:radius:RAD1# protocol PAP
```

shared-secret

Use the `shared-secret` command to set the shared secret used with the RADIUS server. The `shared-secret` command is accessible from the vnsmode:radius:<named_RADIUS_server> context of the CLI.

shared-secret *shared secret*

Parameters

<i>shared secret</i>	Specifies the shared secret that is used between the RADIUS Server and the Wireless Appliance
----------------------	---

Examples

The following example sets the shared secret to “abc” for the RADIUS server named RAD1:

```
EWC.extremenetworks.com:vnsmode:radius:RAD1# shared-secret abc
```

mac-format-1x

Use this command to override the default MAC address colon-separated format (for example 00:11:22:33:44:55) with the Global Authentication MAC Address Format (for Mac Based Authentication) for the following attributes:

- Calling-Station-Id attribute of the RADIUS packet
- Called-Station-Id attribute (if Called-Station-Id is not overridden by Zone name)
- AP BSSID Mac in one of the vendor attributes
- User-Name attribute (Mac Based Authentication)

This command is available from the vnsmode:radius context. It is enabled for new deployments. You must manually enable this setting for upgraded deployments.

`mac-format-1x` (**enable** | **disable**)

Parameters

enable	Use MAC-Based Authentication MAC address format for user authentication and accounting via RADIUS
disable	Disable mac-format and use MAC address colon-separated format.

Examples

This example sets the authentication to MAC-Based Authentication MAC address format for user authentication and accounting via RADIUS.

```
EWC.extremenetworks.com:vnsmode:radius# mac-format-1x enable
```

rateprofile

Executing the `rateprofile` command moves you into the vnsmode:rateprofile context, which contains the following commands to manage bandwidth rate control profiles.

The following commands are available in the vnsmode:rateprofile context:

- [create](#) on page 268
- [delete](#) on page 269
- [show](#) on page 269

create

Use the `create` command to create a bandwidth rate control profile with an average rate in kbps. You can create up to 128 profiles. The `create` command is accessible from the vnsmode:rateprofile context of the CLI.

In the vnsmode:rateprofile context, use the command to delete a bandwidth rate control profile, and use the `show` command to display existing rate control profiles.

After you run the `create` command, run the `apply` command to implement the changes.

```
create profile_name average rate
```

Parameters

<i>profile_name</i>	Specifies the name of the rate control profile. If you are using a profile name that consists of two words and the two words are separated by space, you must put the profile name in double quotes (“”).
<i>average_rate</i>	Specifies committed information rate (CIR) in Kbps. Average Rate (CIR) must be between 128 and 200000 (kbps).

Examples

The following example creates a bandwidth rate control profile named `lowspeed` with 200 Kbps of CIR:

```
EWC.extremenetworks.com:vnsmode:rateprofile# create lowspeed 200
```

The following example creates a bandwidth rate control profile named `high speed` with 700 Kbps of CIR:

```
EWC.extremenetworks.com:vnsmode:rateprofile# create "high speed" 700
```

delete

Use the `delete` command to delete a bandwidth rate control profile. The `delete` command is accessible from the `vnsmode:rateprofile` context of the CLI.

If the rate control profile that you are attempting to delete is being used by any other VNS, the system returns the following message: You can not delete this profile because it is used by other VNS.

```
delete profile_name
```

Parameters

<i>profile_name</i>	Specifies the name of the bandwidth rate control profile to delete.
---------------------	---

Example

The following example deletes the `lowspeed` profile:

```
EWC.extremenetworks.com:vnsmode:rateprofile# delete lowspeed
```

show

Use the `show` command to display all existing bandwidth rate control profiles or a specific profile.

```
show [profile_name]
```

Parameters

<i>profile_name</i>	Specifies the name of a specific rate control profile to display.
---------------------	---

Examples

The following example displays all existing rate control profiles:

```
EWC.extremenetworks.com:vnsmode:rateprofile# show
Unlimited,0
lowspeed,200
```



redirection-url-list

Use the `redirection-url-list` command to create, delete, or modify a redirection URL list. The `redirection-url-list` command is accessible from within the root: `vnsmode:redirection_url` context.

```
redirection-url-list (add redirection url]*>|delete <[ sequence id]*|
[ redirection url]*>)
```

Parameters

add	Adds a URL.
delete	Deletes a URL.
<i>redirection url</i>	Identifies the redirection URL
<i>sequence id</i>	Identifies the sequence of the URL.

Usage

Before you can configure a redirection URL list, enable policy rule-based redirection using the [rule-redirect](#) command.

The URL list can contain up to 255 proper URLs, consisting of Fully-Qualified Domain Name (FQDN) addresses and IPV4 addresses. Duplicate entries are not permitted, and you must ensure that network traffic is accessible to the required IP addresses. The name of the WLAN Service that these entries are created for is displayed on the user interface and on the command line interface. SNMP also displays the URLs when queried through the Policy Profile MIB.

Examples

```
EWC.extremenetworks.com:vnsmode:redirection-url# redirection-url-list add
https://testing.com/login.htm
EWC.extremenetworks.com:vnsmode:redirection-url# show
SeqId          URL
1              https://testing.com/login.htm
```

Related Links

[rule-redirect](#) on page 245

<named-VNS>

Executing the <named-VNS> command, where <named-VNS> refers to the name of a configured VNS, moves you into the vnsmode:<named-VNS> context, which contains commands to configure the settings of the specified individual VNS.

The following commands are available in the vnsmode:<named-VNS> context:

- [auth](#) on page 271
- [non-auth](#) on page 272
- [name](#) on page 272
- [status](#) on page 273
- [sync](#) on page 273
- [wlans-name](#) on page 273
- [show](#) on page 274

auth

Use the `auth` command to assign a default role for authenticated clients. This command is available from the vnsmode:<named-VNS> context.

After you run the `auth` command, run the `apply` command to implement the changes.

auth non-auth | *role-name*

Parameters

non-auth	Use the default role for non-authenticated clients for authenticated clients.
<i>role-name</i>	Specifies the name of the role to use as the default role for authenticated clients.

Usage

When you assign a default authenticated role to this VNS, the same rules apply as when a VNS is created. That is — if the VNS's WLAN Service has a mode of:

- “std” then the referenced role must have a topology of mode “b@ap,” “b@ac,” or “routed”
- “3pap” then the referenced role must have a physical topology mode

Examples

The following example specifies that the role named “auth-users” should be used as the default role for authenticated users for the VNS named VNS1:

```
EWC.extremenetworks.com:vnsmode:VNS1# auth auth-users
```

This example specifies that the same role used as the default role for non-authenticated users should be used for authenticated users for the VNS named VNS1:

```
EWC.extremenetworks.com:vnsmode:VNS1# auth non-auth
EWC.extremenetworks.com:vnsmode:VNS1# apply
```

non-auth

Use the `non-auth` command to change the default role for non-authenticated clients. This command is available from the `vnsmode:<named-VNS>` context.

After you run the `non-auth` command, run the `apply` command to implement the changes.

non-auth *role-name*

Parameters

<i>role-name</i>	Specifies the name of the role to use as the default role for non-authenticated clients.
------------------	--

Usage

When you change the default non-authenticated role for this VNS, the same rules apply as when a VNS is created. That is – if the VNS’s WLAN Service has a mode of:

- “std” then the referenced role must have a topology of mode “b@ap,” “b@ac,” or “routed”
- “3pap” then the referenced role must have a physical topology mode

Examples

The following example specifies that the role named “non-auth-users” should be used as the default role for non-authenticated users for the VNS named VNS1:

```
EWC.extremenetworks.com:vnsmode:VNS1# non-auth non-auth-users
EWC.extremenetworks.com:vnsmode:VNS1# apply
```

name

Use the `name` command in the `vnsmode:<named-VNS>` context to change the name of the current VNS.

After you run the `name` command, run the `apply` command to implement the changes.

name *VNS-name*

Parameters

<i>VNS-name</i>	Specifies the new name for the current VNS.
-----------------	---

Example

The following example changes the name of VNS1 to VNS2, then uses the `show` command to display information for the current VNS, including its name:

```
EWC.extremenetworks.com:vnsmode:VNS1# name VNS2
EWC.extremenetworks.com:vnsmode:VNS1# apply
EWC.extremenetworks.com:vnsmode:VNS1# show
WLAN service: test
Non-authenticated: p4
Authenticated: same as non-authenticated
Restrict available role set: disable
Enable status: enable
```



```
Synchronize: disable
Name: VNS2
```

status

Use the `status` command in the `vnsmode:<named-VNS>` context to enable or disable the current VNS.

After you run the `status` command, run the `apply` command to implement the changes.

status (**enable** | **disable**)

Parameters

enable	Enables the VNS.
disable	Disables the VNS.

Examples

This example disables the current VNS named VNS1:

```
EWC.extremenetworks.com:vnsmode:VNS1# status disable
EWC.extremenetworks.com:vnsmode:VNS1# apply
```

sync

Use the `sync` command in the `vnsmode:<named-VNS>` context to enable or disable automatic synchronization of this VNS across paired controllers. Refer to the *Wireless User Guide* for more information about synchronization of VNSs.

After you run the `sync` command, run the `apply` command to implement the changes.

sync (**enable** | **disable**)

Parameters

enable	Enables automatic synchronization of this VNS across paired controllers.
disable	Disables automatic synchronization of this VNS.

Examples

This example enables automatic synchronization of the current VNS, named VNS1, across paired controllers:

```
EWC.extremenetworks.com:vnsmode:VNS1# sync enable
EWC.extremenetworks.com:vnsmode:VNS1# apply
```

wlans-name

Use the `wlans-name` command in the `vnsmode:<named-VNS>` context to associate a different WLAN Service with the current VNS. Only one WLAN Service can be associated with a VNS at a time.

After you run the `wlans-name` command, run the `apply` command to implement the changes.

wlans-name *WLAN-Service-name*

Parameters

<i>WLAN-Service-name</i>	Specifies the name of the .WLAN Service to associate with this VNS.
--------------------------	---

Example

This example changes the associated WLAN Service to wlan4 for the VNS named VNS1:

```
EWC.extremenetworks.com:vnsmode:VNS1# wlans-name wlan4
EWC.extremenetworks.com:vnsmode:VNS1# apply
```

show

Use the `show` command in the `vnsmode:<named-VNS>` context to display information about the current VNS.

show

Parameters

None.

Example

This example displays information about the current VNS named VNS1:

```
EWC.extremenetworks.com:vnsmode:VNS1# show
WLANS service: wlan4
Non-authenticated: p4
Authenticated: same as non-authenticated
Restrict available role set: disable
Enable status: enable
Synchronize: enable
Name: VNS1
```

Common Filter Configuration Commands

The commands in this section are common to the configuration of both AP filters and AC filters. Each filter must be configured in its own context ([acfilters](#) on page 251 or [apfilters](#) on page 252).

- [create](#) on page 274
- [config](#) on page 278
- [delete](#) on page 280
- [move](#) on page 281

create

Use the `create` command to create, insert, or append a new filter rule into an AP or AC filter list for a `<named-role>`. The `create` command is accessible from within the `vnsmode:<default-role>:acfilters` and `vnsmode:<default-role>:apfilters` contexts.

Use the following syntax to specify a position value and protocol for a filter rule in the filter list. No application is specified.

```
create [pos] proto protocol eth ether-type mac MAC address (ipaddress/mask | IPv6
| interface-subnet | interface-ip | any) [(port port [port]) | (type-code type
[type])] in (none|src|dst|both) out (none|src|dst|both) (allow | deny | none |
contain2vlan vlan-id | redirect) priority (0-7 | none) tos-dscp (0-FF/(FF/FE/FC/
F8/F0/E0/C0/80)|none) cos (named cos|none) traffic-mirror (<none|enable|
prohibited>)
```

Use the following syntax to specify an application in the filter rule definition for an AP or AC filter list.

```
create pos application app_id in (none|apply) out (none|apply) (allow|deny|none|
contain2vlan|redirect) cos (<named cos>|none) traffic-mirror (<none|enable|
prohibited>)
```

Use the following syntax to specify a custom application in the L7 layer of the filter rule definition for an AP or AC filter list.

```
create pos app-signature app_id group group name name app name in (none|apply)
out (none|apply) (allow|deny|none|contain2vlan\redirect) cos (named cos|none)
traffic-mirror (none|enable|prohibited)
```

Parameters

<i>pos</i>	Specifies a position value for this filter in the filter list. Valid values are from 0 - 255.
proto <i>protocol</i>	Specifies the protocol for this filter rule by number or name. Valid number values are from 0 - 255. Valid name values are: <ul style="list-style-type: none"> • udp - UDP protocol • tcp - TCP protocol • ah - Authentication Header protocol • esp - Encapsulating Security Payload protocol • icmp - ICMP protocol • icmpv6 - ICMP-IPv6 protocol • any - Any protocol • gre - Generic Route Encapsulation protocol • 0-255 - number value of protocol
eth <i>ether-type</i>	<i>ether-type</i> : 4 hex digits from 0001-FFFF, or any. The following well known values are converted into hex values, IPv4, ARP, RARP, DECnet Phase IV, AppleTalk (EtherTalk), AppleTalk Address Resolution Protocol (AARP), Novell IPX (alt), Novell, Profinet, and IPv6. Note: IPv6 is supported for Layer 2 bridging for both B@AC and B@AP topologies.
mac <i>MAC address</i>	<i>MAC address</i> : MAC or CIDR address, or any.
<i>ipaddress/mask</i> IPv6 interface-subnet interface-ip any	The IP address and/or mask for this filter rule. The IP address is in IPv6 format. Use the IP address and mask configured for the associated topology for this filter rule. Use the IP address of the associated topology for this filter rule. Use any IP address or mask for this filter rule.

port <i>port</i> [<i>port</i>]	Specifies a TCP or UDP port or port range to which this filter rule will be applied. The first <i>port</i> value specifies either the port or the start of a port range. The second <i>port</i> value optionally specifies the end of a range. This parameter is valid only when either TCP or UDP is the specified protocol. Valid port values are from 0 - 65535.
type-code <i>type</i> [<i>type</i>]	Specifies an ICMP type code or range of ICMP type codes. The first <i>type</i> value specifies either the ICMP type code or the start of a type code range. The second <i>type</i> value optionally specifies the end of a type code range. This parameter is valid only when ICMP is the specified protocol. Valid <i>type</i> values are from 0 - 255.
in (none src dst both)	Specifies the direction of packet flow. — <i>in</i> specifies a packet flow from the AP to the AC. <i>none</i> specifies that the <i>in</i> direction will not be used as matching criteria in the filter rule. <i>dst</i> specifies that the IP address for this filter rule is the destination of the packet flow. <i>src</i> specifies that the IP address for this filter rule is the source of the packet flow. <i>both</i> specifies that the IP address for this filter rule can be either source or destination.
out (none src dst both)	Specifies the direction of packet flow. — <i>out</i> specifies a packet flow from the AC to the AP. <i>none</i> specifies that the <i>out</i> direction will not be used as matching criteria in the filter rule. <i>dst</i> specifies that the IP address for this filter rule is the destination of the packet flow. <i>src</i> specifies that the IP address for this filter rule is the source of the packet flow. <i>both</i> specifies that the IP address for this filter rule can be either source or destination.
allow deny none contain2vlan <i>vlan-id</i> redirect	Specifies whether packets are allowed or denied (or ignored), or put in the containment VLAN (you must specify the VLAN by its ID), or redirected when meeting the criteria specified in the filter rule.
priority (<i>0-7</i> none)	Specifies the packet priority. Valid values are 0-7; the highest priority is 7. Specifying <i>none</i> means priority level will not be used as matching criteria in this CoS.
tos-dscp (<i>tos-dscp value/mask value</i> none)	Specifies the type of service in the filter rule. Valid values are 0-FF for ToS/DSCP and FF FE FC F8 F0 E0 C0 80 for mask. Specifying <i>none</i> means <i>tos/dscp</i> value is not used as matching criteria in the filter rule.
cos (<i>named-cos</i> none)	Specifies the class of service in the filter rule. The <i>named-cos</i> must already be created by the create command in the <i>cos</i> context. Specifying <i>none</i> means CoS is not used as matching criteria in the filter rule.
traffic-mirror	Specifies the behavior applied to a traffic mirror: <i>none</i> specifies the filter rule is not configured for traffic mirror. <i>enable</i> specifies that the traffic rule is enabled for traffic mirror <i>prohibited</i> specifies that the traffic rule is prohibited for traffic mirror.
application <i>app_id</i>	Specifies an application on the filter rule definition.
app-signature <i>app_id</i>	Specifies a custom application on the L7 layer of the filter definition rule.
group <i>group</i>	Specifies the pre-defined group, of which the (L7) custom application is a member.
name <i>app name</i>	Specifies the application name for the (L7) custom application.

Usage

If the specified rule position already contains a filter rule, specifying a rule using this command inserts a rule in the specified position in the list and re-sequences all rules below this filter down by one position. Use the `create` command to insert or append a rule at the specified position.

Examples

The following example shows the default filter rules applied to the Auth role:

```
EWC.extremenetworks.com:vnsmode:Auth# create p6
EWC.extremenetworks.com:vnsmode:Auth# show p6 acfilter
Enable AP filtering: disable
filter 1 (default) proto none 0.0.0.0 all_ports in dst out none allow
filter 2 (default) proto none 0.0.0.0 all_ports in none out src allow
```

The following example creates a (basic mode) filter rule 1 that allows UDP traffic in both directions from IP address 192.168.10.0/24 for ports 10 through 2000:

```
EWC.extremenetworks.com:vnsmode:Auth:acfilters# create 1 proto udp
192.168.10.0/24 port 10 2000 in dst out src allow
EWC.extremenetworks.com:vnsmode:Auth:acfilters# apply
EWC.extremenetworks.com:vnsmode:Auth:acfilters# show
Enable AP filtering: disable
filter 1 proto udp 192.168.10.0 255.255.255.0 port 10 2000 in dst out src
allow
filter 2 (default) proto none 0.0.0.0 all_ports in dst out none allow
filter 3 (default) proto none 0.0.0.0 all_ports in none out src allow
```

The following example creates a filter rule 1 that is inserted into the rule list at position 1 resequencing the current rule 1. This filter rule allows TCP traffic in both directions from IP address 192.168.0.0/16 for ports 10 through 2000:

```
EWC.extremenetworks.com:vnsmode:Auth:acfilters# create 1 proto tcp
192.168.0.0/16 port 10 2000 in dst out src allow
EWC.extremenetworks.com:vnsmode:Auth:acfilters# show
Enable AP filtering: disable
filter 1 proto tcp 192.168.0.0 255.255.0.0 port 10 2000 in dst out src allow
filter 2 proto udp 192.168.10.0 255.255.255.0 port 10 2000 in dst out src
allow
filter 3 (default) proto none 0.0.0.0 all_ports in dst out none allow
filter 4 (default) proto none 0.0.0.0 all_ports in none out src allow
```

The following example creates a filter rule for ToS-DSCP B8/FF and CoS Best Effort (note quotes around the named CoS because of the space):

```
EWC.extremenetworks.com:vnsmode:Auth:acfilters# create proto udp
192.168.0.0/32 in dst out src none priority none tos-dscp B8/FF cos "Best
Effort"
```

config

Use the `config` command to modify an existing AP or AC filter rule for this <named-role>. The `config` command is accessible from within the `vnsmode:<default-role>:acfilters` and `vnsmode:<default-role>:apfilters` contexts.

```
config [pos] proto protocol eth ether-type mac MAC address (ipaddress/mask | IPv6
| interface-subnet | interface-ip | any) [(port port [port]) | (type-code type
[type])] in (none|src|dst|both) out (none|src|dst|both) (allow | deny | none |
contain2vlan vlan-id | redirect) priority (0-7 | none) tos-dscp (0-FF/(FF/FE/FC/
F8/F0/E0/C0/80)|none) cos (named cos|none) traffic-mirror (<none|enable|
prohibited>)
```

Use the following syntax to modify an existing AP or AC application ID filter rule.

```
config pos application app_id in (none|apply) out (none|apply) (allow|deny|none|
contain2vlan|redirect) cos (<named cos>|none) traffic-mirror (<none|enable|
prohibited>)
```

Use the following syntax to modify a custom application in the L7 layer of the filter rule definition for an AP or AC filter list.

```
config pos app-signature app_id group group name name app name in (none|apply)
out (none|apply) (allow|deny|none|contain2vlan\redirect) cos (named cos|none)
traffic-mirror (none|enable|prohibited)
```

Parameters

<i>pos</i>	Specifies a position value for this filter in the filter list. Valid values are from 0 - 255.
proto <i>protocol</i>	Specifies the protocol for this filter rule by number or name. Valid number values are from 0 - 255. Valid name values are: <ul style="list-style-type: none"> • udp - UDP protocol • tcp - TCP protocol • ah - Authentication Header protocol • esp - Encapsulating Security Payload protocol • icmp - ICMP protocol • icmpv6 - ICMP-IPv6 protocol • any - Any protocol • gre - Generic Route Encapsulation protocol • 0-255 - number value of protocol
eth <i>ether-type</i>	<i>ether-type</i> : 4 hex digits from 0001-FFFF, or any. The following well known values are converted into hex values, IPv4, ARP, RARP, DECnet Phase IV, AppleTalk (EtherTalk), AppleTalk Address Resolution Protocol (AARP), Novell IPX (alt), Novell, Profinet, and IPv6. Note: IPv6 is supported for Layer 2 bridging for both B@AC and B@AP topologies.
mac <i>MAC address</i>	<i>MAC address</i> : MAC or CIDR address, or any.

<i>ipaddress/mask</i> IPv6 interface-subnet interface-ip any	The IP address and/or mask for this filter rule. The IP address is in IPv6 format. Use the IP address and mask configured for the associated topology for this filter rule. Use the IP address of the associated topology for this filter rule. Use any IP address or mask for this filter rule.
port <i>port</i> [<i>port</i>]	Specifies a TCP or UDP port or port range to which this filter rule will be applied. The first <i>port</i> value specifies either the port or the start of a port range. The second <i>port</i> value optionally specifies the end of a range. This parameter is valid only when either TCP or UDP is the specified protocol. Valid port values are from 0 - 65535.
type-code <i>type</i> [<i>type</i>]	Specifies an ICMP type code or range of ICMP type codes. The first <i>type</i> value specifies either the ICMP type code or the start of a type code range. The second <i>type</i> value optionally specifies the end of a type code range. This parameter is valid only when ICMP is the specified protocol. Valid <i>type</i> values are from 0 - 255.
in (none src dst both)	Specifies the direction of packet flow. — in specifies a packet flow from the AP to the AC. none specifies that the in direction will not be used as matching criteria in the filter rule. dst specifies that the IP address for this filter rule is the destination of the packet flow. src specifies that the IP address for this filter rule is the source of the packet flow. both specifies that the IP address for this filter rule can be either source or destination.
out (none src dst both)	Specifies the direction of packet flow. — out specifies a packet flow from the AC to the AP. none specifies that the out direction will not be used as matching criteria in the filter rule. dst specifies that the IP address for this filter rule is the destination of the packet flow. src specifies that the IP address for this filter rule is the source of the packet flow. both specifies that the IP address for this filter rule can be either source or destination.
allow deny none contain2vlan <i>vlan-id</i> redirect	Specifies whether packets are allowed or denied (or ignored), or put in the containment VLAN (you must specify the VLAN by its ID), or redirected when meeting the criteria specified in the filter rule.
priority (<i>0-7</i> none)	Specifies the packet priority. Valid values are 0-7; the highest priority is 7. Specifying none means priority level will not be used as matching criteria in this CoS.
tos-dscp (<i>tos-dscp value/mask value</i> none)	Specifies the type of service in the filter rule. Valid values are 0-FF for ToS/DSCP and FF FE FC F8 F0 E0 C0 80 for mask. Specifying none means tos/dscp value is not used as matching criteria in the filter rule.
cos (<i>named-cos</i> none)	Specifies the class of service in the filter rule. The <i>named-cos</i> must already be created by the create command in the cos context. Specifying none means CoS is not used as matching criteria in the filter rule.
traffic-mirror	Specifies the behavior applied to a traffic mirror: none specifies the filter rule is not configured for traffic mirror. enable specifies that the traffic rule is enabled for traffic mirror prohibited specifies that the traffic rule is prohibited for traffic mirror.
application <i>app_id</i>	Specifies an application on the filter rule definition.
app-signature <i>app_id</i>	Specifies a custom application on the L7 layer of the filter definition rule.

group <i>group</i>	Specifies the pre-defined group, of which the (L7) custom application is a member.
name <i>app name</i>	Specifies the application name for the (L7) custom application.

Usage

If the specified rule position already contains a filter rule, the `config` command overwrites the existing rule. Use the `create` command to insert or append a rule at the specified position.

Examples

The following example overwrites a pre-existing filter rule 1 with a rule that allows ICMP traffic types 9 through 31 in both directions for the associated topology's interface subnet and mask:

```
EWC.extremenetworks.com:vnsmode:p1:acfilters# config 1 proto icmp interface-
subnet type 9 31 in dst out src allow
EWC.extremenetworks.com:vnsmode:p1:acfilters# apply
EWC.extremenetworks.com:vnsmode:p1:acfilters# show
Enable AP filtering: disable
filter 1 proto icmp interface-subnet type 9 31 in dst out src allow
filter 2 proto udp 192.168.10.0 255.255.255.0 port 10 2000 in dst out src
allow
filter 3 (default) proto none 0.0.0.0 all_ports in dst out none allow
filter 4 (default) proto none 0.0.0.0 all_ports in none out src allow
```

The following example configures a filter rule that sets a ToS-DSCP as B8/FF and CoS as HTTP Traffic (note the quotes around the CoS name because of the space):

```
EWC.extremenetworks.com:vnsmode:Auth:acfilters# config 1 proto tcp
192.168.0.0/32 in dst out src none priority none tos-dscp B8/FF cos "HTTP
Traffic"
```

delete

Use the `delete` command to remove a filter rule from the filter list. The `delete` command is accessible from within the `vnsmode:<default-role>:acfilters` and `vnsmode:<default-role>:apfilters` contexts.

delete *pos*

Parameters

<i>pos</i>	Specifies the filter rule list position of the filter to be deleted. Valid values are 0 -255.
------------	---

Examples

The following example deletes filter rule 1 and displays the remaining default deny all rule:

```
EWC.extremenetworks.com:vnsmode:p1:acfilters# delete 1
EWC.extremenetworks.com:vnsmode:p1:acfilters# show
Enable AP filtering: disable
filter 1 (default) proto none 0.0.0.0 all_ports both deny
```


move

Use the `move` command to update the priority of a filter rule by moving the rule from its current position in the filter list (source) to a different list position (up or down). The `move` command is accessible from within the `vnsmode:<default-role>:acfilters` and `vnsmode:<default-role>:apfilters` contexts.

move *src-pos dest-pos*

Parameters

<i>src-pos dest-pos</i>	Specifies the current (source) position in the filter list of the rule to be moved, followed by the new (destination) list position for the filter rule. Valid values are 0 -255. List position 1 is top priority.
-------------------------	--

Example

The following example:

- Moves the rule in list position 2 to list position 1
- Displays the new list ordering:

```
EWC.extremenetworks.com:vnsmode:p1:acfilters# move 2 1
EWC.extremenetworks.com:vnsmode:p1:acfilters# show
Enable AP filtering: disable
filter 1 proto udp 192.168.10.0 255.255.255.0 port 10 2000 both allow
filter 2 proto tcp 192.168.10.0 255.255.255.0 port 10 2000 both allow
filter 3 (default) proto none 0.0.0.0 all_ports both deny
EWC.extremenetworks.com:vnsmode:p1:acfilters#
```

19 w lans Commands

```
clients
create
delete
remote-ssid
show
<WLAN-service-name>
hotspot
```

This section describes commands used to define and configure WLAN services for the network. These commands are located in the `w lans` context of the CLI. Execute the `w lans` command at the root level to enter `w lans` context.

All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the `w lans` context:

- [clients](#) on page 282 — See [clients](#) on page 282 for commands in the `wlan:clients` context.
- [create](#) on page 286
- [delete](#) on page 287
- [remote-ssid](#) on page 287
- [show](#) on page 287
- [<WLAN-service-name>](#) on page 289 — See for commands in the `wlan:<WLAN-service-name>` context.
- [hotspot](#) on page 346

clients

The `clients` context provides commands which are used to configure guest access features on the Wireless Appliance. Switch to the `clients` context from the `w lans` context to access the following commands on the Wireless Appliance.

A guest portal WLAN service must be created on this controller before the `clients` context command and the context's associated commands are available. For more on creating a guest portal WLAN service, see [mode](#) on page 310.

The following commands are available in the `wlan:clients` context.

- [client](#) on page 283
- [descr](#) on page 283
- [enable](#) on page 284
- [endofday](#) on page 284

- [export_clients](#) on page 285
- [import_clients](#) on page 285
- [startofday](#) on page 286

client

Use the `client` command to configure the guest portal client access account.

```
[no] client id name passwd acct_start account_lifetime session_lifetime
```

Parameters

<i>id</i>	Specifies the ID of the guest access account and must begin with the string "Guest-"
<i>name</i>	Specifies the name of the client
<i>passwd</i>	Specifies the password used by the client
<i>acct_start</i>	Specifies the activation start time of the client account (in the form YYYY-MM-DD HH:MM:SS)
<i>account_lifetime</i>	Specifies the amount of time the client account will remain viable
<i>session_lifetime</i>	Specifies the amount of time the client session will remain viable

Examples

The following example configures a client guest access account named "Lobby":

```
EWC.extremenetworks.com:wlans:clients# client Guest-lobby Lobby 1234abcd
2009-12-01 12:00:00 12 12
EWC.extremenetworks.com:wlans:clients# show
Guest-lobby    Lobby  1234abcd          2009-12-01 12:00:00    12
12            00:00    00:00    disabled
```

descr

Use the `descr` command to add a description to the specified guest portal client access account.

```
descr id descriptive_text
```

Parameters

<i>id</i>	Specifies the ID of the guest access account and must begin with the string "Guest-"
<i>descriptive_text</i>	Specifies the description for the guest client

Examples

The following example sets a description for the client guest access account with ID "Guest-lobby":

```
EWC.extremenetworks.com:wlans:clients# descr Guest-lobby The lobby guest
client account.
EWC.extremenetworks.com:wlans:clients# show descr
```

```

Guest-lobby    Lobby    1234abcd      2009-12-01 12:00:00    12
12            The lobby guest client account.      00:00    00:00    disabled

```

The following example clears the description for the client guest access account with ID “Guest-lobby”:

```

EWC.extremenetworks.com:wlans:clients# descr Guest-lobby
EWC.extremenetworks.com:wlans:clients# show
Guest-lobby    Lobby    1234abcd      2009-12-01 12:00:00    12
12            00:00    00:00    disabled

```

enable

Use the `enable` command to enable or disable the guest portal access account

```
[no] enable id
```

Parameters

<i>id</i>	Specifies the ID of the guest access account and must begin with the string “Guest-”
-----------	--

Examples

The following example enables the guest access account:

```

EWC.extremenetworks.com:wlans:clients# enable Guest-lobby
EWC.extremenetworks.com:wlans:clients# show
Guest-lobby    Lobby    1234abcd      2009-12-01 12:00:00    12
12            00:00    08:00    enabled

```

The following example disables the guest access account:

```

EWC.extremenetworks.com:wlans:clients# no enable Guest-lobby
EWC.extremenetworks.com:wlans:clients# show
Guest-lobby    Lobby    1234abcd      2009-12-01 12:00:00    12
12            00:00    08:00    disabled

```

endofday

Use the `endofday` command to configure the duration of the guest portal access account.

```
[no] endofday id HH:MM
```

Parameters

<i>id</i>	Specifies the ID of the guest access account and must begin with the string “Guest-”
<i>HH:MM</i>	Specifies the duration of the guest client in a <HH:MM> hours and minutes format

Example

The following example sets the duration of the guest access account to 8 hours:

```

EWC.extremenetworks.com:wlans:clients# endofday Guest-lobby 08:00
EWC.extremenetworks.com:wlans:clients# show

```

```

Guest-lobby    Lobby    1234abcd    2009-12-01 12:00:00    12
12             00:00    08:00    disabled

```

export_clients

Use the `export_clients` command to export all current client information from the system to a file.

```
export_clients server user dir file
```

Parameters

<i>server</i>	Specifies the IP address of an FTP server to export the file to
<i>user</i>	Specifies the username with which to login in to the FTP server
<i>dir</i>	Specifies the directory path containing the clients export file
<i>file</i>	Specifies the clients export file name

Example

The following example exports all current client information from the system to a file named `clients_export`:

```

EWC.extremenetworks.com:wlans:clients# export_clients 192.168.4.1 admin /
support clients_export_file
Please input password:
Attempting to upload file using ncftp ...

```

import_clients

Use the `import_clients` command to import client information into the system from a file.

```
import_clients server user dir file
```

Parameters

<i>server</i>	Specifies the IP address of an FTP server to import the file from
<i>user</i>	Specifies the username with which to login in to the FTP server
<i>dir</i>	Specifies the directory path containing the clients import file
<i>file</i>	Specifies the clients import file name

Example

The following example imports the previously exported file created by the [page 285](#) command:

```

EWC.extremenetworks.com.com:wlans:clients# import_clients 192.168.4.1 admin /
support clients_export_file
Please input password:
Attempting to download file...

```

startofday

Use the `startofday` command to configure the time for start of day for the guest portal access account.

```
[no] startofday id HH:MM
```

Parameters

<i>id</i>	Specifies the ID of the guest access account and must begin with the string "Guest-"
<i>HH:MM</i>	Specifies the account activation time. The default is 00:00.

Example

The following example sets the account activation time of the guest access account to 07:00 hours:

```
EWC.extremenetworks.com:wlans:clients# startofday Guest-lobby 07:00
EWC.extremenetworks.com:wlans:clients# show
Guest-lobby    Lobby    1234abcd    2009-12-01 12:00:00    12
12             07:00    07:00     disabled
```

create

Use the `create` command to create a WLAN service configuration. The `create` command is accessible from the `wlans` context of the CLI.

```
create WLANS-string mode (mesh|wds|std|3pap|remote) ssid ssid-string | create
WLANS-string mode (std|remote) ssid ssid-string hs-type (enabled|osu)
```

Parameters

<i>WLANS-name</i>	Specifies the name of the WLAN service
mode (mesh wds std 3pap remote)	Specifies the mode of the WLAN service
ssid ssid-string	Specifies the SSID of the WLAN service
hs-type (enabled osu)	Specifies whether the WLANS is a basic hotspot or an online signup hotspot. To enable hotspot, the mode must be <code>std</code> or <code>remote</code> . The WLAN Service status for new hotspots is disabled by default. To enable the WLAN Service, you must first configure the privacy and authentication settings. Once the hotspot is configured, the hotspot type cannot be modified. If you need to modify the hotspot type, you must create a new WLANS.

Example

The following example creates and then displays the details of a WLAN service hotspot configuration named `hs-wlan` in `std` mode:

```
EWC.extremenetworks.com:wlans# create hs-wlan mode std ssid hs-wlan hs-type
enabled
EWC.extremenetworks.com:wlans# hs-wlan
EWC.extremenetworks.com:wlans:hs-wlan# show
Service type: std
Hotspot type: enabled
```

```
Name: hs-wlan
Enable/disable WLAN Service: disable
Remotable: disable
Inter-WLAN Service Roaming: enable
Associated WLANs: hs-wlan
Egress Filtering: disable
```

delete

Use the `delete` command to delete a WLAN service configuration. The `delete` command is accessible from the `wlans` context of the CLI.

```
delete WLANS-name
```

Parameters

<i>WLANS-name</i>	Specifies the name of the WLAN service to delete
-------------------	--

Example

The following example deletes the WLAN service named `test-wlan`:

```
EWC.extremenetworks.com:wlans# delete test-wlan
```

remote-ssid

Use the `remote-ssid` command to display the available remote SSIDs within the Wireless Appliance's mobility domain.

```
remote-ssid
```

Parameters

None.

Usage

The `remote-ssid` command reports the remote SSIDs only if the `remoteable` command is set to enable. For more information, see [remoteable](#) on page 338.

Example

The following example displays the currently available remote SSIDs:

```
EWC.extremenetworks.com:wlans# remote-ssid
There is no remotable SSID in the mobility domain.
```

show

Use the `show` command from the `wlans` context to display WLAN service configuration information.

show [*WLANS-name*]

Parameters

<i>WLANS-name</i>	Specifies to display information about the specific WLAN service
-------------------	--

Usage

The Radio Mode field displays the 802.11 modulations that the AP's radios are configured to use.

Examples

The following example displays a list of all WLAN service configuration information:

```
EWC.extremenetworks.com:wlans# show
Name Service Type Enabled SSID Privacy Auth Mode Radio Mode

osu std enabled osu none disabled off
hs std enabled hs wpa 8021x off
std std enabled std none internal off
```

The following example displays configuration information for the WLAN service named "hs":

```
EWC.extremenetworks.com:wlans# show hs
Service type: std
Hotspot type: enabled
Name: hs
Enable/disable WLAN Service: enable
Remotable: disable
Inter-WLAN Service Roaming: enable
Associated WLANs: hs
Egress Filtering: disable
Radio1 Radio2 AP Name
          3705i
          3805i
          ap3935i
          3965
          3805e
          ap3805i3
          3825i1
          ap3935e
SSID: hs
Default topology:
Pre-authentication timeout(minutes): 5
Post-authentication timeout(minutes): 30
Session timeout(minutes): 0
Enable/disable block MU to MU traffic: disable
Default CoS: No CoS
Default Traffic Mirror: prohibited
Enable/disable Netflow support: disable
Unauthenticated Behavior: discard-unauth-traffic
Radio Mode: off
```


<WLAN-service-name>

The `<WLAN-service-name>` command, where `<WLAN-service-name>` is the name of a given WLAN service, moves you into the `wlan:<WLAN-service-name>` context, which contains commands to configure the settings of the specified individual WLAN service.

The following commands are available in the `wlan:<WLAN-service-name>` context. Different commands are available depending on the type of WLAN server being configured.

- [3pap](#) on page 289
- [aplist](#) on page 290
- [aplist-wds \(WDS\)](#) on page 291
- [aplist-wds \(Mesh\)](#) on page 292
- [appl-visibility](#) on page 292
- [auth](#) on page 293 — See [auth](#) on page 293 for commands in the `wlan:<WLAN-service-name>:auth` context.
- [cp-http](#) on page 320
- [default-cos](#) on page 321
- [default-topology](#) on page 321
- [direct-client-traffic](#) on page 322
- [egress-filtering](#) on page 323
- [name](#) on page 323
- [priv](#) on page 324 — See for commands in the `wlan:<WLAN-service-name>:priv` context.
- [psk](#) on page 329
- [qos-policy](#) on page 330 — See for commands in the `wlan:<WLAN-service-name>:qos-policy` context.
- [remoteable](#) on page 338
- [rf](#) on page 338 — See for commands in the `wlan:<WLAN-service-name>:rf` context.
- [show](#) on page 342
- [ssid](#) on page 343
- [status](#) on page 343
- [sync](#) on page 344
- [timeout-post](#) on page 344
- [timeout-pre](#) on page 344
- [timeout-session](#) on page 345
- [unauth-behaviour](#) on page 345

3pap

Use the `3pap` command to add a third party AP to the WLAN service configuration. Use the `[no]` form of the command to remove a third party AP from the WLAN service configuration. The `3pap` command is accessible from the `wlan:<WLAN-service-name>` context of the CLI when the WLAN service type is 3PAP.

After you run the `3pap` command, run the `apply` command to implement the changes.

```
[no] 3pap A.B.C.D HH:HH:HH:HH:HH:HH
```

Parameters

<i>A.B.C.D</i>	Specifies the IPv4 address of the third party AP to add to or remove from the WLAN service
<i>HH:HH:HH:HH:HH:HH</i>	Specifies the MAC address of the third party AP to add to or remove from the WLAN service

Usage

This command is only available when the WLAN service type is third party AP (3pap).

Example

The following example adds a third party AP by IP and MAC address to the WLAN service named "3pap-test":

```
EWC.extremenetworks.com:wlans:3pap-test# 3pap 1.2.3.4 11:22:33:44:55:66
EWC.extremenetworks.com:wlans:test# apply
```

aplist

Use the `aplist` command to add or remove an AP to or from the WLAN service configuration. The `aplist` command is accessible from the `wlan:<WLAN-service-name>` context of the CLI when the WLAN service type is standard.

After you run the `aplist` command, run the `apply` command to implement the changes.

```
[no] aplist ap-name radio1|radio2|both
```

Parameters

<i>ap-name</i>	Specifies the name of the AP to add or remove from the WLAN service. The no form of the command removes the AP
radio1 radio2 both	Specifies to use radio1, radio2, or both with the WLAN service

Usage

This command is only available when the WLAN service type is STD.

Example

The following example adds an AP by serial number to the WLAN service named "test" and then displays the list of Wireless APs:

```
EWC.extremenetworks.com:wlans:test# aplist 0500000000000000 both
EWC.extremenetworks.com:wlans:test# apply
EWC.extremenetworks.com:wlans:test# show aplist
Wireless AP Services:
Wireless AP: 0500000000000000 both
```

aplist-wds (WDS)

Use the `aplist-wds` command to add or remove an AP to or from a WDS type WLAN service configuration. The `aplist-wds` command is accessible from the `wlan:<WLAN-service-name>` context of the CLI when the WLAN service type is WDS.

[aplist-wds \(Mesh\)](#) on page 292 for information about using the command to configure a dynamic mesh WLAN service.

Use this command to configure the following:

- Role on radio 1
- Role on radio 2
- Preferred parent
- Backup parent
- Work group bridging

After you run the `aplist-wds` command, run the `apply` command to implement the changes.

```
aplist-wds ap-name ((radio1 none|child|parent|both radio2 none|child|parent|
both)|(both none|child|parent|both)) [pref-parent ap-name | Any-Parent] [backup-
parent ap-name | Any-Parent] [wkgbridge on|off]
no aplist-wds ap-name radio1|radio2|both
```

Parameters

radio1 none child parent both	Specifies the AP's role on Radio1
radio2 none child parent both	Specifies the AP's role on Radio2
both none child parent both	Specifies the AP's role on both radios
pref-parent ap-name Any Parent	Specifies the AP's parent
backup-parent ap-name Any Parent	Specifies the AP's backup parent
wkgbridge off on	Configures the work group bridging

Usage

This command is only available when the WLAN service type is WDS.

Example

The following example reflects the following:

- AP Lancaster is serving as a child of AP Aruba on radio radio1
- AP Auberon is the backup parent of AP Lancaster
- Work group bridging is switched off

```
EWC.extremenetworks.com:wlan:shopfloor_WDS_wlan# aplist-wds Lancaster
radio1 child radio2 parent pref-parent Aruba backup-parent Auberon
```

```
wkgbridge off
EWC.extremenetworks.com:wlans:shopfloor_WDS_wlan# apply
```

aplist-wds (Mesh)

Use the `aplist-wds` command to add an AP to a dynamic mesh type WLAN service configuration. The `aplist-wds` command is accessible from the `wlans:<WLAN-service-name>` context of the CLI when the WLAN service type is mesh.

[aplist-wds \(WDS\)](#) on page 291 for information about using the command to configure a WDS type of WLAN service.

```
aplist-wds ap-name (none|portal|mesh) [wkgbridge (on|off)] [radio1|radio2]
```

Parameters

<i>ap-name</i>	Name of the AP being assigned to the WLAN service.
none portal mesh	none = default, not assigned to the WLAN service. portal = the AP is a mesh portal (equivalent to parent in static mesh WLANs). mesh = the AP is a mesh AP.
wkgbridge (on off)	Configures the work group bridging
radio1 radio2	For a dual-band radio AP, if more than one available radio matches the backhaul radio settings, select one of the radios for backhaul.

Usage

An AP can be assigned to either a static mesh/WDS WLAN service or a dynamic mesh WLAN service, but not to both types of mesh service at the same time.

On dual-band APs, if only one radio matches the backhaul radio band, selecting a radio is optional. If a radio is selected but it is the wrong one, the system will print an error message.

If more than one radio matches the backhaul radio band, then selecting a radio is mandatory and an error message will print if no radio is selected.

Example

The following example adds the AP named `lab-ap1` as a mesh portal with work group bridging on for dynamic mesh WLAN `mesh1-wlan`:

```
EWC.extremenetworks.com:wlans:mesh1-wlan# aplist-wds lab-ap1 portal wkgbridge
on
```



appl-visibility

Use the `appl-visibility` command to enable ExtremeWireless application visibility. The `appl-visibility` command is accessible from within the `root:wlans:<named-wlan>` context.

```
appl-visibility enable | disable
```

Parameters

enable disable	Enables or disables the ExtremeWireless Application Visibility feature.
--------------------------------	---

Example

The following example enables application visibility on the specified WLANs.

```
EWC.extremenetworks.comwlan:<WLAN-service-name>#appl-visibility enable
```

auth

The **auth** command moves you into the authentication context, wlan:<WLAN-service-name>:auth, for the configuration of authentication settings for the WLAN service being configured. The WLANs auth context supports the following authentication types:

- MAC
- 802.1X mode
- Captive Portal Authentication modes: internal, external, guest portal, and guest splash

When you first enter the auth context, MAC, 802.1x and Captive Portal Authentication modes default to disabled. MAC authentication can be configured in any authentication mode. The availability of non-MAC authentication commands depends upon the current mode. The Usage section for each authentication command specifies mode information for that command. See [mode](#) on page 310 for further information on setting the authentication mode.

The following commands are available in the wlan:<WLAN-service-name>:auth context.

- [aaa-redirect](#) on page 294
- [access-reject-without-cui](#) on page 294
- [captiveportal](#) on page 295 — See for commands in the wlan:<WLAN-service-name>:auth:captiveportal context.
- [cdr](#) on page 304
- [config](#) on page 305
- [config exit](#) on page 306
- [fast-failover](#) on page 306
- [include-cui-type](#) on page 307
- [interim](#) on page 307
- [mac](#) on page 308
- [mac-acct](#) on page 308
- [mac-auto-authenticate](#) on page 308
- [mac-allow-unauthorized](#) on page 309
- [mac-roam](#) on page 310
- [mode](#) on page 310
- [move](#) on page 311
- [nasid](#) on page 312
- [nasip](#) on page 313
- [password](#) on page 313
- [protocol](#) on page 314

- [radius-timeout-policy](#) on page 314
- [remove](#) on page 315
- [show](#) on page 315
- [use-policy-zone](#) on page 316
- [vsa-ap](#) on page 316
- [vsa-egress](#) on page 317
- [vsa-ingress](#) on page 317
- [vsa-policy](#) on page 318
- [vsa-ssid](#) on page 318
- [vsa-topology](#) on page 319
- [vsa-vns](#) on page 319

aaa-redir

Use the `aaa-redir` command to enable or disable AAA redirect.

After you run the `aaa-redir` command, run the `apply` command to implement the changes.

aaa-redir enable | disable

Parameters

enable disable	Specify to enable or disable AAA redirect
-------------------------	---

Usage

The 8021x authentication mode must be set for this command to be available. For more information, see [mode](#) on page 310.

Example

The following example enables AAA redirect:

```
EWC.extremenetworks.com:wlans:cn1-AAA:auth# aaa-redir enable
EWC.extremenetworks.com:wlans:cn1-AAA:auth# apply
```

access-reject-without-cui

Use the `access-reject-without-cui` command to enable or disable treatment of Access-Accept without Chargeable-User-Identity attribute as Access-Reject. The `access-reject-without-cui` command is accessible from the `wlans:<named wlans>:auth` context of the CLI.

access-reject-without-cui (enable | disable)

Parameters

enable	Enables the treatment of Access-Accept without Chargeable-User-Identity attribute as Access-Reject.
disable	Disables the treatment of Access-Accept without Chargeable-User-Identity attribute as Access-Reject.

Examples

The following example enables the treatment of Access-Accept without Chargeable-User-Identity attribute as Access-Reject:

```
EWC.extremenetworks.com:wlan:Lab184-AAA:auth# access-reject-without-cui
enable
```

captiveportal

The Wireless Appliance can use Captive Portal authentication for Service Set Identifier (SSID) network assignments. The Captive Portal is a browser-based authentication mechanism that forces unauthenticated users to a web page.

The `captiveportal` command moves you to context `wlan:<WLAN-service-name>:auth:captiveportal`, which contains commands used to configure Captive Portal support. The `wlan:<WLAN-service-name>:auth:mode` command ([mode](#) on page 310) determines which commands are available in the `captiveportal` context.

The following commands are available in the `wlan:<WLAN-service-name>:auth:captiveportal` context.

- [add-ip-port](#) on page 295
- [copy-cpfile](#) on page 296
- [cp-ssl](#) on page 296
- [custom](#) on page 297
- [extcpip](#) on page 297
- [extredir](#) on page 298
- [extsecret](#) on page 298
- [fqdn](#) on page 299
- [guestportalacctlifetime](#) on page 299
- [guestportalprefix](#) on page 300
- [maxsessionlifetime](#) on page 300
- [minpasswlength](#) on page 301
- [redirect](#) on page 302
- [send-login](#) on page 303
- [set-acct-lifetime](#) on page 303
- [tos-override](#) on page 304

add-ip-port

Use this command to enable or disable the ability to add a controller IP address and port to the redirection URL. The `add-ip-port` command is available in the `wlan:<WLAN-service-name>:auth:captiveportal` context for external captive portal mode only.

add-ip-port enable | disable

Parameters

enable	Enable adding a controller IP address and port to the redirection URL.
disable	Disable adding a controller IP address and port to the redirection URL. This is the default.

copy-cpfile

Use this command to download a zip file containing customized web pages. The `copy-cpfile` command is available from the `wlan:<WLAN-service-name>:auth:captiveportal` context.

copy-cpfile `scp|ftp` *server user password dir file*

Parameters

scp ftp	Specifies whether to use FTP or SCP to download the file.
<i>server</i>	The IP address of the FTP or SCP server.
<i>user</i>	The user name to log in to the server.
<i>password</i>	The password for file transfer protocol.
<i>dir</i>	The directory on the server where the file is located.
<i>file</i>	The name of the file containing the web pages.

Example

This example uses FTP to copy the file “cpcustom.zip” located in the /tmp directory on FTP server 192.168.3.10, using log in credentials “root” and “mypasswd”:

```
EWC.extremenetworks.com:wlans:Lab126-12-Int-CP:auth:captiveportal# copy-cpfile ftp 192.168.3.10 root mypasswd /tmp cpcustom.zip
```

cp-ssl

Use the `cp-ssl` command to enable or disable HTTPS support on a WLAN service configured for external authentication. The `cp-ssl` command is available only if mode is set to external. For more information about the `mode` command, see [mode](#) on page 310.

cp-ssl `enable|disable`

Parameters

enable	Enable HTTPS support on the WLAN service configured for external authentication.
disable	Disable HTTPS support on the WLAN service configured for external authentication.

Usage

By default, HTTPS support is disabled.

Example

The following example enables HTTPS support on the WLAN service:

```
EWC.extremenetworks.com:wlans:external_wlan:auth:captiveportal# cp-ssl enable
EWC.extremenetworks.com:wlans:external_wlan:auth:captiveportal# apply
```


custom

Use the `custom` command, within context `wlan:<WLAN-service-name>:auth:captiveportal`, to configure communications options for custom captive portal settings.

After you run the `custom` command, run the `apply` command to implement the changes.

custom local | web

Parameters

local	Sets captive portal communications options to local
web	Sets captive portal communications options to web

Usage

If customized captive portal content was previously downloaded to the controller using the `copy-custom` command, `custom` can only be successfully set to `local`. The internal or splash authentication mode must be set for this command to be available. For more information, see [mode](#) on page 310.

Example

The following example sets the captive portal communications options to `web`:

```
EWC.extremenetworks.com:wlans:new-wlans:auth:captiveportal# custom web
EWC.extremenetworks.com:wlans:new-wlans:auth:captiveportal# apply
```

extcpip

Use the `extcpip` command, within context `wlan:<WLAN-service-name>:auth:captiveportal`, to specify the IP address and the server access port on the Wireless Appliance for communication with an external authentication server.

After you run the `extcpip` command, run the `apply` command to implement the changes.

extcpip A.B.C.D:port

Parameters

A.B.C.D	Specifies the IP address of the controller's server access port for communication to an external authentication server.
port	Specifies the port number within the range: 32768 - 65535

Usage

Either the external authentication mode or 802.1x with `aaa-redir` must be set for this command to be available. For more information, see [mode](#) on page 310.

Example

The following example specifies the interface and server access port for access to an external authentication server:

```
EWC.extremenetworks.com:wlans:CNL-7-CP:auth:captiveportal# extcpip
10.0.0.1:33333
EWC.extremenetworks.com:wlans:CNL-7-CP:auth:captiveportal# apply
```

extredir

Use the `extredir` command, within context `wlan:<WLAN-service-name>:auth:captiveportal`, to specify the External Redirection URL.

After you run the `extredir` command, run the `apply` command to implement the changes.

extredir *value_string* | **none**

Parameters

<i>value_string</i>	Specifies a URL beginning with <code>http://</code>
none	Specifies that no external redirection URL is configured

Usage

The external authentication mode must be set for this command to be available. For more information, see [mode](#) on page 310.

Example

The following example specifies an External Redirection URL:

```
EWC.extremenetworks.com:wlans:CNL-7-CP:auth:captiveportal# extredir http://
192.168.4.89:80
EWC.extremenetworks.com:wlans:CNL-7-CP:auth:captiveportal# apply
```

extsecret

Use the `extsecret` command, within context `wlan:<WLAN-service-name>:auth:captiveportal`, to define the Shared Secret password common to both the Wireless Appliance and the external web server.

After you run the `extsecret` command, run the `apply` command to implement the changes.

extsecret *value_string* | **none**

Parameters

<i>value_string</i>	Specifies a password
none	Specifies that no password is configured

Usage

The external authentication mode must be set for this command to be available. For more information, see [mode](#) on page 310.

Example

The following example creates a Shared Secret password:

```
EWC.extremenetworks.com:wlans:CNL-7-CP:auth:captiveportal# extsecret
5eCretH4nD5h4k3
EWC.extremenetworks.com:wlans:CNL-7-CP:auth:captiveportal# apply
```

fqdn

Use the `fqdn` command, within context `wlan:<WLAN-service-name>:auth:captiveportal`, to replace the Gateway IP address with a Fully Qualified Domain Name (FQDN).

After you run the `fqdn` command, run the `apply` command to implement the changes.

fqdn *value_string* | **none**

Parameters

<i>value_string</i>	Specifies a domain name
none	Specifies that the Gateway IP address is not replaced with a FQDN

Usage

The `guestportal`, `internal`, or `splash` authentication mode must be set for this command to be available. For more information, see `mode` on page 310.

Example

The following example replaces the Gateway IP address with a domain name:

```
EWC.extremenetworks.com:vnsmode:CNL-7-CP:auth:captiveportal# fqdn
cp.siemens.com
EWC.extremenetworks.com:vnsmode:CNL-7-CP:auth:captiveportal# apply
```

guestportalacctlifetime

Use the `guestportalacctlifetime` command, within context `wlan:<WLAN-service-name>:auth:captiveportal`, to configure the lifetime for the guest portal access account, in days.

After you run the `guestportalacctlifetime` command, run the `apply` command to implement the changes.

[no] `guestportalacctlifetime` *days*

Parameters

<i>days</i>	Specifies the number of days the account remains valid
-------------	--

Usage

The `guestportal` authentication mode must be set for this command to be available. For more information, see `mode` on page 325.

Example

The following example sets the guest portal account lifetime to one day:

```
EWC.extremenetworks.com:wlans:CNL-CP:auth:captiveportal#
guestportalacctlifetime 1
EWC.extremenetworks.com:wlans:CNL-CP:auth:captiveportal# apply
EWC.extremenetworks.com:wlans:CNL-CP:auth:captiveportal# show
guestportalacctlifetime
guestportalacctlifetime 1
```

guestportalprefix

Use the `guestportalprefix` command, within context `wlan:<WLAN-service-name>:auth:captiveportal`, to configure the user ID prefix for the guest portal access account.

After you run the `guestportalprefix` command, you must run the `apply` command to implement the changes.

guestportalprefix prefix

Parameters

<i>prefix</i>	Specifies the maximum number of hours for the session time of the guestportal access account
---------------	--

Usage

The guestportal authentication mode must be set for this command to be available. For more information, see [mode](#) on page 310.

Example

The following example sets the guest portal prefix to the string “TEST”:

```
EWC.extremenetworks.com:wlans:CNL-CP:auth:captiveportal# guestportalprefix
TEST
EWC.extremenetworks.com:wlans:CNL-CP:auth:captiveportal# apply
EWC.extremenetworks.com:wlans:CNL-CP:auth:captiveportal# show
guestportalprefix
guestportalprefix          TEST
```

maxsessionlifetime

Use the `maxsessionlifetime` command, within context `wlan:<WLAN-service-name>:auth:captiveportal`, to configure the maximum session lifetime for the guest portal access account, in hours.

After you run the `maxsessionlifetime` command, run the `apply` command to implement the changes.

`[no] maxsessionlifetime hours`

Parameters

<i>hours</i>	Specifies the maximum number of hours for the session time of the guestportal access account
--------------	--

Usage

The guestportal authentication mode must be set for this command to be available. For more information, see [mode](#) on page 310.

Example

The following example sets the maximum session lifetime for the guest portal account to one hour:

```
EWC.extremenetworks.com:wlans:CNL-CP:auth:captiveportal# maxsessionlifetime 1
EWC.extremenetworks.com:wlans:CNL-CP:auth:captiveportal# apply
EWC.extremenetworks.com:wlans:CNL-CP:auth:captiveportal# show
maxsessionlifetime
maxsessionlifetime      1
```

minpasswlength

Use the `minpasswlength` command, within context `wlan:<WLAN-service-name>:auth:captiveportal`, to set the minimum acceptable character length for the password for the guest portal access account.

After you run the `minpasswlength` command, run the `apply` command to implement the changes.

minpasswlength <1,32>

Parameters

<i>length</i>	Specifies the minimum acceptable character length for the guest portal access account password. Length can range from 1 to 32 characters.
---------------	---

Usage

The guestportal authentication mode must be set for this command to be available. For more information, see [mode](#) on page 310.

Example

The following example sets the minimum length for the guest portal access account password to 12 characters:

```
EWC.extremenetworks.com:wlans:CNL-CP:auth:captiveportal# minpasswlength 12
EWC.extremenetworks.com:wlans:CNL-CP:auth:captiveportal# apply
EWC.extremenetworks.com:wlans:CNL-CP:auth:captiveportal# show minpasswlength
minpasswlength 12
```

pwd-charset

Use this command to select a password character set. The `pwd-charset` command is available in the `wlan:<WLAN-service-name>:auth:captiveportal` context.

pwd-charset *greek|cyrilic|latin*

Parameters

greek	Determines that the greek character set is used when generating a password pattern.
cyrilic	Determines that the cyrilic character set is used when generating a password pattern.
latin	Determines that the latin character set is used when generating a password pattern.

Usage

The guest portal WLAN must be configured.

pwd-ignore-similar

Use this command to enable or disable the ability to ignore similar characters when generating the password pattern. The `pwd-ignore-similar` command is available in the `wlan:<WLAN-service-name>:auth:captiveportal` context.

pwd-ignore-similar enable | disable

Parameters

enable	Enable ignoring similar characters when generating the password pattern.
disable	Disable ignoring similar characters when generating the password pattern.

pwd-pattern

Use this command to set the password pattern. The `pwd-pattern` command is available in the `wlan:<WLAN-service-name>:auth:captiveportal` context.

pwd-pattern string | none

Parameters

<i>string</i>	The password pattern character string.
none	No character string is set.

Usage

The guest portal WLAN must be configured.

pwd-pattern-select

Use this command to select a password pattern. The `pwd-pattern-select` command is available in the `wlan:<WLAN-service-name>:auth:captiveportal` context.

pwd-pattern-select custom | phone-number | random | postal-code | two-words

Parameters

custom	Generate a custom password pattern. Allows the user to type a password pattern in the Pattern field or to use the key pad.
phone-number	Use the predefined phone-number pattern to generate a password pattern.
random	Use the predefined random pattern to generate a password pattern.
postal-code	Use the predefined postal-code pattern to generate a password pattern.
two-words	Use the predefined two-word pattern to generate a password pattern.

Usage

The guest portal WLAN must be configured.

redirect

Use the `redirect` command, within context `wlan:<WLAN-service-name>:auth:captiveportal`, to specify the Default Redirection URL.

After you run the `redirect` command, run the `apply` command to implement the changes.

redirect *value_string* | **none**

Parameters

<i>value_string</i>	Specifies a URL beginning with <code>http://</code>
none	Specifies that no Default Redirection URL is configured

Usage

The `guestportal`, `internal` or `splash` authentication mode must be set for this command to be available. For more information, see `mode` on page 310.

Example

The following example specifies the internal network URL to which to redirect connecting users:

```
EWC.extremenetworks.com:vnsmode:CNL-7-CP:auth:captiveportal# redirect http://
192.168.1.38
EWC.extremenetworks.com:vnsmode:CNL-7-CP:auth:captiveportal# apply
```

send-login

Use this command to specify the type of captive portal redirection URL for successful logins. The `send-login` command is available from the `wlan:<WLAN-service-name>:auth:captiveportal` context.

send-login *original-dest* | **cp-session** | **custom**

Parameters

original-dest	Use the original destination value configured by the Wireless Assistant GUI.
cp-session	Use the captive portal session page value configured by the Wireless Assistant GUI.
custom	Use the custom specific URL value configured by the Wireless Assistant GUI.

Example

This example specifies that the type of successful login redirection URL is custom:

```
EWC.extremenetworks.com:wlans:Lab126-12-Int-CP:auth:captiveportal# send-login
custom
```

set-acct-lifetime

Use this command to enable or disable the ability of the Guest Administrator to set account lifetimes. The `set-acct-lifetime` command is available from the `wlan:<WLAN-service-name>:auth:captiveportal` context for guest portal mode only.

set-acct-lifetime **enable** | **disable**

Parameters

enable	Enables the ability of the Guest Administrator to set account lifetimes.
disable	Disables the ability of the Guest Administrator to set account lifetimes. Disabled is the default.

Usage

If this feature is enabled, after the guest administrator logs in, the “Account Lifetime” field will be enabled when updating accounts or adding new guest accounts.

Example

This example enables the ability of the Guest Administrator to set account lifetimes:

```
EWC.extremenetworks.com:wlans:Lab126-12-GuestP:auth:captiveportal# set-acct-lifetime enable
```

tos-override

Use the `tos-override` command, within context `wlan:<WLAN-service-name>:auth:captiveportal`, to enable or disable external portal integration with Policy Manager (NAC). This command is available when the named WLAN service is in “external” mode.

After you run the `tos-override` command, run the `apply` command to implement the changes.

tos-override (enable tos *HH*) | disable

Parameters

enable tos	Enables ToS override
<i>HH</i>	Specifies a hexadecimal value for ToS override. For the NAC integration, this should be 40 (0x40)
disable	Disables ToS override

Usage

This command is used to configure an external portal integration with NAC where HTTP traffic for non authenticated users is tagged with a ToS override value. To integrate with NAC, you must use this command to set the hexadecimal ToS override value on the controller to 0x40.

The external authentication mode must be set for this command to be available. For more information, see [mode](#) on page 310.

Example

The following example enables ToS override with the hex value required for NAC integration (0x40):

```
EWC.extremenetworks.com:wlans:new-wlans:auth:captiveportal# tos-override
enable tos 40
EWC.extremenetworks.com:wlans:new-wlans:auth:captiveportal# apply
EWC.extremenetworks.com:wlans:new-wlans:auth:captiveportal# show tos-override
ToS override for NAC Value(Hex):0x40
```

cdr

Use the `cdr` command to enable or disable the collection of Wireless Controller accounting information. The `cdr` command is accessible from the `wlan:<WLAN-service-name>:auth` context of the CLI.

After you run the `cdr` command, run the `apply` command to implement the changes.

cdr enable | disable

Parameters

enable disable	Specifies to enable or disable the collection of Wireless Controller accounting information
-------------------------	---

Usage

The `cdr` command is available in all authentication modes. For more information, see [mode](#) on page 310.

Example

The following example enables the collection of Wireless Controller accounting information:

```
EWC.extremenetworks.com:wlans:test:auth# cdr enable
EWC.extremenetworks.com:wlans:test:auth# apply
EWC.extremenetworks.com:wlans:test:auth# show cdr
Collecting accounting information of Wireless Controller: enable
```

config

The `config` command defines RADIUS server settings for the named WLAN service in the current context, overriding default RADIUS server configuration. The `config` command is accessible from the `wlan:<WLAN-service-name>:auth` context of the CLI. Use this command to configure the RADIUS server as an accounting, authentication or MAC authentication server.

```
config (radius (role acct|auth|mac) [prot CHAP | PAP | MS-CHAP | MS-CHAP2])
```

Parameters

<i>radius</i>	Specifies the name of the RADIUS server to configure
role acct auth mac	Specifies the role of the RADIUS server as accounting, authentication, or MAC authentication server, respectively.
prot CHAP PAP MS-CHAP MS-CHAP2]	Specifies the Authentication type

Usage

The `config` command is not available when the authentication mode is `guestportal`. When the authentication mode is disabled, MAC must be enabled for this command to be available. For authentication `mode` command information, see [mode](#) on page 310. For `mac` command information, see [mac](#) on page 308.

For third party APs SSIDs, this command is only visible when `mac` is set to enable and only `mac` authentication is supported.

After executing the `config` command to configure a RADIUS server, you can proceed to configure additional server attributes such as NAS ID and NAS IP address. When you are finished configuring RADIUS server attributes, use the `exit` command to return to the `wlan:<WLAN-service-name>` context.

Example

The following example configures the RADIUS server “radius1” as an authentication server:

```
EWC.extremenetworks.com:wlans:cnl-AAA:auth# config radius1 role auth prot PAP
EWC.extremenetworks.com:wlans:cnl-AAA:auth# show
Current selected Radius server radius1 role auth
Priority Name      Role  NAS IP                NAS ID          Auth Type
1       radius1  auth  Use VNS IP address   Use VNS name    PAP
NAS identifier: Use VNS name
NAS IP address: Use VNS IP address
Authentication type: PAP
```

config exit

Use the `config exit` command to exit the RADIUS server configuration mode. The `config exit` command is accessible from the `wlans:<WLAN-service-name>:auth` context of the CLI.

```
config exit
```

Parameters

None

Usage

Using the `config exit` command from within the RADIUS server configuration command mode exits the `wlans:<WLAN-service-name>:auth` RADIUS server configuration context and places you in the `wlans:<WLAN-service-name>:auth` context.

Example

The following example exits the RADIUS server configuration command mode:

```
EWC.extremenetworks.com:wlans:cnl-AAA:auth# config exit
EWC.extremenetworks.com:wlans:cnl-AAA:auth#
```

fast-failover

Use the `fast-failover` command in the `wlans:<WLAN-service-name>:auth` RADIUS server configuration context to enable or disable the sending of interim account records (to the RADIUS server) when a failover occurs and the session home moves to the availability partner.

After you run the `fast-failover` command, run the `apply` command to implement the changes.

```
fast-failover (enable | disable)
```

Parameters

enable	Enables the sending of interim account records to RADIUS for fast failover.
disable	Disables the sending of interim account records to RADIUS for fast failover.

Usage

This command overwrites the global RADIUS fast-failover command.

To get to the RADIUS server configuration, enter the `config <named radius> role acct` command. After applying changes, exit the RADIUS server configuration context by the `config exit` command.

Examples

This example disables fast failover:

```
EWC.extremenetworks.com:wlans:cn1-AAA:auth# fast-failover disable
EWC.extremenetworks.com:wlans:cn1-AAA:auth# apply
```

include-cui-type

Use the `include-cui-type` command to enable or disable including the Chargeable-User-Identity attribute in the Access-Request message. The `include-cui-type` command is accessible from the `wlans:<named wlans>:auth` context of the CLI.

include-cui-type (**enable** | **disable**)

Parameters

enable	Enables the Chargeable-User-Identity attribute in Access-Request message.
disable	Disables the Chargeable-User-Identity attribute in Access-Request message.

Examples

The following example enables the Chargeable-User-Identity attribute in Access-Request message:

```
EWC.extremenetworks.com:wlans:Lab184-AAA:auth# include-cui-type enable
```

interim

Use the `interim` command to configure the RADIUS accounting server interim accounting interval. The `interim` command is accessible from the `wlans:<WLAN-service-name>:auth` context of the CLI.

interim *interim-interval-value*

Parameters

<i>interim-interval-value</i>	Specify an integer value in minutes for the interim interval. The default value is 30 minutes.
-------------------------------	--

Usage

The `interim` command is not available when the authentication mode is `guestportal`. When the authentication mode is disabled, MAC must be enabled for this command to be available. For authentication `mode` command information, see `mode` on page 310. For `mac` command information, see `mac` on page 308.

Example

The following example sets the interim value to 40 minutes:

```
EWC.extremenetworks.com:wlans:test:auth# interim 40
```

mac

Use the `mac` command to enable or disable MAC based authentication. The `mac` command is accessible from the `wlan:<WLAN-service-name>:auth` context of the CLI.

mac enable | disable

Parameters

enable disable	Specifies to enable or disable MAC based authentication
-------------------------	---

Usage

The `mac` command is not available in the guest splash and guest portal authentication modes. For more information, see [mode](#) on page 310.

Example

The following example enables MAC authentication for the test WLANS:

```
EWC.extremenetworks.com:wlans:test:auth# mac enable
EWC.extremenetworks.com:wlans:test:auth# show mac
MAC based authorization: enable
```

mac-acct

Use the `mac-acct` command in the `wlan:<WLAN-service-name>:auth` context to enable or disable the beginning of RADIUS accounting after MAC-based authorization completes.

After you run the `mac-acct` command, run the `apply` command to implement the changes.

mac-acct (enable | disable)

Parameters

enable	Enables the recording of MAC account records on RADIUS after authorization.
disable	Disables the recording of MAC account records on RADIUS after authorization.

Usage

This command is available only when MAC-based authorization is enabled (see [mac](#) command in the `wlan:<WLAN-service-name>:auth` context).

Example

This example disables RADIUS recording of MAC records after authentication:

```
EWC.extremenetworks.com:wlans:cn1-AAA:auth# mac-acct disable
EWC.extremenetworks.com:wlans:cn1-AAA:auth# apply
```

mac-auto-authenticate

Use the `mac-auto-authenticate` command to automatically authenticate authorized users. The `mac-auto-authenticate` command is accessible from the `wlan:<WLAN-service-name>:auth` context of the CLI.

After you run the `mac-auto-authenticate` command, run the `apply` command to implement the changes.

mac-auto-authenticate enable | disable

Parameters

enable disable	Specify to enable or disable automatic authentication of authorized users
-------------------------	---

Usage

The `mac-auto-authenticate` command is available in all authentication modes, if MAC authentication is enabled, using the `mac enable` command. For authentication `mode` command information, see [mode](#) on page 310. For `mac` command information, see [mac](#) on page 308.

Example

The following example enables automatic authentication of authorized users on the `cnl-mac` WLANS service:

```
EWC.extremenetworks.com:wlans:cnl-mac:auth# mac-auto-authenticate enable
EWC.extremenetworks.com:wlans:cnl-mac:auth# apply
```

mac-allow-unauthorized

Use the `mac-allow-unauthorized` command to allow the authentication of unauthorized users. The `mac-allow-unauthorized` command is accessible from the `wlans:<WLAN-service-name>:auth` context of the CLI.

After you run the `mac-allow-unauthorized` command, run the `apply` command to implement the changes.

mac-allow-unauthorized enable | disable

Parameters

enable disable	Specify to enable or disable the authentication of unauthorized users on this WLANS service
-------------------------	---

Usage

The `mac-allow-unauthorized` command is available in all authentication modes, if MAC authentication is enabled, using the `mac enable` command. For authentication `mode` command information, see [mode](#) on page 310. For `mac` command information, see [mac](#) on page 308.

Example

The following example enables the authentication of unauthorized users for the `cnl-mac` WLANS service:

```
EWC.extremenetworks.com:wlans:cnl-mac:auth# mac-allow-unauthorized enable
EWC.extremenetworks.com:wlans:cnl-mac:auth# apply
```

mac-roam

Use the `mac-roam` command to enable, disable, or allow area change for MAC-based authentication on roam. The `mac-roam` command is accessible from the `wlans:<WLAN-service-name>:auth` context of the CLI.

After you run the `mac-roam` command, run the `apply` command to implement the changes.

mac-roam never | inter-ap-roam | inter-area-roam

Parameters

never	Specify MAC authentication on roam as disabled.
inter-ap-roam	Specify MAC authentication on roam as enabled.
inter-area-roam	Specify MAC authentication on roam as allowing area change.

Usage

The `mac-roam` command is not available in the guest splash and guest portal authentication modes, if MAC authentication is enabled, using the `mac enable` command. For authentication `mode` command information, see [mode](#) on page 310. For `mac` command information, see [mac](#) on page 308.

Example

The following example enables MAC authentication on roam for the `cnl-mac` WLAN service:

```
EWC.extremenetworks.com:wlans:cnl-mac:auth# mac-roam inter-ap-roam
EWC.extremenetworks.com:wlans:cnl-mac:auth# apply
```

mode

Use the `mode` command to configure the authentication mode for the WLAN service. The `mode` command determines which authentication commands are available.

The `mode` command is accessible from the `wlan:<WLAN-service-name>:auth` context of the CLI.

For information on the captive portal context, see [default-topology](#) on page 321.

After you run the `mode` command, run the `apply` command to implement the changes.

mode disabled | 8021x | internal | external | guestportal | splash | external-by-firewall

Parameters

disabled	Disables authentication modes
8021x	Enters the 802.1x authentication mode
internal	Enters the internal captive portal authentication mode
external	Enters the external captive portal authentication mode
guestportal	Enters the guestportal captive portal authentication mode
splash	Specifies the guest splash captive portal authentication mode
external-by-firewall	Enters the external by firewall authentication mode

External-by-firewall

You can configure the external-by-firewall parameter with additional commands.

add-ap-name-sn	Enable or disable adding AP name and serial number to redirection URL.
add-bssid	Enable or disable adding associated BSSID to redirection URL.
add-ip-port	Enable or disable adding IP and Port to redirection URL.
add-mac	Enable or disable adding User's MAC address to redirection URL.
add-role	Enable or disable adding currently assigned role to redirection URL.
add-sign	Enable or disable adding signature to redirection URL.
add-time	Enable or disable adding timestamp request received by controller to redirection URL.
add-vlan	Enable or disable adding containment VLAN (if any) of assigned role to redirection URL.
add-vns	Enable or disable adding VNS Name to redirection URL.
apply	Apply the command setting.
cp-https	Enable or disable https support.
end	Return to the base mode.
exit	Return to the previous mode.
extredirect	Set external redirection URL.
extsecret	Set the Shared Secret password.
fqdn	Set the string to replace the Gateway IP address with a FQDN.
identity	Set Identity.
logout	Logout.
send-login	Type of CP redirection URL.
show	Display settings.

Example

The following example sets the authentication mode to external captive portal:

```
EWC.extremenetworks.com:wlans:test:auth# mode external
EWC.extremenetworks.com:wlans:test:auth# apply
EWC.extremenetworks.com:wlans:test:auth# show mode
Authentication mode: external
```

move

Use the `move` command, from within the RADIUS server configuration command mode, to change the position of a RADIUS server in the RADIUS server list. The `move` command is accessible from the `wlans:<WLAN-service-name>:auth` context of the CLI.

After you run the `move` command, run the `apply` command to implement the changes.

```
move current-position new-position
```

Parameters

<i>current-position</i>	Specifies the current position of the RADIUS server in the RADIUS server list. Valid values are from 1 - 32.
<i>new-position</i>	Specifies the new position of the RADIUS server in the RADIUS server list. Valid values are from 1 - 32.

Usage

You must be in RADIUS server configuration mode for the `move` command to be available. Use the `config` command to enter RADIUS server configuration mode. For more information, see [config](#) on page 305.

Example

The following example moves the RADIUS server in the RADIUS server list position 2 to position 1 in the RADIUS server list:

```
EWC.extremenetworks.com:wlans:cnl-AAA:auth# move 2 1
EWC.extremenetworks.com:wlans:cnl-AAA:auth# apply
```

nasid

Use the `nasid` command to identify the Network Access Server (NAS) to be used with the RADIUS server being configured. The `nasid` command is accessible from the `wlans:<WLAN-service-name>:auth` context of the CLI.

After you run the `nasid` command, run the `apply` command to implement the changes.

nasid *string* | **vnsname**

Parameters

<i>string</i>	Specify the ID for the NAS
vnsname	Specifies that the VNS name should be used for the NAS ID

Usage

The NAS ID defaults to the VNS name if this command is not used to specify a NAS ID.

You must be in RADIUS server configuration mode for the `nasid` command to be available. Use the `config` command to enter RADIUS server configuration mode. For more information, see [config](#) on page 305.

Example

The following example sets the NAS ID for this RADIUS server configuration to the VNS name for the `cnl-AAA` WLANS auth context:

```
EWC.extremenetworks.com:wlans:cnl-AAA:auth# nasid vnsname
EWC.extremenetworks.com:wlans:cnl-AAA:auth# apply
EWC.extremenetworks.com:wlans:cnl-AAA:auth# show nasid
NAS identifier: Use VNS name
```


nasip

Use the `nasip` command to configure the NAS IP address to be used with the RADIUS server being configured. The `nasip` command is accessible from the `wlans:<WLAN-service-name>:auth` context of the CLI.

After you run the `nasip` command, run the `apply` command to implement the changes.

```
nasip A.B.C.D | vnsip
```

Parameters

<i>A.B.C.D</i>	Specify the NAS IP address
vnsip	Specifies that the VNS IP address should be used for the NAS IP address

Usage

The NAS IP address defaults to the VNS IP address if this command is not used to specify a NAS IP address.

You must be in RADIUS server configuration mode for the `nasip` command to be available. Use the `config` command to enter RADIUS server configuration mode. For more information, see [config](#) on page 305.

Example

The following example sets the NAS IP address for this RADIUS server configuration to the VNS IP address for the `cnl-AAA` WLANS auth context:

```
EWC.extremenetworks.com:wlans:cnl-AAA:auth# nasip vnsip
EWC.extremenetworks.com:wlans:cnl-AAA:auth# apply
EWC.extremenetworks.com:wlans:cnl-AAA:auth# show nasip
NAS identifier: Use VNS IP address
```

password

Use the `password` command to specify the MAC authentication password to be used with the RADIUS server being configured. The `password` command is accessible from within the RADIUS server configuration mode from the `wlans:<WLAN-service-name>:auth` context of the CLI.

After you run the `password` command, run the `apply` command to implement the changes.

```
password password
```

Parameters

<i>password</i>	Specify the MAC authentication password
-----------------	---

Usage

You must be in RADIUS server configuration mode for the `password` command to be available. Use the `config` command to enter RADIUS server configuration mode. For more information, see [config](#) on page 305.

Example

The following example sets the MAC authentication password to techdoc:

```
EWC.extremenetworks.com:wlans:cn1-AAA:auth# password techdoc
EWC.extremenetworks.com:wlans:cn1-AAA:auth# apply
```

protocol

Use the `protocol` command to configure the authentication protocol to be used with the RADIUS server being configured. The `protocol` command is accessible from the `wlans:<WLAN-service-name>:auth` context of the CLI.

After you run the `protocol` command, run the `apply` command to implement the changes.

protocol **CHAP** | **PAP** | **MS-CHAP** | **MS-CHAP2**

Parameters

CHAP	Configures the Challenge Handshake Authentication Protocol as the authentication protocol
PAP	Configures the Password Authentication Protocol as the authentication protocol
MS-CHAP	Configures the Windows specific version of CHAP as the authentication protocol
MS-CHAP2	Configures the Windows specific version (Version 2) of CHAP as the authentication protocol

Usage

You must be in RADIUS server configuration mode for the `protocol` command to be available. Use the `config` command to enter RADIUS server configuration mode. For more information, see [config](#) on page 305.

Example

The following example configures the CHAP protocol as the authentication protocol for this RADIUS server:

```
EWC.extremenetworks.com:wlans:cn1-AAA:auth# protocol CHAP
EWC.extremenetworks.com:wlans:cn1-AAA:auth# apply
```

radius-timeout-policy

The `radius-timeout-policy` command within context `wlan:<WLAN-service-name>:auth` sets the specified policy from the list of configured policies to apply when the authentication request to the RADIUS server times out. By default, the `treat-like-access-reject` policy is applied when authentication requests time out.

After you run the `protocol` command, run the `apply` command to implement the changes.

radius-timeout-policy *policy name* | **treat-like-access-reject**

Parameters

<i>policy name</i>	Specifies the name of the policy to apply when an authentication request times out.
treat-like-access-reject	Specifies that the authentication request be treated as an authentication failure when the authentication request times out. This is the default.

Usage

The following configurations must already be in place before this command is available:

- <radius-server>
- config <radius-server> role mac
- mac enable

See [role_commands](#) for creating and naming policies.

Example

The following example selects the p6 policy to apply when authentication queries to this RADIUS server time out:

```
EWC.extremenetworks.com:wlans:new-wlans:auth# radius-timeout-policy p6
```

remove

The `remove` command within context `wlan:<WLAN-service-name>:auth` removes the specified RADIUS server from the list of configured RADIUS servers.

```
remove radius
```

Parameters

<i>radius</i>	Specifies the name of the RADIUS server to remove.
---------------	--

Example

The following example removed the RADIUS server “radius1” from the list of RADIUS servers to be used with the “new-wlans” WLAN:

```
EWC.extremenetworks.com:wlans:new-wlans:auth# remove radius1
```

show

Use the `show` command to display the current authentication settings of the specified individual WLAN service. The `show` command is accessible from the `wlan:<WLAN-service-name>:auth` context of the CLI.

The following example displays the current authentication settings for the WLAN service named Lab126-12-AAA:

```
EWC.extremenetworks.com:wlans:Lab126-12-AAA:auth# show
No radius server has been selected
Priority Name Role NAS IP NAS ID Auth Type
1 IAS auth Use VNS IP address Use VNS name EAP
1 IAS acct Use VNS IP address Use VNS name
MAC-based authorization: disable
```

```

Authentication mode: 8021x
AP as VSA attribute: enable
SSID as VSA attribute: enable
VNS as VSA attribute: enable
Policy as VSA attribute: enable
Topology as VSA attribute: enable
Ingress rate control as VSA attribute: enable
Egress rate control as VSA attribute: enable
Interim interval (minutes): 0
Collecting accounting information of Wireless Controller: disable
With external: disable

```

Figure 2: Examples

use-policy-zone

Use the `use-policy-zone` command to enable or disable a policy zone at a called station. The `use-policy-zone` command is accessible from the `wlan:<WLAN-service-name>:auth` context of the CLI.

After you run the `use-policy-zone` command, run the `apply` command to implement the changes.

use-policy-zone enable | disable

Parameters

enable disable	Enables or disables the policy zone on this WLAN.
-------------------------	---

Example

The following example enables the policy zone on the test WLAN:

```

EWC.extremenetworks.com:wlans:test:auth# use-policy-zone enable
EWC.extremenetworks.com:wlans:test:auth# apply
EWC.extremenetworks.com:wlans:test:auth# show use-policy-zone
Use policy zone name in Called-Station-Id: enable

```

vsa-ap

Use the `vsa-ap` command to include AP Identification in the message to the RADIUS server. The `vsa-ap` command is accessible from the `wlan:<WLAN-service-name>:auth` context of the CLI.

After you run the `vsa-ap` command, run the `apply` command to implement the changes.

vsa-ap enable | disable

Parameters

enable disable	Enables or disables the inclusion of AP Identification information in messages to the RADIUS server.
-------------------------	--

Usage

The `vsa-ap` command is not available when the authentication mode is `guestportal`. When the authentication mode is disabled, MAC must be enabled for this command to be available. For more information, see [mode](#) on page 310.

Example

The following example enables the inclusion of AP Identification information in messages to the RADIUS server:

```
EWC.extremenetworks.com:wlans:test:auth# vsa-ap enable
EWC.extremenetworks.com:wlans:test:auth# apply
EWC.extremenetworks.com:wlans:test:auth# show vsa-ap
AP as VSA attribute: enable
```

vsa-egress

Use the `vsa-egress` command to include egress rate control information in the message to the RADIUS server. The `vsa-egress` command is accessible from the `wlan:<WLAN-service-name>:auth` context of the CLI.

After you run this command, run the `apply` command to implement the changes.

vsa-egress enable | disable

Parameters

enable disable	Specifies to enable or disable the inclusion of egress rate control information in messages to the RADIUS server
-------------------------	--

Usage

The `vsa-egress` command is not available when the authentication mode is `guestportal`. When the authentication mode is `disabled`, `MAC` must be enabled for this command to be available. For more information, see [mode](#) on page 310.

Example

The following example enables the inclusion of egress rate control information in messages to the RADIUS server:

```
EWC.extremenetworks.com:wlans:test:auth# vsa-egress enable
EWC.extremenetworks.com:wlans:test:auth# apply
EWC.extremenetworks.com:wlans:test:auth# show vsa-egress
Egress rate control as VSA attribute: enable
```

vsa-ingress

Use the `vsa-ingress` command to include ingress rate control information in the message to the RADIUS server. The `vsa-ingress` command is accessible from the `wlan:<WLAN-service-name>:auth` context of the CLI.

After you run this command, run the `apply` command to implement the changes.

vsa-ingress enable | disable

Parameters

enable disable	Specifies to enable or disable the inclusion of ingress rate control information in messages to the RADIUS server.
-------------------------	--

Usage

The `vsa-ingress` command is not available when the authentication mode is guestportal. When the authentication mode is disabled, MAC must be enabled for this command to be available. For more information, see [mode](#) on page 310.

Example

The following example enables the inclusion of ingress rate control information in messages to the RADIUS server:

```
EWC.extremenetworks.com:wlans:test:auth# vsa-ingress enable
EWC.extremenetworks.com:wlans:test:auth# apply
EWC.extremenetworks.com:wlans:test:auth# show vsa-ingress
Ingress as VSA attribute: enable
```

vsa-policy

Use the `vsa-policy` command to include policy information in the message to the RADIUS server. The `vsa-policy` command is accessible from the `wlan:<WLAN-service-name>:auth` context of the CLI.

After you run the `vsa-policy` command, run the `apply` command to implement the changes.

vsa-policy enable | disable

Parameters

enable disable	Specifies to enable or disable the inclusion of policy information in messages to the RADIUS server.
-------------------------	--

Usage

The `vsa-policy` command is not available when the authentication mode is guestportal. When the authentication mode is disabled, MAC must be enabled for this command to be available. For more information, see [mode](#) on page 310.

Example

The following example enables the inclusion of policy information in the message to the RADIUS server:

```
EWC.extremenetworks.com:wlans:test:auth# vsa-policy enable
EWC.extremenetworks.com:wlans:test:auth# apply
EWC.extremenetworks.com:wlans:test:auth# show vsa-policy
Policy as VSA attribute: enable
```

vsa-ssid

Use the `vsa-ssid` command to include SSID information in the message to the RADIUS server. The `vsa-ssid` command is accessible from the `wlan:<WLAN-service-name>:auth` context of the CLI.

After you run the `vsa-ssid` command, run the `apply` command to implement the changes.

vsa-ssid enable | disable

Parameters

enable disable	Specifies to enable or disable the inclusion of SSID information in messages to the RADIUS server.
-------------------------	--

Usage

The `vsa-ssid` command is not available when the authentication mode is guestportal. When the authentication mode is disabled, MAC must be enabled for this command to be available. For more information, see [mode](#) on page 310.

Example

The following example enables the inclusion of SSID information in messages to the RADIUS server:

```
EWC.extremenetworks.com:wlans:test:auth# vsa-ssid enable
EWC.extremenetworks.com:wlans:test:auth# apply
EWC.extremenetworks.com:wlans:test:auth# show vsa-ssid
SSID as VSA attribute: enable
```

vsa-topology

Use the `vsa-topology` command to include topology information in the message to the RADIUS server. The `vsa-topology` command is accessible from the `wlan:<WLAN-service-name>:auth` context of the CLI.

After you run the `vsa-topology` command, run the `apply` command to implement the changes.

vsa-topology enable | disable

Parameters

enable disable	Specifies to enable or disable the inclusion of Topology information in messages to the RADIUS server.
-------------------------	--

Usage

The `vsa-topology` command is not available when the authentication mode is guestportal. When the authentication mode is disabled, MAC must be enabled for this command to be available. For more information, see [mode](#) on page 310.

Example

The following example enables the inclusion of Topology information in messages to the RADIUS server:

```
EWC.extremenetworks.com:wlans:test:auth# vsa-topology enable
EWC.extremenetworks.com:wlans:test:auth# apply
EWC.extremenetworks.com:wlans:test:auth# show vsa-topology
Topology as VSA attribute: enable
```

vsa-vns

Use the `vsa-vns` command to include VNS information in the message to the RADIUS server. The `vsa-vns` command is accessible from the `wlan:<WLAN-service-name>:auth` context of the CLI.

After you run the `vsa-vns` command, run the `apply` command to implement the changes.

vsa-vns enable | disable

Parameters

enable disable	Specifies to enable or disable the inclusion of VNS information in messages to the RADIUS server.
-------------------------	---

Usage

The `vsa-vns` command is not available when the authentication mode is `guestportal`. When the authentication mode is `disabled`, MAC must be enabled for this command to be available. For more information, see [mode](#) on page 310.

Example

The following example enables the inclusion of VNS information in messages to the RADIUS server:

```
EWC.extremenetworks.com:wlans:test:auth# vsa-vns enable
EWC.extremenetworks.com:wlans:test:auth# apply
EWC.extremenetworks.com:wlans:test:auth# show vsa-vns
VNS as VSA attribute: enable
```

backhaul-radio

Use this command to configure the backhaul radio band for a dynamic mesh WLAN service. The `backhaul-radio` command is accessible from the `wlans:<WLAN-service-name>` context of the CLI for dynamic mesh type WLAN services.

backhaul-radio a | bg

Parameters

a	Select the 5 GHz radio band
bg	Select the 2.4 GHz radio band

Usage

After this command has been executed for the dynamic mesh WLAN service being configured, it will no longer be available.

Example

This example selects the 5 GHz radio band for the dynamic mesh WLAN service named `mesh1-wlan`:

```
EWC.extremenetworks.com:wlans:mesh1-wlan# backhaul-radio a
```

cp-http

Use the `cp-http` command to enable HTTP support for a WLANs service captive portal context.

cp-http enable | disable

Parameters

enable	Enables HTTP support for the current context
disable	Disables HTTP support for the current context

Usage

The internal or splash authentication mode must be set for this command to be available. For more authentication mode information, see [mode](#) on page 310.

Example

The following example enables HTTP support for the Lab126-12-GuestSpl WLAN service:

```
EWC.extremenetworks.com:wlans:Lab126-12-GuestSpl:auth:captiveportal# cp-http
enable
```

default-cos

Use the `default-cos` command to assign an existing Class of Service (CoS) as the default CoS for the specified WLAN service. You can also use the `default-cos` command to unassign the default cos. The `default-cos` command is accessible from the `wlans:<WLAN-service-name>` context of the CLI.

For information about Class of Service, refer to [cos Commands](#) on page 430.

default-cos *named-cos* | **none**

Parameters

<i>named-cos</i>	Specify a named-cos to assign to the WLAN service as a default CoS.
none	unassign the default CoS from the WLAN service

Example

The following example assigns the cos my-cos to the WLAN service:

```
EWC.extremenetworks.com:wlans:gpl# default-cos my-cos
```

default-topology

Use the `default-topology` command to assign an existing B@AC, B@AP, or routed topology as the default topology for the specified WLAN service. You can also use the `default-topology` command to unassign the default topology. The `default-topology` command is accessible from the `wlans:<WLAN-service-name>` context of the CLI.

For information about B@AC, B@AP, and routed topologies, refer to [topology Commands](#) on page 387.

default-topology *Default topology name* | **none**

Parameters

<i>Default topology name</i>	Specify default topology to assign to the WLAN service
none	Unassign the default topology from the WLAN service

Example

The following example assigns the topology FS-REMOTE to the WLAN service:

```
EWC.extremenetworks.com:wlans:gp1# default-topology FS-REMOTE
```

default-traffic-mirror

Use the `default-traffic-mirror` command to configure the default traffic mirror. The `default-traffic-mirror` command is accessible from the `wlans:<named-wlan>` context of the CLI.

default-traffic-mirror (**prohibited** | **enable-both-directions** | **enable-in-direction-only**)

Parameters

prohibited enable-in-both-directions enable-in-direction-only	Configures the default traffic mirror for prohibited, enabled in both directions, or enabled in the in direction only.
--	--

Example

The following example configures the default traffic mirror to be enabled in both directions:

```
EWC.extremenetworks.com:wlans:HT_BR# default-traffic-mirror enable-both-directions
```

direct-client-traffic

Use the `direct-client-traffic` command to enable or disable the blocking of direct client to client communication. The `direct-client-traffic` command is accessible from the `wlans:<WLAN-service-name>` context of the CLI.

After you run the `direct-client-traffic` command, run the `apply` command to implement the changes.

direct-client-traffic **enable** | **disable**

Parameters

enable	Specify to block direct client to client communication
disable	Specify to allow direct client to client communication

Example

The following example specifies to block direct client to client communication:

```
EWC.extremenetworks.com:wlans:test# direct-client-traffic enable
EWC.extremenetworks.com:wlans:test# apply
EWC.extremenetworks.com:wlans:test# show direct-client-traffic
Block MU to MU traffic: enable
```

egress-filtering

Use the `egress-filtering` command to enable or disable egress filtering on this WLAN service. The `egress-filtering` command is accessible from the `wlans:<WLAN-service-name>` context of the CLI.

After you run the `egress-filtering` command, run the `apply` command to implement the changes.

egress-filtering enable | disable

Parameters

enable	Enables filtering on this WLAN service.
disable	Disables filtering on this WLAN service.

Example

The following example enables filtering on the test WLAN:

```
EWC.extremenetworks.com:wlans:test# egress-filtering enable
EWC.extremenetworks.com:wlans:test# apply
EWC.extremenetworks.com:wlans:test# show
Egress Filtering: enable
```

interwlan-roaming

Use this command to enable or disable inter-WLAN roaming on this WLAN service. The `interwlan-roaming` command is accessible from the `wlan:<WLAN-service-name>` context of the CLI.

interwlan-roaming enable|disable

Parameters

enable	Enables the inter-WLAN roaming feature for this WLAN service. This is the default setting.
disable	Disables the inter-WLAN roaming feature.

Example

This example disables inter-WLAN roaming on the WLAN service named test:

```
EWC.extremenetworks.com:test# interwlan-roaming disable
```

name

Use the `name` command to modify the name of this WLAN service. The `name` command is accessible from the `wlan:<WLAN-service-name>` context of the CLI when the WLAN service type is STD.

After you run the `name` command, run the `apply` command to implement the name change.

name *WLAN-service-name*

Parameters

<i>WLAN-service-name</i>	Specifies the name to use for this WLAN service
--------------------------	---

Example

The following example changes the name of the test WLAN serve to “not-test”:

```
EWC.extremenetworks.com:wlans:test# name not-test
EWC.extremenetworks.com:wlans:test# apply
EWC.extremenetworks.com:wlans:test# show name
Name: not-test
```

netflow

Use the `netflow` command to enable or disable NetFlow on the named WLAN. The `netflow` command is accessible from the `wlans:<named-wlan>` context of the CLI.

netflow (enable | disable)

Parameters

enable disable	Enables or disables NetFlow on the named WLAN.
-------------------------	--

Example

The following example enables NetFlow on the HT_BR WLAN:

```
EWC.extremenetworks.com:wlans:HT_BR# netflow enable
```

priv

The `priv` command moves you to the `wlan:<WLAN-service-name>:priv` context, which contains commands to configure the privacy mode of the specified individual WLAN service.

The following commands are available in the `wlan:<WLAN-service-name>:priv` context.

- [group-key-ps](#) on page 325
- [mode](#) on page 325
- [wep](#) on page 326
- [wpa-broadcast-rekey](#) on page 327
- [wpa-v1](#) on page 327
- [wpa-v2](#) on page 328
- [wpa-v2-key-mgmt](#) on page 328

fast-transition

Use the `fast-transition` command to enable and disable 802.11r Fast Transition. The `fast-transition` command is accessible from the `wlan:<WLAN-service-name>:priv` context of the CLI.

fast-transition enable | disable

Parameters

enable disable	Enables or disables 802.11r Fast Transition.
-------------------------	--

Example

The following example enables 802.11k Fast Transition support on the WLAN service:

```
EWC.extremenetworks.com:wlans:AZ-723-WLAN1:priv# fast-transition enable
```

group-key-ps

Use the `group-key-ps` command to enable or disable the group key power save retry. The `group-key-ps` command is available only if the `mode` command is set to `wpa-psk`. The `group-key-ps` command is accessible from the `wlan:<WLAN-service-name>;priv` context of the CLI when the WLAN service type is STD.

group-key-ps enable | disable

Parameters

enable	Specify to enable the group key power save retry.
disable	Specify to disable the group key power save retry.

Example

The following example enable the group key power save retry on the WLAN CNL-208-0:

```
EWC.extremenetworks.com:wlans:CNL-208-0:priv# group-key-ps enable
```

mfp

Use the `mfp` command to configure MFP. The `mfp` command is accessible from the `wlan:<WLAN-service-name>;priv` context of the CLI.

mfp require | enable | disable

Parameters

require enable disable	Sets MFP to require, enable, or disable.
-----------------------------------	--

Example

The following example enables MFP on the WLAN service:

```
EWC.extremenetworks.com:wlans:AZ-723-WLAN1:priv# mfp enable
```

mode

Use the `mode` command to set the privacy mode of this WLAN service. The `mode` command is accessible from the `wlan:<WLAN-service-name>;priv` context of the CLI when the WLAN service type is STD.

After you run the `mode` command, you run the `apply` command to implement the name change.

mode none | wep | wpa | wpa-psk | dynwep

Parameters

none	Disables privacy mode
wep	Specifies the WEP privacy mode
wpa	Specifies the WPA privacy mode
wpa-psk	Specifies the WPA-PSK privacy mode
dynwep	Specifies the dynamic WEP privacy mode

Usage

Once you have set the privacy mode, new commands become available in the wlan:<WLAN-service-name>:priv context. For example, setting the privacy mode to `wep` provides an additional command (`wep` on page 326) that you can use to configure WEP settings.

Example

The following example changes the privacy mode of the WLAN service named “test” to WPA-PSK:

```
EWC.extremenetworks.com:wlans:test:priv# mode wpa-psk
EWC.extremenetworks.com:wlans:test:priv# apply
EWC.extremenetworks.com:wlans:test:priv# show mode
Privacy mode: wpa-psk
```

wep

Use the `wep` command to configure WEP privacy settings. The `wep` command is accessible from the wlan:<WLAN-service-name>:priv context of the CLI.

After you run the `wep` command, run the `apply` command to implement the name change.

```
wep key-length 64|128|152 ((key value) | (pass-phrase strings)) [key-idx (1|2|3|4)]
```

Parameters

key-length 64 128 152	Specifies the length of the WEP key (64, 128, or 152 bits)
key value	Specifies the WEP key as a hex value
pass-phrase strings	Specifies the WEP key as a plain text string
key-idx (1 2 3 4)	Specifies the WEP key index

Usage

The `wep` command is available when the privacy `mode` on page 325 is set to `wep`. For more information, see `mode` on page 325.

Example

The following example sets the WEP key to 64 bits in length with a pass phrase string of “S1==p”:

```
EWC.extremenetworks.com:wlans:test:priv# wep key-length 64 pass-phrase S1==p
EWC.extremenetworks.com:wlans:test:priv# apply
EWC.extremenetworks.com:wlans:test:priv# show wep
Static Keys(WEP):
  WEP key length: 64
```

```
Input method: input string
WEP string: Sl=p
```

wpa-broadcast-rekey

Use the `wpa-broadcast-rekey` command to configure the re-key interval for group keys. The `wpa-broadcast-rekey` command is accessible from the `wlan:<WLAN-service-name>;priv` context of the CLI.

After you run the `wpa-broadcast-rekey` command, run the `apply` command to implement the name change.

wpa-broadcast-rekey none | 30-86400

Parameters

none	Disables the re-key interval for group keys
30-86400	Specifies the re-key interval for group keys in seconds

Usage

The `wpa-broadcast-rekey` command is available when the privacy `mode` on page 325 is set to `wpa` or `wpa-psk`. For more information, see `mode` on page 325.

Example

The following example sets the WPA re-key interval to 300 seconds:

```
EWC.extremenetworks.com:wlans:test:priv# wpa-broadcast-rekey 300
EWC.extremenetworks.com:wlans:test:priv# apply
EWC.extremenetworks.com:wlans:test:priv# show wpa-broadcast-rekey
Broadcast re-key interval (seconds): 300
```

wpa-v1

Use the `wpa-v1` command to configure the WPA v1 encryption protocol. The `wpa-v1` command is accessible from the `wlan:<WLAN-service-name>;priv` context of the CLI.

After you run the `wpa-v1` command, run the `apply` command to implement the name change.

wpa-v1 auto | tkip | none

Parameters

auto tkip none	Specifies the WPA v1 encryption protocol
---------------------------	--

Usage

The `wpa-v1` command is available when the privacy `mode` on page 325 is set to `wpa` or `wpa-psk`. For more information, see `mode` on page 325.

Example

The following example displays the WPA v1 encryption protocol, sets the WPA v1 encryption protocol to TKIP, and displays the setting:

```
EWC.extremenetworks.com:wlans:test:priv# show wpa-v1
WPA v.1 encryption is not enabled
EWC.extremenetworks.com:wlans:test:priv# wpa-v1 tkip
EWC.extremenetworks.com:wlans:test:priv# apply
EWC.extremenetworks.com:wlans:test:priv# show wpa-v1
WPA v.1 encryption:
```

wpa-v2

Use the `wpa-v2` command to configure the WPA v2 encryption protocol. The `wpa-v2` command is accessible from the `wlan:<WLAN-service-name>;priv` context of the CLI.

After you run the `wpa-v2` command, run the `apply` command to implement the name change.

wpa-v2 auto | aes | none

Parameters

auto aes none	Specifies the WPA v2 encryption protocol
--------------------------	--

Usage

The `wpa-v2` command is available when the `privacy mode` on page 325 is set to `wpa` or `wpa-psk`. For more information, see `mode` on page 325.

Example

The following example displays the WPA v2 encryption protocol, sets the WPA v2 encryption protocol to AES, and displays the setting:

```
EWC.extremenetworks.com:wlans:test:priv# show wpa-v2
WPA v.2 encryption is not enabled
EWC.extremenetworks.com:wlans:test:priv# wpa-v2 aes
EWC.extremenetworks.com:wlans:test:priv# apply
EWC.extremenetworks.com:wlans:test:priv# show wpa-v2
WPA v.2 encryption: aes
```

wpa-v2-key-mgmt

Use the `wpa-v2-key-mgmt` command to configure WPA v2 key management options. The `wpa-v2-key-mgmt` command is accessible from the `wlan:<WLAN-service-name>;priv` context of the CLI.

After you run the `wpa-v2-key-mgmt` command, run the `apply` command to implement the name change.

wpa-v2-key-mgmt none | both | pre-auth | okc

Parameters

none both pre-auth okc	Specifies WPA v2 key management from these options, respectively: none, both pre-authorization and Opportunistic Key Caching (OKC), pre-authorization only, or OKC only
-------------------------------------	---

Usage

The `wpa-v2-key-mgmt` command is available when the privacy `mode` on page 325 is set to `wpa`. This command is not available when the privacy mode is set to `wpa-psk`. For more information, see `mode` on page 325.

Example

The following example sets WPA v2 key management to both pre-authorization and Opportunistic Key Caching (OKC):

```
EWC.extremenetworks.com:wlans:test:priv# wpa-v2-key-mgmt both
EWC.extremenetworks.com:wlans:test:priv# apply
EWC.extremenetworks.com:wlans:test:priv# show wpa-v2-key-mgmt
Key Management Options: both
```

psk

Use the `psk` command to configure a pre-shared key in a dynamic mesh or WDS WLAN service. The `psk` command is accessible from the `wlan:<WLAN-service-name>` context of the CLI for a dynamic mesh or WDS WLAN service.

After you run the `psk` command, run the `apply` command to implement the changes.

psk *shared-secret*

Parameters

<i>shared-secret</i>	Specify a pre-shared key for this dynamic mesh or WDS WLAN service with a key length of between 8 and 63 characters
----------------------	---

Usage

After this command has been used to configure the pre-shared key for a WLAN service, it will no longer be available.

Example

The following example configures the pre-shared key for the WDS WLAN service `wds-test` as `testsecret`:

```
EWC.extremenetworks.com# wlans
EWC.extremenetworks.com:wlans# wds-test
EWC.extremenetworks.com:wlans:wds-test# psk testsecret
EWC.extremenetworks.com:wlans:wds-test# apply
EWC.extremenetworks.com:wlans:wds-test# show
Service type: wds
Pre-shared Key: testsecret
Name: wds-test
Enable status: enable
Pre-shared Key: testsecret
SSID: wdstest
EWC.extremenetworks.com:wlans:wds-test#
```

qos-policy

The `qos-policy` command moves you to the `wlan:<WLAN-service-name>:qos_policy` context, which provides commands for the configuration of QoS support options for the WLAN service.

The following commands are available in the `wlan:<WLAN-service-name>:qos_policy` context.

- [dot11e](#) on page 331
- [downlink](#) on page 331
- [flex-client-access](#) on page 332
- [legacy](#) on page 332
- [priority-map](#) on page 333
- [priority-override](#) on page 333
- [priority-override-dscp](#) on page 334
- [priority-override-up](#) on page 334
- [turbo-voice](#) on page 335
- [uapsd](#) on page 335
- [uplink](#) on page 336
- [wmm](#) on page 336
- [video-admission-control](#) on page 337
- [voice-admission-control](#) on page 337

beffort-admission-control

Use the `beffort-admission-control` command to enable or disable Global Admission Control for Best Effort (BE). The `beffort-admission-control` command is accessible from the `wlans:<named wlans>:qos-policy` context of the CLI.

beffort-admission-control (enable | disable)

Parameters

enable	Enables Global Admission Control for Best Effort (BE).
disable	Disables Global Admission Control for Best Effort (BE).

Examples

The following example enables Global Admission Control for Best Effort (BE):

```
EWC.extremenetworks.com:wlans:v1WLAN:qos-policy# beffort-admission-control
enable
```

bground-admission-control

Use the `bground-admission-control` command to enable or disable Global Admission Control for Background (BK). The `bground-admission-control` command is accessible from the `wlans: <named wlans>:qos-policy` context of the CLI.

bground-admission-control (enable | disable)

Parameters

enable	Enables Global Admission Control for Background (BK).
disable	Disables Global Admission Control for Background (BK).

Examples

The following example enables Global Admission Control for Background (BK):

```
EWC.extremenetworks.com:wlans:v1WLAN:qos-policy# bground-admission-control
enable
```

dot11e

Use the `dot11e` command to enable or disable 802.11e radio QoS support. The `dot11e` command is accessible from the `wlan:<WLAN-service-name>:qos-policy` context of the CLI.

After you run the `dot11e` command, run the `apply` command to implement the changes.

dot11e enable | disable

Parameters

enable disable	Specify to enable or disable 802.11e radio QoS support
-------------------------	--

Example

The following example enables 802.11e support on the Wireless Appliance:

```
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# dot11e enable
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# apply
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# show dot11e
802.11e: enable
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy#
```

downlink

Use the `downlink` command to manage downlink policer action for this WLANS. The `downlink` command is accessible from the `wlan:<WLAN-service-name>:qos-policy` context of the CLI.

After you run the `downlink` command, run the `apply` command to implement the changes.

downlink downgrade | drop | do-nothing

Parameters

downgrade	Specifies that the transmission's data packets are forced to be downgraded to the next priority when a TSPEC violation is discovered.
drop	Specifies that the transmission's data packets are forced to be dropped when a TSPEC violation is discovered.
do-nothing	Specifies that the TSPEC violations are allowed to continue when they are discovered. Data transmissions will continue and no action is taken against the violating transmissions.

Example

The following example defines the QoS downlink policy to drop the transmission's data packets when a TSPEC violation is discovered:

```
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# downlink drop
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# apply
```

flex-client-access

Use the `flex-client-access` command to enable or disable flexible client access to the wireless medium. The `flex-client-access` command is accessible from the `wlan:<WLAN-service-name>:qos-policy` context of the CLI.

After you run the `flex-client-access` command, run the `apply` command to implement the changes.

flex-client-access enable | disable

Parameters

enable disable	Enables or disables flexible client access to the wireless medium.
-------------------------	--

Example

The following example enables flexible client access to the wireless medium:

```
EWC.extremenetworks.com:wlans:test:qos-policy# flex-client-access enable
EWC.extremenetworks.com:wlans:test:qos-policy# apply
EWC.extremenetworks.com:wlans:test:qos-policy# show flex-client-access
Flex client access: enable
```

legacy

Use the `legacy` command to enable or disable the legacy solution, which gives all packets on the VNS high priority. The `legacy` command is accessible from the `wlan:<WLAN-service-name>:qos-policy` context of the CLI.

After you run the `legacy` command, run the `apply` command to implement the changes.

legacy enable | disable

Parameters

enable disable	Enables or disables the legacy solution.
-------------------------	--

**Note**

Legacy Wireless QoS support cannot be re-enabled once it has been disabled.

Example

The following example enables the legacy solution for the VNS:

```
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# legacy enable
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# apply
```

```
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# show legacy
Legacy: enable
```

priority-map

Use the `priority-map` command to configure Differentiated Service Code Point (DSCP) classification by mapping Service Class user priority levels to DSCP codepoints. The `priority-map` command is accessible from the `wlan:<WLAN-service-name>:qos-policy` context of the CLI.

After you run the `priority-map` command, run the `apply` command to implement the changes.

```
priority-map dscp 0-64 user-priority 0-7 qos-map 0/1
```

Parameters

dscp 0-64	Specifies a DSCP codepoint value.
user-priority 0-7	Specifies the Service Class value to be assigned to a DSCP codepoint.
qos-map 0/1	Configure DSCP markings to pre-defined QoS service classes. This parameter is used when only a subset of DSCP to UP mappings need to be advertised to the client. Use this parameter for WLAN hotspots. Hotspot type must be Enabled.

Example

The following example assigns a Service class of 7 to DSCP codepoint 24:

```
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# priority-map dscp 24 user-
priority 7 qos-map 1
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# apply
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# show priority-map
DSCP CLASSIFICATION
      dscp-marking    service-class    QoS Map
      0                02                0
      1                00                1
      23               00                0
      24               07                1
      25               00                1
```

priority-override

Use the `priority-override` command to override the priority for all packets in the WLANS. The `priority-override` command is accessible from the `wlan:<WLAN-service-name>:qos-policy` context of the CLI.

After you run the `priority-override` command, run the `apply` command to implement the changes.

```
priority-override enable | disable
```

Parameters

enable disable	Enables or disables priority override for all packets in the WLANS.
-------------------------	---

Example

The following example overrides priority for all packets on WLANS CNL-7-CP:

```
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# priority-override enable
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# apply
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# show priority-override
Priority override: enable
```

priority-override-dscp

Use the `priority-override-dscp` command to override existing DSCP codepoint assignments for priority processing and use a single DSCP codepoint for the WLANS. The `priority-override-dscp` command is accessible from the `wlan:<WLAN-service-name>:qos-policy` context of the CLI.

After you run the `priority-override-dscp` command, run the `apply` command to implement the changes.

```
priority-override-dscp 0-64
```

Parameters

0-64	Specifies a DSCP codepoint value. Default value: 0.
------	---

Usage

This command is only active if the `priority-override` command has been enabled. For more information, see [priority-override](#) on page 333.

Example

The following example overrides all existing DSCP codepoint assignments and uses DSCP codepoint 2 for the CNL-7-CP WLANS:

```
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# priority-override-dscp 2
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# apply
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# show priority-override-dscp
DSCP marking: 2
```

priority-override-up

Use the `priority-override-up` command to override existing Service Class settings for priority processing and configure a single Service Class value for the WLANS. The `priority-override-up` command is accessible from the `wlan:<WLAN-service-name>:qos-policy` context of the CLI.

After you run the `priority-override-up` command, run the `apply` command to implement the changes.

```
priority-override-up 0-7
```

Parameters

0-7	Specifies a Service Class value. Default value: 1.
-----	--

Usage

This command is only active if the `priority-override` command has been enabled. For more information, see [priority-override](#) on page 333.

Example

The following example overrides all existing Service Class settings and configures a single Service Class of 4 for the CNL-7-CP WLANS:

```
EWC.extremenetworks.com:wlans:CNL-7-CP:qos_policy# priority-override-up 4
EWC.extremenetworks.com:wlans:CNL-7-CP:qos_policy# apply
EWC.extremenetworks.com:wlans:CNL-7-CP:qos_policy# show priority-override-up
Service class: 4
```

turbo-voice

Use the `turbo-voice` command to enable or disable Turbo Voice optimization. The `turbo-voice` command is accessible from the `wlan:<WLAN-service-name>:qos-policy` context of the CLI.

After you run the `turbo-voice` command, run the `apply` command to implement the changes.

turbo-voice enable | disable

Parameters

enable disable	Enables or disables Turbo Voice optimization on the WLANS.
-------------------------	--

Usage

This command is only active when either the `wmm`, `802.11e`, or `legacy` commands have been enabled.

Example

The following example enables Turbo Voice on the CNL-7-CP WLANS:

```
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# turbo-voice enable
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# apply
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# show turbo-voice
Turbo voice: enable
```

uapsd

Use the `uapsd` command to enable Unscheduled Automatic Power Save Delivery (U-APSD) on the VNS. Use the `no` form of the command to disable it. The `uapsd` command is accessible from the `wlan:<WLAN-service-name>:qos-policy` context of the CLI.

After you run the `uapsd` command, run the `apply` command to implement the changes.

uapsd enable | disable

Parameters

enable disable	Enables or disables U-APSD. Default value: disabled.
-------------------------	--

Usage

This command is only available when either the `802.11e` or `wmm` commands have been enabled. For more information see [dot11e](#) on page 331 and [wmm](#) on page 336.

Example

The following example enables U-APSD on the CNL-7-CP WLANS:

```
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# uapsd enable
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# apply
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# show uspsd
Enable U-APSD: enable
```

uplink

Use the `uplink` command to manage the uplink policer action for this WLANS. The `uplink` command is accessible from the `wlan:<WLAN-service-name>:qos-policy` context of the CLI.

After you run the `uplink` command, run the `apply` command to implement the changes.

uplink delts | do-nothing

Parameters

delts	Specifies that TSPEC violations will end when they are discovered. This action deletes the TSPEC.
do-nothing	Specifies that TSPEC violations are allowed to continue when they are discovered. Data transmissions will continue and no action is taken against the violating transmissions.

Usage

This command is only active if the Video and Voice Admission Control is set to enable. See [video-admission-control](#) on page 337 and [voice-admission-control](#) on page 337.

Example

The following example defines the uplink policer action to end TSPEC violations by deleting the TSPEC for the CNL-7-CP WLANS:

```
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# uplink delts
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# apply
```

wmm

Use the `wmm` command to enable Wi-Fi Multimedia enhancements for audio, video, and voice applications. The `wmm` command is accessible from the `wlan:<WLAN-service-name>:qos-policy` context of the CLI.

After you run the `wmm` command, run the `apply` command to implement the changes.

wmm enable | disable

Parameters

enable disable	Enables or disables Wi-Fi Multimedia enhancements on the WLANS.
-------------------------	---

Example

The following example enables Wi-Fi Multimedia enhancements on the CNL-7-CP WLANS:

```
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# wmm enable
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# apply
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# show wmm
WMM: enable
```

video-admission-control

Use the `video-admission-control` command to enable or disable global admission control for video. The `video-admission-control` command is accessible from the `wlan:<WLAN-service-name>:qos-policy` context of the CLI.

After you run the `video-admission-control` command, run the `apply` command to implement the changes.

video-admission-control enable | disable

Parameters

enable disable	Enables or disables video admission control for the WLANS.
-------------------------	--

Usage

Enabling video admission control automatically enables voice admission control. Disabling video admission control automatically disables voice admission control.

Example

The following example enables global admission control for video:

```
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# video-admission-control
enable
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# apply
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# show video-admission-
control
Use Global Admission Control for Video (VI): enable
```

voice-admission-control

Use the `voice-admission-control` command to enable global admission control for voice for WLANS. The `voice-admission-control` command is accessible from the `wlan:<WLAN-service-name>:qos-policy` context of the CLI.

After you run the `voice-admission-control` command, run the `apply` command to implement the changes.

voice-admission-control enable | disable

Parameters

enable disable	Enables or disables global admission control for voice for WLANS.
-------------------------	---

Usage

This command is only available when either the `802.11e` or `wmm` commands have been enabled. For more information, see [dot11e](#) on page 331 and [wmm](#) on page 336.

Example

The following example enables global admission control for voice for the CNL-7-CP WLANS:

```
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# voice-admission-control
enable
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# apply
EWC.extremenetworks.com:wlans:CNL-7-CP:qos-policy# show voice-admission-
control
Use Global Admission Control for Voice (VO): enable
```

remoteable

Use the `remoteable` command to enable or disable the SSID advertisement to the mobility domain. The `remoteable` command is accessible from the `wlan:<WLAN-service-name>` context of the CLI.

After you run the `remoteable` command, run the `apply` command to implement the changes.

remoteable enable | disable

Parameters

enable disable	Enables or disables the SSID advertisement to the mobility domain.
-------------------------	--

Example

The following example enables the SSID advertisement for the CNL-7-CP WLANS:

```
EWC.extremenetworks.com:wlans:CNL-7-CP# remoteable enable
EWC.extremenetworks.com:wlans:CNL-7-CP# apply
EWC.extremenetworks.com:wlans:CNL-7-CP# show remoteable
Remote Service: enable
```

rf

The `rf` command moves you to the `wlan:<WLAN-service-name>:rf` context, which contains commands to configure RF options for the WLAN service.

The following commands are available in the `wlan:<WLAN-service-name>:rf` context.

- [11h-power-reduction](#) on page 339
- [11h-support](#) on page 339
- [11k-beacon-rep](#) on page 340
- [11k-quiet-ie](#) on page 340
- [11k-support](#) on page 340
- [energy-save-mode](#) on page 341
- [process-client-ie](#) on page 341

- [show](#) on page 341
- [ssid-suppress](#) on page 342

11h-power-reduction

Use the `11h-power-reduction` command to enable or disable automatic power reduction of transmissions using the 802.11h standard. The `11h-power-reduction` command is accessible from the `wlan:<WLAN-service-name>:rf` context of the CLI.

After you run the `11h-power-reduction` command, run the `apply` command to implement the changes.

11h-power-reduction enable | disable

Parameters

enable disable	Enables or disables automatic power reduction of transmissions using the 802.11h standard.
-------------------------	--

Example

The following example enables the power reduction feature on the WLAN service:

```
EWC.extremenetworks.com:wlans:test:rf# 11h-power-reduction enable
EWC.extremenetworks.com:wlans:test:rf# apply
EWC.extremenetworks.com:wlans:test:rf# show 11h-power-reduction
Apply power reduction to 11h clients: enable
```

11h-support

802.11h support on the Wireless Appliance will allow clients to operate with the maximum available transmission power in 5Ghz bands. The `11h-support` command is accessible from the `wlan:<WLAN-service-name>:rf` context of the CLI.

Use the `11h-support` command to enable 802.11h support on the WLAN service.

After you run the `11h-support` command, run the `apply` command to implement the changes

11h-support enable | disable

Parameters

enable disable	Enables or disables 802.11h support on the Wireless Appliance.
-------------------------	--

Example

The following example enables 802.11h support on the WLAN service:

```
EWC.extremenetworks.com:wlans:test:rf# 11h-support enable
EWC.extremenetworks.com:wlans:test:rf# apply
EWC.extremenetworks.com:wlans:test:rf# show 11h-support
Enable 11h support: enable
```

11k-beacon-rep

Use the `11k-beacon-rep` command to enable and disable 802.11k beacon reports on AP 37xx and 38xx appliances. The `11k-beacon-rep` command is accessible from the `wlan:<WLAN-service-name>:rf` context of the CLI.

**Note**

The `11k-beacon-rep` command is only available after the `11k-support` command is enabled.

11k-beacon-rep enable | disable

Parameters

enable disable	Enables or disables 802.11k beacon reports on AP 37xx and 38xx appliances.
-------------------------	--

Example

The following example enables 802.11k beacon reports on the WLAN service:

```
EWC.extremenetworks.com:wlans:AZ-723-WLAN1:rf# 11k-beacon-rep enable
```

11k-quiet-ie

Use the `11k-quiet-ie` command to enable and disable 802.11k Quiet IE on AP 37xx and 38xx appliances. The `11k-quiet-ie` command is accessible from the `wlan:<WLAN-service-name>:rf` context of the CLI.

**Note**

The `11k-quiet-ie` command is only available after the `11k-support` command is enabled.

11k-quiet-ie enable | disable

Parameters

enable disable	Enables or disables 802.11k Quiet IE on AP 37xx and 38xx appliances.
-------------------------	--

Example

The following example enables 802.11k Quiet IE on the WLAN service:

```
EWC.extremenetworks.com:wlans:AZ-723-WLAN1:rf# 11k-quiet-ie enable
```

11k-support

Use the `11k-support` command to enable and disable 802.11k support on AP 37xx and 38xx appliances. The `11k-support` command is accessible from the `wlan:<WLAN-service-name>:rf` context of the CLI.

11k-support enable | disable

Parameters

enable disable	Enables or disables 802.11k support on AP 37xx and 38xx appliances.
-------------------------	---

Example

The following example enables 802.11k support on the WLAN service:

```
EWC.extremenetworks.com:wlans:AZ-723-WLAN1:rf# 11h-support enable
```

energy-save-mode

Use the `energy-save-mode` command to enable or disable the AP energy saving mode. The `energy-save-mode` command is accessible from the `wlan:<WLAN-service-name>:rf` context of the CLI.

energy-save-mode enable | disable

Parameters

enable disable	Enables or disables the AP energy saving mode on the WLAN service.
-------------------------	--

Example

The following example enables AP energy saving mode:

```
EWC.extremenetworks.com:wlans:CNL-7-CP:rf# energy-save-mode enable
```

process-client-ie

Use the `process-client-ie` command to enable or disable the processing of Information Element 10 (IE 10). The `process-client-ie` command is accessible from the `wlan:<WLAN-service-name>:rf` context of the CLI.

After you run the `process-client-ie` command, run the `apply` command to implement the changes.

process-client-ie enable | disable

Parameters

enable disable	Enables or disables the processing of Information Element 10 (IE 10) on the Wireless Appliance.
-------------------------	---

Example

The following example enables IE 10 processing:

```
EWC.extremenetworks.com:wlans:CNL-7-CP:rf# process-client-ie enable
EWC.extremenetworks.com:wlans:CNL-7-CP:rf# apply
```

show

Use the `show` command to display the current RF settings of the specified individual WLAN service. The `show` command is accessible from the `wlan:<WLAN-service-name>:rf` context of the CLI.

Example

The following example displays the current RF settings for the WLAN service named "test":

```
EWC.extremenetworks.com:wlans:test:rf# show
Process client IE requests: disable
Enable 11h support: disable
Apply power reduction to 11h clients: disable
```

```
Suppress SSID: disable
Energy save mode: disable
```

ssid-suppress

Use the `ssid-suppress` command to allow or prevent the SSID from being broadcast by the Wireless AP. The `ssid-suppress` command is accessible from the `wlan:<WLAN-service-name>:rf` context of the CLI.

After you run the `ssid-suppress` command, run the `apply` command to implement the changes.

ssid-suppress enable | disable

Parameters

enable disable	Enables or disables the suppression of broadcast of the SSID.
-------------------------	---

Example

The following example prevents SSID broadcasts:

```
EWC.extremenetworks.com:wlans:CNL6-AAA# ssid-suppress enable
EWC.extremenetworks.com:wlans:CNL6-AAA# apply
```

show

Use the `wlan:<WLAN-service-name>:show` command to display the current settings of the specified individual WLAN service. The `show` command is accessible from the `wlan:<WLAN-service-name>` context of the CLI.

Examples

The following example displays the current WLAN service settings for the WLAN service named “test”:

```
EWC.extremenetworks.com:wlans:test# show
Service type: std
Name: test
Synchronize: disable
Enable status: enable
Wireless AP Services:
Wireless AP: 04099202012xxxxx
Wireless AP: 04099202012xxxxx
Wireless AP: 05000092030xxxxx
SSID: _ssidtest
pre-authentication timeout(minutes): 5
post-authentication timeout(minutes): 30
session timeout(minutes): 0
Block MU to MU traffic: disable
```

This example displays the settings for the dynamic mesh WLAN service named `mesh1-wlan`:

```
EWC.extremenetworks.com:wlans:mesh1-wlan# show
Service type: mesh
Pre-shared Key:
SSID: mesh1
Backhaul Radio Band: a
```

```
Name: mesh1-wlan
Enable/disable WLAN Service: enable
aplist-wds 0500008043050236 portal wkgbridge on
Radio Mode: off
```

ssid

Use the `ssid` command to specify the Service Set Identifier (SSID) for the WLAN service being configured. The `ssid` command is accessible from the `wlan:<WLAN-service-name>` context of the CLI.

After you run the `ssid` command, run the `apply` command to implement the changes.

ssid *string*

Parameters

<i>string</i>	Specifies a string for the SSID. The SSID string can range in length from 1 to 32 characters.
---------------	---

Example

The following example specifies and then displays the SSID:

```
EWC.extremenetworks.com:wlans:test# ssid testssid
EWC.extremenetworks.com:wlans:test# apply
EWC.extremenetworks.com:wlans:test# show ssid
SSID: testssid
```

status

Use the `status` command to enable or disable this WLAN service. The `status` command is accessible from the `wlan:<WLAN-service-name>` context of the CLI.

After you run the `status` command, run the `apply` command to implement the changes.

status **enable** | **disable**

Parameters

enable disable	Enables or disables this WLAN service.
--------------------------------	--

Example

The following example enables this WLAN service:

```
EWC.extremenetworks.com:wlans:test# status enable
EWC.extremenetworks.com:wlans:test# apply
EWC.extremenetworks.com:wlans:test# show status
Enable status: enable
```

sync

Use the `sync` command to enable or disable automatic synchronization of this WLAN service across paired Wireless Appliances. The `sync` command is accessible from the `wlan:<WLAN-service-name>` context of the CLI.

After you run the `sync` command, run the `apply` command to implement the changes.

sync enable | disable

Parameters

enable disable	Enables or disables automatic synchronization of this WLAN service across paired Wireless Appliances.
-------------------------	---

Example

The following example enables synchronization for this WLAN service:

```
EWC.extremenetworks.com:wlans:test# sync enable
EWC.extremenetworks.com:wlans:test# apply
EWC.extremenetworks.com:wlans:test# show sync
Synchronize: enable
```

timeout-post

Use the `timeout-post` command to set the post-authentication timeout value (in minutes) for this WLAN service. The `timeout-post` command is accessible from the `wlan:<WLAN-service-name>` context of the CLI.

After you run the `timeout-post` command, run the `apply` command to implement the changes.

timeout-post 0-999999

Parameters

0-999999	Specify the post-authentication timeout value in minutes for this WLAN service.
-----------------	---

Example

The following example sets the post-authentication timeout value to 10 minutes for this WLAN service:

```
EWC.extremenetworks.com:wlans:test# timeout-post 10
EWC.extremenetworks.com:wlans:test# apply
```

timeout-pre

Use the `timeout-pre` command to set the pre-authentication timeout value (in minutes) for this WLAN service. The `timeout-pre` command is accessible from the `wlan:<WLAN-service-name>` context of the CLI.

After you run the `timeout-pre` command, run the `apply` command to implement the changes.

timeout-pre 0-999999

Parameters

<code>0-999999</code>	Specify the pre-authentication timeout value in minutes for this WLAN service.
-----------------------	--

Example

The following example sets the pre-authentication timeout value to 10 minutes for this WLAN service:

```
EWC.extremenetworks.com:wlans:test# timeout-pre 10
EWC.extremenetworks.com:wlans:test# apply
EWC.extremenetworks.com:wlans:test# show timeout-pre
pre-authentication timeout(minutes): 10
```

timeout-session

Use the `timeout-session` command to set the session timeout value (in minutes) for this WLAN service. The `timeout-session` command is accessible from the `wlan:<WLAN-service-name>` context of the CLI.

After you run the `timeout-session` command, run the `apply` command to implement the changes.

```
timeout-session 0-999999
```

Parameters

<code>0-999999</code>	Specify the session timeout value in minutes for this WLAN service.
-----------------------	---

Example

The following example sets the session timeout value to never for this WLAN service:

```
EWC.extremenetworks.com:wlans:test# timeout-session 0
EWC.extremenetworks.com:wlans:test# apply
EWC.extremenetworks.com:wlans:test# show timeout-session
session timeout(minutes): 0
```

unauth-behaviour

Use the `unauth-behaviour` command to set the WLAN service response to unauthenticated traffic. The `unauth-behaviour` command is accessible from the `wlan:<WLAN-service-name>` context of the CLI.

There are two responses (behaviours) that can be applied to unauthenticated traffic:

- discard it
- apply the default non-authentication policy to it

If 1x authentication has been selected for this WLAN service, then “discard unauthenticated traffic” is the only behavior that is applied. If captive portal has been selected for this WLAN service (without 1x or MAC authentication), the default non-authentication policy is applied.

After you run the `unauth-behaviour` command, run the `apply` command to implement the changes.

```
unauth-behaviour nonauth-policy | discard-unauth-traffic
```

Parameters

nonauth-policy	Specifies that the non-authentication policy is applied to unauthenticated traffic.
discard-unauth-traffic	Specifies that unauthenticated traffic is discarded. This is the default.

Example

The following example applies the non-authentication policy to unauthenticated traffic for this WLAN service:

```
EWC.extremenetworks.com:wlans:test# unauth-behaviour nonauth-policy
EWC.extremenetworks.com:wlans:test# apply
EWC.extremenetworks.com:wlans:test# show unauth-behaviour
Unauthenticated Behaviour: nonauth-policy
```

hotspot

A hotspot-enabled WLANS is under the wlans context. The context for the following hotspot commands is as follows: **root > wlans > <hotspot enabled wlan> > hotspot**. Use these commands to configure the hotspot-enabled WLANS.

- [apply](#) on page 21
- [end](#) on page 21
- [exit](#) on page 22
- [hs-3gpp](#) on page 347
- [hs-ant](#) on page 347
- [hs-ccap](#) on page 347
- [hs-dgaf](#) on page 348
- [hs-domain](#) on page 348
- [hs-down-load](#) on page 348
- [hs-down-speed](#) on page 349
- [hs-hessid](#) on page 349
- [hs-internet-avail](#) on page 349
- [hs-nai-realm](#) on page 350
- [hs-natype](#) on page 351
- [hs-ofn-venue](#) on page 351
- [hs-osu](#) on page 352
- [hs-rc](#) on page 352
- [hs-up-load](#) on page 352
- [hs-up-speed](#) on page 353
- [hs-v4avail](#) on page 353
- [hs-v6avail](#) on page 353
- [hs-venue-group](#) on page 354
- [hs-venue-type](#) on page 354
- [provider-config](#) on page 357
- [redirect-url](#) on page 366

Examples

```
EWC.extremenetworks.com:wlans:hs-wlan# hotspot
```

hs-3gpp

Use the `hs-3gpp` command from the hotspot context to configure the 3GPP Cellular Network for the hotspot.

```
hs-3gpp (add|delete) (mcc mnc)
```

Parameters

add delete	Specifies to add or remove 3GPP Cellular Network for the hotspot.
<i>mcc mnc</i>	Cellular network IDs in the form of mobile country code, mobile network code (MCC, MNC).

Usage

The MNC and MCC must be a 3-digit, positive number.

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-3gpp add 333 111
```

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-3gpp delete 333 111
```

hs-ant

Use the `hs-ant` command from the hotspot context to configure the hotspot ANQP access network type.

```
hs-ant (private|private-guest|public-charge|public-free)
```

Parameters

private private-guest public-charge public-free	Specifies the hotspot ANQP access network type.
--	---

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-ant private
```

hs-ccap

Use the `hs-ccap` command from the hotspot context to configure the connection capability for the hotspot.

```
hs-ccap (add|delete) (ah|udp|tcp|esp) port (unknown|open|closed)
```

Parameters

(add delete)	Specifies whether to add or delete a connection capability.
(ah udp tcp esp)	Specifies the protocol.
<i>port</i>	Specifies the port number in the range 0 to 65535.
(unknown open closed)	Specifies the port status.

Usage

For protocols esp and ah the port number must be set to 0.

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-ccap add tcp 192 open
```

hs-dgaf

Use the `hs-dgaf` command from the hotspot context to configure hotspot downstream group-addressed forwarding.

hs-dgaf (enable|disable)

Parameters

(enable disable)	Enable or disable Downstream Group-Address Forwarding. This option is disabled by default. When DGAF is disabled, the AP is not forwarding downstream group-addressed frames.
-------------------------	---

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-dgaf enable
```

hs-domain

Use the `hs-domain` command from the hotspot context to configure the hotspot ANQP domain name.

hs-domain *string*

Parameters

<i>string</i>	Specifies hotspot ANQP domain name.
---------------	-------------------------------------

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-domain my-isp.org
```

hs-down-load

Use the `hs-down-load` command from the hotspot context to configure the hotspot WLAN metrics downlink load.

hs-down-load (0-255)

Parameters

(0-255)	Specifies the WLAN metrics downlink load.
---------	---

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-down-load 250
```

hs-down-speed

Use the `hs-down-speed` command from the hotspot context to configure the hotspot WLAN metrics downlink speed.

hs-down-speed (0-2147483647)

Parameters

(0-2147483647)	Specifies the hotspot WLAN metrics downlink speed in kbps.
----------------	--

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-down-speed 2147483647
```

hs-hessid

Use the `hs-hessid` command from the hotspot context to configure the hotspot ANQP HESSID. A single SSID can be used across multiple WLANs (BSS). Therefore, the HESSID helps a client identify when the BSSID belongs to a homogenous BSS with identical configuration. Beacons with the same {HESSID, SSID} pair belong to the same WLAN. The {HESSID, SSID} pair must be unique for each WLAN. By default, the HESSID is set to the MAC address of the controller Ethernet port. Hotspots can have the same HESSID as long as the SSID is unique. If opting to configure the HESSID manually, we recommend using an AP BSSID as the HESSID.

In a mobility domain, manually configure the HESSID to a unique value, differentiating it from the value used in the controller's WLAN.

hs-hessid *mac addr*

Parameters

<i>mac addr</i>	Specifies the mac address of the controller Ethernet port.
-----------------	--

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-hessid 00:0C:29:C2:C7:1A
```

hs-internet-avail

Use the `hs-internet-avail` command from the hotspot context to configure the hotspot internet availability.

hs-internet-avail (enable|disable)*Parameters*

enable disable	Enables or disables internet availability.
-----------------------	--

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-internet-avail enable
```

hs-nai-realm

Use the `hs-nai-realm` command from the hotspot context to configure the NAI Realm for the hotspot.

hs-nai-realm (add|delete NAI Realm EAP_method[EAP_method] ,*) | (delete NAI Realm)

Parameters

add delete NAI Realm EAP_method[EAP_method] ,*	The the NAI (Network Access Identification) Realms list is a FQDN of the service provider. This is a list of realms that can be successfully authenticated. Each realm can have up to 8 supported EAP methods. Valid EAP Methods include: EAP-TLS EAP-TTLS-PAP EAP-TTLS-CHAP EAP-SIM-SIM EAP-TTLS-MSCHAP EAP-TTLS-MSCHAPv2 EAP-AKA2-USIM EAP-AKA-USIM
--	---

Usage

Consider the following when configuring an NAI Realm list for each hotspot:

- Add all realms that can authenticate a mobile device's log on credentials or certificate credentials, including the realms of all roaming partners that are accessible from the hotspot AP. Include the realm of the home SP.
- Add a realm for the PLMN ID. This is the cellular network identity based on public land mobile network (PLMN) information.
- You can configure the EAP method list to support devices that do not know the EAP methods that are being used by a given service provider.
- If the device has been provisioned with the home service provider, the device does not need to use the EAP methods in the NAI Realm List. The mobile device knows the EAP method required to authenticate against its home service provider and automatically uses it.
- Keep your DNS server records up to date, so that mobile devices can resolve the server domain names (FQDN).

For more information, see the ExtremeWireless *User Guide*.

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-nai-realm add LS620 EAP-TLS
```

hs-natype

Use the `hs-natype` command from the hotspot context to configure the Network Authentication Type for the hotspot.

hs-natype (HttpHttpsRedirection|OnlineEnrollmentSupported|AcceptanceOfTermsAndConditions|DNSRedirection)

Parameters

HttpHttpsRedirection	Redirect Http or Https automatically.
OnlineEnrollmentSupported	Authentication supports online enrollment.
AcceptanceOfTermsAndConditions	Redirection is accomplished after user accepts Terms and Conditions.
DNSRedirection	DNS redirection serves a web page other than what the end user had requested.

Usage

Before you can use `hs-natype`, create a hotspot enabled WLANS.

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-na-type HttpHttpsRedirection
```

hs-ofn-venue

Use the `hs-ofn-venue` command from the hotspot context to configure the hotspot venue identification.

hs-ofn-venue (add|update|delete) lang operator venue

Parameters

(add update delete)	Add, update, or delete a venue. Specify a language, operator name, and venue name.
<i>operator</i>	Operator name. If using spaces in <operator> string, surround the string with double quotes.
<i>lang</i>	Language code. See Language Codes on page 365.
<i>venue</i>	Venue name. If using spaces in <venue> string, surround the string with double quotes.

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-ofn-venue add tha JohnDoe
CityCenter
```

hs-osu

Use the `hs-osu` command from the hotspot context to configure the OSU WLAN.

hs-osu *wlan*

Parameters

<i>wlan</i>	Specifies the WLAN that is configured for online signup. The WLAN must be created before running this command. See the command create on page 286.
-------------	--

Usage

The WLAN must be created before running this command.

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot#hs-osu My_Hotspot_OSU
```

hs-rc

Use the `hs-rc` command from the hotspot context to configure the roaming consortium for the hotspot. Configure authentication of mobile devices to the members of a roaming consortium, or to a particular SP that has a roaming consortium.

hs-rc (**add|delete**) *rc*

Parameters

(add delete) <i>rc</i>	Add or delete a roaming consortium value.
---------------------------------	---

Usage

The *rc* can be a 6 or 10-digit hexadecimal number.

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-rc AA2211
```

hs-up-load

Use the `hs-up-load` command from the hotspot context to configure the hotspot WLAN metrics Uplink load.

hs-up-load (0-255)

Parameters

(0-255)	Specifies the hotspot WLAN metrics Uplink load.
---------	---

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-up-load 255
```


hs-up-speed

Use the `hs-up-speed` command from the hotspot context to configure the hotspot WLAN metrics Uplink speed.

hs-up-speed (0-2147483647)

Parameters

(0-2147483647)	Specifies the WLAN metrics Uplink speed in kbps.
----------------	--

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-up-speed 2147483647
```

hs-v4avail

Use the `hs-v4avail` command from the hotspot context to configure the hotspot ANQP IPV4 availability.

hs-v4avail (NA|public|restricted|singleNAT|doubleNAT|restricted-singleNAT|restricted-doubleNAT|unknown)

Parameters

(NA public restricted singleNAT doubleNAT restricted-singleNAT restricted-doubleNAT unknown)	The mobile device uses the IP Address Type Availability information to make network selection decisions. Specify the level of restriction for the IPV4 network.
--	---

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-v4avail public
```

hs-v6avail

Use the `hs-v6avail` command from the hotspot context to configure the hotspot ANQP IPV6 availability.

hs-v6avail (NA|available|unknown)

Parameters

(NA available unknown)	The mobile device uses the IP Address Type Availability information to make network selection decisions. Specify the level of restriction for the IPV6 network.
------------------------	---

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-v6avail public
```

hs-venue-group

Use the `hs-venue-group` command from the hotspot context to configure the hotspot venue group information.

hs-venue-group (**Unspecified**|**Assembly**|**Business**|**Educational**|**FactoryIndustrial**|**Institutional**|**Mercantile**|**Residential**|**Storage**|**UtilityMisc**|**Vehicular**|**Outdoor**)

Parameters

(Unspecified Assembly Business Educational FactoryIndustrial Institutional Mercantile Residential Storage UtilityMisc Vehicular Outdoor)	Specifies the hotspot venue group.
--	------------------------------------

Usage

You have the option to specify a venue type value after you specify a venue group value. For more information, see [hs-venue-type](#) on page 354.

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-venue-group Assembly
```

hs-venue-type

Use the `hs-venue-type` command from the hotspot context to configure the hotspot venue type.

hs-venue-type *venue_type*

Parameters

<i>venue_type</i>	For a list of possible type values, see Table 7: Hotspot Venue Group - Type Values on page 355.
-------------------	---

Usage

You must specify a venue group before you can specify a venue type value. For more information, see [hs-venue-group](#) on page 354.

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-venue-group Assembly hs-venue-type Arena
```

Venue Group - Type Values

Table 7: Hotspot Venue Group - Type Values

Venue Group	Venue Type
Unspecified	Unspecified
	Reserved
Assembly	Unspecified
	Arena
	Stadium
	Passenger Terminal (e.g., airport, bus, ferry, train station)
	Amphitheatre
	Amusement Park
	Place of Worship
	Convention Centre
	Library
	Museum
	Restaurant
	Theatre
	Bar
	Coffee Shop
	Zoo or Aquarium
	Emergency Coordination Centre
Reserved	
Business	Unspecified
	Doctor or Dentist office
	Bank
	Fire Station
	Police Station
	Post Office
	Professional Office
	Research and Development Facility
	Attorney Office
	Reserved
Educational	Unspecified
	School, Primary
	School, Secondary
	University or College

Table 7: Hotspot Venue Group - Type Values (continued)

Venue Group	Venue Type
	Reserved
FactoryIndustrial	Unspecified
	Factory
	Reserved
Institutional	Unspecified
	Hospital
	Long-Term Care Facility (e.g., Nursing home, Hospice, etc.)
	Alcohol and Drug Rehabilitation Center
	Group Home
	Prison or Jail
	Reserved
Mercantile	Unspecified
	Retail Store
	Grocery Market
	Automotive Service Station
	Shopping Mall
	Gas Station
	Reserved
Residential	Unspecified
	Private Residence
	Hotel or Motel
	Dormitory
	Boarding House
	Reserved
Storage	Unspecified
	Reserved
UtilityMisc	Unspecified
	Reserved
Vehicular	Unspecified
	Automobile or Truck
	Airplane
	Bus
	Ferry
	Ship or Boat

Table 7: Hotspot Venue Group - Type Values (continued)

Venue Group	Venue Type
	Train
	Motor Bike
	Reserved
Outdoor	Unspecified
	Muni-mesh Network
	City Park
	Rest Area
	Traffic Control
	Bus Stop
	Kiosk
	Reserved

provider-config

Use the `provider-config` command from the hotspot context to configure the hotspot OSU service provider. The following list of commands are in the provider-config context:

- `hs-provider-desc1` on page 358
- `hs-provider-desc2` on page 358
- `hs-provider-frn1` on page 358
- `hs-provider-frn2` on page 359
- `hs-provider-icon` on page 359
- `hs-provider-lang1` on page 359
- `hs-provider-lang2` on page 361
- `hs-provider-methods` on page 363
- `hs-provider-nai` on page 363
- `hs-provider-uri` on page 364
- `remove` on page 364
- `apply` on page 364

provider-config *service-uri*

Parameters

<i>service-uri</i>	Specifies the provider Uniform Resource Identifier (URI).
--------------------	---

Usage

The Service URI must be a valid URL that starts with `https://`. Once you have specified the provider URI, you can issue the specific configuration commands. Use the exit command to go back to the hotspot context. From there you can issue a command to configure another service URI.

Examples

This example shows how to enter the provider-config context for a given URI:

```
EWC.extremenetworks.com:wlans:hs-wlan:hotspot# provider-config https://
oserver.example.com/sign-up/smartphone/index.html
```

After the desired changes are made, this example returns to the hotspot context:

```
EWC.extremenetworks.com:wlans:hs-wlan:hotspot# provider-config exit.
```

hs-provider-desc1

Use the `hs-provider-desc1` command from the provider-config context to configure the OSU provider description.

hs-provider-desc1 *description*

Parameters

<i>description</i>	Specify the OSU provider first description.
--------------------	---

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# provider-config https://
Enetworks.com
```

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-provider-desc1 "First
description"
```

hs-provider-desc2

Use the `hs-provider-desc2` command from the provider-config context to configure the OSU provider description.

hs-provider-desc2 *description*

Parameters

<i>description</i>	Specify the OSU provider description.
--------------------	---------------------------------------

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# provider-config https://
Enetworks.com
```

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-provider-desc2 "Second
description"
```

hs-provider-frn1

Use the `hs-provider-frn1` command from the provider-config context to configure the hotspot OSU provider first friendly name.

hs-provider-frn1 *friendly name*

Parameters

<i>friendly name</i>	Name for the provider online signup.
----------------------	--------------------------------------

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# provider-config https://
Enetworks.com
```

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-provider-frn1 ENetworks
```

hs-provider-frn2

Use the `hs-provider-frn2` command from the provider-config context to configure the hotspot OSU provider second friendly name. This is used when configuring more than one language.

hs-provider-frn2 *friendly name*

Parameters

<i>friendly name</i>	Name for the provider online signup.
----------------------	--------------------------------------

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# provider-config https://
Enetworks.com
```

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-provider-frn2 BigNetworks
```

hs-provider-icon

Use the `hs-provider-icon` command from the provider-config context to configure the hotspot OSU provider icon. Provider icons can be uploaded through the GUI. This allows you to select from the existing icons on the controller.

hs-provider-icon *provider-icon*

Parameters

<i>provider-icon</i>	Specifies the hotspot OSU provider icon file.
----------------------	---

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# provider-config https://
Enetworks.com
```

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-provider-icon bird.png
```

hs-provider-lang1

Use the `hs-provider-lang1` command from the provider-config context to configure the hotspot OSU provider first language.

hs-provider-lang1 *language*

Parameters

<i>language</i>	Specifies the hotspot OSU provider first language. For more information, see Language Codes on page 365.
-----------------	--

Usage

The following is a list of valid language codes:

jpn	Japanese
alb	Albanian
gle	Irish
ara	Arabic
pol	Polish
ind	Indonesian
spa	Spanish; Castilian
arm	Armenian
cze	Czech
est	Estonian
fre	French
eng	English
chi	Chinese
tur	Turkish
hrv	Croatian
swe	Swedish
ukr	Ukrainian
per	Persian
lit	Lithuanian
aus	Australian languages
gre	Greek, Modern (1453-)
kor	Korean
fin	Finnish
hun	Hungarian
fil	Filipino; Pilipino
ger	German
rum	Romanian; Moldavian; Moldovan
por	Portuguese
dan	Danish
mac	Macedonian
mon	Mongolian
bul	Bulgarian

rus	Russian
lav	Latvian
ita	Italian
geo	Georgian
nor	Norwegian
vie	Vietnamese
bat	Baltic languages
bel	Belarusian
baq	Basque
dut	Dutch; Flemish
slv	Slovenian
bos	Bosnian
aze	Azerbaijani
cat	Catalan; Valencian
srp	Serbian
afr	Afrikaans
tha	Thai

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# provider-config https://Enetworks.com
```

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-provider-lang1 afr
```

hs-provider-lang2

Use the `hs-provider-lang2` command from the provider-config context to configure the hotspot OSU provider second language.

hs-provider-lang2 *language*

Parameters

<i>language</i>	Specifies the hotspot OSU provider second language. For more information, see Language Codes on page 365.
-----------------	---

Usage

The following is a list of valid language codes:

jpn	Japanese
alb	Albanian
gle	Irish
ara	Arabic
pol	Polish
ind	Indonesian

spa	Spanish; Castilian
arm	Armenian
cze	Czech
est	Estonian
fre	French
eng	English
chi	Chinese
tur	Turkish
hrv	Croatian
swe	Swedish
ukr	Ukrainian
per	Persian
lit	Lithuanian
aus	Australian languages
gre	Greek, Modern (1453-)
kor	Korean
fin	Finnish
hun	Hungarian
fil	Filipino; Pilipino
ger	German
rum	Romanian; Moldavian; Moldovan
por	Portuguese
dan	Danish
mac	Macedonian
mon	Mongolian
bul	Bulgarian
rus	Russian
lav	Latvian
ita	Italian
geo	Georgian
nor	Norwegian
vie	Vietnamese
bat	Baltic languages
bel	Belarusian
baq	Basque
dut	Dutch; Flemish
slv	Slovenian
bos	Bosnian

aze	Azerbaijani
cat	Catalan; Valencian
srp	Serbian
afr	Afrikaans
tha	Thai

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# provider-config https://Enetworks.com
```

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-provider-lang2 srp
```

hs-provider-methods

Use the `hs-provider-methods` command from the provider-config context to configure the hotspot OSU provider method.

hs-provider-methods (*method[,method]**)

Parameters

<i>(method[,method]*)</i>	Specifies the hotspot OSU provider methods.
---------------------------	---

Usage

The following are valid methods: `oma` , `soap`.

They are case sensitive.

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# provider-config https://
Enetworks.com
```

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-provider-methods oma, soap
```

hs-provider-nai

Use the `hs-provider-nai` command from the provider-config context to configure the hotspot OSU user name.

hs-provider-nai *user-name*

Parameters

<i>user-name</i>	Specifies the hotspot OSU user name.
------------------	--------------------------------------

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# provider-config https://
Enetworks.com
```

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-provider-nai ENetworks_HotSpot
```

hs-provider-uri

Use the `hs-provider-uri` command from the provider-config context to configure the hotspot OSU server Universal Resource Identifier (URI).

hs-provider-uri *server-uri*

Parameters

<i>server-uri</i>	Specifies the hotspot OSU server Universal Resource Identifier (URI).
-------------------	---

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# provider-config https://
Enetworks.com
```

```
EWC.extremenetworks.com:wlans:hs:hotspot# hs-provider-uri https://
PhonesRUs.com
```

remove

Use the `remove` command from the provider-config context to remove the OSU configured provider.

remove *service-uri*

Parameters

<i>service-uri</i>	The provider's service URI.
--------------------	-----------------------------

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# provider-config https://
Enetworks.com
```

```
EWC.extremenetworks.com:wlans:hs:hotspot# remove https://PhonesRUs.com
```

apply

Use the `apply` command from the provider-config context to apply changes to the provider-config context.

apply

Usage

The following validation is necessary on the apply command:

- At least one method needs to be selected.
- At least one language with Friendly Name needs to be set.
- ICON is required.

Parameters

There are no parameters.

Examples

Once the provider has been configured, use `apply` to apply the changes.

```
EWC.extremenetworks.com:wlans:hs:hotspot# provider-config https://
Enetworks.com

EWC.extremenetworks.com:wlans:hs:hotspot# hs-provider-methods oma, soap

EWC.extremenetworks.com:wlans:hs:hotspot# hs-provider-provider-frnl ENetworks

EWC.extremenetworks.com:wlans:hs:hotspot# hs-provider-icon bird.png

EWC.extremenetworks.com:wlans:hs:hotspot# apply
```

Language Codes

The following is a list of valid language codes you can use to configure a hotspot:

jpn	Japanese
alb	Albanian
gle	Irish
ara	Arabic
pol	Polish
ind	Indonesian
spa	Spanish; Castilian
arm	Armenian
cze	Czech
est	Estonian
fre	French
eng	English
chi	Chinese
tur	Turkish
hrv	Croatian
swe	Swedish
ukr	Ukrainian
per	Persian
lit	Lithuanian
aus	Australian languages
gre	Greek, Modern (1453-)
kor	Korean
fin	Finnish
hun	Hungarian
fil	Filipino; Pilipino

ger	German
rum	Romanian; Moldavian; Moldovan
por	Portuguese
dan	Danish
mac	Macedonian
mon	Mongolian
bul	Bulgarian
rus	Russian
lav	Latvian
ita	Italian
geo	Georgian
nor	Norwegian
vie	Vietnamese
bat	Baltic languages
bel	Belarusian
baq	Basque
dut	Dutch; Flemish
slv	Slovenian
bos	Bosnian
aze	Azerbaijani
cat	Catalan; Valencian
srp	Serbian
afr	Afrikaans
tha	Thai

redirect-url

Use the `redirect-url` command from the hotspot context to configure the Redirect URL for the hotspot.

redirect-url (*url*)

Parameters

<i>url</i>	Destination URL for the redirect action.
------------	--

Usage

hs-natype is configured as HttpHttpsRedirection or AcceptanceOfTermsAndConditions.

For more information, see [hs-natype](#) on page 351.

Examples

```
EWC.extremenetworks.com:wlans:hs:hotspot# redirect-url https://enetworks.com
```

20 role Commands

role Context

create

delete

show

<named-role>

Common Filter Configuration Commands

This section describes commands used to define and configure role (policy) for the Wireless Appliance. These commands are located in the role (formerly policy) context of the CLI. Execute the `role` command at the root level to enter the role context. Refer to Section 6.10, “Configuring Policy,” in the *Wireless User Guide* for more information about role/policy configuration.

A role is a collection of attributes and rules that determine how to handle the traffic of users accessing the wired network through the WLAN service. Role assignment applies topology and traffic behavior to a user regardless of SSID or VNS assignment. Traffic behavior is defined in roles by configuring a rate control setting and filter rules for the AC or AP.

Roles do not need to be fully specified. Unspecified attributes are retained by the user or inherited from the global default-role. Refer to [default-role](#) on page 249 for information on configuring the global default-role.

A role either specifies or defaults to:

- A topology
- An inbound and outbound rate control profile
- A set of filters

All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

role Context

The following commands are available at the highest (first) level of the role context:

- [create](#) on page 369
- [delete](#) on page 369
- [show](#) on page 370
- [<named-role>](#) on page 370— See [<named-role>](#) on page 370 for commands in the role:<named-role> context.

For commands for configuring AC (controller) and AP filters, see [Common Filter Configuration Commands](#) on page 379.

create

Use the `create` command to create a new role, specifying a name for the new role. The `create` command is accessible from the role context.

```
create role-name
```

Parameters

<i>role-name</i>	Specifies the name of the role. A role name can be made up of all alpha-numeric characters, as well as special characters: -!#\$:
------------------	---

Usage

The default values for a newly created role are:

- Default Filter: disabled
- AC Filter: Controller filtering is active, with a default filter of deny in both directions
- Ingress rate profile: no-change
- Egress rate profile: no-change
- Topology: no-change
- Filtering on the AP: disabled
- Synchronization: disabled

Examples

The following example creates and then displays the details of a role named Auth:

```
EWC.extremenetworks.com:role# create Auth
EWC.extremenetworks.com:role# show Auth
Assigned topology: no change
Ingress rate profile: no change
Egress rate profile: no change
Filter settings: enable
Enable AP filtering: disable
Name: Auth
EWC.extremenetworks.com:role# show Auth acfilter
Enable AP filtering: disable
filter 1 (default) proto none 0.0.0.0 all_ports in dst out none allow
filter 2 (default) proto none 0.0.0.0 all_ports in none out src allow
```

delete

Use the `delete` command to delete a role, specifying the name of the role to be deleted. The `delete` command is accessible from the role context of the CLI.

```
delete role-name
```

Parameters

<i>role-name</i>	Specifies the name of the role to delete.
------------------	---

The following example deletes the role named Auth:

```
EWC.extremenetworks.com:role# delete Auth
```

show

Use the show command to display role configuration information. The `show` command is accessible from within the role context.

```
show {role | role-name}
```

Parameters

role	Specifies that information for all configured policies be displayed.
<i>role-name</i>	Specifies that information for the named role be displayed.

Examples

The following example displays the current list of configured policies:

```
EWC.extremenetworks.com:role# show
Role name           Topology           Class of Service   Mode
Filter defined
CNL-208-ACTT1       CNL-208-ACTT1rt1   No CoS
routed Yes
CNL-208-4110-NonAuthRole  CNL-208-4110-ACTT2  COS_LOW_LOW_Legacy  routed
Yes
CNL-208rt-CPAuthRole    CNL-208rt-CPTopology  COS_LOW_Gold_Legacy  routed
Yes
CNL-208-bridgeAC       TOPOLOGY-BAC-208-0   No CoS
b@ac Yes
```

The following example displays configuration information for the role named CNL-208-ACTT1:

```
EWC.extremenetworks.com:role# show CNL-208-ACTT1
Assigned topology: CNL-208-ACTT1rt1
Filter settings: enable
Enable AP filtering: disable
Name: CNL-208-ACTT1
Synchronize: enable
Default Class of Service: No CoS <named-role>
```

<named-role>

The `<named-role>` command, where `<named-role>` refers to the name of a given role, provides access to the `role:<named-role>` context.

The `role:<named-role>` context provides commands for the configuration of the `<named-role>`. A `<named-role>` must first be created using the `create` command in the role context. Once created it becomes available as a command, allowing access to the `role: <named-role>` context for that role. For example, to enter the `<named-role>` context for the role named `p6`, use the command `p6` from the role context, created using the `create p6` command.

After you complete configuration changes for a <named-role>, run the `apply` command before exiting the `role:<named-role>` context to implement the changes.

The following commands are available in the `role:<named-role>` context.

- [access-control](#) on page 371
- [ulfilterap](#) on page 375
- [egress-vlans](#) on page 372
- [name](#) on page 373
- [filter-status](#) on page 374
- [sync](#) on page 374
- [ulfilterap](#) on page 375
- [apcustom](#) on page 375
- [acfilters](#) on page 376 — See [acfilters](#) on page 376 for commands in the `role:<named-role>:acfilters` context.
- [apfilters](#) on page 376 — See [apfilters](#) on page 376 for commands in the `role:<named-role>:apfilters` context.
- [show](#) on page 377
- [traffic-mirror](#) on page 378
- [redirection-url](#) on page 378

access-control

Use the `access-control` command to configure access to APs and/or controllers assigned this role. The `access-control` command is accessible from within the `role:<named-role>` context.

access-control (**none** | **no-change** | **allow** | **deny** | **new** | *containment vlan-id* | **redirect**)

Parameters

none	Specifies no access allowed.
no-change	Specifies no change to current access status (keep using previous role/filter).
allow	Specifies access allowed.
deny	Specifies access denied.
new	Specifies new.
<i>containment vlan-id</i>	Specifies a containment VLAN access, by the VLAN ID.
redirect	Specifies redirection based on policy rules.

Usage

If the `access-control` command is set to `no-change`, any filters that exist in the previous role are applied to this station. For example, if the previous role is the `default-role`, `default-role` filters are applied to this station.

The `show named-role` command, within the role context, and the `show` command, within a `role:<named-role>` context, specify the current role-status command setting with the line “Do not change role settings when this Role is applied.”.

Examples

The following example enables access to AC and AP filter configuration within the `pl <named-role>` context:

```
EWC.extremenetworks.com:role:pl# access-control no-change
EWC.extremenetworks.com:role:pl# apply
EWC.extremenetworks.com:role:pl# show
Assigned topology: Seg1_Routed
Ingress rate profile: no change
Egress rate profile: no change
Do not change role settings when this Role is applied: enable
Name: Auth
Synchronize: disable
```

default-cos

Use the `default-cos` command to configure a default Class of Service for this role. The `default-cos` command is accessible from the `role:<named-role>` context.

default-cos *cos name* | **no-change**

Parameters

<i>cos name</i>	Specifies the default CoS for this role. The <i>cos name</i> must be already created by the <code>create</code> command in the <code>cos</code> context.
no-change	Specifies that no class of service change is associated with this role. When applying this role to a user at runtime, the user retains the class of service currently enforced.

Example

```
EWC.extremenetworks.com:role:pl# default-cos my-cos
```

egress-vlans

Use the `egress-vlans` command to add, update, or delete static untagged VLANs (topologies) on the egress list of this role.

The `egress-vlans` command is accessible from within the `role:<named-role>` context.

egress-vlans (**add** | **update** | **delete**) (*topology-name* [, *topology-name*]*)

Parameters

add update delete	Specifies whether the specified VLAN (topology) is to be added, deleted, or updated on an egress list for this role.
<i>topology-name</i> [, <i>topology-name</i>]	Specifies the name of a topology to be added, deleted, or updated on the VLAN egress list. Multiple VLANs may be included in a comma-separated list.

Examples

The following example adds VLANs 2111, 2121, and 2101 to the egress-list of the Auth role:

```
EWC.extremenetworks.com:role:Auth# egress-vlans 2111,2121,2101
EWC.extremenetworks.com:role:Auth# apply
```

The following example deletes VLAN 2111 from the egress-list of the Auth role:

```
EWC.extremenetworks.com:role:Auth# egress-vlans 2111,2121,2101
EWC.extremenetworks.com:role:Auth# apply
```

name

Use the `name` command to change the name of a role. The `name` command is accessible from within the `role:<named-role>` context.

name *new-name*

Parameters

<i>new-name</i>	Specifies the new name for this <named-role>.
-----------------	---

Usage

You must enter the `apply` command before exiting the `role:<named-role>` context for the role name change to take affect. The CLI prompt will not change until you exit and re-enter the `role:<named-role>` context.

Examples

The following example:

- Renames the role p1 to role1
- Applies the change
- Displays the role1 configuration
- Exits `role:<named-role>` context
- Re-enters the `role:<named-role>` context as role1

```
EWC.extremenetworks.com:role# p1
EWC.extremenetworks.com:role:p1# name role1
EWC.extremenetworks.com:role:p1# apply
EWC.extremenetworks.com:role:p1# show
Assigned topology: no change
Ingress rate profile: no change
Egress rate profile: no change
Do not change filter settings when this Role is applied: disable
Enable AP filtering: disable
Name: role1
Synchronize: disable
EWC.extremenetworks.com:role:p1# exit
EWC.extremenetworks.com:role# role1
EWC.extremenetworks.com:role:role1#
```

filter-status

Use the `filter-status` command to enable or disable a checkbox, which allows you to inherit filter rules from currently applied role. Selecting the **Inherit filter rules from currently applied role** checkbox overwrites any pre-existing filter settings. If the checkbox is not selected, the wireless client uses filter settings from a previously applied role. If filters have not been defined, the system enforces filters from the Global Default Role.

filter-status enable|disable

Parameters

enable	The Inherit filter rules from currently applied role checkbox is available in the wireless client.
disable	The Inherit filter rules from currently applied role checkbox is not available in the wireless client.

Examples

The following example enables the **Inherit filter rules from currently applied role** checkbox in the wireless client:

```
EWC.extremenetworks.com# filter-status enable
```

The following example disables the **Inherit filter rules from currently applied role** checkbox in the wireless client:

```
EWC.extremenetworks.com# filter-status disable
```

sync

Use the `sync` command to enable or disable automatic synchronization of this <named-role> across paired controllers. Refer to the section entitled “Using the Sync Summary,” in the *Wireless User Guide* for more information about synchronization of policies.

The `sync` command is accessible from within the `role:<named-role>` context.

sync {enable | disable}

Parameters

enable disable	Enables or disables automatic synchronization of this <named-role> across paired controllers.
-------------------------	---

Examples

The following example enables the synchronization of the p1 role across controllers:

```
EWC.extremenetworks.com:role:p1# sync enable
EWC.extremenetworks.com:role:p1# apply
EWC.extremenetworks.com:role:p1# show
Assigned topology: no change
Ingress rate profile: no change
Egress rate profile: no change
Do not change filter settings when this Role is applied: disable
```

```

Enable AP filtering: disable
Name: p1
Synchronize: enable
EWC.extremenetworks.com:role:p1#

```

ulfilterap

Use the `ulfilterap` command to enable filtering on the AP. The `ulfilterap` command is accessible from the `role:<named-role>` context.

ulfilterap {**enable** | **disable**}

Parameters

enable disable	Provides for the enabling or disabling of filtering on the AP for this <code>role:<named-role></code> context.
--------------------------------	--

Usage

When filtering is enabled on the AP, wireless APs obtain client filter information from the Wireless Appliance. Filter rules defined on the controller are applied by wireless APs. In addition, direct inter-Wireless AP communication allows Wireless APs to exchange client filter information as clients roam from one Wireless AP to another.

The filter setting feature must be disabled using the `filter disable` command for the `apfilters` command to be visible in the CLI.

See [apcustom](#) on page 375 to apply custom filters for the AP.

Examples

The following example enables filtering on the AP for this `role:p1` context:

```

EWC.extremenetworks.com:role:p1# ulfilterap enable
EWC.extremenetworks.com:role:p1#

```

apcustom

Use the `apcustom` command to enable AP custom filters. The `apcustom` command is accessible from the `role:<named-role>` context.

apcustom {**enable** | **disable**}

Parameters

enable disable	Provides for the enabling or disabling of AP custom filters for this <code>role:<named-role></code> context.
--------------------------------	--

Usage

Enabling AP custom filters provides for the ability to access the `role:<named-role>:apfilters` context using the `apfilters` command. The `apfilters` command allows for the configuration of additional filters for the APs.

Filtering on the AP must be enabled using the `ulfilterap enable` command for the `apcustom` command to be visible in the CLI.

Examples

The following example enables AP custom filters for the `role:p1:apfilters` context:

```
EWC.extremenetworks.com:role:p1# ulfilterap enable
EWC.extremenetworks.com:role:p1# apcustom enable
EWC.extremenetworks.com:role:p1#
```

acfilters

Use the `acfilters` command to enter the `role:<named-role>:acfilters` context for the configuring of AC filters. AC filter rules are applied at the controller. The `acfilters` command is accessible from within the `role:<named-role>` context.

AC filtering is not available when the associated topology is configured for Bridge at AP. AC filtering is available when the associated topology is set to either Bridge at AC or Routed.

The following commands are available in the `role:<named-role>:acfilters` context.

- [create](#) on page 379
- [config](#) on page 382
- [delete](#) on page 385
- [move](#) on page 385

acfilters

Parameters

None.

Usage

The “no-change” filter setting must be disabled by the `access-control` command for the `acfilters` command to be visible in the CLI.

Examples

The following example enters the `role:<named-role>:acfilters` context for the Auth `<named-role>`:

```
EWC.extremenetworks.com:role:Auth# acfilters
EWC.extremenetworks.com:role:Auth:acfilters#
```

apfilters

Use the `apfilters` command to enter the `role:<named-role>:apfilters` context for the configuring of AP custom filters. AP custom filters are applied at the AP. The `apfilters` command is accessible from the `role:<named-role>` context. Execute the `ulfilterap enable` command and the `apcustom enable` command before the `apfilters` command is visible.

The following commands are available in the `role:<named-role>:apfilters` context.

- [create](#) on page 379
- [config](#) on page 382
- [delete](#) on page 385
- [move](#) on page 385

apfilter

Parameters

None.

Usage

The apply custom filters to AP feature must be enabled using the `apcustom enable` command for the `apfilters` command to be visible in the CLI.

Examples

The following example enters the `role:<named-role>:apfilters` context for the `p1 <named-role>`:

```
EWC.extremenetworks.com:role:p1# ulfilterap enable
EWC.extremenetworks.com:role:p1# apcustom enable
EWC.extremenetworks.com:role:p1# apfilters
EWC.extremenetworks.com:role:p1:apfilters#
```

show

Use the `show` command to display the `<named-role>` configuration information for the current `role:<named-role>` context. The `show` command is accessible from within the `role:<named-role>` context.

show

Parameters

None.

Examples

The following example displays the `CNL-208-ACTT1` role configuration from within the `role:<named-role>` context:

```
EWC.extremenetworks.com:role:CNL-208-ACTT1# show
Assigned topology: CNL-208-ACTT1rt1
Filter settings: enable
Enable AP filtering: disable
Name: CNL-208-ACTT1
Synchronize: enable
Default Class of Service: No CoS
EWC.extremenetworks.com:role:CNL-208-ACTT1#
```

traffic-mirror

Use the `traffic-mirror` command to configure the traffic mirror. The `traffic-mirror` command is accessible from the `role:<named-role>` context of the CLI.

traffic-mirror (**none** | **enable** | **prohibited**)

Parameters

none enable prohibited	Configures the traffic mirror for none, enable, or prohibited for the named WLAN.
--	---

Example

The following example configures the traffic mirror to be prohibited:

```
EWC.extremenetworks.com:role:HT_BR# traffic-mirror prohibited
```



redirection-url

Use the `redirection-url` command to configure a redirection URL from the command line. The `redirection-url` command is accessible from within the `role: <named-role>` context.

redirection-url *id* | *redirection url*)

Parameters

<i>id</i>	An index number that identifies the redirection URL in the database.
<i>redirection url</i>	Identifies the redirection URL

Usage

Before configuring the redirection URL:

- Enable policy rule-based redirection. See [rule-redirect](#) on page 245.
- Create the redirection URL. See [redirection-url-list](#) on page 270.
- Enable AC Filtering
- Create a filter with the protocol = TCP and Access Control = Redirect.

Examples

You can specify a redirection URL by its sequence ID or by the actual URL. To display the list of possible redirection URLs associated with the role, type `redirection-url`.

```
Available Redirection URL:
0      Own WLAN
1      http://2.2.2.2
2      http://3.3.3.138
3      http://3.3.3.140
4      (ffecp) http://192.168.11.22:/logincode_m-f.php?hwc=10.12.0.1
```

When External Captive Portal URLs exist, they are automatically added to the list.

The following example specifies the redirection-url by sequence ID.

```
EWC.extremenetworks.com:role:role1#: redirection-url 1
```

Related Links

[rule-redirect](#) on page 245

[redirection-url-list](#) on page 270

[acfilters](#) on page 251

[extredir](#) on page 298

Common Filter Configuration Commands

The commands in this section are common to the configuration of both AP filters and AC filters. Each filter must be configured in its own context ([acfilters](#) on page 376 or [apfilters](#) on page 376).

- [create](#) on page 379
- [config](#) on page 382
- [delete](#) on page 385
- [move](#) on page 385

create

Use the `create` command to create, insert, or append a new filter rule into an AP or AC filter list for a <named-role>. The `create` command is accessible from within the `role:<named-role>:acfilters` and `role:<named-role>:apfilters` contexts.

Use the following syntax to specify a position value and protocol for a filter rule in the filter list. No application is specified.

```
create [pos] proto protocol eth ether-type mac MAC address (ipaddress/mask | IPv6
| interface-subnet | interface-ip | any) [(port port [port]) | (type-code type
[type])] in (none|src|dst|both) out (none|src|dst|both) (allow | deny | none |
contain2vlan vlan-id | redirect) priority (0-7 | none) tos-dscp (0-FF/(FF/FE/FC/
F8/F0/E0/C0/80)|none) cos (named cos|none) traffic-mirror (<none|enable|
prohibited>)
```

Use the following syntax to specify an application in the filter rule definition for an AP or AC filter list.

```
create pos application app_id in (none|apply) out (none|apply) (allow|deny|none|
contain2vlan|redirect) cos (<named cos>|none) traffic-mirror (<none|enable|
prohibited>)
```

Use the following syntax to specify a custom application in the L7 layer of the filter rule definition for an AP or AC filter list.

```
create pos app-signature app_id group group name name app name in (none|apply)
out (none|apply) (allow|deny|none|contain2vlan\redirect) cos (named cos|none)
traffic-mirror (none|enable|prohibited)
```

Parameters

<i>pos</i>	Specifies a position value for this filter in the filter list. Valid values are from 0 - 255.
proto <i>protocol</i>	Specifies the protocol for this filter rule by number or name. Valid number values are from 0 - 255. Valid name values are: <ul style="list-style-type: none"> • udp - UDP protocol • tcp - TCP protocol • ah - Authentication Header protocol • esp - Encapsulating Security Payload protocol • icmp - ICMP protocol • icmpv6 - ICMP-IPv6 protocol • any - Any protocol • gre - Generic Route Encapsulation protocol • 0-255 - number value of protocol
eth <i>ether-type</i>	<i>ether-type</i> : 4 hex digits from 0001-FFFF, or any. The following well known values are converted into hex values, IPv4, ARP, RARP, DECnet Phase IV, AppleTalk (EtherTalk), AppleTalk Address Resolution Protocol (AARP), Novell IPX (alt), Novell, Profinet, and IPv6. Note: IPv6 is supported for Layer 2 bridging for both B@AC and B@AP topologies.
mac <i>MAC address</i>	<i>MAC address</i> : MAC or CIDR address, or any.
<i>ipaddress/mask</i> IPv6 interface-subnet interface-ip any	The IP address and/or mask for this filter rule. The IP address is in IPv6 format. Use the IP address and mask configured for the associated topology for this filter rule. Use the IP address of the associated topology for this filter rule. Use any IP address or mask for this filter rule.
port <i>port</i> [<i>port</i>]	Specifies a TCP or UDP port or port range to which this filter rule will be applied. The first <i>port</i> value specifies either the port or the start of a port range. The second <i>port</i> value optionally specifies the end of a range. This parameter is valid only when either TCP or UDP is the specified protocol. Valid port values are from 0 - 65535.
type-code <i>type</i> [<i>type</i>]	Specifies an ICMP type code or range of ICMP type codes. The first <i>type</i> value specifies either the ICMP type code or the start of a type code range. The second <i>type</i> value optionally specifies the end of a type code range. This parameter is valid only when ICMP is the specified protocol. Valid <i>type</i> values are from 0 - 255.
in (none src dst both)	Specifies the direction of packet flow. — in specifies a packet flow from the AP to the AC. none specifies that the in direction will not be used as matching criteria in the filter rule. dst specifies that the IP address for this filter rule is the destination of the packet flow. src specifies that the IP address for this filter rule is the source of the packet flow. both specifies that the IP address for this filter rule can be either source or destination.

out (none src dst both)	Specifies the direction of packet flow. — out specifies a packet flow from the AC to the AP. none specifies that the out direction will not be used as matching criteria in the filter rule. dst specifies that the IP address for this filter rule is the destination of the packet flow. src specifies that the IP address for this filter rule is the source of the packet flow. both specifies that the IP address for this filter rule can be either source or destination.
allow deny none contain2vlan <i>vlan-id</i> redirect	Specifies whether packets are allowed or denied (or ignored), or put in the containment VLAN (you must specify the VLAN by its ID), or redirected when meeting the criteria specified in the filter rule.
priority (<i>0-7</i> none)	Specifies the packet priority. Valid values are 0-7; the highest priority is 7. Specifying none means priority level will not be used as matching criteria in this CoS.
tos-dscp (<i>tos-dscp value/mask value</i> none)	Specifies the type of service in the filter rule. Valid values are 0-FF for ToS/DSCP and FF FE FC F8 F0 E0 C0 80 for mask. Specifying none means tos/dscp value is not used as matching criteria in the filter rule.
cos (<i>named-cos</i> none)	Specifies the class of service in the filter rule. The <i>named-cos</i> must already be created by the create command in the cos context. Specifying none means CoS is not used as matching criteria in the filter rule.
traffic-mirror	Specifies the behavior applied to a traffic mirror: none specifies the filter rule is not configured for traffic mirror. enable specifies that the traffic rule is enabled for traffic mirror prohibited specifies that the traffic rule is prohibited for traffic mirror.
application <i>app_id</i>	Specifies an application on the filter rule definition.
app-signature <i>app_id</i>	Specifies a custom application on the L7 layer of the filter definition rule.
group <i>group</i>	Specifies the pre-defined group, of which the (L7) custom application is a member.
name <i>app name</i>	Specifies the application name for the (L7) custom application.

Usage

If the specified rule position already contains a filter rule, specifying a rule using this command inserts a rule in the specified position in the list and resequences all rules below this filter down by one position. Use the **create** command to insert or append a rule at the specified position.

Examples

The following example shows the default filter rules applied to a role:

```
EWC.extremenetworks.com:role# create p6
EWC.extremenetworks.com:role# show p6 acfilter
Enable AP filtering: disable
filter 1 (default) proto none 0.0.0.0 all_ports in dst out none allow
filter 2 (default) proto none 0.0.0.0 all_ports in none out src allow
```

The following example creates a (basic mode) filter rule 1 that allows UDP traffic in both directions from IP address 192.168.10.0/24 for ports 10 through 2000:

```
EWC.extremenetworks.com:role:Auth:acfilters# create 1 proto udp
192.168.10.0/24 port 10 2000 in dst out src allow
EWC.extremenetworks.com:role:Auth:acfilters# apply
EWC.extremenetworks.com:role:Auth:acfilters# show
Enable AP filtering: disable
filter 1 proto udp 192.168.10.0 255.255.255.0 port 10 2000 in dst out src
allow
filter 2 (default) proto none 0.0.0.0 all_ports in dst out none allow
filter 3 (default) proto none 0.0.0.0 all_ports in none out src allow
```

The following example creates a filter rule 1 that is inserted into the rule list at position 1 resequencing the current rule 1. This filter rule allows TCP traffic in both directions from IP address 192.168.0.0/16 for ports 10 through 2000:

```
EWC.extremenetworks.com:role:Auth:acfilters# create 1 proto tcp
192.168.0.0/16 port 10 2000 in dst out src allow
EWC.extremenetworks.com:role:Auth:acfilters# show
Enable AP filtering: disable
filter 1 proto tcp 192.168.0.0 255.255.0.0 port 10 2000 in dst out src allow
filter 2 proto udp 192.168.10.0 255.255.255.0 port 10 2000 in dst out src
allow
filter 3 (default) proto none 0.0.0.0 all_ports in dst out none allow
filter 4 (default) proto none 0.0.0.0 all_ports in none out src allow
```

The following example creates a filter rule for ToS-DSCP B8/FF and CoS Best Effort (note quotes around the named CoS because of the space):

```
EWC.extremenetworks.com:role:Auth:acfilters# create proto udp 192.168.0.0/32
in dst out src none priority none tos-dscp B8/FF cos "Best Effort"
```

config

Use the `config` command to modify an existing AP or AC filter rule for this <named-role>. The `config` command is accessible from within the `role:<named-role>:acfilters` and `role:<named-role>:apfilters` contexts.

```
config[pos] proto protocol eth ether-type mac MAC address (ipaddress/mask | IPv6
| interface-subnet | interface-ip | any) [(port port [port]) | (type-code type
[type])] in (none|src|dst|both) out (none|src|dst|both) (allow | deny | none |
contain2vlan vlan-id | redirect) priority (0-7 | none) tos-dscp (0-FF/(FF/FE/FC/
F8/F0/E0/C0/80)|none) cos (named cos|none) traffic-mirror (<none|enable|
prohibited>)
```

Use the following syntax to modify an existing AP or AC application ID filter rule.

```
config pos application app_id in (none|apply) out (none|apply) (allow|deny|none|
contain2vlan|redirect) cos (<named cos>|none) traffic-mirror (<none|enable|
prohibited>)
```

Use the following syntax to modify a custom application in the L7 layer of the filter rule definition for an AP or AC filter list.

```

config pos app-signature app_id group group name name app name in (none|apply)
out (none|apply) (allow|deny|none|contain2vlan\redirect) cos (named cos|none)
traffic-mirror (none|enable|prohibited)

```

Parameters

pos	Specifies a position value for this filter in the filter list. Valid values are from 0 - 255.
proto <i>protocol</i>	Specifies the protocol for this filter rule by number or name. Valid number values are from 0 - 255. Valid name values are: <ul style="list-style-type: none"> • udp - UDP protocol • tcp - TCP protocol • ah - Authentication Header protocol • esp - Encapsulating Security Payload protocol • icmp - ICMP protocol • icmpv6 - ICMP-IPv6 protocol • any - Any protocol • gre - Generic Route Encapsulation protocol • 0-255 - number value of protocol
eth <i>ether-type</i>	<i>ether-type</i> : 4 hex digits from 0001-FFFF, or any. The following well known values are converted into hex values, IPv4, ARP, RARP, DECnet Phase IV, AppleTalk (EtherTalk), AppleTalk Address Resolution Protocol (AARP), Novell IPX (alt), Novell, Profinet, and IPv6. Note: IPv6 is supported for Layer 2 bridging for both B@AC and B@AP topologies.
mac <i>MAC address</i>	<i>MAC address</i> : MAC or CIDR address, or any.
<i>ipaddress/mask</i> IPv6 interface-subnet interface-ip any	The IP address and/or mask for this filter rule. The IP address is in IPv6 format. Use the IP address and mask configured for the associated topology for this filter rule. Use the IP address of the associated topology for this filter rule. Use any IP address or mask for this filter rule.
port <i>port</i> [<i>port</i>]	Specifies a TCP or UDP port or port range to which this filter rule will be applied. The first <i>port</i> value specifies either the port or the start of a port range. The second <i>port</i> value optionally specifies the end of a range. This parameter is valid only when either TCP or UDP is the specified protocol. Valid port values are from 0 - 65535.
type-code <i>type</i> [<i>type</i>]	Specifies an ICMP type code or range of ICMP type codes. The first <i>type</i> value specifies either the ICMP type code or the start of a type code range. The second <i>type</i> value optionally specifies the end of a type code range. This parameter is valid only when ICMP is the specified protocol. Valid <i>type</i> values are from 0 - 255.
in (none src dst both)	Specifies the direction of packet flow. — in specifies a packet flow from the AP to the AC. none specifies that the in direction will not be used as matching criteria in the filter rule. dst specifies that the IP address for this filter rule is the destination of the packet flow. src specifies that the IP address for this filter rule is the source of the packet flow. both specifies that the IP address for this filter rule can be either source or destination.

out (none src dst both)	Specifies the direction of packet flow. — out specifies a packet flow from the AC to the AP. none specifies that the out direction will not be used as matching criteria in the filter rule. dst specifies that the IP address for this filter rule is the destination of the packet flow. src specifies that the IP address for this filter rule is the source of the packet flow. both specifies that the IP address for this filter rule can be either source or destination.
allow deny none contain2vlan <i>vlan-id</i> redirect	Specifies whether packets are allowed or denied (or ignored), or put in the containment VLAN (you must specify the VLAN by its ID), or redirected when meeting the criteria specified in the filter rule.
priority (<i>0-7</i> none)	Specifies the packet priority. Valid values are 0-7; the highest priority is 7. Specifying none means priority level will not be used as matching criteria in this CoS.
tos-dscp (<i>tos-dscp value/mask value</i> none)	Specifies the type of service in the filter rule. Valid values are 0-FF for ToS/DSCP and FF FE FC F8 F0 E0 C0 80 for mask. Specifying none means tos/dscp value is not used as matching criteria in the filter rule.
cos (<i>named-cos</i> none)	Specifies the class of service in the filter rule. The <i>named-cos</i> must already be created by the create command in the cos context. Specifying none means CoS is not used as matching criteria in the filter rule.
traffic-mirror	Specifies the behavior applied to a traffic mirror: none specifies the filter rule is not configured for traffic mirror. enable specifies that the traffic rule is enabled for traffic mirror prohibited specifies that the traffic rule is prohibited for traffic mirror.
application <i>app_id</i>	Specifies an application on the filter rule definition.
app-signature <i>app_id</i>	Specifies a custom application on the L7 layer of the filter definition rule.
group <i>group</i>	Specifies the pre-defined group, of which the (L7) custom application is a member.
name <i>app name</i>	Specifies the application name for the (L7) custom application.

Usage

If the specified rule position already contains a filter rule, the **config** command overwrites the existing rule. Use the **create** command to insert or append a rule at the specified position.

Examples

The following example overwrites a pre-existing filter rule 1 with a rule that allows ICMP traffic types 9 through 31 in both directions for the associated topology's interface subnet and mask:

```
EWC.extremenetworks.com:role:p1:acfilters# config 1 proto icmp interface-
subnet type 9 31 in dst out src allow
EWC.extremenetworks.com:role:p1:acfilters# apply
EWC.extremenetworks.com:role:p1:acfilters# show
Enable AP filtering: disable
filter 1 proto icmp interface-subnet type 9 31 in dst out src allow
filter 2 proto udp 192.168.10.0 255.255.255.0 port 10 2000 in dst out src
allow
filter 3 (default) proto none 0.0.0.0 all_ports in dst out none allow
filter 4 (default) proto none 0.0.0.0 all_ports in none out src allow
```


The following example configures a filter rule that sets a ToS-DSCP as B8/FF and CoS as HTTP Traffic (note the quotes around the CoS name because of the space):

```
EWC.extremenetworks.com:role:Auth:acfilters# config 1 proto tcp
192.168.0.0/32 in dst out src none priority none tos-dscp B8/FF cos "HTTP
Traffic"
```

delete

Use the `delete` command to remove a filter rule from the filter list. The `delete` command is accessible from within the `role:<named-role>:acfilters` and `role:<named-role>:apfilters` contexts.

delete *pos*

Parameters

<i>pos</i>	Specifies the filter rule list position of the filter to be deleted. Valid values are from 0-255.
------------	---

Examples

The following example deletes filter rule 1 and displays the remaining default deny all rule:

```
EWC.extremenetworks.com:role:p1:acfilters# delete 1
EWC.extremenetworks.com:role:p1:acfilters# show
Enable AP filtering: disable
filter 1 (default) proto none 0.0.0.0 all_ports both deny
```

move

Use the `move` command to update the priority of a filter rule by moving the rule from its current position in the filter list (source) to a different list position (up or down). The `move` command is accessible from within the `role:<named-role>:acfilters` and `role:<named-role>:apfilters` contexts.

move *src-pos dest-pos*

Parameters

<i>src-pos dest-pos</i>	Specifies the current (source) position in the filter list of the rule to be moved, followed by the new (destination) list position for the filter rule. Valid values are from 0 -255. List position 1 is top priority.
-------------------------	---

Examples

The following example:

- Moves the rule in list position 2 to list position 1
- Displays the new list ordering:

```
EWC.extremenetworks.com:role:p1:acfilters# move 2 1
EWC.extremenetworks.com:role:p1:acfilters# show
Enable AP filtering: disable
filter 1 proto udp 192.168.10.0 255.255.255.0 port 10 2000 both allow
filter 2 proto tcp 192.168.10.0 255.255.255.0 port 10 2000 both allow
```

```
filter 3 (default) proto none 0.0.0.0 all_ports both deny
EWC.extremenetworks.com:role:pl:acfilters#
```

21 topology Commands

create
delete
internal-vlanid
multicast-support
show
<named-topology>
topology-group

This section describes commands used to define and configure topology objects used by policy and VNS objects. These commands are located in the topology context of the CLI. Execute the `topology` command at the root level to enter topology context.

All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the topology context:

- [create](#) on page 387
- [delete](#) on page 388
- [internal-vlanid](#) on page 389
- [multicast-support](#) on page 389
- [show](#) on page 390
- [<named-topology>](#) on page 390 — See [<named-topology>](#) on page 390 for commands in the topology:<named-topology> context.

create

Use the `create` command to create a topology object. The `create` command is accessible from the topology context of the CLI.

```
create topology name (b@ac vlanid port port name tag | untag) | (b@ap vlanid tag | untag) | (routed A.B.C.D/0-32) | (physical vlanid) port port name tag | untag>  
A.B.C.D./0-32)
```

Parameters

<i>topology name</i>	Specifies the name of the topology.
b@ac	Specifies a Bridge Traffic locally at Controller topology.
b@ap	Specifies a Bridge Traffic locally at Access Point topology.
routed	Specifies a routed topology.

physical	Specifies a physical topology.
vlanid	VLAN ID assigned to this topology. Value can be in range 1-4094.
tag untag	Specifies tagged or untagged VLAN.
port port-name	Specifies the name of the layer 2 port.
A.B.C.D/0-32	Layer 3 IP address and mask assigned to this physical topology.

Usage

The following are available topology types:

- Admin — The native, pre-defined topology of the Wireless Appliance management port. This topology is named Admin. You cannot create topologies with the name Admin.
- B@AC — Bridge Traffic Locally at controller. Requires Layer 2 configuration. May optionally have Layer 3 configuration. Layer 3 configuration would be necessary if services (such as DHCP) are required over the configured network segment, or if controller management operations are intended to be done through the configured interface.
- B@AP — Bridge Traffic Locally at AP. Requires Layer 2 configuration. Does not require Layer 3 configuration. Bridge Traffic at the AP topologies do not require the definition of a corresponding IP address since all traffic for users in that topology will be directly bridged by the Wireless AP at the local network point of attachment (VLAN at AP port).



Note

IPv6 is supported for Layer 2 bridging for both B@AC and B@AP topologies.

- Routed — Routed topology. Routed topologies do not need any Layer 2 configuration, but do require Layer 3 configuration.
- Physical — Physical Ethernet port topology. Physical topologies are not pre-defined; they must be created.

You can choose from four of the topology types (modes) when creating a topology:

- B@AC
- B@AP
- Routed
- Physical

Only B@AC, B@AP, and Routed topologies can be assigned to policies.

Example

The following example creates a B@AC topology named bac1, with a VLAN ID of 2, using the esa1 controller port:

```
EWC.extremenetworks.com:topology# create bac1 b@ac 2 port esa1
```

delete

Use the `delete` command to delete a topology object. The `delete` command is accessible from the topology context of the CLI.

You cannot delete the Admin topology. Also, you cannot delete a topology that is in use by a policy.

delete *topology name*

Parameters

<i>topology name</i>	Specifies the name of the topology to delete.
----------------------	---

Example

The following example deletes the topology named test:

```
EWC.extremenetworks.com:topology# delete test
```

internal-vlanid

Use the `internal-vlanid` command to set an internal management VLAN ID. The `internal-vlanid` command is available from the topology context of the CLI.

internal-vlanid <1-4094>

Parameters

<i>1-4094</i>	The internal management VLAN ID.
---------------	----------------------------------

Example

This following example sets the internal management VLAN ID of the topology:

```
EWC.extremenetworks.com:topology# internal-vlanid 2
```

multicast-support

Use the `multicast-support` command to configure multicast support for a physical topology. The `multicast-support` command is accessible from the topology context of the CLI.

multicast-support *physical topology name* | **none**

Parameters

<i>physical topology name</i>	Specifies the name of the physical topology to have multicast support.
none	Disables multicast-support.

Example

This example enables multicast support on the phy1 topology:

```
EWC.extremenetworks.com:topology# multicast-support phy1
```

This example disables multicast support for the topology context:

```
EWC.extremenetworks.com:topology# multicast-support none
```

show

Use the `show` command to display topology configuration information.

```
show [topology name]
```

Parameters

<i>topology name</i>	Displays information about the specified topology.
----------------------	--

Examples

The following example displays information for all configured topologies:

```
EWC.extremenetworks.com:topology# show
Name                Mode          L2:VlanId,tagged,port
L3:IP,GW,DHCP      L3:IPv6,Auto-Generated
Admin              admin         N/A,N/A,Admin
192.168.3.13,192.168.3.7,N/A fd66:2280:2668::0013,fd66:228:2668:0000:862b:
2bff:fe60:2a8a 64;fe80:0000:0000:0000:862b:2bff:fe60:2a8a 64
Bridged at AP      untagged      b@ap 123,enable,N/A
Port1              physical     103,disable,Port1    10.13.0.1,10.13.0.9,local
Port2              physical     2,disable,Port2     10.13.1.1,none,none
Port3              physical     U,disable,Port3     10.0.2.1,none,none
Port4              physical     U,disable,Port4     10.0.3.1,none,none
Seg1_Routed        routed       N/A,N/A,N/A         172.16.209.1,none,local
Seg2_Routed        routed       N/A,N/A,N/A         172.16.210.1,none,local
ACTT_Seg1_Routed   routed       N/A,N/A,N/A         10.13.16.1,none,local
ACTT_Seg2_Routed   routed       N/A,N/A,N/A         10.13.32.1,none,local
route1             routed       N/A,N/A,N/A         5.5.5.5,none,local
TopoFor313         b@ap 553,enable,N/A
Topology global info:
Internal VLAN ID: 1
Multicast support: disabled
```

The following example displays information for a physical topology named esa0:

```
EWC.extremenetworks.com:topology:esa0# show
Topology mode: physical
Name: esa0
3rd party: disable
Layer 3 presence: enable
```

<named-topology>

The `<named-topology>` command, where `<named-topology>` refers to the name of a given topology, moves you into the `topology:<named-topology>` context, which contains commands to configure the settings of the specified individual topology.

The following commands are available in the topology:<named-topology> context.

- [3rd-party](#) on page 391
- [l2](#) on page 391 — for commands in the topology:<named-topology>:l2 context.
- [l3](#) on page 396 — for commands in the topology:<named-topology>:l3 context.
- [l3presence](#) on page 415
- [mode](#) on page 416
- [name](#) on page 416
- [show](#) on page 417
- [strict-subnet](#) on page 417
- [sync](#) on page 418

3rd-party

Use the `3rd-party` command to enable or disable a third-party port in a physical topology. Only one physical topology can have `3rd-party` set to enable. The `3rd-party` command is available from the topology:<named-topology> context of the CLI for physical topologies.

3rd-party enable | disable

Parameters

enable	Enables a 3rd-party port on the specified physical topology.
disable	Disables a 3rd-party port on the specified physical topology.

Example

The following example enables a 3rd-party port on a physical topology:

```
EWC.extremenetworks.com:topology:esa0# 3rd-party enable
EWC.extremenetworks.com:topology:esa0# show
Name: esa0
3rd party: enable
```

l2

Use the `l2` command to enter the topology:<named-topology>:l2 context of the CLI for b@ac, b@ap, physical, and routed topologies. The l2 context allows you to configure the Layer 2 functions of the topology.

The following commands are available in the topology:<named-topology>:l2 context.

- [arp-proxy](#) on page 392
- [multicast](#) on page 392 — for commands in the topology:<named-topology>:l2:multicast context.
- [port](#) on page 395
- [show](#) on page 395
- [tagged](#) on page 396
- [vlanid](#) on page 396

arp-proxy

Use the `arp-proxy` command to enable or disable the AP as an ARP proxy for this topology. Only APs to which this topology is applied are enabled/disabled as ARP proxies. The `arp-proxy` command is available from the topology:<named-topology>:l2: context of the CLI for b@ap topologies.

arp-proxy enable | disable

Parameters

enable	Enables the ARP proxy for this topology.
disable	Disables the ARP proxy for this topology.

Example

This example enables the ARP proxy for the test topology:

```
EWC.extremenetworks.com:topology:test:l2# arp-proxy enable
```

multicast

Use the `multicast` command to enter the topology:<named-topology>:l2: multicast context of the CLI for b@ac, b@ap, physical, and routed topologies.

The following commands are available in the topology:<named-topology>:l2: multicast context.

- [config](#) on page 392
- [create](#) on page 393
- [delete](#) on page 394
- [filter](#) on page 394
- [move](#) on page 394

config

Use the `config` command to configure an existing multicast filter. To create a multicast filter, use the `create` command. See [create](#) on page 393. The `config` command is available from the topology:<named-topology>:l2:multicast context of the CLI for b@ac, b@ap, and routed topologies.

config [*pos*] (*A.B.C.D[/0-32]* | **IPv6** | **vocera** | **svp** | **mdns** | **mdnsv6** | **all** | **allv6**)
(**on**|**off**)

Parameters



pos default	Specifies the optional position to insert the rule.
A.B.C.D[/0-32] IPv6 vocera svp mdns mdnsv6 all allv6	<p>Specifies the IP address and mask of a multicast group or that the multicast group is pre-defined.</p> <ul style="list-style-type: none"> • IPv6 format • svp: Spectralink SVP (224.0.1.116) • vocera: Vocera Mcst (230.230.0.0/20) • mdns mDNS/Bonjour (224.0.0.251) • mDNSV6/Bonjour (FF02::FB) • all (allow all: 0.0.0.0/0) • allv6 (allow all v6 Multicast(FF00::/8)) <p>Note: IPv6 is supported for Layer 2 bridging for both B@AC and B@AP topologies.</p>
on off	Specifies whether wireless replication is enabled. The default is off.

Example

This example configures an existing multicast filter:

```
EWC.extremenetworks.com:topology:techpubs_test_ac:l2:multicast# config 1
225.1.1.0/32 on
```

create

Use the `create` command to create a multicast filter rule. The `create` command is available from the topology:<named-topology>:l2:multicast context of the CLI for b@ac, b@ap, and routed topologies.

```
create [pos] (A.B.C.D[/0-32] | IPv6 | vocera | svp | mdns | mdnsv6 | all | allv6)
(on|off)
```

Parameters

pos default	Specifies the optional position to insert the rule.
A.B.C.D[/0-32] IPv6 vocera svp mdns mdnsv6 all allv6	<p>Specifies the IP address and mask of a multicast group or that the multicast group is pre-defined.</p> <ul style="list-style-type: none"> • IPv6 format • svp: Spectralink SVP (224.0.1.116) • vocera: Vocera Mcst (230.230.0.0/20) • mdns mDNS/Bonjour (224.0.0.251) • mDNSV6/Bonjour (FF02::FB) • all (allow all: 0.0.0.0/0) • allv6 (allow all v6 Multicast(FF00::/8)) <p>Note: IPv6 is supported for Layer 2 bridging for both B@AC and B@AP topologies.</p>
on off	Specifies whether wireless replication is enabled. The default is off.

Example

This example creates a multicast filter rule:

```
EWC.extremenetworks.com:topology:techpubs_test_ac:l2:multicast# create 1
225.1.1.0/32 on
```

delete

Use the `delete` command to delete a multicast filter rule. The `delete` command is available from the `topology:<named-topology>:l2:multicast` context of the CLI for b@ac, b@ap, and routed topologies.

delete *pos*

Parameters

<i>pos</i>	The position of the multicast filter rule.
------------	--

Example

This example deletes a multicast filter rule at position 2:

```
EWC.extremenetworks.com:topology:test:l2:multicast# delete 2
```

filter

Use the `filter` command to enable or disable multicast filtering support. The `filter` command is available from the `topology:<named-topology>:l2:multicast` context of the CLI for b@ac, b@ap, and routed topologies.

filter **enable** | **disable**

Parameters

enable	Indicates that multicast filtering support is enabled.
disable	Indicates that multicast filtering support is disabled.

Example

This example enables multicast filtering support:

```
EWC.extremenetworks.com:topology:test:l2:multicast# filter enable
```

move

Use the `move` command to change the order of multicast rules. The `move` command is available from the `topology:<named-topology>:l2:multicast` context of the CLI for b@ac, b@ap, and routed topologies.

move *pos pos*

Parameters

<i>pos</i>	The current position of the multicast rule. Possible values are 0-255.
<i>pos</i>	The new position of the multicast rule. Use a number one greater than the last rule to move a rule to the bottom of the list. Possible values are 0-255.

Example



This example moves multicast rule 2 to the bottom of the list (after position 4):

```
EWC.extremenetworks.com:topology:test:l2:multicast# move 2 5
```

show

Use the `show` command to show multicast support for the specified topology. The `show` command is available from the `topology:<named-topology>:l2: multicast` context of the CLI for b@ac, b@ap, and routed topologies.

show

Parameters

None

Example

This example shows the multicast support for a topology named r1:

```
EWC.extremenetworks.com:topology:r1:l2:multicast# show
Multicast support: disable
```

port

Use the `port` command to assign a port to a topology. The `port` command is available from the `topology:<named-topology>:l2` context of the CLI for b@ac and physical topologies.

port *port name*

Parameters

<i>port name</i>	Specifies the name of the port.
------------------	---------------------------------

Example

This example assigns port esa1 to the topology named r1:

```
EWC.extremenetworks.com:topology:r1:l2:port# port esa1
```

show

Use the `show` command to show layer 2 information about the specified topology. The `show` command is available from the `topology:<named-topology>:l2` context of the CLI for b@ac, b@ap, and routed topologies.

show

Parameters

None

Example

This example shows layer 2 information for a b@ac topology named briAC_test:

```
EWC.extremenetworks.com:topology:briAC_test:l2# show
Port: esa0
```

```
VLAN tagging: enable
VLAN ID: 333
Foreign Port: esa0
```

tagged

Use the `tagged` command to enable or disable 802.1Q VLAN tagging. The `tagged` command is available from the `topology:<named-topology>:l2` context of the CLI for `b@ap`, `b@ac`, and physical topologies.

tagged enable | disable

Parameters

enable	Indicates that 802.1Q VLAN tagging will be enabled.
disable	Indicates that 802.1Q VLAN tagging will be disabled.

Example

This following example enables 802.1Q VLAN tagging on the physical topology named `esa1`:

```
EWC.extremenetworks.com:topology:esa1:l2# tagged enable
```

vlanid

Use the `vlanid` command to configure the VLAN ID of a physical topology or change the VLAN ID of `b@ac` or `b@ap` topologies. The `vlanid` command is available from the `topology:<named-topology>:l2` context of the CLI for `b@ac`, `b@ap`, and physical topologies.

vlanid 1-4094

Parameters

1-4094	The VLAN ID that you want to assign to the topology.
---------------	--

Example

This following example sets the VLAN ID of the topology named `test` to 2:

```
EWC.extremenetworks.com:topology:test:l2# vlanid 2
```

l3

Use the `l3` command to enter the `topology:<named-topology>:l3` context of the CLI for Admin, `b@ac`, `b@ap`, physical, and routed topologies. The `l3` context allows you to configure the Layer 3 functions of the topology. The `l3` context is now available in `b@ac` mode when `l3presence` is set to `disable`. For more information, see [l3presence](#) on page 415.

The following commands are available in the `topology:<named-topology>:l3` context.

- [ap-register](#) on page 397
- [cert](#) on page 397
- [copy-csr](#) on page 399

- [dhcp](#) on page 399 — See [dhcp](#) on page 399 for commands in the topology:<named-topology>:l3:dhcp context.
- [exceptions](#) on page 406 — See [exceptions](#) on page 406 for commands in the topology:<named-topology>:l3:exceptions context.
- [foreign-ip](#) on page 410
- [gateway](#) on page 410
- [gateway-ipv6](#) on page 411
- [gen-certreq](#) on page 411
- [ip](#) on page 412
- [ipv6](#) on page 412
- [mgmt](#) on page 413
- [mtu](#) on page 413
- [netmask](#) on page 413 for named topologies with disabled l3presence. See [l3presence](#) on page 415.
- [nexthop](#) on page 414
- [ospf-advert](#) on page 414
- [ospf-cost](#) on page 415
- [show](#) on page 415

ap-register

Use the `ap-register` command to enable or disable AP registration through the named topology. The `ap-register` command is available from the topology:<named-topology>:l3 context of the CLI for b@ac and physical topologies.

ap-register enable | disable

Parameters

enable	Enables AP registration through this interface.
disable	Disables AP registration through this interface.

Example

The following example enables AP registration:

```
EWC.extremenetworks.com:topology:esa0:l3# ap-register enable
```

cert

Use the `cert` command to define certificate settings for the named topology in the current context.

Using the `cert` command with the default option removes the certificate from the named topology and assigns the factory default certificate to it.

```
cert ((pkcs12 scp|ftp server user password dir filename certpassword [chainfile] [ipv6]) | (pem-der scp|ftp server user password dir filename keyfile certpassword [chainfile] [ipv6])) | (csr-cert scp|ftp server user password dir filename [chainfile] [ipv6])) | permanent | permanent-chain [ipv6] | default [ipv6]
```



Parameters

pkcs12	Indicates that <filename> certificate file is in the PKCS #12 format.
pem-der	Indicates that the <filename> certificate file and <keyfile> key file are PEM/DER encoded.
csr-cert	Indicates that the <filename> is a certificate signing request file.
scp ftp	Indicates that either SCP or FTP should be used to download the certificate file.
server	IP address of the server from which the file should be downloaded
user	Userid of the account to login with on the SCP or FTP server
password	Password associated with the <user> userid
dir	Directory in which to find the PKCS #12 certificate file, CSR file, or PEM/DER encoded certificate file and key file.
filename	The name of the PKCS #12, PEM/DER, or CSR certificate file to use with the port. This must be a PKCS #12 file if the permanent option is not used.
keyfile	The PEM/DER encoded private key file
certpassword	Password to use with the private key file
chainfile	A PEM-formatted CA (Certification Authority) chain certificate file. If you choose to install this optional certificate, you must do so when specifying the PCKCS #12 or PEM/DER certificates.
permanent	Indicates that the certificate to use is already in the permanent key store. This is used by the export and show commands to show which certificate is assigned to each port. The certificate will then be applied to the wireless assistant virtual website bound to the port the context of which the command was issued in.
permanent-chain	Indicates that the chain certificate to use is already in the permanent key store. This is used by the export and show commands to show which certificate is assigned to each port. The certificate will then be applied to the wireless assistant virtual website bound to the port the context of which the command was issued in.
default	Indicates that the interface should use the factory default certificate and key.
ipv6	Specifies that the certificate is IPv6.

Usage

Use the `cert` command to define certificate settings for the named topology in the current context. With the `cert` command, you can either to assign a downloaded PKCS #12 file, CSR file, or PEM/DER files to the named topology or to reset the named topology to use the factory default certificate. The `cert` command is available from the topology:<named-topology>:13 context of the CLI for Admin, b@ac, physical, and routed topologies.

When you use the `cert` command to assign a PKCS #12 file, CSR file, or PEM/DER files to an interface, you must select either SCP or FTP as the file transfer mechanism and specify the PKCS#12 file, CSR file, or PEM/DER files. The command then attempts to download the specified PKCS#12 file, CSR file, or PEM/DER files, and, if successful, converts the PKCS#12 file, CSR file, or PEM/DER files into a certificate and key. The command confirms that the certificate password works with the private key file then assigns both the certificate and key to the named topology. If the indicated file name cannot be found, this command generates an error.

Using the `cert` command with the default option removes the certificate from the named topology and assigns the factory default certificate to it.

Examples

The following example downloads a PKCS #12 certificate file and a chain certificate using FTP and applies it to the topology named `3rdFL_lab`:

```
EWC.extremenetworks.com:topology:3rdFL_lab:13# cert pkcs12
ftp 1.1.1.1 user2 abc123 certs/ 3rdFL_lab.pfx abcd1234 chain.crt
```

The following example downloads a PEM/DER certificate file, a PEM/DER key file, and a chain certificate using FTP and applies it to the topology named `3rdFL_lab`:

```
EWC.extremenetworks.com:topology:3rdFL_lab:13# cert pem-der
ftp 1.1.1.1 user2 abc123 certs/ 3rdFL_lab.crt privatekey.pem abcd1234
chain.crt
```

The following example downloads a signed certificate using FTP and applies it to the topology named `3rdFL_lab`:

```
EWC.extremenetworks.com:topology:3rdFL_lab:13# cert csr-cert ftp 192.168.1.8
user2 abc123 certs/ signed_1yr_3rdFL_lab.crt
```

copy-csr

Use this command to upload a topology certificate signing request to a server. The `copy-csr` command is available in the topology:<named-topology>:13 context.

```
copy-csr scp|ftp server user password dir [ipv6]
```

Parameters

scp ftp	Specifies the type of server, FTP or SCP, to which the file will be uploaded.
<i>server</i>	IP address of the FTP or SCP server.
<i>user</i>	User name to login to the server.
<i>password</i>	User password.
<i>dir</i>	Directory on server to put the certificate signing request file.
ipv6	Specifies that the certificate is IPv6.

Example

```
EWC.extremenetworks.com:topology:test:13# copy-csr ftp 192.168.1.1 root
mypasswd /tmp ipv6
```

dhcp

Use the `dhcp` command to enter the topology:<named-topology>:13:dhcp context of the CLI for b@ac, physical, and routed topologies.

The following commands are available in the topology:<named-topology>:13: dhcp context.

- [dhcp-servers](#) on page 400
- [dls](#) on page 400
- [dls-address](#) on page 401
- [dns](#) on page 401
- [domain](#) on page 402
- [exclude](#) on page 402
- [foreign-gateway](#) on page 402
- [foreign-range](#) on page 403
- [gateway](#) on page 403
- [lease-default](#) on page 404
- [lease-max](#) on page 404
- [mode](#) on page 404
- [range](#) on page 405
- [show](#) on page 405
- [wins](#) on page 406

dhcp-servers

Use the `dhcp-servers` command to configure DHCP relay servers. The `dhcp-servers` command is available from the `topology:<named-topology>!3:dhcp` context of the CLI for b@ac and routed topologies. This command is visible only when mode is set to relay. See [mode](#) on page 404.

dhcp-servers (*A.B.C.D* [,*A.B.C.D* [...]]) | **none**

Parameters

<i>A.B.C.D</i> [, <i>A.B.C.D</i> [...]]	Specifies qualified IPv4 address of DHCP relay servers.
none	Clears DHCP relay servers.

Example

The following example sets the IP address of the DHCP relay server as 10.0.1.10:

```
EWC.extremenetworks.com:topology:test:13:dhcp# mode relay
EWC.extremenetworks.com:topology:test:13:dhcp# dhcp-servers 10.0.1.10
```

dls

Use the `dls` command to enable or disable DLS (HiPath Deployment Services). The `dls` command is available from the `topology:<named-topology>!3:dhcp` context of the CLI for b@ac and routed topologies. This command is visible only when mode is set to local. See [mode](#) on page 404.

After you run the `dls` command, run the `apply` command to implement the changes.

dls enable | **disable**

Parameters

enable	Enables DLS.
disable	Disables DLS.



Examples

The following example enables DLS:

```
EWC.extremenetworks.com:topology:test:l3:dhcp# mode local
EWC.extremenetworks.com:topology:test:l3:dhcp# dls enable
```

The following example disables DLS:

```
EWC.extremenetworks.com:topology:test:l3:dhcp# mode local
EWC.extremenetworks.com:topology:test:l3:dhcp# dls disable
```

dls-address

Use the `dls-address` command to configure the DLS server address and port. The `dls-address` command is available from the `topology:<named-topology>:l3:dhcp` context of the CLI for b@ac and routed topologies. This command is visible only when mode is set to local and dls is set to enable. See [mode](#) on page 404.

```
dls-address (A.B.C.D | name) port 0-65535
```

Parameters

<i>A.B.C.D name</i>	Specifies the qualified IPv4 address or name.
port 0-65535	Specifies the DLS port number. This is an optional parameter. The default port is 18433.

Example

The following example sets the DLS address as 10.10.0.10:

```
EWC.extremenetworks.com:topology:test:l3:dhcp# mode local
EWC.extremenetworks.com:topology:test:l3:dhcp# dls enable
EWC.extremenetworks.com:topology:test:l3:dhcp# dls-address 10.10.0.10
```

dns

Use the `dns` command to specify the IP addresses for one or more DNS servers. The `dns` command is available from the `topology:<named-topology>:l3:dhcp` context of the CLI for b@ac, physical, and routed topologies. This command is visible only when mode is set to local. See [mode](#) on page 404.

After you run the `dns` command, run the `apply` command to implement the changes.

```
dns (DNS server [,DNS server [...]]) | none
```

Parameters

<i>DNS server</i>	Specifies the IP address of a DNS server.
none	Clears the DNS server.

Example



The following example specifies the IP addresses of two DNS servers:

```
EWC.extremenetworks.com:topology:test:l3:dhcp# mode local
EWC.extremenetworks.com:topology:test:l3:dhcp# dns 192.168.1.2, 192.168.1.3
EWC.extremenetworks.com:topology:test:l3:dhcp# apply
```

domain

Use the `domain` command to configure a domain name. The `domain` command is available from the `topology:<named-topology>:l3:dhcp` context of the CLI for b@ac, physical, and routed topologies. This command is visible only when mode is set to local. See [mode](#) on page 404.

domain *domain name* | **none**

Parameters

<i>domain name</i>	Specifies the domain name or an IPv4 address.
none	Clears the domain name.

Example

The following example sets the domain name as my-domain:

```
EWC.extremenetworks.com:topology:test:l3:dhcp# mode local
EWC.extremenetworks.com:topology:test:l3:dhcp# domain my-domain
```

exclude

Use the `exclude` command to exclude an IP address or a range of IP addresses from the DHCP Address Range. The `exclude` command is available from the `topology:<named-topology>:l3:dhcp` context of the CLI for b@ac, physical, and routed topologies. This command is visible only when mode is set to local. See [mode](#) on page 404.

exclude *A.B.C.D* [*A.B.C.D*] [**delete** | (**comment** *comment string*)]

Parameters

<i>A.B.C.D</i> [<i>A.B.C.D</i>]	Specifies the IP address or range of IP addresses.
delete	Clears the IP addresses.
comment <i>comment string</i>	A comment about the excluded IP address or range of IP addresses.

Example

The following example excludes the address range 10.0.1.10-10.0.1.20:

```
EWC.extremenetworks.com:topology:test:l3:dhcp# mode local
EWC.extremenetworks.com:topology:test:l3:dhcp# exclude 10.0.1.10 10.0.1.20
```

foreign-gateway

Use the `foreign-gateway` command to configure the remote Wireless Appliance in a paired controller configuration. The `foreign-gateway` command is available from the `topology:<named-topology>:l3:dhcp` context of the CLI for routed topologies. This command is visible only when mode is set to local. See [mode](#) on page 404.

foreign-gateway *A.B.C.D* | **none**

Parameters

<i>A.B.C.D</i>	Specifies the IP address of the remote Wireless Appliance.
none	Clears the IP address of the remote Wireless Appliance.

Example

The following example clears the IP address of the remote Wireless Appliance:

```
EWC.extremenetworks.com:topology:routed1:13:dhcp# mode local
EWC.extremenetworks.com:topology:routed1:13:dhcp# foreign-gateway none
```

foreign-range

Use the `foreign-range` command to configure the DHCP pool of addresses for a remote Wireless Appliance in a paired controller configuration. The `foreign-range` command is available from the `topology:<named-topology>:13: dhcp` context of the CLI for b@ac and routed topologies. This command is visible only when mode is set to local. See [mode](#) on page 404.

foreign-range *A.B.C.D A.B.C.D*

Parameters

<i>A.B.C.D</i>	Specifies the first IP address in the IP address range.
<i>A.B.C.D</i>	Specifies the last IP address in the IP address range.

Example

The following example specifies the IP address range:

```
EWC.extremenetworks.com:topology:routed2:13:dhcp# mode local
EWC.extremenetworks.com:topology:routed2:13:dhcp# foreign-range 10.44.6.2
10.44.6.254
```

gateway

Use the `gateway` command to specify the gateway IP address. The `gateway` command is available from the `topology:<named-topology>:13:dhcp` context of the CLI for b@ac and physical topologies. For information about the `gateway` command for the Admin topology, see [gateway](#) on page 410.

gateway *A.B.C.D* | **none**

Parameters

<i>A.B.C.D</i>	Specifies the IP address of the remote Wireless Appliance.
none	Clears the IP address of the remote Wireless Appliance.

Example

The following example clears the gateway IP address:

```
EWC.extremenetworks.com:topology:esal:13:dhcp# gateway none
```

lease-default

Use the `lease-default` command to set the default time limit, in seconds, that an IP address would be assigned by the DHCP server to a wireless device. The `lease-default` command is available from the `topology:<named-topology>:!3:dhcp` context of the CLI for b@ac, physical, and routed topologies. This command is visible only when mode is set to local. See [mode](#) on page 404.

After you run the `lease-default` command, run the `apply` command to implement the changes.

lease-default *int*

Parameters

<i>int</i>	Specifies the time limit in seconds.
------------	--------------------------------------

Example

The following example sets the default lease time to 34000 seconds:

```
EWC.extremenetworks.com:topology:routed2:13:dhcp# mode local
EWC.extremenetworks.com:topology:routed2:13:dhcp# lease 34000
EWC.extremenetworks.com:topology:routed2:13:dhcp# apply
```

lease-max

Use the `lease-max` command to set the maximum time limit, in seconds, that an IP address would be assigned by the DHCP server to a wireless device. The `lease-max` command is available from the `topology:<named-topology>:!3:dhcp` context of the CLI for b@ac, physical, and routed topologies. This command is visible only when mode is set to local. See [mode](#) on page 404.

After you run the `lease-max` command, run the `apply` command to implement the changes.

lease-max *int*

Parameters

<i>int</i>	Specifies the time limit in seconds.
------------	--------------------------------------

Example

The following example sets the maximum time to keep a DHCP-ed IP address to 2592000 seconds:

```
EWC.extremenetworks.com:topology:routed2:13:dhcp# mode local
EWC.extremenetworks.com:topology:routed2:13:dhcp# lease-max 2592000
EWC.extremenetworks.com:topology:routed2:13:dhcp# apply
```

mode

Use the `mode` command to specify the type of DHCP server to be used. The `mode` command is available from the `topology:<named-topology>:!3:dhcp` context of the CLI for b@ac, physical, and routed topologies.

After you run the `mode` command, run the `apply` command to implement the changes.

For b@ac topologies:

mode local | relay | none

For physical topologies:



mode local | none

For routed topologies:

mode local | relay

Parameters

local	Indicates that the controller itself acts as the DHCP server.
relay	Indicates that a DHCP relay server will be used.
none	Indicates that the Wireless Appliance will not treat the DHCP messages specially.

Example

The following example configures the routed topology named routed2 to use a local DHCP server on the controller:

```
EWC.extremenetworks.com:topology:routed2:13:dhcp# mode local
EWC.extremenetworks.com:topology:routed2:13:dhcp# apply
```

range

Use the `range` command to configure the DHCP pool of addresses. The `range` command is available from the `topology:<named-topology>:13:dhcp` context of the CLI for b@ac, physical, and routed topologies. This command is visible only when mode is set to local. See [mode](#) on page 404.

After you run the `range` command, run the `apply` command to implement the changes.

range *A.B.C.D A.B.C.D*

Parameters

<i>A.B.C.D</i>	Specifies the first IP address in the IP address range.
<i>A.B.C.D</i>	Specifies the last IP address in the IP address range.

Example

The following example defines the DHCP range of IP addresses:

```
EWC.extremenetworks.com:topology:routed2:13:dhcp# mode local
EWC.extremenetworks.com:topology:routed2:13:dhcp# range 192.168.1.30
192.168.1.54
EWC.extremenetworks.com:topology:routed2:13:dhcp# apply
```

show

Use the `show` command to display DHCP information for the specified topology. The `show` command is available from the `topology:<named-topology>:13:dhcp` context of the CLI for b@ac, physical, and routed topologies.

The output of the `show` command is determined by how mode is set. See [mode](#) on page 404.

show

Parameters

None

Examples

The following example shows DHCP information for a physical topology with mode set to local:

```
EWC.extremenetworks.com:topology:esal:l3:dhcp# show
DHCP option: local
Gateway: 10.0.1.2
Address range: 10.109.1.2 10.109.1.254
exclude 10.109.1.5(interface address)
DNS servers:
Domain name:
Max lease time: 2592000
Default lease time: 36000
WINS servers:
```

wins

Use the `wins` command to specify the IP address for the Windows Internet Naming Service (WINS) server. The `wins` command is available from the `topology:<named-topology>:l3:dhcp` context of the CLI for `b@ac`, `physical`, and `routed` topologies. This command is visible only when mode is set to `local`. See [mode](#) on page 404.

After you run the `wins` command, run the `apply` command to implement the changes.

```
wins (WINS server [,WINS server [...]]) | none
```

Parameters

<code>WINS server</code> [<code>WINS server</code> [...]]	Specifies the qualified IPv4 IP address or name of one or more WINS servers.
none	Clears the IP addresses and indicates that no WINS server is present.

Examples

The following example specifies the IP addresses of two WINS servers:

```
EWC.extremenetworks.com:topology:r1:l3:dhcp# mode local
EWC.extremenetworks.com:topology:r1:l3:dhcp# wins 192.168.1.3, 192.168.1.4
EWC.extremenetworks.com:topology:r1:l3:dhcp# apply
```

exceptions

Use the `exceptions` command to enter the `topology:<named-topology>:l3:exceptions` context of the CLI for `b@ac`, `physical`, and `routed` topologies. In this context, you can configure exception filters.

The following commands are available in the `topology:<named-topology>:l3:exceptions` context.

- [config](#) on page 407
- [create](#) on page 408
- [delete](#) on page 409
- [move](#) on page 409
- [show](#) on page 409



config

Use the `config` command to configure an existing exception filter. The `config` command is available from the `topology:<named-topology>:l3:exceptions` context of the CLI for b@ac, physical, and routed topologies.

```
config pos proto {udp|tcp|ah|esp|none|icmp|gre|0-255} A.B.C.D/0-32 [(port 0-65535[ 0-65535])|(type 0-255 [0-255])] in (none|src|dst|both) (allow|deny)
```

Parameters

<code>pos</code>	Specifies a position value for this filter in the filter list. Valid values are from 0-255.
<code>proto {udp tcp ah esp none icmp gre 0-255}</code>	Specifies the protocol for this filter rule by number or name. Valid number values are from 0-255. Valid name values are: <ul style="list-style-type: none"> • udp - UDP protocol • tcp - TCP protocol • ah - Authentication Header protocol • esp - Encapsulating Security Payload protocol • none - No protocols • icmp - ICMP protocol • gre - Generic Route Encapsulation protocol
<code>A.B.C.D/0-32</code>	Specifies the IPv4 IP address and mask.
<code>(port 0-65535[0-65535])</code>	Specifies a TCP or UDP port or port range to which this filter rule will be applied. The first value specifies either the port or the start of a port range. The second value optionally specifies the end of a port range. This parameter is only valid when either TCP or UDP is the specified protocol. Valid port values are from 0-65535.
<code>(type 0-255 [0-255])</code>	Specifies an ICMP type or range of ICMP types. This parameter is only valid when ICMP is the specified protocol. Valid values are from 0-255.
<code>in (none src dst both)</code>	Specifies the direction of packet flow — in specifies a packet flow from the AP to the AC. none specifies that the in direction will not be used as matching criteria in the filter rule. dst specifies that the IP address for this filter rule is the destination of the packet flow. src specifies that the IP address for this filter rule is the source of the packet flow. both specifies that the IP address for this filter rule can be either source or destination.
<code>(allow deny)</code>	Specifies whether packets will be allowed or denied when meeting the criteria specified in the filter rule.

Usage

If the specified exception filter position already contains an exception filter, the `config` command overwrites the existing exception filter. Use the `create` command to insert or append an exception filter at the specified position.

Example

The following example modifies an existing filter:

```
EWC.extremenetworks.com:topology:r1:l3:exceptions# config 2 proto tcp
1.1.1.1/32 port 80 in dst allow
```

create

Use the `create` command to create an exception filter. The `create` command is available from the `topology:<named-topology>:l3:exception` context of the CLI for `b@ac`, physical, and routed topologies.

```
create pos proto {udp|tcp|ah|esp|none|icmp|gre|0-255} A.B.C.D/0-32 [(port
0-65535[ 0-65535])](type 0-255 [0-255])] in (none|src|dst|both) (allow|deny)
```

Parameters

<i>pos</i>	Specifies a position value for this filter in the filter list. Valid values are from 0-255.
proto { udp tcp ah esp none icmp gre <i>0-255</i> }	Specifies the protocol for this filter rule by number or name. Valid number values are from 0-255. Valid name values are: <ul style="list-style-type: none"> • udp - UDP protocol • tcp - TCP protocol • ah - Authentication Header protocol • esp - Encapsulating Security Payload protocol • none - No protocols • icmp - ICMP protocol • gre - Generic Route Encapsulation protocol
<i>A.B.C.D/0-32</i>	Specifies the IPv4 IP address and mask.
(port <i>0-65535</i> [<i>0-65535</i>])	Specifies a TCP or UDP port or port range to which this filter rule will be applied. The first value specifies either the port or the start of a port range. The second value optionally specifies the end of a port range. This parameter is only valid when either TCP or UDP is the specified protocol. Valid port values are from 0-65535.
(type <i>0-255</i> [<i>0-255</i>])	Specifies an ICMP type or range of ICMP types. This parameter is only valid when ICMP is the specified protocol. Valid values are from 0-255.
in (none src dst both)	Specifies the direction of packet flow — <code>in</code> specifies a packet flow from the AP to the AC. <code>none</code> specifies that the <code>in</code> direction will not be used as matching criteria in the filter rule. <code>dst</code> specifies that the IP address for this filter rule is the destination of the packet flow. <code>src</code> specifies that the IP address for this filter rule is the source of the packet flow. <code>both</code> specifies that the IP address for this filter rule can be either source or destination.
(allow deny)	Specifies whether packets will be allowed or denied when meeting the criteria specified in the filter rule.

Usage

If the specified exception filter position already contains an exception filter, specifying an exception filter using this command inserts the exception filter in the specified position in the list and resequences all

filters below this filter down by one position. Use the `create` command to insert or append a rule at the specified position.

Example

The following example creates an exception filter:

```
EWC.extremenetworks.com:topology:r1:l3:exceptions# create 2 proto tcp
1.1.1.1/32 port 80 in dst deny
```

delete

Use the `delete` command to delete an exception filter. The `delete` command is available from the `topology:<named-topology>:l3:exceptions` context of the CLI for b@ac, physical, and routed topologies.

delete *pos*

Parameters

<i>pos</i>	Specifies the position of the exception filter (0-255).
------------	---

Example

The following example deletes the exception filter at position 2:

```
EWC.extremenetworks.com:topology:r1:l3:exceptions# delete 2
```

move

Use the `move` command to change the order (position) of an exception filter. The `move` command is available from the `topology:<named-topology>:l3:exceptions` context of the CLI for b@ac, physical, and routed topologies.

move *pos pos*

Parameters

<i>pos</i>	Specifies the current position of the exception filter (0-255).
<i>pos</i>	Specifies the new position of the exception filter (0-255).

Example

The following example moves exception filter at position 4 to 25:

```
EWC.extremenetworks.com:topology:r1:l3:exceptions# move 4 25
```

show

Use the `show` command to display a list of exception filters. The `show` command is available from the `topology:<named-topology>:l3:exceptions` context of the CLI for b@ac, physical, and routed topologies.

In the `show` command output, the (I) indicates that the exception filter is an internal (read-only) filter that has been pre-defined.

show

Parameters

None

Examples

The following example displays the exception filters for the r1 topology.

```
EWC.extremenetworks.com:topology:r1:l3:exceptions# show
Exception filter(I): 1027 proto tcp 11.11.11.17 255.255.255.255 port 60606
both deny
Exception filter(I): 1028 proto tcp 0.0.0.0 255.255.255.255 port 50200 both
deny
Exception filter(I): 1029 proto tcp 11.11.11.17 255.255.255.255 port 32768
65535 both allow
Exception filter(I): 1030 proto udp 11.11.11.17 255.255.255.255 port 32768
65535 both allow
Exception filter(I): 1031 proto udp 11.11.11.17 255.255.255.255 port 67 both
allow
Exception filter(I): 1032 proto udp 255.255.255.255 255.255.255.255 port 67
both allow
Exception filter(I): 1033 proto icmp 11.11.11.17 255.255.255.255 port 0 255
both allow
Exception filter(I): 1034 proto none 0.0.0.0 both deny
```

foreign-ip

Use the `foreign-ip` command to specify the IP address and subnet mask of the foreign controller. The `foreign-ip` command is available from the `topology:<named-topology>:l3` context of the CLI for b@ac and routed topologies.

```
foreign-ip A.B.C.D/0-32
```

Parameters

<code>A.B.C.D/0-32</code>	Specifies the IP address and subnet mask.
---------------------------	---

Usage

The `foreign-ip` command is not available when a controller is in standalone mode.

Once an availability pair is established between two controllers, the `foreign-ip` command is only visible after "sync" is enabled.

Example

The following example specifies the IP address and mask of the foreign controller:

```
EWC.extremenetworks.com:topology:r1# sync enable
EWC.extremenetworks.com:topology:r1# l3
EWC.extremenetworks.com:topology:r1:l3:# foreign-ip
```

gateway

Use the `gateway` command to specify the gateway IP address. The `gateway` command is available from the `topology:<named-topology>:l3` context of the CLI for the Admin topology.

```
gateway A.B.C.D | none
```

Parameters

<i>A.B.C.D</i>	Specifies the gateway IP address.
none	Clears the gateway IP address.

Example

The following example clears the gateway IP address:

```
EWC.extremenetworks.com:topology:Admin:13:# gateway none
```

gateway-ipv6

Use the `gateway-ipv6` command to specify an IPv6 gateway IP address. The `gateway-ipv6` command is available from the `topology:<named-topology>:I3` context of the CLI for the Admin topology only.

```
gateway-ipv6 A:B:C:D:E:F:G:H | none
```

Parameters

<i>A:B:C:D:E:F:G:H</i>	Specifies the gateway IPv6 address.
none	Clears the gateway IPv6 address.

Example

The following example defines the gateway IPv6 address:

```
EWC.extremenetworks.com:topology:Admin:13:# gateway-ipv6 fd66:2280:2668::2
```

gen-certreq

Use this command to generate a certificate signing request and private key for the named topology. The `gen-certreq` command is available from the `topology:<named-topology>:I3` context of the CLI.

```
gen-certreq cn [(location country state city) (organization name unit) (email email-address)] [ipv6] [key-size 1024|2048]
```

Parameters

cn	Common name that you want to assign to the controller interfaces. This is a mandatory parameter. If the common name is an IPv6 address, a [] is needed around the IPv6 address (see example, below).
location	Keyword indicating that the next three parameters specify the location where the controller is operating.
<i>country</i>	The name of the country where the controller is located. You must use the two-letter ISO abbreviation for the country.
<i>state</i>	The name of the state or province where the controller is located.
<i>city</i>	The name of the city where the controller is located.
organization	Keyword indicating that the next two parameters specify the name of the organization to which the controller belongs.
<i>name</i>	Organization name.

unit	Organization unit name.
email	Key word that identifies the following parameter as an email address.
email_addr	Email address.
ipv6	Specifies that the certificate supports IPv6 addressing.
key-size	Specifies that the certificate supports key size. Valid key size values are 1024 or 2048.

Usage

If a DNS name is used as the common name, a DNS lookup is performed. If the DNS name is not found, a warning is displayed.

Once the CSR file has been created, you can copy it to an FTP or SCP server using the [page 399](#) command `copy-csr` on page 399. You can apply the certificate with the [page 397](#) command `cert` on page 397.

Example

The following example shows a certificate request with a common name that is an IPv6 address:

```
EWC.extremenetworks.com:ap:topology:Seg1_Routed:l3# gen_cerreq
[fd66:2280:2668::12] location CA Ontario Mississauga organization
mnj_Ware_House Service email me@email.com ipv6 key-size 2048
```

ip

Use the `ip` command to specify the Wireless Appliance IP address and subnet mask for physical and routed topologies or the interface IP address and subnet mask for b@ac topologies. The `ip` command is available from the topology:<named-topology>:l3 context of the CLI for Admin, b@ac, physical, and routed topologies.

```
ip A.B.C.D/0-32
```

Parameters

A.B.C.D/0-32	Specifies the IP address and subnet mask.
---------------------	---

Example

The following example specifies an IP address and subnet mask:

```
EWC.extremenetworks.com:topology:r1:l3:# ip 10.109.0.1/30
```

ipv6

Use the `ipv6` command to specify a management IPv6 address and subnet mask for the Wireless Appliance. The `ipv6` command is available from the topology:<named-topology>:l3 context of the CLI for the Admin topology only.

```
ipv6 A:B:C:D:E:F:G:H/0-64 | none
```

Parameters

<code>A:B:C:D:E:F:G:H/0-64</code>	Specifies the IPv6 address and subnet mask.
<code>none</code>	Specifies that there is no IPv6 address configured for this controller.

Example

The following example specifies an IP address and subnet mask:

```
EWC.extremenetworks.com:topology:Admin:l3:# ipv6 fd66:2280:2668::13/64
```

mgmt

Use the `mgmt` command to allow or prohibit management traffic. The `mgmt` command is available from the `topology:<named-topology>:l3` context of the CLI for `b@ac`, `physical`, and `routed` topologies.

mgmt enable | disable

Parameters

<code>enable</code>	Enables management traffic.
<code>disable</code>	Disable management traffic.

Example

The following example enables management traffic:

```
EWC.extremenetworks.com:topology:r1:l3:# mgmt enable
```

mtu

Use the `mtu` command to set the interface MTU (Maximum Transmission Unit), which specifies the maximum allowable size, in bytes, of a data packet on the Ethernet port. The `mtu` command is available from the `topology:<named-topology>:l3` context of the CLI for `Admin`, `b@ac`, `physical`, and `routed` topologies.

mtu 576-1500

Parameters

<code>576-1500</code>	Specifies the size, in bytes, of the MTU.
-----------------------	---

Example

The following example sets the size of the MTU to 1500 bytes:

```
EWC.extremenetworks.com:topology:r1:l3:# mtu 1500
```

netmask

Use the `netmask` command to optionally configure a netmask for a `B@AC` or `B@AP` topology. The `netmask` command is available from the `topology:<named-topology>` context of the CLI for `b@ap` or `b@ac` topologies with disabled `l3presence`. If configured, the netmask will be used in the RADIUS Accounting Framed-IP-Netmask attribute (assuming RADIUS accounting is using this topology).

netmask (netmask | CIDR | none)

Parameters

<i>netmask</i>	Specifies the netmask in dotted-decimal notation.
<i>CIDR</i>	Specifies the number of bits in the netmask that make up the network ID.
none	Specifies that no netmask is configured.

Example

The following example sets the netmask for the bap topology to 24 (equivalent to netmask 255.255.255.0):

```
EWC.extremenetworks.com:topology:bap:l3# netmask 24
```

nexthop

Use the `nexthop` command to set the IP address of the next hop router through which traffic will be directed. The `nexthop` command is available from the `topology:<named-topology>:l3` context of the CLI for routed topologies.

After you run the `nexthop` command, run the `apply` command to implement the changes.

```
nexthop A.B.C.D | none
```

Parameters

<i>A.B.C.D</i>	Specifies the IP address of the next hop router.
none	Clears the IP address of the next hop router.

Example

The following example sets the IP address of the next hop router (169.232.75.1):

```
EWC.extremenetworks.com:topology:r1:l3:# nexthop 169.232.75.1
```

ospf-advert

Use the `ospf-advert` command to enable or disable OSPF advertisements on the topology. The `ospf-advert` command is available from the `topology:<named-topology>:l3` context of the CLI for routed topologies.

After you run the `ospf-advert` command, run the `apply` command to implement the changes.

```
ospf-advert enable | disable
```

Parameters

enable	Enables OSPF advertisements.
disable	Disables OSPF advertisements.

Example

The following example enables OSPF advertisements:

```
EWC.extremenetworks.com:topology:r1:l3:# ospf-advert enable
```

ospf-cost

Use the `ospf-cost` command to set the OSPF route cost value. The `ospf-cost` command is available from the `topology:<named-topology>:l3` context of the CLI for routed topologies.

After you run the `ospf-cost` command, run the `apply` command to implement the changes.

```
ospf-cost 1-50000
```

Parameters

<code>1-50000</code>	Specifies the OSPF route cost value.
----------------------	--------------------------------------

Examples

The following example sets the OSPF route cost value to 6000:

```
EWC.extremenetworks.com:topology:r1:l3# ospf-cost 6000
```

show

Use the `show` command to display Layer 3 information. The `show` command is available from the `topology:<named-topology>:l3` context of the CLI for Admin, b@ac, physical, and routed topologies.

```
show
```

Parameters

None

Examples

The following example displays Layer 3 information for a physical topology:

```
EWC.extremenetworks.com:topology:esa0:l3# show
Interface IP 10.109.0.1 255.255.255.0
AP Registration: enable
Allow management traffic: disable
Factory default certificate/key
MTU: 1500
```

The following example displays Layer 3 information for a b@ac topology:

```
EWC.extremenetworks.com:topology:bridged_ac1:l3# show
Interface IP 0.0.0.0 0.0.0.0
AP Registration: disable
Allow management traffic: disable
Factory default certificate/key
Strict Subnet Adherence: enable
MTU: 1436
```

l3presence

As of Release 9.21, you can access Layer 3 on a b@ac topology when `l3presence` is disabled. For releases prior to 9.21, you must enable Layer 3 on a b@ac topology to access Layer 3 commands in the `topology:<named-topology>:l3` context. Use the `l3presence` command to enable or disable Layer 3 on

a b@ac topology. The `l3presence` command is available from the topology:<named-topology> context of the CLI for b@ac topologies.

l3presence enable | disable

Parameters

enable	Enables Layer 3.
disable	Disables Layer 3.

Example

The following example enables Layer 3 on a b@ac topology:

```
EWC.extremenetworks.com:topology:bridged_ac1# l3presence enable
```

mode

Use the `mode` command to change the mode of an existing b@ac, b@ap, or routed topology. You can configure the mode of a topology only if the topology is not associated with a policy. The `mode` command is available from the topology:<named-topology> context of the CLI for b@ac, b@ap, and routed topologies.

mode b@ap | b@ac | routed

Parameters

b@ap b@ac routed	Specifies the mode of the topology.
-----------------------------	-------------------------------------

Example

The following example changes the mode of the topology to b@ap:

```
EWC.extremenetworks.com:topology:bridged_ac1# mode b@ap
```

name

Use the `name` command to change the name of an existing b@ac, b@ap, or routed topology. The `name` command is available from the topology:<named-topology> context of the CLI for b@ac, b@ap, and routed topologies.

name topology name

Parameters

<i>topology name</i>	Specifies the name of the topology.
----------------------	-------------------------------------

Example

The following example changes the name of the topology to bridged_ac2:

```
EWC.extremenetworks.com:topology:bridged_ac1# name bridged_ac2
```



show

Use the `show` command to display information about a topology. The `show` command is available from the topology:<named-topology> context of the CLI for Admin, b@ac, b@ap, physical, and routed topologies.

show

Parameters

None

Examples

The following examples shows configuration information for the Admin topology:

```
EWC.extremenetworks.com:topology:Admin# show
Name: Admin
```

The following example shows configuration information for a b@ac topology:

```
EWC.extremenetworks.com:topology:BridgedAC2# show
Synchronize: disable
Name: BridgedAC2
Layer 3 presence: disable
```

The following example shows configuration information for a b@ap topology:

```
EWC.extremenetworks.com:topology:BridgedAP2# show
Synchronize: enable
Name: BridgedAP2
```

The following example shows configuration information for a physical topology:

```
EWC.extremenetworks.com:topology:esa0# show
Name: esa0
3rd party: disable
```

The following example shows configuration information for a routed topology:

```
EWC.extremenetworks.com:topology:r1# show
Topology mode: routed
Synchronize: enable
Name: r1
```

strict-subnet

Use the `strict-subnet` command to enable or disable strict subnet adherence on a b@ac topology. The `strict-subnet` command is available from the topology:<named-topology> context of the CLI for b@ac topologies.

strict-subnet enable | disable

Parameters

enable	Enables strict subnet adherence.
disable	Disables strict subnet adherence.

Example

The following example enables strict subnet adherence on a b@ac topology:

```
EWC.extremenetworks.com:topology:bridged_acl# strict-subnet enable
```

sync

Use the `sync` command to enable or disable automatic synchronization of this topology across paired controllers. The `sync` command is available from the `topology:<named-topology>` context of the CLI for b@ac, b@ap, and routed topologies.

sync enable | disable

Parameters

enable	Enables synchronization.
disable	Disables synchronization.

Example

The following example enables synchronization:

```
EWC.extremenetworks.com:topology:r1# sync enable
```

topology-group

Executing the `topology-group` command moves you into the `topology:topology-group` context, in which you can create or delete topology groups. The `topology-group` command is entered in the topology context.

A Topology Group is a list of topologies associated with a unique name and a VLAN ID. All the topologies in a defined topology group have the same type: either B@AC or routed. Any time the controller MU Session Manager assigns a role, any topology group in the role will be replaced by a member topology contained in the group. If a topology group is referenced multiple times, only 1 topology from the group is selected. A different user could be assigned a different member topology from the topology group. Different sessions may be assigned to a different topology in a topology group.

The following commands are available in the `topology:topology-group` context.

- [create](#) on page 419
- [delete](#) on page 419
- [show](#) on page 419
- [<topology-group-name>](#) on page 420 to specify a name for this topology group

create

Use the `create` command to create a topology group object. The `create` command is accessible from the topology group context of the CLI.

```
create topology-group-name first-group-member(b@ac | routed) vlanid
```

Parameters

<i>topology-group-name</i>	Specifies the name of the topology group.
<i>first-group-member</i>	Specifies the first topology group member.
b@ac	Specifies a Bridge Traffic locally at Controller topology for this group.
routed	Specifies a routed topology for this group.
<i>vlanid</i>	VLAN ID assigned to this topology group. Value can be in range 1-4094.

Example

The following example creates a routed topology type group named top-group, with a first member name routed_topology, and a VLAN ID of 232:

```
EWC.extremenetworks.com:topology:topology-group# create top-group
routed_topology routed 232
```

delete

Use the `delete` command to delete a topology group object. The `delete` command is accessible from the topology group context of the CLI.

```
delete topology-group-name
```

Parameters

<i>topology-group-name</i>	Specifies the name of the topology group.
----------------------------	---

Example

The following example deletes a routed topology type group named top-group:

```
EWC.extremenetworks.com:topology:topology-group# delete top-group
```

show

Use the `show` command to display information about a topology group. The `show` command is available from the topology:topology-group context of the CLI.

```
show
```

Parameters

None

Example

The following example shows topology group configuration information:

```
C5110-2.chantry:topology:topology-group:TG5# show
Topology mode: routed
Name: TG5
VLAN ID: 105
Member List: V801data:Topology
```

<topology-group-name>

Executing the <topology-group-name> command moves you into the topology:topology-group:top-group-name context, in which you can add, update, or delete topology group name members or display topology group name information. The <topology-group-name> command is entered in the topology:topology-group context.

The following commands are available in the topology:topology-group:top-group-name context.

- [members](#) on page 420 to add, update, or delete a topology group member
- [name](#) to change the topology group name
- [show](#) on page 421
- [vlanid](#)

members

Use the `members` command to add, update, or delete a topology group member. The `members` command is accessible from the topology group name context of the CLI.

```
members [(add|update|delete)] topology_name [topology_name]*
```

Parameters

add	Specifies that a new topology name is being added to the group.
update	Specifies the topology name of an existing member that is being updated for the group.
delete	Specifies the topology name of an existing member that is being removed from the group.
<i>topology_name</i>	Specifies a topology name.
[<i>topology_name</i>]*	Optionally, specifies one or more additional topology names separated by a space.

Usage

The group member must have same topology mode type as the topology group.

Example

The following example adds topologies `routed_803` and `Routed1` to the topology group for this context:

```
EWC.extremenetworks.com:topology:topology-group:top-group-name# members add
routed_803 Routed1
```

name

Use the `name` command to change the name of a topology group. The `name` command is accessible from the topology group name context of the CLI.

name *topology_name*

Parameters

<i>topology_name</i>	Specifies a topology name.
----------------------	----------------------------

Usage

The group member must have same topology mode type as the topology group.

Example

The following example changes the name of a topology group from `tg1` to `tg1_new`:

```
EWC.extremenetworks.com:topology:topology-group:tg1# name tg1_new
```

show

Use the `show` command to display information about a topology group. The `show` command is available from the topology:topology-group:top-group-name context of the CLI.

show

Parameters

None

Example

The following example shows topology group configuration information:

```
C5110-2.chantry:topology:topology-group:TG5# show
Topology mode: routed
Name: TG5
VLAN ID: 105
Member List: V801data:Topology
```

vlanid

Use the `vlanid` command to change the VLAN ID of a topology group. The `vlanid` command is accessible from the topology group name context of the CLI.

vlanid *id*

Parameters

<i>id</i>	Specifies a VLAN ID number. Valid VLAN ID numbers are 1-4094.
-----------	---

Usage

The group member must have same topology mode type as the topology group.



Example

The following example changes the VLAN ID of a topology group to 1235:

```
EWC.extremenetworks.com:topology:topology-group:tg1# vlanid 1235
```

22 Location-Based-Service (lbs) Commands

multicast
port
service
server-ip
show
Related commands

This section describes commands used to enable and configure a location-based service on a Wireless Appliance and Wireless APs. These commands are located in the lbs context of the CLI. Execute the `lbs` command at the root level to enter lbs context.

Aeroscout and Ekahau are the currently-supported location-based servers.

All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the lbs context:

- [multicast](#) on page 423
- [port](#) on page 424
- [service](#) on page 424
- [server-ip](#) on page 425
- [show](#) on page 425

For information on related commands that are available in other contexts, see [Related commands](#) on page 426.

multicast

Use the `multicast` command to set the location-based server multicast address. The `multicast` command is accessible from the lbs context of the CLI.

```
multicast 0x:0x:0x:0x:0x:0x
```

Parameters

<code>0x:0x:0x:0x:0x:0x</code>	Specifies the multicast address of the location-based server, in hexadecimal format.
--------------------------------	--

Usage

This command is visible only if a location-based service has been enabled via the `service` command.

The default multicast address is 00:00:00:00:00:00

Examples

The following example sets the multicast address of the Ekahau server to 01:18:8e:00:00:00:

```
EWC.extremenetworks.com:lbs# service ekahau
EWC.extremenetworks.com:lbs# multicast 01:18:8e:00:00:00
```

port

Use the `port` command to set the location-based server port address. The `port` command is accessible from the `lbs` context of the CLI.

```
port 0-65535
```

Parameters

<code>0-65535</code>	Specifies the port address of the location-based server. Enter at least 2 digits (for example, 06 for port 6).
----------------------	--

Usage

This command is visible only if a location-based service has been enabled via the `service` command.

The default port address is 00

Examples

The following example sets the port address of the Ekahau server to 06:

```
EWC.extremenetworks.com:lbs# service ekahau
EWC.extremenetworks.com:lbs# port 06
```

service

Use the `service` command to enable or disable an AeroScout or Ekahau location-based service on the Wireless Appliance. The `service` command is accessible from the `lbs` context of the CLI.

```
service disable | aeroscout | ekahau
```

Parameters

<code>disable</code>	Disables location-based service.
<code>aeroscout</code>	Enables Aeroscout location-based service.
<code>ekahau</code>	Enables Ekahau location-based service.

Usage

Use the `server-ip` command to specify the IP address of the AeroScout/Ekahau server, after you enable the service.

Examples

The following example enables the Aeroscout location-based service:

```
EWC.extremenetworks.com# lbs
EWC.extremenetworks.com:lbs# service aeroscout
```

server-ip

Use the `server-ip` command to set the location-based server IP address. The `server-ip` command is accessible from the lbs context of the CLI.

```
server-ip A.B.C.D
```

Parameters

<i>A.B.C.D</i>	Specifies the IP address of the location-based server.
----------------	--

Usage

This command is visible only if a location-based service has been enabled via the `service` command.

The default IP address is 0.0.0.0.

Examples

The following example sets the IP address of the AeroScout server to 192.168.3.100:

```
EWC.extremenetworks.com:lbs# service aeroscout
EWC.extremenetworks.com:lbs# server-ip 192.168.3.100
```

show

Use the `show` command to display information about the location-based service. The `show` command is accessible from the lbs context of the CLI.

```
show
```

Parameters

None.

Examples

The following example displays information for the Ekahau location-based service:

```
EWC.extremenetworks.com:lbs# show
LBS status: ekahau
LBS server address: 100.200.30.40
Ekahau server port: 6
Ekahau multicast address: 01:18:8e:00:00:00
```

Related commands

The following commands in other contexts relate to location-based service:

- [lbs-status](#) on page 426
- [show](#) on page 426

lbs-status

The `lbs-status` command allows you to enable or disable the collection of AeroScout/Ekahau tags on a specific AP or all APs of a given type.

The `lbs-status` command is accessible from the following contexts:

- `ap:<serial>` — Use the `lbs-status` command in this context to enable or disable the collection of AeroScout/Ekahau tags on a specific AP. See [location](#) on page 124.
- `ap:defaults:11n` — Use the `lbs-status` command in this context to enable or disable the collection of AeroScout/Ekahau tags on all 38xx APs. See [lbs-status](#) on page 122.

show

The `show` command allows you to display configuration information, including `lbs-status`, for a specific AP or all APs of a specific type.

The `show` command is accessible from the following contexts:

- `ap:<serial>` — Use the `show` command in this context to display configuration information for a specific AP. See [show](#) on page 136.
- `ap:defaults:11n` — Use the `show` command in this context to display configuration information for all 38xx APs. See [show](#) on page 110.

23 web Commands

guestportal-admin-timeout
timeout
showvns
show

The `web` command refers to the web context, which contains commands used to configure the web settings. The `web` command is accessible from the root context of the CLI.

The following commands are available in the web context:

- `guestportal-admin-timeout` on page 427
- `timeout` on page 428
- `showvns` on page 428
- `show` on page 429

guestportal-admin-timeout

Use the `guestportal-admin-timeout` command to configure the time after which the web sessions of guest administrator users (guestportal user type) times out. The `guestportal-admin-timeout` command is accessible from the web context of the CLI.

After you have run the `guestportal-admin-timeout` command, run the `apply` command to implement the changes.

```
guestportal-admin-timeout hh:mm | mm
```

Parameters

<i>hh:mm</i>	Specifies time in hh:mm format — hours:minutes , range 1 minute to 7 days.
<i>mm</i>	Specifies time in number of minutes.

Examples

The following example sets the web session timeout to one hour and 30 minutes:

```
EWC.extremenetworks.com:web# guestportal-admin-timeout 01:30
```

The following example sets the web session timeout to 30 minutes:

```
EWC.extremenetworks.com:web# guestportal-admin-timeout 30
```

timeout

Use the `timeout` command to configure the time after which the web session times out. The `timeout` command is accessible from the web context of the CLI.

After you have run the `timeout` command, run the `apply` command to implement the changes.

```
timeout hh:mm | mm
```

Parameters

<i>hh:mm</i>	Specifies time in hh:mm format — hours:minutes, range 1 minute to 7 days.
<i>mm</i>	Specifies time in number of minutes, 1-59.

Examples

The following example sets the web session timeout to one hour and 30 minutes:

```
EWC.extremenetworks.com:web# timeout 01:30
```

The following example sets the web session timeout to two hours (120 minutes):

```
EWC.extremenetworks.com:web# timeout 120
```

showvns

Use the `showvns` command to display the VNS names in the Wireless AP SSID list on the controller's user interface (Wireless AP screen). Use the `no` form of the command to remove the VNS names in the Wireless AP SSID list. The `showvns` command is accessible from the web context of the CLI.

After you have run the `showvns` command, run the `apply` command to implement the changes.

```
showvns  
no showvns
```

Parameters

None

Examples

The following example displays the VNS names in the Wireless AP SSID list on the controller's user interface (Wireless AP screen):

```
EWC.extremenetworks.com:web# showvns
```

The following example removes the VNS names in the Wireless AP SSID list on the controller's user interface (Wireless AP screen):

```
EWC.extremenetworks.com:web# no showvns
```

show

Use the `show` command to display the web settings.

show

Parameters

None

Examples

The following example displays the web settings:

```
EWC.extremenetworks.com:web# show
timeout 34:0
showvns
```

24 cos Commands

```
create
delete
show
<named-cos>
```

This section describes commands used to define and configure class of service (CoS) for the Wireless Appliance. These commands are located in the `cos` context of the CLI. Execute the `cos` command at the root level to enter `cos` context. Refer to “Configuring Classes of Service” in the *Wireless User Guide* for detailed information about class of service configuration.

A class of service is a collection of attributes and rules that determine how a frame is forwarded through the network relative to other packets. The CoS defines actions to be taken when rate limits are exceeded for a specific traffic type. Use CoS to apply priority marking, inbound and outbound rate control settings, and filter rules.

All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The CoS context was introduced with V8.01.

The following commands are available in the `cos` context:

- `create`
- `delete`
- `show`
- `<named-cos>` — for commands in the `cos : <named-cos>` context.

create

Use the `create` command to create a new CoS, specifying a name for the new CoS. The `create` command is accessible from the `cos` context.

```
create cos-name
```

Parameters

<i>cos-name</i>	Specifies the name of the CoS. A CoS name can be made up of all alpha-numeric characters, as well as special characters: <code>!#\$.</code>
-----------------	---

Usage

The name “No CoS” is a predefined, reserved name. It is used as a default. No CoS cannot be deleted and the only modification allowed to it is use-wlan-marking.

Example

The following example creates a CoS named my-cos:

```
EWC.extremenetworks.com:cos# create my-cos
```

delete

Use the `delete` command to delete a CoS specifying the name of the CoS to be deleted. The `delete` command is accessible from the `cos` context of the CLI.

```
delete cos-name
```

Parameters

<i>cos-name</i>	Specifies the name of the CoS to delete.
-----------------	--

Example

The following example deletes the CoS named my-cos:

```
EWC.extremenetworks.com:policy# delete my-cos
```

show

Use the `show` command to display a summary of all `cos` objects, or a specific named `cos`. The `show` command is accessible from within the `cos` context.

```
show
```

Parameters

<i>cos-name</i>	Specifies that information for the named <code>cos</code> be displayed.
-----------------	---

Examples

The following example displays the current list of CoS configuration information:

```
EWC.extremenetworks.com:cos# show
CoS name      802.1p  ToS/DSCP  Inbound Rate Profile  Outbound Rate Profile
TXQ
No CoS       -      -         -                     -
lab10-c1     -      0x7C/0xFF -                     -          3
Legacy CoS   -      -         -                     -
```

<named-cos>

The `<named-cos>` command, where `<named-cos>` refers to the name of a given CoS, provides access to the `cos:<named-cos>` context.

The `cos:<named-cos>` context provides commands for the configuration of the `<named-cos>`. A `<named-cos>` must first be created using the `create` command in the `cos` context. Once created it becomes available as a command, allowing access to the `cos:<named-cos>` context for that CoS. For example, to enter the `<named-cos>` context for the `cos` named `my-cos`, use the command `my-cos` from the `cos` context, created using the `create <cos-name>` command.

After you complete configuration changes for a `<named-cos>`, run the `apply` command before exiting the `cos:<named-cos>` context to implement the changes.

The following commands are available in the `cos:<named-cos>` context.

- [show](#) on page 432
- [name](#) on page 433
- [sync](#) on page 433
- [use-wlan-marking](#) on page 434
- [priority](#) on page 435
- [tos-dscp-mask](#) on page 435
- [rateprf-in](#) on page 436
- [rateprf-out](#) on page 436
- [transmit-queue](#) on page 437

show

Use the `show` command to display the `<named-cos>` configuration information for the current `cos:<named-cos>` context. The `show` command is accessible from within the `cos:<named-cos>` context.

show

Parameters

None.

Examples

The following example displays the `my-cos` CoS configuration from within the `cos:<named-cos>` context:

```
EWC.extremenetworks.com:cos# my-cos
EWC.extremenetworks.com:cos:my-cos# show
Name: my-cos
Use Legacy Priority Override defined in the WLAN Service: disable
802.1p Priority: none
ToS/DSCP Marking:
Mask:
Inbound Rate Limit:
Outbound Rate Limit:
Transmit Queue: none
```



```
Synchronize: enable
EWC.extremenetworks.com:cos:my-cos#
```

name

Use the `name` command to change the name of a CoS. The `name` command is accessible from within the `cos:<named-cos>` context.

name *new-name*

Parameters

<i>new-name</i>	Specifies the new name for this <named-cos>.
-----------------	--

Usage

You must enter the `apply` command before exiting the `cos:<named-cos>` context for the CoS name change to take affect. The CLI prompt does not change until you exit and re-enter the `cos:<named-cos>` context.

Examples

The following example:

- Renames the CoS `your-cos` to `my-cos`
- Applies the change
- Displays the `my-cos` configuration
- Exits `cos:<named-cos>` context
- Re-enters the `cos:<named-cos>` context as `my-cos`

```
EWC.extremenetworks.com:cos# your-cos
EWC.extremenetworks.com:cos:your-cos# name my-cos
EWC.extremenetworks.com:cos:your-cos# apply
EWC.extremenetworks.com:cos:your-cos# show
Name: my-cos
Use Legacy Priority Override defined in the WLAN Service: disable
802.1p Priority: none
ToS/DSCP Marking:
Mask:
Inbound Rate Limit:
Outbound Rate Limit:
Transmit Queue: none
Synchronize: enable
EWC.extremenetworks.com:cos:your-cos# exit
EWC.extremenetworks.com:cos# my-cos
EWC.extremenetworks.com:cos:my-cos#
```

sync

Use the `sync` command to enable or disable automatic synchronization of this `<named-cos>` across paired controllers. Refer to the section entitled “Using the Sync Summary,” in the *Wireless User Guide* for more information about synchronization of CoS.

The `sync` command is accessible from within the `cos:<named-cos>` context.

sync {**enable** | **disable**}

Parameters

enable disable	Enables or disables automatic synchronization of this <named-cos> across paired controllers.
--------------------------------	--

Examples

The following example enables the synchronization of the my-cos CoS across controllers:

```
EWC.extremenetworks.com:cos:my-cos# sync enable
EWC.extremenetworks.com:cos:my-cos# apply
EWC.extremenetworks.com:cos:my-cos# show
Name: my-cos
Use Legacy Priority Override defined in the WLAN Service: disable
802.1p Priority: none
ToS/DSCP Marking:
Mask:
Inbound Rate Limit:
Outbound Rate Limit:
Transmit Queue: none
Synchronize: enable
EWC.extremenetworks.com:cos:my-cos#
```

use-wlan-marking

Use the use-wlan-marking command to enable or disable WLAN (ToS/DSCP) marking in WLAN service.

The use-wlan-marking command is accessible from within the cos:<named-cos> context.

use-wlan-marking {**enable** | **disable**}

Parameters

enable	Enables WLAN service to use the legacy priority value taken from the WLAN.
disable	Disables WLAN service from applying the legacy priority taken from the WLAN; the priority value of this CoS is used instead. This is the default.

Usage

When WLAN marking is enabled, the WLAN service applies legacy priority override settings defined in WLAN Quality of Service (QoS) tables to received packets before sending them on.

When WLAN marking is disabled, the WLAN service applies the User Priority (UP) value defined for this CoS to received packets before sending them on. Use the **priority** command in the cos:<named-cos> context to configure a priority value for this CoS.

For a detailed explanation of TOS/DSCP, User Priority determination, and WLAN marking, refer to the *Wireless User Guide*, “Configuring Classes of Service” chapter.

Example

The following example enables WLAN marking using the legacy priority value taken from the WLAN in WLAN service:

```
EWC.extremenetworks.com:cos:my-cos# use-wlan-marking enable
```

priority

Use the `priority` command to configure 802.1p user priority (UP) for this CoS.

The `priority` command is accessible from within the `cos:<named-cos>` context.

priority *0-7* | **none**

Parameters

<i>0-7</i>	Defines user priority level for this CoS; 7 is highest priority.
none	User priority level is not assigned for this CoS.

Usage

WLAN marking must be disabled when you use this command.

Example

The following example assigns a user priority value of 3 to the CoS:

```
EWC.extremenetworks.com:cos:my-cos# priority 3
```

tos-dscp-mask

Use the `tos-dscp-mask` command to configure a ToS/DSCP marking value and mask, in hexadecimal. If WLAN marking is enabled, the ToS or DSCP value (only one or the other is present in the received packet) is taken from the WLAN. Enter the value/mask combination you want used.

The `tos-dscp-mask` command is accessible from within the `cos:<named-cos>` context.

tos-dscp-mask (*tos-dscp/mask*) | **none**

Parameters

<i>tos-dscp</i>	Valid values, in hexadecimal., for ToS/DSCP are 0-FF.
<i>mask</i>	Valid values, in hexadecimal., for mask are 0-FF.
none	ToS /DSCP values are not used.

Usage

The slash (/) is a literal separator of *tos/dscp* and *mask* values.

Example

The following example configures a ToS-DSCP marking value (1E) and a mask value of FF:

```
EWC.extremenetworks.com:cos:my-cos# tos-dscp-mask 1E/FF
```

rateprf-in

Use the `rateprf-in` command to associate an already existing rate profile as an ingress rate profile for a CoS. The `rateprf-in` command is accessible from the `cos:<named-cos>` context.

rateprf-in *profile* | **none**

Parameters

<i>profile</i>	Specifies the ingress rate profile to configure for this <code>wlans:default-cos</code> context.
none	Specifies that the ingress rate profile is used for this <code>wlans:default-cos</code> context.

Usage

Refer to [rateprofile](#) on page 268 for rate profile configuration information.

Examples

The following example configures the default-policy with the DocRateIn ingress rate profile:

```
EWC.extremenetworks.com:cos:my-cos# rateprf-in DocRateIn
EWC.extremenetworks.com:cos:my-cos# apply
EWC.extremenetworks.com:cos:my-cos# show
Assigned topology: guestPortal
Ingress rate profile: DocRateIn
Egress rate profile: Unlimited
Enable AP filtering: disable
Synchronize: enable
EWC.extremenetworks.com:cos:my-cos#
```

rateprf-out

Use the `rateprf-out` command to configure an already existing rate profile for an outbound rate limit for CoS. The `rateprf-out` command is accessible from the `cos:<named-cos>` context.

rateprf-out *profile* | **none**

Parameters

<i>profile</i>	Specifies the egress rate profile to configure for this <code>cos:<named-cos></code> context.
none	Specifies that the egress rate profile will not be used for this <code>wlans:default-cos</code> context.

Usage

Refer to [rateprofile](#) on page 268 for rate profile configuration information.

Examples

The following example configures the my-cos CoS with the DocRateOut egress rate profile:

```

EWC.extremenetworks.com:cos:my-cos# rateprf-out DocRateOut
EWC.extremenetworks.com:cos:my-cos# apply
EWC.extremenetworks.com:cos:my-cos# show
Assigned topology: guestPortal
Ingress rate profile: DocRateIn
Egress rate profile: DocRateOut
Enable AP filtering: disable
Synchronize: enable
EWC.extremenetworks.com:cos:my-cos#

```

transmit-queue

Use the `transmit-queue` command to configure a transmit queue for this CoS. This transmit queue assignment is an override to the default transmit queue assignment specified in the 802.1p priority, that is applied without remarking the original 802.1p field in the packet.

The `transmit-queue` command is accessible from within the `cos:<named-cos>` context.

transmit-queue 0-7 | none

Parameters

0-7	Sets transmit queue for this CoS.
none	No transit queue specified for this CoS.

Example

The following example assigns transmit queue 3 to the CoS:

```

EWC.extremenetworks.com:cos:my-cos# transmit-queue 3

```

25 site Commands

create
delete
show site
<named-site>

This section describes commands used to define and configure sites at which an authentication server is local and have greater autonomy than wireless stations in a network based on centralized controllers and authentication. These commands are located in the site context of the CLI. Execute the `site` command at the root level to enter site context. Refer to “Configuring Sites” in the *Wireless User Guide* for detailed information about the use of sites and site configuration.

A site consists of APs, topologies, policies, Class of Service (CoS), and RADIUS servers that together define a site. A site can use any policy or CoS defined on the controller. Bridged at AP, Bridged at Controller, or Routed topologies defined on the controller are valid for sites, although the survivability benefit of sites is best enhanced in Bridged at AP topologies. Sites are assigned to WLAN Services in the same manner as AP load groups. When an AP is assigned to a site, the controller pre-loads the AP with the configured topologies, policies, CoS, and RADIUS server configurations of the site. The AP can then use these configurations independently of the controller.

All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The site context was introduced with V8.11.

The following commands are available in the site context:

- `create`
- `delete`
- `show site`
- `<named-site>` — for commands in the `site:<named-site>` context.

create

Use the `create` command to create a new site, specifying a name for the new site. The `create` command is accessible from the site context.

```
create site-name
```

Parameters

<code><i>site-name</i></code>	Specifies the name of the site. A site name can be up to 255 alpha-numeric characters, including special characters: -!#\$.
-------------------------------	---

Example

The following example creates a site named site1:

```
EWC.extremenetworks.com:site# create site1
```

delete

Use the `delete` command to delete a site specifying the name of the site to be deleted. The `delete` command is accessible from the site context of the CLI.

```
delete site-name
```

Parameters

<code>site-name</code>	Specifies the name of the site to delete.
------------------------	---

Example

The following example deletes the site named site1:

```
EWC.extremenetworks.com:policy# delete site1
```

show site

Use the `show site` command to display a summary of all site objects, or a specific named site. The `show site` command is accessible from within the site context.

```
show site
```

Parameters

<code>site-name</code>	Specifies that information for the named site be displayed.
------------------------	---

Example

The following example displays the current list of site configuration information:

```
EWC.extremenetworks.com:site# show site
site name    Site ID
site1        1
site2        2
site3        3
```

<named-site>

The `<named-site>` command, where `<named-site>` refers to the name of a given site, provides access to the `site:<named-site>` context.

The `site:<named-site>` context provides commands for the configuration of the `<named-site>`. A `<named-site>` must first be created using the `create` command in the site context. Once created it becomes available as a command, allowing access to the `site:<named-site>` context for that site. For example, to enter the `<named-site>` context for the site named `site1`, use the command `site1` from the site context, created using the `create <site-name>` command.

After you have completed configuration changes for a `<named-site>`, you must run the `apply` command before exiting the `site:<named-site>` context to implement the changes.

The following commands are available in the `site:<named-site>` context.

- [assign-ap](#) on page 440
- [assign-policy](#) on page 441
- [assign-wlan](#) on page 442
- [band-preference](#) on page 442
- [config](#) on page 443
- [custom](#) on page 443
- [dns](#) on page 444
- [local-radius](#) on page 444
- [move](#) on page 445
- [name](#) on page 445
- [nasid](#) on page 446
- [nasip](#) on page 446
- [password](#) on page 447
- [ping](#) on page 447
- [protocol](#) on page 448
- [radio1-load](#) on page 448
- [radio2-load](#) on page 448
- [radio1-load](#) on page 448
- [radio1-loadcontrol](#) on page 449
- [radio2-loadcontrol](#) on page 449
- [radio1-strictlimit](#) on page 450
- [radio2-strictlimit](#) on page 450
- [remove](#) on page 450
- [replace-station-id](#) on page 451
- [secure-tunnel](#) on page 451
- [secure-tunnel-ap](#) on page 452
- [secure-tunnel-control](#) on page 452
- [secure-tunnel-lifetime](#) on page 452
- [show](#) on page 453

assign-ap

Use the `assign-ap` command to add or remove an AP from the site.

The `assign-ap` command is accessible from the `site:<named-site>` context.

assign-ap (**add|delete**) *ap serial*

Parameters

add delete	Specifies whether to add or delete the identified AP.
<i>ap serial</i>	Specifies the AP to be assigned by its serial number.

Usage

You specify the AP by its serial number. If you enter the command without an AP serial number, the CLI displays a list of available APs by their serial numbers and, if named to the system by an `ap:<serial>` context `name` command, the AP name.

Examples

The following example shows a listing of available APs:

```
EWC.extremenetworks.com:site:site1# assign-ap
The available APs:
0500009353050067 (EWC-3801)
050000829F737045 (050000829F737045)
0409920201204015 (C25-AP3710)
0500009203050048 (C25-AP3705-50048)
0500009203050013 (C25-AP3705)
10490066235A0000 (AP-3801-Ext)
0509920201203250 (EWC-AP-3710-3705-Ext)
0002000819006723 (C25-AP3801)
0002010803508865 (0002010803508865)
10210066235A0000 (C25-AP3705)
```

This example shows AP added to the site1 site:

```
EWC.extremenetworks.com:site:site1# assign-ap add 050000829F737045
```

assign-policy

Use the `assign-policy` command to assign (or remove) a policy to or from the site.

The `assign-policy` command is accessible from the `site:<named-site>` context.

assign-policy (**add|delete**) *policy-name*

Parameters

add delete	Specifies whether to add or delete the policy.
<i>policy-name</i>	Specifies the policy to be assigned to or removed from the site.

Usage

You specify the policy by its name. If you enter the command without a `<policy-name>`, the CLI displays a list of available policies by the names they were given when they were created.

Examples

The following example shows a listing of available policies:

```
EWC.extremenetworks.com:site:site1# assign-policy
The available policies:
WirelessAuthPolicy
WirelessNonAuthPolicy
C25TV1NonAuthPolicy
C25TV1AuthPolicy
mitigatorNonAuthPolicy
mitigatorAuthPolicy
```

The following example assigns a policy to site1:

```
EWC.extremenetworks.com:site:site1# assign-policy add WirelessAuthPolicy
```

assign-wlan

Use the assign-wlan command to configure a WLAN assignment to the site.

The assign-wlan command is accessible from the site:<named-site> context.

```
assign-wlan wlan-name (none|radio1|radio2|both)
```

Parameters

<i>wlan-name</i>	Specifies the named WLAN service to assign to this site.
none radio1 radio2 both	Specifies the radio(s) on the site to which the WLAN service is applied.

Usage

You specify the WLAN by its name. If you enter the command without a <wlan-name>, the CLI displays a list of available WLANs by the names they were given when they were created.

Example

The following example shows a listing of available WLANs:

```
EWC.extremenetworks.com:site:site1# assign-wlan
The available WLANs:
WirelessWLAN
C25TV1WLAN
mitigatorWLAN
```

The following example assigns a WLAN to site1 for Radio1:

```
EWC.extremenetworks.com:site:site1# assign-wlan WirelessWLAN radio1
```

band-preference

Use the band-preference command to enable or disable this site as a band preferencing load group. Refer to the *Wireless User Guide* for a detailed description of radio band preferencing.

The `band-preference` command is accessible from within the `site:<named-site>` context.

band-preference enable | disable

Parameters

enable disable	Enables or disables band preferencing for this site.
-------------------------	--

Example

The following example enables band preferencing on site1:

```
EWC.extremenetworks.com:site:site1# band-preference enable
```

config

Use the `config` command to configure a RADIUS server as the local authentication server for APs assigned to this site. The `config` command is accessible from the `site:<named-site>` context.

config radius name [prot (CHAP|PAP|MS-CHAP|MS-CHAP2)] | exit

Parameters

<i>radius name</i>	Specifies the RADIUS server to be assigned to this site, and enters config mode for the named server.
prot CHAP PAP MS-CHAP MS-CHAP2	Specifies the authentication protocol to be used with this RADIUS server. Values are CHAP, PAP, MS-CHAP, and MS-CHAP2.
exit	Exits config mode.

Usage

Enter `config radius name` to enter config mode for that server. Enter `config exit` to exit config mode.

Example

The following example assigns RADIUS server R-1 to site1, and enters config mode for R-1:

```
EWC.extremenetworks.com:site:site1# config R-1
```

custom

Use the `custom` command to enable or disable VNS customization (overwriting of defaults) by the RADIUS server.

The `custom` command is accessible from the `site:<named-site>` context.

custom (enable | disable)

Parameters

enable disable	Enables or disables VNS customization (overwriting of defaults) by the server.
-------------------------	--

Usage

The CLI <named-site> context must be in config mode for a RADIUS server to execute the `custom` command. Use the `config radius name` command to enter config mode. Use `config exit` to exit config mode.

Example

The following example enables VNS customization by the RADIUS server:

```
EWC.extremenetworks.com:site:site1# custom enable
```

dns

Use the `dns` command to configure an IP address for a Domain Name Server for this site. The `dns` command is accessible from the `site:<named-site>` context.

```
dns A.B.C.D
```

Parameters

<code>A.B.C.D</code>	Specifies the IP address of the Domain Name Server for <named-site>.
----------------------	--

Usage

You must enter the `apply` command for the DNS setting to take affect.

Example

The following example defines an IP address for the DNS:

```
EWC.extremenetworks.com:site:site1# dns 192.168.001.002
EWC.extremenetworks.com:site:site1# apply
```

local-radius

Use the `local-radius` command to enable or disable authentication by the defined local RADIUS server for this site. The `local-radius` command is accessible from the `site:<named-site>` context.

```
local-radius (enable | disable)
```

Parameters

<code>enable disable</code>	Enables or disables local RADIUS authentication.
-------------------------------	--

Usage

You must enter the `apply` command before exiting the `site:<named-site>` context for the RADIUS authentication change to take affect. The CLI prompt does not change until you exit and re-enter the `site:<named-site>` context.

Example

The following example enables local authentication on site1:

```
EWC.extremenetworks.com:site:site1# local-radius enable
```

move

Use the `move` command to change the order of this authentication server on this site. The `move` command is accessible from the `site:<named-site>` context.

move *1-32 1-32*

Parameters

<i>1-32</i>	Specifies a value in an ordered list of servers for this authentication server on this site. Enter the first (current) position of the server, then the new position of the server in the server order.
-------------	---

Usage

The CLI `<named-site>` context must be in config mode for a RADIUS server, to execute the `move` command. Use the `config radius name` command to enter config mode. Use `config exit` to exit config mode.

You must enter the `apply` command before exiting the `site:<named-site>` context for the site name change to take affect. The CLI prompt does not change until you exit and re-enter the `site:<named-site>` context.

Example

The following example moves the authentication server from position 1 to 2 in the order:

```
EWC.extremenetworks.com:site:site1# move 1 2
```

name

Use the `name` command to change the name of a site. The `name` command is accessible from within the `site:<named-site>` context.

name *new-name*

Parameters

<i>new-name</i>	Specifies the new name for this <code><named-site></code> .
-----------------	---

Usage

You must enter the `apply` command before exiting the `site:<named-site>` context for the site name change to take affect. The CLI prompt does not change until you exit and re-enter the `site:<named-site>` context.

Example

The following example:

- Renames the site `site1` to `site9`
- Applies the change
- Displays the `site9` configuration
- Exits `site:<named-site>` context
- Re-enters the `site:<named-site>` context as `site9`

```
EWC.extremenetworks.com:site# site1
EWC.extremenetworks.com:site:site1# name site9
EWC.extremenetworks.com:site:site1# apply
EWC.extremenetworks.com:site:site1# show
Name: site9
...
EWC.extremenetworks.com:site:site1# exit
EWC.extremenetworks.com:site# site9
EWC.extremenetworks.com:site:site9#
EWC.extremenetworks.com:site:site9# show
Name: site9
...
EWC.extremenetworks.com:site:site9#
```

nasid

Use the `nasid` command to configure an NAS identifier for this site. The `nasid` command is accessible from the `site:<named-site>` context.

nasid *string* | **vnsname**

Parameters

<i>string</i>	Specifies an NAS identifier for this <named-site>.
vnsname	Specifies that the VNS name is used as the NAS identifier for this <named-site>.

Usage

The CLI <named-site> context must be in config mode for a RADIUS server to execute the `nasid` command. Use the `config radius name` command to enter config mode. Use `config exit` to exit config mode.

Example

The following example configures a VNS name as a NAS ID for `site1`:

```
EWC.extremenetworks.com:site:site1# nasid vnsname
```

nasip

Use the `nasip` command to configure an NAS IP address for this site. The `nasip` command is accessible from the `site:<named-site>` context. Use `config exit` to exit config mode.

nasip *A.B.C.D* | **vnsip**

Parameters

<i>A.B.C.D</i>	Specifies an IP address for this <named-site>.
vnsip	Specifies that the VNS IP address is used as the IP address for this <named-site>.

Usage

The CLI <named-site> context must be in config mode for a RADIUS server to execute the **nasip** command. Use the **config radius name** command to enter config mode.

Example

The following example configures a VNS IP address as the IP address for site1:

```
EWC.extremenetworks.com:site:site1# nasip vnsip
```

password

Use the **password** command to set the authentication password for this site. The **password** command is accessible from the site:<named-site> context.

password *string*

Parameters

<i>string</i>	Specifies an authentication password for this <named-site>.
---------------	---

Usage

The CLI <named-site> context must be in config mode for a RADIUS server to execute the **password** command. Use the **config radius name** command to enter config mode. Use **config exit** to exit config mode.

Example

The following example sets the authentication password to “user99” for site1:

```
EWC.extremenetworks.com:site:site1# password user99
```

ping

Use the **ping** command to ping the specified IP address for a response. The **ping** command is accessible from the site:<named-site> context.

ping [**source-interface** (**name** *name*) | (**number** *id*)] *ip address*

Parameters

[source-interface (name <i>name</i>) (number <i>id</i>)]	Specifies that the source interface be pinged, by name or by ID number.
<i>ip address</i>	Specifies an IP address for the server. The IP address can be either IPv4 (A.B.C.D) or IPv6 (A:B:C:D:E:F:G:H) format.

Example

The following example pings the RADIUS server configured for site1:

```
EWC.extremenetworks.com:site:site1# ping source-interface name james
192.168.77.7
```

protocol

Use the `protocol` command to set the authentication password for this site. The `protocol` command is accessible from the `site:<named-site>` context.

protocol (**CHAP** | **PAP** | **MS-CHAP** | **MS-CHAP2**)

Parameters

CHAP PAP MS-CHAP MS-CHAP2	Specifies an authentication protocol type. Valid values are CHAP, PAP, MS-CHAP, and MS-CHAP2.
---	---

Usage

The CLI `<named-site>` context must be in config mode for a RADIUS server to execute the `protocol` command. Use the `config radius name` command to enter config mode. Use `config exit` to exit config mode.

Example

The following example sets the authentication protocol to PAP:

```
EWC.extremenetworks.com:site:site1# protocol PAP
```

radio1-load

Use the `radio1-load` command to configure the maximum clients for the load balance group on Radio1. The `radio1-load` command is accessible from the `site:<named-site>` context.

radio1-load *value*

Parameters

<i>value</i>	Specifies the maximum clients for the load balance group. Valid values are 5-60.
--------------	--

Example

The following example sets the maximum clients value for the Radio1 load balance group:

```
EWC.extremenetworks.com:site:site1# radio1-load 55
```

radio2-load

Use the `radio2-load` command to configure the maximum clients for the load balance group on Radio2. The `radio2-load` command is accessible from the `site:<named-site>` context.

radio2-load *value*

Parameters

<i>value</i>	Specifies the maximum clients for the load balance group. Valid values are 5-60.
--------------	--

Example

The following example sets the maximum clients value for the Radio2 load balance group:

```
EWC.extremenetworks.com:site:site1# radio2-load 55
```

radio1-loadcontrol

Use the `radio1-loadcontrol` command to enable or disable load control (soft load limits) on Radio1 only. The `radio1-loadcontrol` command is accessible from the `site:<named-site>` context.

Radio Load Control activates only when the number of clients on the radio reaches the configured limit, and does not disconnect any clients already connected. This is the default and preferred mode of load control. Load control can be enabled on one radio and disabled on the other. Members of a WLAN load control group are assigned to both radios and cannot be load controlled individually.

radio1-loadcontrol (enable | disable)

Parameters

(enable disable)	Enables or disables the load control function on Radio1.
---------------------------	--

Example

The following example enables load control on Radio1:

```
EWC.extremenetworks.com:site:site1# radio1-loadcontrol enable
```

radio2-loadcontrol

Use the `radio2-loadcontrol` command to enable or disable load control (soft load limits) on Radio2 only. The `radio2-loadcontrol` command is accessible from the `site:<named-site>` context.

Radio Load Control activates only when the number of clients on the radio reaches the configured limit, and does not disconnect any clients already connected. This is the default and preferred mode of load control. Load control can be enabled on one radio and disabled on the other. Members of a WLAN load control group are assigned to both radios and cannot be load controlled individually.

radio2-loadcontrol (enable | disable)

Parameters

(enable disable)	Enables or disables the load control function on Radio2.
---------------------------	--

Example

The following example disables load control on Radio2:

```
EWC.extremenetworks.com:site:site1# radio2-loadcontrol disable
```

radio1-strictlimit

Use the `radio1-strictlimit` command to enable or disable strict enforcement of hard load limits on Radio1. When enabled, any clients in excess of the configured limits on the radio are immediately disconnected. The `radio1-strictlimit` command is accessible from the `site:<named-site>` context.

radio1-strictlimit (**enable** | **disable**)

Parameters

(enable disable)	Enables or disables the strict enforcement of load limits on Radio1.
---------------------------	--

Usage

Radio Load Control must be enabled for this radio before this command can take effect.

Example

The following example enables strict load limiting on Radio1:

```
EWC.extremenetworks.com:site:site1# radio1-strictlimit enable
```

radio2-strictlimit

Use the `radio2-strictlimit` command to enable or disable strict enforcement of load limits on Radio2. When enabled, any clients in excess of the configured limits on the radio are immediately disconnected. The `radio2-strictlimit` command is accessible from the `site:<named-site>` context.

radio2-strictlimit (**enable** | **disable**)

Parameters

(enable disable)	Enables or disables the strict enforcement of load limits on Radio2.
---------------------------	--

Usage

Radio Load Control must be enabled for this radio before this command can take effect.

Example

The following example disables strict load limiting on Radio2:

```
EWC.extremenetworks.com:site:site1# radio2-strictlimit disable
```

remove

Use the `remove` command to remove the named RADIUS server from this site. The `remove` command is accessible from the `site:<named-site>` context.

remove *radius name*

Parameters

<i>radius name</i>	Specifies the name of the RADIUS server used on this site.
--------------------	--

Example

The following example removes server R-1 as the RADIUS server from site1:

```
EWC.extremenetworks.com:site:site1# remove R-1
```

replace-station-id

Use the `replace-station-id` command to enable or disable the call station ID replacement with site name function. The `replace-station-id` command is accessible from the `site:<named-site>` context.

replace-station-id (enable | disable)

Parameters

enable disable	Enables or disables the replacement of the call station ID with the site name.
-------------------------	--

Example

The following example enables call station replacement:

```
EWC.extremenetworks.com:site:site1# replace-station-id enable
```

secure-tunnel

Use the `secure-tunnel` command to enable or disable a secure tunnel on this site. The `secure-tunnel` command is accessible from the `site:<named-site>` and `ap:defaults:38xx` contexts.

secure-tunnel (disable | control | data | debug)

Parameters

disable	Disables a secure tunnel on this site.
control	Enables a secure tunnel by encrypting control traffic between the AP and the controller.
data	Enables a secure tunnel by encrypting control and data traffic between the AP and the controller.
debug	Enables tunnel in debug mode, which preserves keys without encryption.

Usage

If enabling a secure tunnel, specify the type of traffic this tunnel will encrypt and carry: control traffic, or control and data traffic. Secure tunneling can also be used for debug mode (keys are preserved without encryption).

Example

The following example enables a secure tunnel that encrypts control and data traffic on site1:

```
EWC.extremenetworks.com:site:site1# secure-tunnel data
```

secure-tunnel-ap

Use the `secure-tunnel-ap` command to enable or disable the encryption of control traffic between APs on this site. The `secure-tunnel-ap` command is accessible from the `site:<named-site>` context.

secure-tunnel-ap (**enable** | **disable**)

Parameters

enable disable	Enables or disables secure tunnels between APs on this site.
--------------------------------	--

Usage

The `secure-tunnel` command must be enabled before the `secure-tunnel-ap` command can be run.

Example

The following example enables secure tunnels between APs on site1:

```
EWC.extremenetworks.com:site:site1# secure-tunnel enable
EWC.extremenetworks.com:site:site1# secure-tunnel-ap enable
```

secure-tunnel-control

Use the `secure-tunnel-control` command to enable or disable the encryption of control traffic between APs on this site and their controllers. The `secure-tunnel-control` command is accessible from the `site:<named-site>` context.

secure-tunnel-control (**enable** | **disable**)

Parameters

enable disable	Enables or disables secure tunnels between APs on this site and controllers.
--------------------------------	--

Usage

The `secure-tunnel` command must be enabled before the `secure-tunnel-control` command can be run.

Example

The following example enables secure tunnels between APs and controllers on site1:

```
EWC.extremenetworks.com:site:site1# secure-tunnel enable
EWC.extremenetworks.com:site:site1# secure-tunnel-control enable
```

secure-tunnel-lifetime

Use the `secure-tunnel-lifetime` command to enable or configure the lifetime (the number of hours the tunnel remains enabled) of this tunnel. The `secure-tunnel-lifetime` command is accessible from the `site:<named-site>` context.

secure-tunnel-lifetime *hours*

Parameters

<i>hours</i>	Specifies the number of hours the tunnel will remain enabled.
--------------	---

Usage

The `secure-tunnel` command must be enabled before the `secure-tunnel-lifetime` command can be run. The default is 10 hours. When this value expires, the tunnel becomes disabled. Use the `secure-tunnel disable` command to terminate a tunnel.

Example

The following example enables a secure tunnel for 20 hours:

```
EWC.extremenetworks.com:site:site1# secure-tunnel-lifetime 20
```

show

Use the `show` command to display the <named-site> configuration information for the current site:<named-site> context. The `show` command is accessible from within the site:<named-site> context.

Syntax

show

Parameters

None.

Example

The following example displays the site1 site configuration from within the site:<named-site> context:

```
EWC.extremenetworks.com:site# site1
EWC.extremenetworks.com:site:site1# show
Name: site1
Local Radius Authentication: enable
Band Preference: disable
Radio1 Load Control: disable
Radio2 Load Control: disable
DNS servers: 0.0.0.0
policy assignment: Unauth,Auth,SiteAuth
WLAN service assignment:
wlan_east both
No radius server has been selected
Priority Name Role NAS IP NAS ID Auth Type
1 NPS_R2 auth Use VNS IP address Use VNS name MS-CHAP2
Secure Tunnel: enable
Control Traffic Encryption(Controller): enable
Control Traffic Encryption(APs): enable
Replace Station ID: enable
EWC.extremenetworks.com:site:site1#
```

26 RF Location Commands

location-engine
default-height
auto-tracking
default-env-mode
floor-plan
on-demand
publish
show
area-tracking

This section describes commands used to enable and configure the Radio Frequency (RF) Location engine on a Wireless Appliance to determine location and perform tracking on wireless mobile users through Wireless APs. These commands are located in the location context of the CLI. Execute the `location` command at the root level to enter location context.

Refer to the section entitled “Using the RF Location Engine” in the *Wireless User Guide* for more information about RF Location configuration.

All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the `location` context:

- [location-engine](#) on page 454
- [default-height](#) on page 455
- [auto-tracking](#) on page 455
- [default-env-mode](#) on page 456
- [floor-plan](#) on page 456
- [on-demand](#) on page 458
- [export](#) on page 457
- [import](#) on page 457
- [copy](#) on page 31
- [delete](#) on page 458
- [publish](#) on page 458
- [show](#) on page 459

location-engine

Use the `location-engine` command to enable or disable the RF Location engine on this controller.

The `location-engine` command is accessible from the location context of the CLI.

location-engine (**enable** | **disable**)

Parameters

enable disable	Enables or disables the location engine on this controller.
--------------------------------	---

Examples

The following example enables the RF location engine:

```
EWC.extremenetworks.com:location# location-engine enable
```

default-height

Use the `default-height` command to set the default height of the APs from the floor, for use if the floor plan does not specify a height for APs. The `default-height` command is accessible from the location context of the CLI.

default-height *centimeters*

Parameters

<i>centimeters</i>	Specifies the default height, in centimeters, of APs from the floor. Valid values are 0 - 1000.
--------------------	---

Usage

If the floor plan specifies a height for AP placement, that value will be used. If there is no floor plan, or the floor plan does not specify AP placement heights, then this command applies. The default value for the *centimeters* parameter is 3.

Examples

The following example sets the default height of APs to 06 centimeters:

```
EWC.extremenetworks.com:location# default-height 06
EWC.extremenetworks.com:location# apply
```

auto-tracking

Use the `auto-tracking` command to enable or disable auto-tracking. When auto-tracking is enabled, the RF Location engine tracks and reports the location of all associated users (users with sessions on the controller), up to the system limit (2,500).

The `auto-tracking` command is accessible from the location context.

auto-tracking (**none**|**clients**|**all**)

Parameters

none	Location engine will auto-track on-demand users only.
clients	Enables auto-tracking by location engine for associated clients and on-demand users.
all	Enables auto-tracking by location engine for associated clients, on-demand users, and non-associated clients.

Example

The following example enables auto-tracking:

```
EWC.extremenetworks.com:location# auto-tracking all
```

default-env-mode

Use the `default-env-mode` command to set the default mode for the environment in which the APs at this location are operating. The `default-env-mode` command is accessible from the location context of the CLI.

```
default-env-mode ( 0 | 1 | 2 | 3 | 4 )
```

Parameters

0 1 2 3 4	<p>Specifies the default environmental mode for this location. Valid values are:</p> <ul style="list-style-type: none"> • 0: Indoor open space (halls, auditoriums) • 1: Office Environment with light divisions (cubicles) • 2: Office Environment with dry walls divisions • 3: Office Environment with hard divisions (brick) • 4: Interior Walls (need be defined in the floor plan)
--------------------------	---

Examples

The following example sets the default environmental mode to indoor open space:

```
EWC.extremenetworks.com:location# default-env-mode 0
```

floor-plan

Use the `floor-plan` command to enter the location:floor-plan context. The `area-tracking` command is accessible from the location context of the CLI.

The following commands are available in the location:floor-plan context:

- [copy](#) on page 31
- [delete](#) on page 458
- [end](#) on page 21
- [exit](#) on page 22
- [export](#) on page 457

- [help](#) on page 22
- [import](#) on page 457
- [logout](#) on page 23
- [show](#) on page 459

export

Use the `export` command to export the floor plan to the user-readable XML format. The `export` command is accessible from the `location:floor-plan` context of the CLI.

export *floor-id*

Parameters

<i>floor-id</i>	Specifies the name of the XML file to be created of the floor plan (<code><floor-id>.xml</code>).
-----------------	---

Usage

This command creates an XML representation of the internal floor plan and stores it in a local file named `<floor-id>.xml`. This file can then be copied to a remote location using the `copy [stream]` command.

Examples

The following example creates an XML version of the floor plan for the Salem second floor:

```
EWC.extremenetworks.com:location:floor-plan# export salem-second-floor
```

import

Use the `import` command to create a floor plan from a locally stored file to an internal representation that can be used by the location engine. The `import` command is accessible from the `location:floor-plan` context of the CLI.

import *filename*

Parameters

<i>filename</i>	Specifies the name of the XML file from which the floor plan will be created.
-----------------	---

Usage

This command creates an internal floor plan from an XML file stored locally. This file can be copied from a remote location using the `copy [stream]` command. This command converts the XML file image to an internal representation named `<filename>` (minus the `.xml` extension).

Examples

The following example creates a floor plan called “Salem-third-floor” from the `Salem-third-floor.xml` file:

```
EWC.extremenetworks.com:location:floor-plan# import Salem-third-floor.xml
```

delete

Use the `delete` command to delete a floor plan from the location engine. The `delete` command is accessible from the `location:floor-plan` context of the CLI.

delete *floor-id*

Parameters

<i>floor-id</i>	Specifies the name of the floor plan to be deleted.
-----------------	---

Usage

Obtain the exact name of the floor plans by using the `show` command in this context.

Examples

The following example deletes floor plan Salem-third-floor:

```
EWC.extremenetworks.com:location:floor-plan# delete floor-id
```

on-demand

Use the `on-demand` command to track clients that may or may not be associated (have current sessions) with the controller's APs. Clients are identified by their MAC or user name. The `on-demand` command is accessible from the `location` context of the CLI.

on-demand (**add** *MAC*) | (**remove** *MAC*)

Parameters

add remove	Add or remove an on-demand client from tracking.
<i>MAC</i>	Specifies a client to be added or removed, by MAC address.

Usage

A maximum of 32 on-demand users may be tracked at once.

Examples

The following example adds client with MAC address 00:1B:21:31:CF:31 for on-demand tracking:

```
EWC.extremenetworks.com:location# on-demand add 00:1B:21:31:CF:31
```

publish

Use the `publish` command to enter the `publish` context. The `publish` command is accessible from the `location` context of the CLI.

Syntax

publish

Parameters

None.

Example

The following example provides for entering the location publish context:

```
EWC.extremenetworks.com:location# publish
```

show

Use the `show` command to display location context settings, the number of currently located users, and the number of RSS readings per second. The `show` command is accessible from the location context of the CLI.

Syntax

show

Parameters

None.

Example

The following example displays information for the location of users:

```
EWC.extremenetworks.com:location# show
```

area-tracking

Use the `area-tracking` command to enable or disable Location Area Tracking. When area-tracking is enabled, the Location Engine tracks client locations within pre-defined map areas. When the clients change map areas, a notification is sent. If area-tracking is disabled, then Area Roaming is used instead. For more information on Area Roaming, see [mac-roam](#) on page 310.

The `area-tracking` command is accessible from the location context.

area-tracking (**enable** | **disable**)

Parameters

enable disable	Enables or disables area-tracking by the location engine on this controller.
--------------------------------	--

Example

The following example enables area-tracking:

```
EWC.extremenetworks.com:location# area-tracking enable
```

27 Publish Commands

push
interval
unit
push-list
push-client-reporting

This section describes commands used in the publish context on a Wireless Appliance. These commands are located in the publish context of the CLI. Execute the `publish` command in the location context to enter the publish context.

Refer to the section “Using the RF Location Engine” in the *Wireless User Guide* for more information about RF Location configuration.

All CLI commands cache changes. For this reason, sometimes when you make a change in a particular context, the change may not be visible immediately. If this happens, you must exit and re-enter the context in order to ensure that the database is synchronized with the latest change.

The following commands are available in the `publish` context:

- `push` on page 461
- `interval` on page 462
- `unit` on page 462
- `push-list` on page 462
- `push-client-reporting` on page 463

push

Use the `push` command to enable or disable the push operation on this controller. This command is available from the `location:publish` context.

push (enable | disable)

Parameters

enable disable	Enables or disables the push operation on this controller.
-------------------------	--

Examples

The following example enables the push operation on this controller:

```
EWC.extremenetworks.com:location:publish# push enable
```

interval

Use the `interval` command to configure the push interval in minutes. This command is available from the `location:publish` context.

interval *minutes*

Parameters

<i>minutes</i>	Specifies the number of minutes for the push interval. Valid values are: 1, 2, 5, 10, 20, 30, 60, 120, or 240 minutes.
----------------	--

Usage

Location push must be enabled using the `push enable` command for the interval command to take affect.

Examples

The following example sets the location push interval to 30 minutes:

```
EWC.extremenetworks.com:location:publish# interval 30
```

unit

Use the `unit` command to set the location push unit to either meters or feet. This command is available from the `location:publish` context.

unit (0 | 1)

Parameters

0 1	Specifies whether the push unit is in meters (0) or feet (1).
-------	---

Examples

The following example sets the push unit to meters:

```
EWC.extremenetworks.com:location:publish# unit 0
```

push-list

Use the `push-list` command to configure a push URL list. This command is available from the `location:publish` context.

```
push-list (add <[userid userid-string password password-string url url]*>|delete  
<[url/sequenceId]*>)
```

Parameters

add delete	Specifies whether the URL is being added or deleted from the push list.
userid <i>userid-string</i>	Specifies a user ID.
password <i>password-string</i>	Specifies a password.
url [<i>url</i>]*	Specifies one or more URLs, delineated by a space, to add to the location push list.
<i>sequenceId</i>	ID of the URL. You can delete the URL by the sequence ID.

Usage

- Keywords **userid**, **password**, and **url** are required parts of the 'push-list add' command.
- The URL must begin with `http://` or `https://`.
- Use a set of quotes to indicate a blank user ID or blank password value.
- You can delete the URL by the sequence ID.

Examples

The following example adds the `www.myurl.com` URL to the push list:

```
EWC.extremenetworks.com:location:publish# push-list add userid UserID1
password qwerty12345 url https://www.myurl.com
```

The following example adds a URL with a blank User ID and password:

```
EWC.extremenetworks.com:location:publish# push-list add userid " password "
url http://www.test.com/test
```

The following example shows the URLs in the push list:

```
EWC.extremenetworks.com:location:publish# show

SequenceId  Userid  Password          url
-----
1           1       *                http://1.1.1.1
2           2       *****          http://1.1.1.2
3           3       *****          http://1.1.1.121
```

The following example deletes the second URL by sequence ID:

```
EWC.extremenetworks.com:location:publish# push-list delete 2.
```



push-client-reporting

Use the `push-client-reporting` command to generate a unique report with data from the `MU_Table`, published through the REST Push Publisher. The `push-client-reporting` command is accessible from within the `location:publish` context.

push-client-reporting (enable | disable)

Parameters

enable disable	Enables or disables the push operation on the controller.
-------------------------	---

Usage

In location-based applications and user traffic analytics, integrating partners often require more detail than simply the location of a MAC address. The client reporting option allows users to generate a report with details from the MU-Table.

Examples

The following example enables the push operation on this controller:

```
EWC.extremenetworks.com:location:publish# push-mu-reporting enable
```