



## **Cisco Embedded Wireless Controller on Catalyst Access Points Command Reference for Cisco IOS XE Bengaluru 17.5.x**

**First Published:** 2021-03-31

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### PREFACE

#### **Preface** xxiii

Document Conventions xxiii

Related Documentation xxv

Obtaining Documentation and Submitting a Service Request xxv

---

### CHAPTER 1

#### **Using the Command-Line Interface** 1

Information About Using the Command-Line Interface 2

Command Modes 2

Understanding Abbreviated Commands 4

No and Default Forms of Commands 4

CLI Error Messages 4

Configuration Logging 5

Using the Help System 5

---

### CHAPTER 2

#### **Configuration Commands: a to f** 7

aaa accounting identity 12

aaa accounting update periodic interval-in-minutes 14

aaa authentication dot1x 15

aaa authentication login 16

aaa authorization 17

aaa authorization credential download default 21

aaa group server ldap 22

aaa group server radius 23

aaa local authentication default authorization 24

aaa new-model 25

aaa server radius dynamic-author 27

aaa session-id	29
aaa-override	31
aaa-policy	32
aaa-realm enable	33
absolute-timer	34
access-list	35
access-list acl-ace-limit	37
accounting-list	38
acl-policy	39
active-query timer	40
address	41
address prefix	43
allow at-least min-number at-most max-number	44
ap	45
ap auth-list	46
ap auth-list ap-cert-policy allow-mic-ap	47
ap auth-list ap-cert-policy allow-mic-ap trustpoint	48
ap auth-list ap-cert-policy mac-address MAC-address   serial-number AP-serial-number policy-type mic	49
ap auth-list ap-policy	50
ap capwap retransmit	51
ap capwap timers	52
ap country	54
ap dot11	55
ap dot11 24ghz   5ghz rrm ndp-mode	56
ap dot11 24ghz cleanair	57
ap dot11 24ghz dot11g	58
ap dot11 24ghz rate	59
ap dot11 rrm channel cleanair-event	61
default ap dot11 24ghz cleanair device	62
ap dot11 24ghz rrm channel cleanair-event	64
ap dot11 24ghz rrm channel device	65
ap dot11 24ghz rrm optimized-roam	66
ap dot11 24ghz rx-sop threshold	67

ap dot11 24ghz shutdown	68
ap dot11 5ghz channelswitch quiet	69
ap dot11 5ghz cleanair	70
default ap dot11 5ghz cleanair device	71
ap dot11 5ghz power-constraint	72
ap dot11 5ghz rate	73
ap dot11 5ghz rrm channel cleanair-event	74
ap dot11 5ghz rrm channel device	75
ap dot11 5ghz rx-sop threshold	76
ap dot11 5ghz shutdown	77
ap dot11 5ghz smart-dfs	78
ap dot11 beaconperiod	79
ap dot11 cac media-stream	80
ap dot11 cac multimedia	83
ap dot11 cac voice	84
ap dot11 cleanair	87
ap dot11 cleanair device	88
ap dot11 dot11n	89
ap dot11 dtpc	92
ap dot11 edca-parameters	94
ap dot11 load-balancing denial	96
ap dot11 load-balancing window	97
ap dot11 rf-profile	98
ap dot11 rrm	99
ap dot11 rrm channel	102
ap dot11 rrm channel dca	103
ap dot11 rrm coverage	105
ap dot11 rrm group-member	107
ap dot11 rrm group-mode	108
ap dot11 rrm logging	109
ap dot11 rrm monitor	111
ap dot11 rrm ndp-type	112
ap dot11 24ghz rrm tpc	113
ap dot11 rrm txpower	114

ap dot11 rrm txpower	115
ap filter	116
ap fra	117
ap image predownload	118
ap name antenna band mode	119
ap name ble	120
ap name clear-personal-ssid	121
ap name controller	122
ap name country	123
ap name crash-file	124
ap name dot11 24ghz slot 0 SI	125
ap name dot11 24ghz slot antenna	126
ap name dot11 24ghz slot beamforming	127
ap name dot11 24ghz slot channel	128
ap name dot11 24ghz slot cleanair	129
ap name dot11 24ghz slot dot11n antenna	130
ap name dot11 24ghz slot dot11ax bss-color	131
ap name dot11 24ghz slot shutdown	132
ap name dot11 dual-band cleanair	133
ap name dot11 dual-band shutdown	134
ap name dot11 rrm profile	135
ap name image	137
ap name indoor	138
ap name ipsla	139
ap name keepalive	140
ap name lan	141
ap name led	142
ap name led-brightness-level	143
ap name location	144
ap name mdsn-ap	145
ap name name new-ap-name	146
ap name no	147
ap name monitor-mode dot11b	148
ap name name	149

ap name network-diagnostics	150
ap name priority	151
ap name reset	152
ap name reset-button	153
ap name role	154
ap name slot	155
ap name static-ip	157
ap name static-ip	158
ap name shutdown	159
ap name usb-module	160
ap name usb-module override	161
ap name vlan-tag	162
ap name write tag-config	163
ap name-regex	164
ap profile	165
ap remote-lan profile-name	166
ap remote-lan shutdown	167
ap remote-lan-policy policy-name	168
ap tag-source-priority	169
ap tag-sources revalidate	170
ap vlan-tag	171
assisted-roaming	172
avg-packet-size packetsize	173
band-select client	174
band-select cycle	175
band-select expire	176
band-select probe-response	177
bss-transition	178
call-snoop	179
captive-bypass-portal	180
capwap-discovery	181
capwap backup	182
cco-password (image-download-mode cco)	183
cco-username (image-download-mode cco)	184

cco-version (image-download-mode cco)	185
cco-auto-check (image-download-mode cco)	186
ccx aironet-iesupport	187
cdp	188
central association	189
central authentication	190
central dhcp	191
central-webauth	192
chassis redundancy keep-alive	193
chassis renumber	194
chassis transport	195
class	196
classify	198
class-map	199
clear chassis redundancy	201
clear mdns-sd cache	202
clear mdns-sd statistics	203
clear platform condition all	204
clear wireless wps rogue ap	205
clear wireless wps rogue client	206
clear wireless wps rogue stats	207
client association limit	208
channel foreign	210
client-l2-vnid	211
convergence	212
coverage	213
crypto key generate rsa	214
crypto pki trustpoint	220
crypto pki trust pool import terminal	221
crypto pki trustpool clean	222
cts inline-tagging	223
cts role-based enforcement	224
cts sgt	225
custom-page login device	226



default	227
description	230
destination	231
destination stealthwatch-cloud	232
device-tracking binding vlan	233
dhcp-tlv-caching	234
dnscrypt	235
domain-name (DHCP)	236
dot11ax twt-broadcast-support	237
dot11 5ghz reporting-interval	238
dot11 reporting-interval	239
dot1x system-auth-control	240
eap profile	242
exclusionlist	243
exporter default-flow-exporter	244
fallback-radio-shut	245
flex	246
flow exporter	247
flow monitor	248
flow record	249
ftp-path	250
ftp-password	251
ftp-server	252
ftp-username	253

---

**CHAPTER 3****Configuration Commands: g to z** 255

idle-timeout	261
image-download-mode	262
inactive-timeout	263
install add file tftp	264
install add profile default	265
install activate	267
install activate auto-abort-timer	268
install activate file	269

install auto-abort-timer stop	270
install commit	271
install remove file backup_image	272
install remove profile default	273
install deactivate	274
install rollback	275
interface vlan	276
ip access-group	277
ip access-list extended	278
ip address	279
ip dhcp pool	281
ip dhcp-relay information option server-override	282
ip dhcp-relay source-interface	284
ip domain-name	285
ip flow monitor	286
ip flow-export destination	287
ip helper-address	288
ip http client secure-ciphersuite	291
ip http secure-ciphersuite	292
ip http secure-server	294
ip http server	296
ip ssh	298
ip ssh version	300
ip tftp blocksize	302
ip verify source	303
ipv4 acl	304
ipv4 dhcp	305
ipv4 flow monitor	306
ipv4 flow monitor output	307
ipv6 flow monitor input	308
ipv6 flow monitor output	309
ipv6 access-list	310
ipv6 acl	312
ipv6-address-type	313

ipv6 address	314
ipv6 dhcp pool	316
ipv6 enable	319
ipv6 mld snooping	321
ipv6 nd managed-config-flag	322
ipv6 nd other-config-flag	323
ipv6 nd ra throttler attach-policy	324
ipv6 nd rguard policy	325
ipv6 snooping policy	327
ipv6 traffic-filter	328
key chain	329
key config-key	330
key config-key password-encrypt	331
license air level	332
license smart (global config)	336
license smart (privileged EXEC)	346
local-admin-mac deny	352
local-auth ap eap-fast	353
local-site	354
location expiry	355
location notify-threshold	356
log-export-mode	357
mab request format attribute	358
mac-filtering	359
match activated-service-template	360
match any	362
match message-type	363
match non-client-nrt	364
match protocol	365
match service-instance	368
match service-type	369
match user-role	370
match username	371
match (access-map configuration)	372

match (class-map configuration)	374
match wlan user-priority	377
max-bandwidth	378
max-through	379
mdns-sd	380
mdns-sd-interface	381
mdns-sd flex-profile	382
mdns-sd profile	383
method fast	384
mgmtuser username	385
mop sysid	386
nac	387
nas-id option2	388
network	389
nmsp cloud-services enable	390
nmsp cloud-services http-proxy	391
nmsp cloud-services server token	392
nmsp cloud-services server url	393
nmsp notification interval	394
nmsp strong-cipher	396
option	397
parameter-map type subscriber attribute-to-service	399
password encryption aes	400
peer-blocking	401
policy	402
police	403
police cir	405
policy-map	406
policy-map	408
port	410
priority priority-value	411
public-ip	412
qos video	413
radius server	414

radius-server attribute wireless accounting call-station-id 415  
radius-server attribute wireless authentication call-station-id 417  
range 419  
record wireless avc basic 420  
redirect 421  
redirect portal 422  
remote-lan 423  
request platform software trace archive 424  
rf tag 425  
rrc-evaluation 426  
security 427  
security dot1x authentication-list 428  
security ft 429  
security pmf 431  
security static-wep-key 433  
security web-auth 434  
security wpa akm 435  
security wpa akm owe 437  
security wpa akm psk 438  
security wpa akm sae 439  
sensor-name 440  
service-key 441  
service-policy (WLAN) 442  
service-policy qos 443  
service-template 444  
service timestamps 445  
session-timeout 447  
set 448  
sftp-image-path (image-download-mode sftp) 455  
sftp-image-server (image-download-mode sftp) 456  
sftp-password (image-download-mode sftp) 457  
sftp-password (trace-export) 458  
sftp-path 459  
sftp-server 460

sftp-username (image-download-mode sftp)	461
sftp-username (trace-export)	462
software auto-upgrade enable	463
statistics ap-system-monitoring alarm-enable	464
statistics ap-system-monitoring alarm-hold-time	465
statistics ap-system-monitoring alarm-retransmit-time	466
statistics ap-system-monitoring cpu-threshold	467
statistics ap-system-monitoring enable	468
statistics ap-system-monitoring mem-threshold	469
statistics ap-system-monitoring sampling-interval	470
statistics ap-system-monitoring stats-interval	471
stealthwatch-cloud-monitor	472
tag rf	473
tag site	474
tftp-image-path (image-download-mode tftp)	475
tftp-image-server (image-download-mode tftp)	476
tftp-path	477
tftp-server	478
trapflags ap ap-stats	479
udp-timeout	480
umbrella-param-map	481
update-timer	482
url	483
urlfilter list	484
usb-enable	485
username	486
violation	488
wgb broadcast-tagging	489
wgb vlan	490
whitelist acl	491
wired-vlan-range	492
config wlan assisted-roaming	493
wireless aaa policy	494
wireless aaa policy	495

wireless autoqos policy-profile	496
wireless broadcast vlan	497
wireless client	498
wireless client mac-address	500
wireless config validate	505
wireless country	507
wireless exclusionlist mac address	508
wireless ipv6 ra wired	509
wireless load-balancing	510
wireless macro-micro steering transition-threshold	511
wireless macro-micro steering probe-suppression	512
wireless management certificate	513
wireless management interface	514
wireless management trustpoint	515
wireless ewc-ap ap ap-type	516
wireless ewc-ap ap capwap	517
wireless ewc-ap ap reload	518
wireless ewc-ap ap shell	519
wireless ewc-ap ap shell username	520
wireless ewc-ap preferred-master	521
wireless ewc-ap factory-reset	522
wireless ewc-ap vrrp vrid	523
wireless profile flex	524
wireless profile image-download default	525
wireless profile policy	526
wireless profile transfer	527
wireless rfid	528
wireless security dot1x	529
wireless security dot1x radius accounting mac-delimiter	531
wireless security dot1x radius accounting username-delimiter	532
wireless security dot1x radius callStationIdCase	533
wireless security dot1x radius mac-authentication call-station-id	534
wireless security dot1x radius mac-authentication mac-delimiter	535
wireless security web-auth retries	536

wireless tag policy	537
wireless tag site	538
wireless wps ap-authentication threshold	539
wireless wps client-exclusion	540
wireless wps mfp ap-impersonation	542
wireless wps rogue network-assurance enable	543
wireless wps rogue ap aaa	544
wireless wps rogue ap aaa polling-interval	545
wireless wps rogue ap init-timer	546
wireless wps rogue ap mac-address rldp initiate	547
wireless wps rogue ap notify-min-rssi	548
wireless wps rogue ap notify-rssi-deviation	549
wireless wps rogue ap rldp alarm-only	550
wireless wps rogue ap rldp alarm-only monitor-ap-only	551
wireless wps rogue ap rldp auto-contain	552
wireless wps rogue ap rldp retries	553
wireless wps rogue ap rldp schedule	554
wireless wps rogue ap rldp schedule day	555
wireless wps rogue ap timeout	556
wireless wps rogue auto-contain	557
wireless wps rogue client aaa	558
wireless wps rogue client mse	559
wireless wps rogue client client-threshold	560
wireless wps rogue client notify-min-rssi	561
wireless wps rogue client notify-rssi-deviation	562
wireless wps rogue rule	563
wireless wps rogue security-level	565
wireless-default radius server	566
wlan policy	567

## CHAPTER 4

**Show Commands** 569

show aaa dead-criteria radius	573
show access-list	575
show ap auth-list	577



show ap auth-list ap-cert-policy	578
show ap auto-rf	579
show ap config	582
show ap crash-file	584
show ap dot11	585
show ap dot11	591
show ap dot11 24ghz	592
show ap dot11 24ghz SI config	593
show ap dot11 24ghz SI device type	594
show ap dot11 5ghz	595
show ap dot11 24ghz cleanair air-quality	597
show ap dot11 24ghz cleanair air-quality	598
show ap dot11 cleanair config	599
show ap dot11 cleanair summary	601
show ap dot11 dual-band summary	602
show ap environment	603
show ap filters active	604
show ap filters all	605
show ap fra	606
show ap gps location	607
show history channel interface dot11Radio all	608
show ap link-encryption	609
show ap lldp neighbors detail	610
show ap lldp neighbors	611
show ap name lldp neighbors detail	612
show ap name lldp neighbors	613
show ap master list	614
show ap multicast mom (multicast over multicast)	615
show ap name auto-rf	616
show ap name ble detail	619
show ap name cablemodem	620
show ap name config	621
show ap name config ethernet	623
show ap name dot11	624

show ap name environment	625
show ap name gps location	626
show ap name mesh neighbor detail	627
show ap name wlan	628
show ap profile	630
show ap rf-profile name	631
show ap rf-profile summary	633
show ap summary	634
show ap tag sources	635
show ap tag summary	636
show ap upgrade	637
show arp	638
show arp summary	639
show avc client	640
show avc wlan	641
show chassis	642
show checkpoint	643
show flexconnect office-extend diagnostics	650
show flow exporter	652
show flow interface	654
show flow monitor	656
show flow record	658
show interfaces	659
show install package	663
show install rollback	664
show install summary	665
show ip	666
show ip nbar protocol-id	667
show ldap attributes	668
show ldap server	669
show license all	670
show license authorization	674
show license data conversion	679
show license eventlog	680

show license history message	681
show license reservation	682
show license status	683
show license summary	692
show license tech	694
show license udi	700
show license usage	701
show platform software sl-infra	704
show platform software tls client summary	705
show platform software client detail	706
show platform software tls statistics	708
show platform software tls session summary	710
show logging profile wireless end timestamp	711
show logging profile wireless filter	712
show logging profile wireless fru	713
show logging profile wireless internal	714
show logging profile wireless level	715
show logging profile wireless module	716
show logging profile wireless reverse	717
show logging profile wireless start	718
show logging profile wireless switch	719
show logging profile wireless to-file	720
show mdns-sd cache	721
show mdns-sd cache detail	722
show mdns-sd cache upn shared	723
show mdns-sd cache upn detail	725
show mdns-sd flexconnect summary	726
show mdns-sd statistics	727
show mdns-sd summary	728
show mdns-sd sp-sdg statistics	729
show nmsp	730
show nmsp cloud-services statistics	731
show nmsp cloud-services summary	732
show nmsp subscription group detail all	733

show nmsp subscription group detail ap-list	734
show nmsp subscription group detail services	735
show nmsp subscription group summary	736
show platform conditions	737
show platform software wlavc status cp-exporter	738
show platform software system all	739
show platform software trace filter-binary	740
show platform software trace level	741
show platform software trace message	744
show platform software trace message license-manager chassis active R0	745
show policy-map	748
show ssh	753
show stealthwatch-cloud connection	754
show stealthwatch-cloud wireless-shim	755
show tech-support wireless	756
show tech-support wireless ap	758
show tech-support wireless client	768
show tech-support wireless radio	772
show tunnel eogre global-configuration	783
show tunnel eogre domain detailed	784
show tunnel eogre domain summary	785
show tunnel eogre gateway summary	786
show tunnel eogre gateway detailed	787
show tunnel eogre manager stats global	788
show tunnel eogre manager stats instance	790
show wireless band-select	792
show wireless client	793
show wireless client mac-address	794
show wireless client mac-address (Call Control)	796
show wireless client mac-address (TCLAS)	797
show wireless client summary	798
show wireless client timers	799
show wireless country	800
show wireless detail	803

show wireless dot11h	804
show wireless dtls connections	805
show wireless exclusionlist	806
show wireless load-balancing	807
show wireless ewc-ap ap summary	808
show wireless ewc-ap ap config-sync	809
show wireless ewc-ap ap image predownload status	810
show wireless ewc-ap country-code	811
show wireless ewc-ap image-master	812
show wireless ewc-ap invalid-image-master	813
show wireless ewc-ap predownload	814
show wireless ewc-ap redundancy summary	815
show wireless ewc-ap redundancy peers	816
show wireless pmk-cache	817
show wireless profile flex	818
show wireless profile policy detailed	819
show wireless rfid	820
show wireless summary	821
show wireless tag rf	822
show wireless urlfilter details	823
show wireless urlfilter summary	824
show wireless vlan details	825
show wireless wgb mac-address	826
show wireless wgb summary	827
show wireless wps rogue ap summary	828
show wireless wps rogue client detailed	829
show wireless wps rogue client summary	830





## Preface

- [Document Conventions](#) , on page xxiii
- [Related Documentation](#), on page xxv
- [Obtaining Documentation and Submitting a Service Request](#), on page xxv

## Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination <b>^D</b> or <b>Ctrl-D</b> means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
<b>bold font</b>	Commands and keywords and user-entered text appear in <b>bold font</b> .
<i>Italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
Courier font	Terminal sessions and information the system displays appear in <code>courier font</code> .
<b>Bold Courier font</b>	<b>Bold Courier font</b> indicates text that the user must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x   y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
{x   y}	Required alternative keywords are grouped in braces and separated by vertical bars.

Convention	Description
[x {y   z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

### Reader Alert Conventions

This document may use the following conventions for reader alerts:



**Note** Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.



**Tip** Means *the following information will help you solve a problem*.



**Caution** Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



**Timesaver** Means *the described action saves time*. You can save time by performing the action described in the paragraph.



**Warning** IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS



## Related Documentation



---

**Note** Before installing or upgrading the device Cisco Embedded Wireless Controller, refer to the release notes.

---



---

**Note** The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

---

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.





# Using the Command-Line Interface

---

- [Information About Using the Command-Line Interface, on page 2](#)

# Information About Using the Command-Line Interface



**Note** Search options on the GUI and CLI are case sensitive.

## Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

You can start a CLI session through a console connection, through Telnet, an SSH, or by using the browser.

When you start a session, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the device reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you can enter any privileged EXEC command or enter global configuration mode.

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the device reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode .

This table describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode.

**Table 1: Command Mode Summary**

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session using Telnet, SSH, or console.	Device>	Enter <b>logout</b> or <b>quit</b> .	Use this mode to <ul style="list-style-type: none"> <li>• Change terminal settings.</li> <li>• Perform basic tests.</li> <li>• Display system information.</li> </ul>

Mode	Access Method	Prompt	Exit Method	About This Mode
Privileged EXEC	While in user EXEC mode, enter the <b>enable</b> command.	Device#	Enter <b>disable</b> to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the <b>configure</b> command.	Device(config)#	To exit to privileged EXEC mode, enter <b>exit</b> or <b>end</b> , or press <b>Ctrl-Z</b> .	Use this mode to configure parameters that apply to the entire device.
VLAN configuration	While in global configuration mode, enter the <b>vlan</b> <i>vlan-id</i> command.	Device(config-vlan)#	To exit to global configuration mode, enter the <b>exit</b> command.  To return to privileged EXEC mode, press <b>Ctrl-Z</b> or enter <b>end</b> .	Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the device startup configuration file.
Interface configuration	While in global configuration mode, enter the <b>interface</b> command (with a specific interface).	Device(config-if)#	To exit to global configuration mode, enter <b>exit</b> .  To return to privileged EXEC mode, press <b>Ctrl-Z</b> or enter <b>end</b> .	Use this mode to configure parameters for the Ethernet ports.
Line configuration	While in global configuration mode, specify a line with the <b>line vty</b> or <b>line console</b> command.	Device(config-line)#	To exit to global configuration mode, enter <b>exit</b> .  To return to privileged EXEC mode, press <b>Ctrl-Z</b> or enter <b>end</b> .	Use this mode to configure parameters for the terminal line.

## Understanding Abbreviated Commands

You need to enter only enough characters for the device to recognize the command as unique.

This example shows how to enter the **show configuration** privileged EXEC command in an abbreviated form:

```
Device# show conf
```

## No and Default Forms of Commands

Almost every configuration command also has a **no** form. In general, use the **no** form to disable a feature or function or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to reenab a disabled feature or to enable a feature that is disabled by default.

Configuration commands can also have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** command enables the command and sets variables to their default values.

## CLI Error Messages

This table lists some error messages that you might encounter while using the CLI to configure your device.

**Table 2: Common CLI Error Messages**

Error Message	Meaning	How to Get Help
% Ambiguous command: "show con"	You did not enter enough characters for your device to recognize the command.	Reenter the command followed by a question mark (?) without any space between the command and the question mark.  The possible keywords that you can enter with the command appear.
% Incomplete command.	You did not enter all of the keywords or values required by this command.	Reenter the command followed by a question mark (?) with a space between the command and the question mark.  The possible keywords that you can enter with the command appear.
% Invalid input detected at '^' marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all of the commands that are available in this command mode.  The possible keywords that you can enter with the command appear.

## Configuration Logging

You can log and view changes to the device configuration. You can use the Configuration Change Logging and Notification feature to track changes on a per-session and per-user basis. The logger tracks each configuration command that is applied, the user who entered the command, the time that the command was entered, and the parser return code for the command. This feature includes a mechanism for asynchronous notification to registered applications whenever the configuration changes. You can choose to have the notifications sent to the syslog.



**Note** Only CLI or HTTP changes are logged.

## Using the Help System

You can enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command.

### SUMMARY STEPS

1. **help**
2. *abbreviated-command-entry ?*
3. *abbreviated-command-entry <Tab>*
4. **?**
5. *command ?*
6. *command keyword ?*

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>help</b> <b>Example:</b> Device# <b>help</b>	Obtains a brief description of the help system in any command mode.
Step 2	<i>abbreviated-command-entry ?</i> <b>Example:</b> Device# <b>di?</b> dir disable disconnect	Obtains a list of commands that begin with a particular character string.
Step 3	<i>abbreviated-command-entry &lt;Tab&gt;</i> <b>Example:</b> Device# <b>sh conf&lt;tab&gt;</b> Device# <b>show configuration</b>	Completes a partial command name.
Step 4	<b>?</b> <b>Example:</b>	Lists all commands available for a particular command mode.

	Command or Action	Purpose
	Device> ?	
<b>Step 5</b>	<p><i>command</i> ?</p> <p><b>Example:</b></p> <p>Device&gt; <b>show</b> ?</p>	Lists the associated keywords for a command.
<b>Step 6</b>	<p><i>command keyword</i> ?</p> <p><b>Example:</b></p> <pre>Device(config)# <b>wireless management</b> ? certificate  Configure certificate details interface    Select an interface to configure transfer     Active transfer profiles trustpoint   Select a trustpoint to configure</pre>	Lists the associated arguments for a keyword.





## Configuration Commands: a to f

---

- [aaa accounting identity](#), on page 12
- [aaa accounting update periodic interval-in-minutes](#) , on page 14
- [aaa authentication dot1x](#), on page 15
- [aaa authentication login](#), on page 16
- [aaa authorization](#), on page 17
- [aaa authorization credential download default](#), on page 21
- [aaa group server ldap](#), on page 22
- [aaa group server radius](#), on page 23
- [aaa local authentication default authorization](#), on page 24
- [aaa new-model](#), on page 25
- [aaa server radius dynamic-author](#), on page 27
- [aaa session-id](#), on page 29
- [aaa-override](#), on page 31
- [aaa-policy](#) , on page 32
- [aaa-realm enable](#) , on page 33
- [absolute-timer](#), on page 34
- [access-list](#), on page 35
- [access-list acl-ace-limit](#), on page 37
- [accounting-list](#), on page 38
- [acl-policy](#), on page 39
- [active-query timer](#), on page 40
- [address](#), on page 41
- [address prefix](#), on page 43
- [allow at-least min-number at-most max-number](#), on page 44
- [ap](#), on page 45
- [ap auth-list](#), on page 46
- [ap auth-list ap-cert-policy allow-mic-ap](#) , on page 47
- [ap auth-list ap-cert-policy allow-mic-ap trustpoint](#), on page 48
- [ap auth-list ap-cert-policy mac-address MAC-address | serial-number AP-serial-number policy-type mic](#), on page 49
- [ap auth-list ap-policy](#), on page 50
- [ap capwap retransmit](#), on page 51
- [ap capwap timers](#), on page 52

- [ap country](#), on page 54
- [ap dot11](#) , on page 55
- [ap dot11 24ghz | 5ghz rrm ndp-mode](#), on page 56
- [ap dot11 24ghz cleanair](#), on page 57
- [ap dot11 24ghz dot11g](#), on page 58
- [ap dot11 24ghz rate](#), on page 59
- [ap dot11 rrm channel cleanair-event](#), on page 61
- [default ap dot11 24ghz cleanair device](#), on page 62
- [ap dot11 24ghz rrm channel cleanair-event](#), on page 64
- [ap dot11 24ghz rrm channel device](#), on page 65
- [ap dot11 24ghz rrm optimized-roam](#), on page 66
- [ap dot11 24ghz rx-sop threshold](#), on page 67
- [ap dot11 24ghz shutdown](#), on page 68
- [ap dot11 5ghz channelswitch quiet](#), on page 69
- [ap dot11 5ghz cleanair](#) , on page 70
- [default ap dot11 5ghz cleanair device](#), on page 71
- [ap dot11 5ghz power-constraint](#), on page 72
- [ap dot11 5ghz rate](#), on page 73
- [ap dot11 5ghz rrm channel cleanair-event](#), on page 74
- [ap dot11 5ghz rrm channel device](#), on page 75
- [ap dot11 5ghz rx-sop threshold](#), on page 76
- [ap dot11 5ghz shutdown](#), on page 77
- [ap dot11 5ghz smart-dfs](#), on page 78
- [ap dot11 beaconperiod](#), on page 79
- [ap dot11 cac media-stream](#), on page 80
- [ap dot11 cac multimedia](#), on page 83
- [ap dot11 cac voice](#), on page 84
- [ap dot11 cleanair](#), on page 87
- [ap dot11 cleanair device](#), on page 88
- [ap dot11 dot11n](#), on page 89
- [ap dot11 dtpc](#), on page 92
- [ap dot11 edca-parameters](#), on page 94
- [ap dot11 load-balancing denial](#), on page 96
- [ap dot11 load-balancing window](#), on page 97
- [ap dot11 rf-profile](#), on page 98
- [ap dot11 rrm](#), on page 99
- [ap dot11 rrm channel](#), on page 102
- [ap dot11 rrm channel dca](#), on page 103
- [ap dot11 rrm coverage](#), on page 105
- [ap dot11 rrm group-member](#), on page 107
- [ap dot11 rrm group-mode](#), on page 108
- [ap dot11 rrm logging](#), on page 109
- [ap dot11 rrm monitor](#), on page 111
- [ap dot11 rrm ndp-type](#), on page 112
- [ap dot11 24ghz rrm tpc](#), on page 113
- [ap dot11 rrm txpower](#), on page 114

- [ap dot11 rrm txpower](#), on page 115
- [ap filter](#) , on page 116
- [ap fra](#), on page 117
- [ap image predownload](#), on page 118
- [ap name antenna band mode](#), on page 119
- [ap name ble](#), on page 120
- [ap name clear-personal-ssid](#), on page 121
- [ap name controller](#), on page 122
- [ap name country](#), on page 123
- [ap name crash-file](#), on page 124
- [ap name dot11 24ghz slot 0 SI](#), on page 125
- [ap name dot11 24ghz slot antenna](#) , on page 126
- [ap name dot11 24ghz slot beamforming](#) , on page 127
- [ap name dot11 24ghz slot channel](#) , on page 128
- [ap name dot11 24ghz slot cleanair](#) , on page 129
- [ap name dot11 24ghz slot dot11n antenna](#), on page 130
- [ap name dot11 24ghz slot dot11ax bss-color](#), on page 131
- [ap name dot11 24ghz slot shutdown](#), on page 132
- [ap name dot11 dual-band cleanair](#), on page 133
- [ap name dot11 dual-band shutdown](#), on page 134
- [ap name dot11 rrm profile](#), on page 135
- [ap name image](#), on page 137
- [ap name indoor](#), on page 138
- [ap name ipsla](#), on page 139
- [ap name keepalive](#), on page 140
- [ap name lan](#), on page 141
- [ap name led](#), on page 142
- [ap name led-brightness-level](#), on page 143
- [ap name location](#), on page 144
- [ap name mdsn-ap](#), on page 145
- [ap name name new-ap-name](#), on page 146
- [ap name no](#), on page 147
- [ap name monitor-mode dot11b](#), on page 148
- [ap name name](#), on page 149
- [ap name network-diagnostics](#), on page 150
- [ap name priority](#), on page 151
- [ap name reset](#), on page 152
- [ap name reset-button](#), on page 153
- [ap name role](#), on page 154
- [ap name slot](#), on page 155
- [ap name static-ip](#), on page 157
- [ap name static-ip](#), on page 158
- [ap name shutdown](#), on page 159
- [ap name usb-module](#), on page 160
- [ap name usb-module override](#), on page 161
- [ap name vlan-tag](#), on page 162

- ap name write tag-config , on page 163
- ap name-regex , on page 164
- ap profile, on page 165
- ap remote-lan profile-name, on page 166
- ap remote-lan shutdown, on page 167
- ap remote-lan-policy policy-name, on page 168
- ap tag-source-priority , on page 169
- ap tag-sources revalidate , on page 170
- ap vlan-tag, on page 171
- assisted-roaming, on page 172
- avg-packet-size packetsize , on page 173
- band-select client, on page 174
- band-select cycle, on page 175
- band-select expire, on page 176
- band-select probe-response, on page 177
- bss-transition, on page 178
- call-snoop, on page 179
- captive-bypass-portal, on page 180
- capwap-discovery, on page 181
- capwap backup, on page 182
- cco-password (image-download-mode cco), on page 183
- cco-username (image-download-mode cco), on page 184
- cco-version (image-download-mode cco), on page 185
- cco-auto-check (image-download-mode cco), on page 186
- ccx aironet-iesupport, on page 187
- cdp, on page 188
- central association, on page 189
- central authentication, on page 190
- central dhcp, on page 191
- central-webauth, on page 192
- chassis redundancy keep-alive, on page 193
- chassis renumber, on page 194
- chassis transport, on page 195
- class, on page 196
- classify, on page 198
- class-map, on page 199
- clear chassis redundancy, on page 201
- clear mdns-sd cache, on page 202
- clear mdns-sd statistics, on page 203
- clear platform condition all, on page 204
- clear wireless wps rogue ap, on page 205
- clear wireless wps rogue client, on page 206
- clear wireless wps rogue stats, on page 207
- client association limit, on page 208
- channel foreign, on page 210
- client-l2-vnid , on page 211

- convergence, on page 212
- coverage, on page 213
- crypto key generate rsa, on page 214
- crypto pki trustpoint, on page 220
- crypto pki trust pool import terminal, on page 221
- crypto pki trustpool clean, on page 222
- cts inline-tagging, on page 223
- cts role-based enforcement, on page 224
- cts sgt, on page 225
- custom-page login device, on page 226
- default, on page 227
- description, on page 230
- destination, on page 231
- destination stealthwatch-cloud, on page 232
- device-tracking binding vlan, on page 233
- dhcp-tlv-caching, on page 234
- dnscrypt, on page 235
- domain-name (DHCP), on page 236
- dot11ax twt-broadcast-support, on page 237
- dot11 5ghz reporting-interval , on page 238
- dot11 reporting-interval, on page 239
- dot1x system-auth-control, on page 240
- eap profile, on page 242
- exclusionlist, on page 243
- exporter default-flow-exporter, on page 244
- fallback-radio-shut, on page 245
- flex , on page 246
- flow exporter, on page 247
- flow monitor, on page 248
- flow record, on page 249
- ftp-path, on page 250
- ftp-password, on page 251
- ftp-server, on page 252
- ftp-username, on page 253

## aaa accounting identity

To enable authentication, authorization, and accounting (AAA) for IEEE 802.1x, MAC authentication bypass (MAB), and web authentication sessions, use the **aaa accounting identity** command in global configuration mode. To disable IEEE 802.1x accounting, use the **no** form of this command.

```
aaa accounting identity {name | default} start-stop {broadcast group {name | radius | tacacs+}
[group {name | radius | tacacs+} ... ] | group {name | radius | tacacs+} [group
{name | radius | tacacs+}... ]}
no aaa accounting identity {name | default}
```

Syntax Description	
<b>name</b>	Name of a server group. This is optional when you enter it after the <b>broadcast group</b> and <b>group</b> keywords.
<b>default</b>	Uses the accounting methods that follow as the default list for accounting services.
<b>start-stop</b>	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested-user process begins regardless of whether or not the start accounting notice was received by the accounting server.
<b>broadcast</b>	Enables accounting records to be sent to multiple AAA servers and send accounting records to the first server in each group. If the first server is unavailable, the uses the list of backup servers to identify the first server.
<b>group</b>	Specifies the server group to be used for accounting services. These are valid server group names: <ul style="list-style-type: none"> <li>• <b>name</b> — Name of a server group.</li> <li>• <b>radius</b> — Lists of all RADIUS hosts.</li> <li>• <b>tacacs+</b> — Lists of all TACACS+ hosts.</li> </ul> <p>The <b>group</b> keyword is optional when you enter it after the <b>broadcast group</b> and <b>group</b> keywords. You can enter more than optional <b>group</b> keyword.</p>
<b>radius</b>	(Optional) Enables RADIUS authorization.
<b>tacacs+</b>	(Optional) Enables TACACS+ accounting.

**Command Default** AAA accounting is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** To enable AAA accounting identity, you need to enable policy mode. To enable policy mode, enter the **authentication display new-style** command in privileged EXEC mode.

This example shows how to configure IEEE 802.1x accounting identity:

```
Device# authentication display new-style
```

Please note that while you can revert to legacy style configuration at any time unless you have explicitly entered new-style configuration, the following caveats should be carefully read and understood.

- (1) If you save the config in this mode, it will be written to NVRAM in NEW-style config, and if you subsequently reload the router without reverting to legacy config and saving that, you will no longer be able to revert.
- (2) In this and legacy mode, Webauth is not IPv6-capable. It will only become IPv6-capable once you have entered new-style config manually, or have reloaded with config saved in 'authentication display new' mode.

```
Device# configure terminal
```

```
Device(config)# aaa accounting identity default start-stop group radius
```

## aaa accounting update periodic interval-in-minutes

To configure accounting update records intervals, use the **aaa accounting update periodic** command.

**aaa accounting update periodic** *interval-in-minutes* [**jitter maximum** *jitter-max-value*]

Syntax Description	periodic	Send accounting update records at regular intervals.
	<1-71582>	Periodic intervals to send accounting update records(in minutes)
	<b>jitter</b>	Set jitter parameters for periodic interval
	<b>maximum</b>	Set maximum jitter value for periodic interval (in seconds)
	<0-2147483>	Maximum jitter value for periodic interval(in seconds). Default is 300 seconds.

**Command Default** None

**Command Modes** Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

### Examples

The following example shows how to configure the interval to five minutes at which the accounting records are updated:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# aaa accounting update periodic 5
```



## aaa authentication dot1x

To specify the authentication, authorization, and accounting (AAA) method to use on ports complying with the IEEE 802.1x authentication, use the **aaa authentication dot1x** command in global configuration mode. To disable authentication, use the **no** form of this command.

```
aaa authentication dot1x {default} method1
no aaa authentication dot1x {default} method1
```

<b>Syntax Description</b>	<b>default</b>	The default method when a user logs in. Use the listed authentication method that follows this argument.
	<i>method1</i>	Specifies the server authentication. Enter the <b>group radius</b> keywords to use the list of all RADIUS servers for authentication.
	<b>Note</b>	Though other keywords are visible in the command-line help strings, only the <b>default</b> and <b>group radius</b> keywords are supported.
<b>Command Default</b>	No authentication is performed.	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** The **method** argument identifies the method that the authentication algorithm tries in the specified sequence to validate the password provided by the client. The only method that is IEEE 802.1x-compliant is the **group radius** method, in which the client data is validated against a RADIUS authentication server.

If you specify **group radius**, you must configure the RADIUS server by entering the **radius-server host** global configuration command.

Use the **show running-config** privileged EXEC command to display the configured lists of authentication methods.

This example shows how to enable AAA and how to create an IEEE 802.1x-compliant authentication list. This authentication first tries to contact a RADIUS server. If this action returns an error, the user is not allowed access to the network.

```
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default group radius
```

## aaa authentication login

To set authentication, authorization, and accounting (AAA) at login, use the **aaa authentication login** command in global configuration mode.

**aaa authentication login** *authentication-list-name* {**group** } *group-name*

Syntax Description	
<i>authentication-list-name</i>	Character string used to name the list of authentication methods activated when a user logs in.
<i>group</i>	Uses a subset of RADIUS servers for authentication as defined by the server group <b>group-name</b> .
<i>group-name</i>	Server group name.

**Command Default** None

**Command Modes** Global Configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.2s	Cisco IOS XE Gibraltar 16.12.1 This command was introduced.

**Usage Guidelines** None

The following example shows how to set an authentication method list named **local\_webauth** to the group type named **local** in local web authentication:

```
Device(config)# aaa authentication login local_webauth local
```

The following example shows how to set an authentication method to RADIUS server group in local web authentication:

```
Device(config)# aaa authentication login webauth_radius group ISE_group
```

## aaa authorization

To set the parameters that restrict user access to a network, use the **aaa authorization** command in global configuration mode. To remove the parameters, use the **no** form of this command.

```
aaa authorization { auth-proxy | cache | commands level | config-commands | configuration
| console | credential-download | exec | multicast | network | onep | policy-if | prepaid
| radius-proxy | reverse-access | subscriber-service | template } { default | list_name }
[method1 [ method2 . . . ]]
```

### Syntax Description

<b>auth-proxy</b>	Runs authorization for authentication proxy services.
<b>cache</b>	Configures the authentication, authorization, and accounting (AAA) server.
<b>commands</b>	Runs authorization for all commands at the specified privilege level.
<i>level</i>	Specific command level that should be authorized. Valid entries are 0 through 15.
<b>config-commands</b>	Runs authorization to determine whether commands entered in configuration mode are authorized.
<b>configuration</b>	Downloads the configuration from the AAA server.
<b>console</b>	Enables the console authorization for the AAA server.
<b>credential-download</b>	Downloads EAP credential from Local/RADIUS/LDAP.
<b>exec</b>	Enables the console authorization for the AAA server.
<b>multicast</b>	Downloads the multicast configuration from the AAA server.
<b>network</b>	Runs authorization for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP Network Control Programs (NCPs), and AppleTalk Remote Access (ARA).
<b>onep</b>	Runs authorization for the ONEP service.
<b>reverse-access</b>	Runs authorization for reverse access connections, such as reverse Telnet.
<b>template</b>	Enables template authorization for the AAA server.
<b>default</b>	Uses the listed authorization methods that follow this keyword as the default list of methods for authorization.
<i>list_name</i>	Character string used to name the list of authorization methods.
<i>method1</i> [ <i>method2</i> ...]	(Optional) An authorization method or multiple authorization methods to be used for authorization. A method may be any one of the keywords listed in the table below.

### Command Default

Authorization is disabled for all actions (equivalent to the method keyword **none**).

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** Use the **aaa authorization** command to enable authorization and to create named methods lists, which define authorization methods that can be used when a user accesses the specified function. Method lists for authorization define the ways in which authorization will be performed and the sequence in which these methods will be performed. A method list is a named list that describes the authorization methods (such as RADIUS or TACACS+) that must be used in sequence. Method lists enable you to designate one or more security protocols to be used for authorization, which ensures a backup system in case the initial method fails. Cisco IOS software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or until all the defined methods are exhausted.



**Note** The Cisco IOS software attempts authorization with the next listed method only when there is no response from the previous method. If authorization fails at any point in this cycle--meaning that the security server or the local username database responds by denying the user services--the authorization process stops and no other authorization methods are attempted.

If the **aaa authorization** command for a particular authorization type is issued without a specified named method list, the default method list is automatically applied to all interfaces or lines (where this authorization type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no authorization takes place. The default authorization method list must be used to perform outbound authorization, such as authorizing the download of IP pools from the RADIUS server.

Use the **aaa authorization** command to create a list by entering the values for the *list-name* and the *method* arguments, where *list-name* is any character string used to name this list (excluding all method names) and *method* identifies the list of authorization methods tried in the given sequence.



**Note** In the table that follows, the **group***group-name*, **group ldap**, **group radius**, and **group tacacs+** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius server** and **tacacs server** commands to configure the host servers. Use the **aaa group server radius**, **aaa group server ldap**, and **aaa group server tacacs+** commands to create a named group of servers.

This table describes the method keywords.

**Table 3: aaa authorization Methods**

Keyword	Description
<b>cache</b> <i>group-name</i>	Uses a cache server group for authorization.

Keyword	Description
<b>group</b> <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the <b>server group</b> <i>group-name</i> command.
<b>group ldap</b>	Uses the list of all Lightweight Directory Access Protocol (LDAP) servers for authentication.
<b>group radius</b>	Uses the list of all RADIUS servers for authentication as defined by the <b>aaa group server radius</b> command.
<b>grouptacacs+</b>	Uses the list of all TACACS+ servers for authentication as defined by the <b>aaa group server tacacs+</b> command.
<b>if-authenticated</b>	Allows the user to access the requested function if the user is authenticated.  <b>Note</b> The <b>if-authenticated</b> method is a terminating method. Therefore, if it is listed as a method, any methods listed after it will never be evaluated.
<b>local</b>	Uses the local database for authorization.
<b>none</b>	Indicates that no authorization is performed.

Cisco IOS software supports the following methods for authorization:

- Cache Server Groups—The router consults its cache server groups to authorize specific rights for users.
- If-Authenticated—The user is allowed to access the requested function provided the user has been authenticated successfully.
- Local—The router or access server consults its local database, as defined by the **username** command, to authorize specific rights for users. Only a limited set of functions can be controlled through the local database.
- None—The network access server does not request authorization information; authorization is not performed over this line or interface.
- RADIUS—The network access server requests authorization information from the RADIUS security server group. RADIUS authorization defines specific rights for users by associating attributes, which are stored in a database on the RADIUS server, with the appropriate user.
- TACACS+—The network access server exchanges authorization information with the TACACS+ security daemon. TACACS+ authorization defines specific rights for users by associating attribute-value (AV) pairs, which are stored in a database on the TACACS+ security server, with the appropriate user.

Method lists are specific to the type of authorization being requested. AAA supports five different types of authorization:

- **Commands**—Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- **EXEC**—Applies to the attributes associated with a user EXEC terminal session.
- **Network**—Applies to network connections. The network connections can include a PPP, SLIP, or ARA connection.




---

**Note** You must configure the **aaa authorization config-commands** command to authorize global configuration commands, including EXEC commands prepended by the **do** command.

---

- **Reverse Access**—Applies to reverse Telnet sessions.
- **Configuration**—Applies to the configuration downloaded from the AAA server.

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type.

Once defined, the method lists must be applied to specific lines or interfaces before any of the defined methods are performed.

The authorization command causes a request packet containing a series of AV pairs to be sent to the RADIUS or TACACS daemon as part of the authorization process. The daemon can do one of the following:

- Accept the request as is.
- Make changes to the request.
- Refuse the request and authorization.

For a list of supported RADIUS attributes, see the module RADIUS Attributes. For a list of supported TACACS+ AV pairs, see the module TACACS+ Attribute-Value Pairs.




---

**Note** Five commands are associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands will not be included in the privilege level command set.

---

The following example shows how to define the network authorization method list named mygroup, which specifies that RADIUS authorization will be used on serial lines using PPP. If the RADIUS server fails to respond, local network authorization will be performed.

```
Device(config)# aaa authorization network mygroup group radius local
```

## aaa authorization credential download default

To set an authorization method list to use local credentials, use the **aaa authorization credential download default** command in global configuration mode.

**aaa authorization credential download default** *group-name*

<b>Syntax Description</b>	<i>group-name</i> Server group name.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Global Configuration				
<b>Command History</b>	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE 16.12.1</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE 16.12.1	This command was introduced.				

The following example shows how to set an authorization method list to use local credentials:

```
Device(config)# aaa authorization credential-download default local
```

## aaa group server ldap

To configure a AAA server group, use the **aaa group server ldap** command.

```
aaa group server ldap group-name
```

<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration (config)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to configure a AAA server group:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# aaa new-model
Device(config)# aaa group server ldap name1
Device(config-ldap-sg)# server server1
Device(config-ldap-sg)# exit
```



## aaa group server radius

To group different RADIUS server hosts into distinct lists and distinct methods, use the **aaa group server radius** command in global configuration mode.

```
aaa group server radius group-name
```

<b>Syntax Description</b>	<i>group-name</i> Character string used to name the group of servers.
---------------------------	-----------------------------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

<b>Usage Guidelines</b>	The authentication, authorization, and accounting (AAA) server-group feature introduces a way to group existing server hosts. The feature enables you to select a subset of the configured server hosts and use them for a particular service.
-------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

A group server is a list of server hosts of a particular type. Currently supported server host types are RADIUS server hosts. A group server is used in conjunction with a global server host list. The group server lists the IP addresses of the selected server hosts.

The following example shows how to configure an AAA group server named **ISE\_Group** that comprises three member servers:

```
Device(config)# aaa group server radius ISE_Group
```

# aaa local authentication default authorization

To configure local authentication method list, use the **aaa local authentication default authorization** command.

**aaa local authentication default authorization** [*method-list-name* | **default**]

<b>Syntax Description</b>	<i>method-list-name</i> Name of the method list.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Global configuration (config)				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.
Release	Modification				
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.				

## Examples

The following example shows how to configure local authentication method list to the default list:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# aaa local authentication default authorization default
```

# aaa new-model

To enable the authentication, authorization, and accounting (AAA) access control model, issue the **aaa new-model** command in global configuration mode. To disable the AAA access control model, use the **no** form of this command.

**aaa new-model**  
**no aaa new-model**

**Syntax Description** This command has no arguments or keywords.

**Command Default** AAA is not enabled.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

**Usage Guidelines** This command enables the AAA access control system.

If the **login local** command is configured for a virtual terminal line (VTY), and the **aaa new-model** command is removed, you must reload the to get the default configuration or the **login** command. If the is not reloaded, the defaults to the **login local** command under the VTY.



**Note** We do not recommend removing the **aaa new-model** command.

The following example shows this restriction:

```
Device(config)# aaa new-model
Device(config)# line vty 0 15
Device(config-line)# login local
Device(config-line)# exit
Device(config)# no aaa new-model
Device(config)# exit
Device# show running-config | b line vty

line vty 0 4
  login local !<=== Login local instead of "login"
line vty 5 15
  login local
!
```

## Examples

The following example initializes AAA:

```
Device(config)# aaa new-model
Device(config)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>aaa accounting</b>	Enables AAA accounting of requested services for billing or security purposes.
<b>aaa authentication arap</b>	Enables an AAA authentication method for ARAP using TACACS+.
<b>aaa authentication enable default</b>	Enables AAA authentication to determine if a user can access the privileged command level.
<b>aaa authentication login</b>	Sets AAA authentication at login.
<b>aaa authentication ppp</b>	Specifies one or more AAA authentication method for use on serial interfaces running PPP.
<b>aaa authorization</b>	Sets parameters that restrict user access to a network.

# aaa server radius dynamic-author

To configure a device as an authentication, authorization, and accounting (AAA) server to facilitate interaction with an external policy server, use the **aaa server radius dynamic-author** command in global configuration mode. To remove this configuration, use the **no** form of this command.

**aaa server radius dynamic-author**  
**no aaa server radius dynamic-author**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The device will not function as a server when interacting with external policy servers.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
12.2(5)SXI	This command was integrated into Cisco IOS Release 12.2(5)SXI.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.
Cisco IOS XE 16.12.1	This command was introduced.

## Usage Guidelines

Dynamic authorization allows an external policy server to dynamically send updates to a device. Once the **aaa server radius dynamic-author** command is configured, dynamic authorization local server configuration mode is entered. Once in this mode, the RADIUS application commands can be configured.

### Dynamic Authorization for the Intelligent Services Gateway (ISG)

ISG works with external devices, referred to as policy servers, that store per-subscriber and per-service information. ISG supports two models of interaction between the ISG device and external policy servers: initial authorization and dynamic authorization.

The dynamic authorization model allows an external policy server to dynamically send policies to the ISG. These operations can be initiated in-band by subscribers (through service selection) or through the actions of an administrator, or applications can change policies on the basis of an algorithm (for example, change session quality of service (QoS) at a certain time of day). This model is facilitated by the Change of Authorization (CoA) RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling ISG and the external policy server each to act as a RADIUS client and server.

## Examples

The following example configures the ISG to act as a AAA server when interacting with the client at IP address 10.12.12.12:

```
aaa server radius dynamic-author
```

```
client 10.12.12.12 key cisco
message-authenticator ignore
```

**Related Commands**

Command	Description
<b>auth-type (ISG)</b>	Specifies the server authorization type.
<b>client</b>	Specifies a RADIUS client from which a device will accept CoA and disconnect requests.
<b>default</b>	Sets a RADIUS application command to its default.
<b>domain</b>	Specifies username domain options.
<b>ignore</b>	Overrides a behavior to ignore certain parameters.
<b>port</b>	Specifies a port on which local RADIUS server listens.
<b>server-key</b>	Specifies the encryption key shared with RADIUS clients.

## aaa session-id

To specify whether the same session ID will be used for each authentication, authorization, and accounting (AAA) accounting service type within a call or whether a different session ID will be assigned to each accounting service type, use the **aaa session-id** command in global configuration mode. To restore the default behavior after the **unique** keyword is enabled, use the **no** form of this command.

```
aaa session-id [{common | unique}]
no aaa session-id [unique]
```

### Syntax Description

<b>common</b>	(Optional) Ensures that all session identification (ID) information that is sent out for a given call will be made identical. The default behavior is <b>common</b> .
<b>unique</b>	(Optional) Ensures that only the corresponding service access-requests and accounting-requests will maintain a common session ID. Accounting-requests for each service will have a different session ID.

### Command Default

The **common** keyword is enabled.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE 16.12.1	This command was integrated in Cisco IOS XE 16.12.1.

### Usage Guidelines

The **common** keyword behavior allows the first session ID request of the call to be stored in a common database; all proceeding session ID requests will retrieve the value of the first session ID. Because a common session ID is the default behavior, this functionality is written to the system configuration after the **aaa new-model** command is configured.



#### Note

The router configuration will always have either the **aaa session-id common** or the **aaa session-id unique** command enabled; it is not possible to have neither of the two enabled. Thus, the **no aaa session-id unique** command will revert to the default functionality, but the **no aaa session-id common** command will not have any effect because it is the default functionality.

The **unique** keyword behavior assigns a different session ID for each accounting type (Auth-Proxy, Exec, Network, Command, System, Connection, and Resource) during a call. To specify this behavior, the unique keyword must be specified. The session ID may be included in RADIUS access requests by configuring the **radius-server attribute 44 include-in-access-req** command. The session ID in the access-request will be the same as the session ID in the accounting request for the same service; all other services will provide unique session IDs for the same call.

### Examples

The following example shows how to configure unique session IDs:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 include-in-access-req
aaa session-id unique
```

### Related Commands

Command	Description
<b>aaa new model</b>	Enables AAA.
<b>radius-server attribute 44 include-in-access-req</b>	Sends RADIUS attribute 44 (Accounting Session ID) in access request packets before user authentication (including requests for preauthentication).



# aaa-override

To enable AAA override on the WLAN, use the **aaa-override** command. To disable AAA override, use the **no** form of this command.

**aaa-override**  
**no aaa-override**

**Syntax Description** This command has no keywords or arguments.

**Command Default** AAA is disabled by default.

**Command Modes** WLAN configuration

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

**Usage Guidelines** You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to enable AAA on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# aaa-override
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

This example shows how to disable AAA on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# no aaa-override
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

# aaa-policy

To map a AAA policy in a WLAN policy profile, use the **aaa-policy** command.

**aaa-policy** *aaa-policy-name*

<b>Syntax Description</b>	<i>aaa-policy-name</i> Name of the AAA policy.
---------------------------	------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	config-wireless-policy
----------------------	------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to map a AAA policy in a WLAN policy profile:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy policy-name
Device(config-wireless-policy)# aaa-policy aaa-policy-name
```

# aaa-realm enable

To enable AAA RADIUS selection by realm, use the **aaa-realm enable** command.

**aaa-realm enable**

---

## Command Default

None

---

## Command Modes

config-aaa-policy

---

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to enable AAA RADIUS section by realm:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless aaa policy aaa-profile-name
Device (config-aaa-policy)# aaa-realm enable
```

## absolute-timer

To enable an absolute timeout for subscriber sessions, use the **absolute-timer** command in service template configuration mode. To disable the timer, use the **no** form of this command.

**absolute-timer** *minutes*  
**no absolute-timer**

### Syntax Description

<i>minutes</i>	Maximum session duration, in minutes. Range: 1 to 65535. Default: 0, which disables the timer.
----------------	------------------------------------------------------------------------------------------------

### Command Default

Disabled (the absolute timeout is 0).

### Command Modes

Service template configuration (config-service-template)

### Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

### Usage Guidelines

Use the **absolute-timer** command to limit the number of minutes that a subscriber session can remain active. After this timer expires, a session must repeat the process of establishing its connection as if it were a new request.

### Examples

The following example shows how to set the absolute timeout to 15 minutes in the service template named SVC\_3:

```
service-template SVC_3
description sample
access-group ACL_2
vlan 113
inactivity-timer 15
absolute-timer 15
```

### Related Commands

Command	Description
<b>event absolute-timeout</b>	Specifies the type of event that triggers actions in a control policy if conditions are met.
<b>inactivity-timer</b>	Enables an inactivity timeout for subscriber sessions.
<b>show service-template</b>	Displays configuration information for service templates.

# access-list

To add an access list entry, use the **access-list** command.

```
access-list {1-99 100-199 1300-1999 2000-2699} [sequence-number] { deny | permit } {
hostname-or-ip-addr [{wildcard-bits | log}] | any [log] | host hostname-or-ip-addr log} | {remark
[line] }
```

Syntax	Description
<i>1-99</i>	Configures IP standard access list.
<i>100-199</i>	Configures IP extended access list.
<i>1300-1999</i>	Configures IP standard access list (expanded range).
<i>2000-2699</i>	Configures IP extended access list (expanded range).
<i>sequence-number</i>	Sequence number of the ACL entry. Valid range is 1 to 2147483647.
<b>deny</b>	Configures packets to be rejected.
<b>permit</b>	Configures packets to be forwarded.
<i>hostname-or-ip-addr</i>	Hostname or the IP address to match.
<i>wildcard-bits</i>	Wildcard bits to match the IP address.
<b>log</b>	Configures log matches against this entry.
<b>any</b>	Any source host.
<b>host</b>	A single host address.
<b>remark</b>	Configures ACL entry comment.
<i>line</i>	The ACL entry comment.

**Command Default** None

**Command Modes** Global Config

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to add an access list entry:

```
Device# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Device(config)# access-list 1 permit any
```

## access-list acl-ace-limit

To set the maximum configurable ace limit for all ACLs, use the **access-list acl-ace-limit** command.

```
access-list acl-ace-limit max-ace-limit
```

<b>Syntax Description</b>	<i>max-ace-limit</i> Maximum number of ace limit for all ACLs. Valid range is 1 to 4294967295.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration (config)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

### Examples

The following example shows how to set the maximum configurable ace limit for all ACLs to 100:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# access-list acl-ace-limit 100
```

## accounting-list

To configure RADIUS accounting servers on , use the **accounting-list** command. To disable RADIUS server accounting, use the **no** form of this command.

**accounting-list** *radius-server-acct*

**no accounting-list**

<b>Syntax Description</b>	<i>radius-server-acct</i> Accounting RADIUS server name.
---------------------------	----------------------------------------------------------

<b>Command Default</b>	RADIUS server accounting is disabled by default.
------------------------	--------------------------------------------------

<b>Command Modes</b>	
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

<b>Usage Guidelines</b>	You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.
-------------------------	----------------------------------------------------------------------------------------------------------------------------------

This example shows how to configure RADIUS server accounting on :

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#
Deviceaccounting-list test
Device
```

This example shows how to disable RADIUS server accounting on :

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#
Deviceno accounting-list test
Device
```



# acl-policy

To configure an access control list (ACL) policy, use the **acl-policy** command.

**acl-policy** *acl-policy-name*

---

## Syntax Description

*acl-policy-name* Name of the ACL policy.

---



---

## Command Default

None

---

## Command Modes

config-wireless-flex-profile

---

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

## Examples

The following example shows how to configure an ACL policy name:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile flex default-flex-profile
Device(config-wireless-flex-profile)# acl-policy my-acl-policy
```

## active-query timer

To configure mDNS global active query, use the **active-query timer** command. To disable the command use the **no** form of this command.

**active-query timer** *15 - 120*

**no active-query timer** *15 - 120*

<b>Syntax Description</b>	<b>active-query timer</b>	Configures the mDNS global active query timer.
	<i>15 - 120</i>	Specifies the active query periodicity in minutes. The default is 30 minutes.

**Command Default** None

**Command Modes** Global configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

**Usage Guidelines** None

### Example

The following example shows how to configure mDNS global active query:

```
Device(config-mdns-sd)# active-query timer 60
```

# address

To specify the IP address of the Rivest, Shamir, and Adelman (RSA) public key of the remote peer that you will manually configure in the keyring, use the **address** command in `rsa-pubkey` configuration mode. To remove the IP address, use the **no** form of this command.

**address** *ip-address*  
**no address** *ip-address*

<b>Syntax Description</b>	<i>ip-address</i> IP address of the remote peer.
---------------------------	--------------------------------------------------

**Command Default** No default behavior or values

**Command Modes** Rsa-pubkey configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.3 T	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
	Cisco IOS XE 16.12.1	This command was integrated into Cisco ISO XE 16.12.1

**Usage Guidelines** Before you can use this command, you must enter the **rsa-pubkey** command in the crypto keyring mode.

**Examples** The following example specifies the RSA public key of an IP Security (IPSec) peer:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```

address

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>crypto keyring</b>	Defines a crypto keyring to be used during IKE authentication.
<b>key-string</b>	Specifies the RSA public key of a remote peer.
<b>rsa-pubkey</b>	Defines the RSA manual key to be used for encryption or signatures during IKE authentication.

# address prefix

To specify an address prefix for address assignment, use the **address prefix** command in interface configuration mode. To remove the address prefix, use the **no** form of this command.

**address prefix ipv6-prefix** [lifetime {valid-lifetime preferred-lifetime | infinite}]  
**no address prefix**

Syntax Description		
<i>ipv6-prefix</i>		IPv6 address prefix.
lifetime {valid-lifetime preferred-lifetime   infinite}]		(Optional) Specifies a time interval (in seconds) that an IPv6 address prefix remains in the valid state. If the <b>infinite</b> keyword is specified, the time interval does not expire.

**Command Default** No IPv6 address prefix is assigned.

**Command Modes** DHCP pool configuration (config-dhcpv6)

Command History	Release	Modification
	12.4(24)T	This command was introduced.

**Usage Guidelines** You can use the **address prefix** command to configure one or several address prefixes in an IPv6 DHCP pool configuration. Each time the IPv6 DHCP address pool is used, an address will be allocated from each of the address prefixes associated with the IPv6 DHCP pool.

**Examples** The following example shows how to configure a pool called engineering with an IPv6 address prefix:

```
Router(config)# ipv6 dhcp pool engineering
Router(config-dhcpv6)# address prefix 2001:1000::0/64 lifetime infinite
```

Related Commands	Command	Description
	<b>ipv6 dhcp pool</b>	Configures a DHCPv6 server configuration information pool and enters DHCPv6 pool configuration mode.

## allow at-least min-number at-most max-number

To limit the number of multicast RAs per device per throttle period in an RA throttler policy, use the **allow at-least min-number at-most max-number** command.

**allow at-least min-number at-most {max-number | no-limit}**

<b>Syntax Description</b>	<b>at-least min-number</b> Enter the minimum guaranteed number of multicast RAs per router before throttling can be enforced. Valid range is 0 to 32.				
	<b>at-most max-number</b> Enter the maximum number of multicast RAs from router by which throttling is enforced. Valid range is 0 to 256.				
	<b>at-most no-limit</b> No upper bound at the router level.				
<b>Command Default</b>	None				
<b>Command Modes</b>	config-nd-ra-throttle				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.
Release	Modification				
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.				

### Examples

The following example shows how to limit the number of multicast RAs per device per throttle period in an RA throttler policy:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ipv6 nd ra-throttler policy ra-throttler-policy-name
Device(config-nd-ra-throttle)# allow at-least 5 at-most 10
```

# ap

To configure cisco APs, use the **ap** command.

**ap** *mac-address*

<b>Syntax Description</b>	<i>mac-address</i> Ethernet MAC address of the AP.
---------------------------	----------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	config
----------------------	--------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.6.1	This command was introduced.

<b>Usage Guidelines</b>	none.
-------------------------	-------

## Example

The following example shows how to configure a Cisco AP:

```
Device(config)# ap F866.F267.7DFB
```

## ap auth-list

To configure the AP authorization list, use the **ap auth-list** command in the global configuration mode. To disable the AP authorization list, use the **no** form of this command.

**ap auth-list** { **authorize-mac** | **authorize-serialNum** | **method-list** *method-list-name* }

**no ap auth-list** { **authorize-mac** | **authorize-serialNum** | **method-list** *method-list-name* }

### Syntax Description

<b>authorize-mac</b>	Configures the AP authorization policy with MAC.
<b>authorize-serialNum</b>	Configures the AP authorization policy with the serial number.
<b>method-list</b>	Configures the AP authorization method list.
<i>method-list-name</i>	Indicates the method list name.

### Command Default

None

### Command Modes

Global configuration (config)

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

### Example

The following example shows how to configure the AP authorization policy with serial number:

```
Device(config) #ap auth-list authorize-serialNum
```



## ap auth-list ap-cert-policy allow-mic-ap

To enable the AP certificate policy during CAPWAP-DTLS handshake, use the **ap auth-list ap-cert-policy allow-mic-ap** command, in the global configuration mode. To disable the AP certificate policy during CAPWAP-DTLS handshake, use the **no** form of this command.

**ap auth-list ap-cert-policy allow-mic-ap**

**no ap auth-list ap-cert-policy allow-mic-ap**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--------------------------------------------

<b>Command Modes</b>	Global configuration (config)
----------------------	-------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

### Example

The following example shows how to configure AP certificate policy during CAPWAP-DTLS handshake:

```
Device# configure terminal
Device(config)# ap auth-list ap-cert-policy
Device(config)# ap auth-list ap-cert-policy allow-mic-ap
```

## ap auth-list ap-cert-policy allow-mic-ap trustpoint

To configure the trustpoint name for the controller certificate chain, use the **ap auth-list ap-cert-policy allow-mic-ap trustpoint** command, in the global configuration mode. To disable the feature, use the **no** form of the command.

**ap auth-list ap-cert-policy allow-mic-ap trustpoint**

**no ap auth-list ap-cert-policy allow-mic-ap trustpoint**

<b>Syntax Description</b>	<i>trustpoint-name</i> Specifies the trustpoint name for the wireless controller certificate chain.
<b>Command Default</b>	None
<b>Command Modes</b>	Global configuration (config)
<b>Command History</b>	<b>Release</b>
	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.5.1 This command was introduced.

### Example

The following example shows how to the trustpoint name for the controller certificate chain:

```
Device# configure terminal
Device(config)# ap auth-list ap-cert-policy
Device(config)# ap auth-list ap-cert-policy allow-mic-ap trustpoint trustpoint-name
```

# ap auth-list ap-cert-policy mac-address MAC-address | serial-number AP-serial-number policy-type mic

To configure the AP certificate policy based on the Ethernet MAC address or based on the assembly serial number of the AP, use the **ap auth-list ap-cert-policy {mac-address *H.H.H* | serial-number *AP-serial-number*} policy-type mic** command. Use the **no** form of this command to disable the feature.

**ap auth-list ap-cert-policy { mac-address *H.H.H* | serial-number *AP-serial-number* } policy-type mic**

**no ap auth-list ap-cert-policy { mac-address *H.H.H* | serial-number *AP-serial-number* } policy-type mic**

Syntax Description		
<b>ap auth-list</b>		Configure the authorization list of the Access Point.
<b>ap-cert-policy</b>		Specifies the AP Certificate Policy during CAPWAP DTLS.
<b>mac-address</b> <i>MAC-address</i>		Configures AP cert policy based on Ethernet MAC.
<b>serial-number</b> <i>AP-serial-number</i>		Configure AP cert policy based on Serial Number.
<b>policy-type</b>		Configures AP certificate policy type.
<b>mic</b>		Selects MIC AP policy.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

## Example

The following example shows how to configure the AP certificate policy based on the Ethernet MAC address or based on the assembly serial number of the AP:

```
Device# configure terminal
Device(config)# ap auth-list ap-cert-policy mac-address 10.1.1 policy-type mic

Device(config)# ap auth-list ap-cert-policy serial-number ap-serial-number policy-type mic
```

## ap auth-list ap-policy

To configure authorization policy for all Cisco lightweight access points joined to the device, use the **ap auth-list ap-policy** command. To disable authorization policy for all Cisco lightweight access points joined to the device, use the **no** form of this command.

```
ap auth-list ap-policy {authorize-ap | lsc | mic | ssc}
no ap auth-list ap-policy {authorize-ap | lsc | mic | ssc}
```

<b>Syntax Description</b>	<b>authorize-ap</b> Enables the authorization policy.				
	<b>lsc</b> Enables access points with locally significant certificates to connect.				
	<b>mic</b> Enables access points with manufacture-installed certificates to connect.				
	<b>ssc</b> Enables access points with self signed certificates to connect.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Global configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE 16.12.1	This command was introduced.				

This example shows how to enable the access point authorization policy:

```
Device(config)# ap auth-list ap-policy authorize-ap
```

This example shows how to enable access points with locally significant certificates to connect:

```
Device(config)# ap auth-list ap-policy lsc
```

This example shows how to enable access points with manufacture-installed certificates to connect:

```
Device(config)# ap auth-list ap-policy mic
```

This example shows how to enable access points with self-signed certificates to connect:

```
Device(config)# ap auth-list ap-policy ssc
```

## ap capwap retransmit

To configure Control and Provisioning of Wireless Access Points (CAPWAP) control packet retransmit count and control packet retransmit interval under the AP profile, use the **ap capwap retransmit** command.

**ap profile default-ap-profile**

**ap capwap retransmit** {**count** *retransmit-count* | **interval** *retransmit-interval*}

<b>Syntax Description</b>	<b>count</b> <i>retransmit-count</i>	Specifies the access point CAPWAP control packet retransmit count. <b>Note</b> The count is from 3 to 8 seconds.
	<b>interval</b> <i>retransmit-interval</i>	Specifies the access point CAPWAP control packet retransmit interval. <b>Note</b> The interval is from 2 to 5 seconds.
<b>Command Default</b>	None	
<b>Command Modes</b>	AP profile configuration (config-ap-profile)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to configure the CAPWAP control packet retransmit count for an access point:

```
Device(config)# ap profile default-ap-profile
```

This example shows how to configure the CAPWAP control packet retransmit interval for an access point:

```
Device(config-ap-profile)# capwap retransmit count 3
```

## ap capwap timers

To configure advanced timer settings under the AP profile mode, use the **ap capwap timers** command.

**ap profile default-ap-profile**

```
ap capwap timers {discovery-timeout seconds | fast-heartbeat-timeout local seconds |
heartbeat-timeout seconds | primary-discovery-timeout seconds | primed-join-timeout seconds}
```

Syntax	Description
<b>discovery-timeout</b>	Specifies the Cisco lightweight access point discovery timeout.  <b>Note</b> The Cisco lightweight access point discovery timeout is how long a Cisco device waits for an unresponsive access point to answer before considering that the access point failed to respond.
<i>seconds</i>	Cisco lightweight access point discovery timeout from 1 to 10 seconds.  <b>Note</b> The default is 10 seconds.
<b>fast-heartbeat-timeout local</b>	Enables the fast heartbeat timer that reduces the amount of time it takes to detect a device failure for local or all access points.
<i>seconds</i>	Small heartbeat interval (from 1 to 10 seconds) that reduces the amount of time it takes to detect a device failure.  <b>Note</b> The fast heartbeat time-out interval is disabled by default.
<b>heartbeat-timeout</b>	Specifies the Cisco lightweight access point heartbeat timeout.  <b>Note</b> The Cisco lightweight access point heartbeat timeout controls how often the Cisco lightweight access point sends a heartbeat keep-alive signal to the Cisco device.  This value should be at least three times larger than the fast heartbeat timer.
<i>seconds</i>	Cisco lightweight access point heartbeat timeout value from 1 to 30 seconds.  <b>Note</b> The default is 30 seconds.
<b>primary-discovery-timeout</b>	Specifies the access point primary discovery request timer. The timer determines the amount of time taken by an access point to discovery the configured primary, secondary, or tertiary device.
<i>seconds</i>	Access point primary discovery request timer from 30 to 3600 seconds.  <b>Note</b> The default is 120 seconds.

<b>primed-join-timeout</b>	Specifies the authentication timeout. Determines the time taken by an access point to determine that the primary device has become unresponsive. The access point makes no further attempts to join the device until the connection to the device is restored.
<i>seconds</i>	Authentication response timeout from 120 to 43200 seconds. <b>Note</b> The default is 120 seconds.

**Command Default**

None

**Command Modes**

AP profile mode (config-ap-profile)

**Command History**

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to configure an access point discovery timeout with the timeout value of 7:

```
Device(config)# ap profile default-ap-profile
```

```
Device(config-ap-profile)# ap capwap timers discovery-timeout 7
```

This example shows how to enable the fast heartbeat interval for all access points:

```
Device(config)# ap profile default-ap-profile
```

```
Device(config-ap-profile)# ap capwap timers fast-heartbeat-timeout 6
```

This example shows how to configure an access point heartbeat timeout to 20:

```
Device(config)# ap profile default-ap-profile
```

```
Device(config-ap-profile)# ap capwap timers heartbeat-timeout 20
```

This example shows how to configure the access point primary discovery request timer to 1200 seconds:

```
Device(config)# ap profile default-ap-profile
```

```
Device(config-ap-profile)# ap capwap timers primary-discovery-timeout 1200
```

This example shows how to configure the authentication timeout to 360 seconds:

```
Device(config)# ap profile default-ap-profile
```

```
Device(config-ap-profile)# ap capwap timers primed-join-timeout 360
```

## ap country

To configure one or more country codes for a device, use the **ap country** command.

**ap country** *country-code*

### Syntax Description

*country-code* Two-letter or three-letter country code or several country codes separated by a comma.

### Command Default

US (country code of the United States of America).

### Command Modes

Global configuration

### Command History

#### Release

Cisco IOS XE 16.12.1

Cisco IOS XE Amsterdam 17.3.1

#### Modification

This command was introduced.

This command has been deprecated.

#### Note

From Cisco IOS XE Amsterdam 17.3.1 onwards, the command **ap country** is deprecated and renamed as **wireless country** *<1 country code>*, where you can enter country codes for more than 20 countries. Although the existing command **ap country** is still functional, it is recommended that you use the **wireless country** *<1 country code>* command.

### Usage Guidelines

The Cisco device must be installed by a network administrator or qualified IT professional and the installer must select the proper country code. Following installation, access to the unit should be password protected by the installer to maintain compliance with regulatory requirements and to ensure proper unit functionality. See the related product guide for the most recent country codes and regulatory domains.

This example shows how to configure country codes on the device to IN (India) and FR (France):

```
Device(config)# ap country IN,FR
```



# ap dot11

To configure Spectrum Intelligence (SI) on Qualcomm based 2.4 GHz or 5 GHz radios, use the **ap dot11 SI** command.

**ap dot11 {24ghz | 5ghz } SI**

<b>Syntax Description</b>	<b>24ghz</b> 2.4 GHz radio	
	<b>5ghz</b> 5 GHz radio	
	<b>SI</b> Enable Spectrum Intelligence (SI). [no] in the command disables SI.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration (config)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to enable SI on 5GHz radio:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap dot11 5ghz SI
```

## ap dot11 24ghz | 5ghz rrm ndp-mode

To configure the operating mode for 802.11a neighbor discovery, use the **ap dot11 {24ghz | 5ghz} rrm ndp-mode** command.

```
ap dot11 { 24ghz | 5ghz } rrm ndp-mode { auto | off-channel }
```

Syntax Description	
<b>auto</b>	Enables the auto mode.
<b>off-channel</b>	Enables NDP packets on RF ASIC radio.

Command Modes	
	Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

### Example

The following example shows how to configure the operating mode for 802.11a neighbor discovery:

```
Device# configure terminal
Device(config)# ap dot11 24ghz or 5ghz rrm ndp-mode auto
```

## ap dot11 24ghz cleanair

To enable CleanAir for detecting 2.4-GHz devices, use the **ap dot11 24ghz cleanair** command in global configuration mode. To disable CleanAir for detecting 2.4-GHz devices, use the **no** form of this command.

**ap dot11 24ghz cleanair**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** Disabled.

---

**Command Modes** Global configuration (config).

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

---

---

**Usage Guidelines** You must enable this CleanAir command before you configure other CleanAir commands.

This example shows how to enable CleanAir for 2.4-GHz devices:

```
Device(config)# ap dot11 24ghz cleanair
```

## ap dot11 24ghz dot11g

To enable the Cisco wireless LAN solution 802.11g network, use the **ap dot11 24ghz dot11g** command. To disable the Cisco wireless LAN solution 802.11g network, use the **no** form of this command.

```
ap dot11 24ghz dot11g
no ap dot11 24ghz dot11g
```

<b>Syntax Description</b>	This command has no keywords and arguments.
---------------------------	---------------------------------------------

<b>Command Default</b>	Enabled
------------------------	---------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

**Usage Guidelines**

Before you enter the **ap dot11 24ghz dot11g** command, disable the 802.11 Cisco radio with the **ap dot11 24ghz shutdown** command.

After you configure the support for the 802.11g network, use the **no ap dot11 24ghz shutdown** command to enable the 802.11 2.4 Ghz radio.

This example shows how to enable the 802.11g network:

```
Device(config)# ap dot11 24ghz dot11g
```

## ap dot11 24ghz rate

To configure 802.11b operational rates, use the **ap dot11 24ghz rate** command.

```
ap dot11 24ghz rate {RATE_11M | RATE_12M | RATE_18M | RATE_1M | RATE_24M |
RATE_2M | RATE_36M | RATE_48M | RATE_54M | RATE_5_5M | RATE_6M | RATE_9M}
{disable | mandatory | supported}
```

### Syntax Description

<b>RATE_11M</b>	Configures the data to be transmitted at the rate of 11 Mbps
<b>RATE_12M</b>	Configures the data to be transmitted at the rate of 12 Mbps
<b>RATE_18M</b>	Configures the data to be transmitted at the rate of 18 Mbps
<b>RATE_1M</b>	Configures the data to be transmitted at the rate of 1 Mbps
<b>RATE_24M</b>	Configures the data to be transmitted at the rate of 24 Mbps
<b>RATE_2M</b>	Configures the data to be transmitted at the rate of 2 Mbps
<b>RATE_36M</b>	Configures the data to be transmitted at the rate of 36 Mbps
<b>RATE_48M</b>	Configures the data to be transmitted at the rate of 48 Mbps
<b>RATE_54M</b>	Configures the data to be transmitted at the rate of 54 Mbps
<b>RATE_5_5M</b>	Configures the data to be transmitted at the rate of 5.5 Mbps
<b>RATE_6M</b>	Configures the data to be transmitted at the rate of 6 Mbps
<b>RATE_9M</b>	Configures the data to be transmitted at the rate of 9 Mbps
<b>disable</b>	Disables the data rate that you specify. Also defines that the clients specify the data rates used for communication.
<b>mandatory</b>	Defines that the clients support this data rate in order to associate with an AP.
<b>supported</b>	Any associated clients support this data rate can communicate with the AP using this rate. However, the clients are not required to use this rate to associate with the AP.

### Command Default

None

### Command Modes

Global configuration (config)

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to configure 802.11b operational rate to 9 Mbps and make it mandatory:

```
Device# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Device(config)# ap dot11 24ghz rate RATE_9M mandatory
```

## ap dot11 rrm channel cleanair-event

To configure CleanAir event-driven Radio Resource Management (RRM) parameters for all 802.11 Cisco lightweight access points, use the **ap dot11 rrm channel cleanair-event** command. When this parameter is configured, CleanAir access points can change their channel when a source of interference degrades the operations, even if the RRM interval has not expired yet.

```
ap dot11 {24ghz | 5ghz} rrm channel {cleanair-event sensitivity value}
```

<b>Syntax Description</b>	<b>24ghz</b>	Specifies the 2.4 GHz band.
	<b>5ghz</b>	Specifies the 5 GHz band.
	<b>sensitivity</b>	Sets the sensitivity for CleanAir event-driven RRM.
	<i>value</i>	Sensitivity value. You can specify any one of the following three optional sensitivity values: <ul style="list-style-type: none"> <li>• <b>low</b>—Specifies low sensitivity.</li> <li>• <b>medium</b>—Specifies medium sensitivity.</li> <li>• <b>high</b>—Specifies high sensitivity.</li> </ul>
<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

This example shows how to set the high sensitivity for CleanAir event-driven RRM:

```
Device(config)# ap dot11 24ghz rrm channel cleanair-event sensitivity high
```

## default ap dot11 24ghz cleanair device

To configure the default state of report generation for 2.4-GHz interference devices, use the **default ap dot11 24ghz cleanair device** command in global configuration mode.

Syntax	Description
<b>canopy</b>	Configures the alarm for canopy interference devices.
<b>cont-tx</b>	Configures the alarm for continuous transmitters.
<b>dect-like</b>	Configures the alarm for Digital Enhanced Cordless Communication (DECT)-like phones.
<b>inv</b>	Configures the alarm for devices using spectrally inverted Wi-Fi signals.
<b>jammer</b>	Configures the alarm for jammer interference devices.
<b>nonstd</b>	Configures the alarm for devices using nonstandard Wi-Fi channels.
<b>superag</b>	Configures the alarm for 802.11 SuperAG interference devices.
<b>tdd-tx</b>	Configures the alarm for Time Division Duplex (TDD) transmitters.
<b>video</b>	Configures the alarm for video cameras.
<b>wimax-fixed</b>	Configures the alarm for WiMax fixed interference devices.
<b>wimax-mobile</b>	Configures the alarm for WiMax mobile interference devices.
<b>report</b>	Displays the device alarm report.
<b>si_fhss</b>	Specifies the QCA SI FHSS.

**Command Default** The alarm for Wi-Fi inverted devices is enabled. The alarm for all other devices is disabled.

**Command Modes** Global configuration (config).



Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines**

You must enable CleanAir using the **ap dot11 24ghz cleanair** command before you configure this command.

This example shows how to enable CleanAir to report when a video camera interferes:

```
Device(config)# default ap dot11 24ghz cleanair device video
```

## ap dot11 24ghz rrm channel cleanair-event

To enable Event-Driven RRM (EDRRM) and the sensitivity for 2.4-GHz devices, use the **ap dot11 24ghz rrm channel cleanair-event** command in global configuration mode. To disable EDRRM, use the **no** form of this command.

```
ap dot11 24ghz rrm channel cleanair-event sensitivity {high | low | medium}
no ap dot11 24ghz rrm channel cleanair-event [sensitivity{high | low | medium}]
```

Syntax Description		
	<b>sensitivity</b>	(Optional) Configures the EDRRM sensitivity of the CleanAir event.
	<b>high</b>	(Optional) Specifies the highest sensitivity to non-Wi-Fi interference as indicated by the air quality (AQ) value.
	<b>low</b>	(Optional) Specifies the least sensitivity to non-Wi-Fi interference as indicated by the AQ value.
	<b>medium</b>	(Optional) Specifies medium sensitivity to non-Wi-Fi interference as indicated by the AQ value.

**Command Default** EDRRM is disabled and the sensitivity is low.

**Command Modes** Global configuration (config).

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

**Usage Guidelines** You must enable EDRRM using the **ap dot11 24ghz rrm channel cleanair-event** command before you configure the sensitivity.

This example shows how to enable EDRRM and set the EDRRM sensitivity to low:

```
Device(config)# ap dot11 24ghz rrm channel cleanair-event
Device(config)# ap dot11 24ghz rrm channel cleanair-event sensitivity low
```

## ap dot11 24ghz rrm channel device

To configure persistent non-Wi-Fi device avoidance in the 802.11b channel, use the **ap dot11 24ghz rrm channel device** command in global configuration mode. To disable persistent device avoidance, use the **no** form of this command.

```
ap dot11 24ghz rrm channel device
no ap dot11 24ghz rrm channel device
```

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** Persistent device avoidance is disabled.

---

**Command Modes** Global configuration (config).

---

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

---



---

**Usage Guidelines** CleanAir-capable monitor mode access points collect information about persistent devices on all configured channels and stores the information in the device. Local and bridge mode access points detect interference devices on the serving channels only.

This example shows how to enable persistent device avoidance:

```
Device(config)# ap dot11 24ghz rrm channel device
```

## ap dot11 24ghz rrm optimized-roam

To configure optimized roaming for 802.11b network, use the **ap dot11 24ghz rrm optimized-roam** command.

**ap dot11 24ghz rrm optimized-roam** [**data-rate-threshold** {**11M** | **12M** | **18M** | **1M** | **24M** | **2M** | **36M** | **48M** | **54M** | **5\_5M** | **6M** | **9M** | **disable**}]

Syntax Description	data-rate-threshold	Configures the data rate threshold for 802.11b optimized roaming.
	<b>11M</b>	Sets the data rate threshold for 802.11b optimized roaming to 11 Mbps
	<b>12M</b>	Sets the data rate threshold for 802.11b optimized roaming to of 12 Mbps
	<b>18M</b>	Sets the data rate threshold for 802.11b optimized roaming to of 18 Mbps
	<b>1M</b>	Sets the data rate threshold for 802.11b optimized roaming to of 1 Mbps
	<b>24M</b>	Sets the data rate threshold for 802.11b optimized roaming to of 24 Mbps
	<b>2M</b>	Sets the data rate threshold for 802.11b optimized roaming to of 2 Mbps
	<b>36M</b>	Sets the data rate threshold for 802.11b optimized roaming to of 36 Mbps
	<b>48M</b>	Sets the data rate threshold for 802.11b optimized roaming to of 48 Mbps
	<b>54M</b>	Sets the data rate threshold for 802.11b optimized roaming to of 54 Mbps
	<b>5_5M</b>	Sets the data rate threshold for 802.11b optimized roaming to of 5.5 Mbps
	<b>6M</b>	Sets the data rate threshold for 802.11b optimized roaming to of 6 Mbps
	<b>9M</b>	Sets the data rate threshold for 802.11b optimized roaming to of 9 Mbps
	<b>disable</b>	Disables the data rate threshold.

**Command Default** None

**Command Modes** Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

### Examples

The following example shows how to configure optimized roaming for 802.11b network:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap dot11 24ghz rrm optimized-roam
```

# ap dot11 24ghz rx-sop threshold

To configure 802.11b radio receiver start-of-packet (RxSOP), use the **ap dot11 24ghz rx-sop threshold** command.

**ap dot11 24ghz rx-sop threshold** {**auto** | **high** | **low** | **medium** | **custom** *rxsop-value*}

Syntax Description	auto	Reverts RxSOP value to the default value.
	high	Sets the RxSOP value to high threshold (–79 dBm).
	medium	Sets the RxSOP value to medium threshold (–82 dBm).
	low	Sets the RxSOP value to low threshold (–85 dBm).
	custom	Sets the RxSOP value to custom threshold (–85 dBm to –60 dBm)
	<i>rxsop-value</i>	
Command Default	None	
Command Modes	Global configuration (config)	
Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Usage Guidelines

RxSOP determines the Wi-Fi signal level in dBm at which an access point's radio demodulates and decodes a packet. Higher the level, less sensitive the radio is and smaller the receiver cell size. The table below shows the RxSOP threshold values for high, medium, low, and custom levels for 2.4-GHz band.

**Table 4: RxSOP Thresholds for 2.4-GHz Band**

High Threshold	Medium Threshold	Low Threshold	Custom Threshold
–79 dBm	–82 dBm	–85 dBm	–85 dBm to –60 dBm

## Examples

The following example shows how to configure 802.11b radio receiver start-of-packet (RxSOP) value to auto:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap dot11 24ghz rx-sop threshold auto
```

## ap dot11 24ghz shutdown

To disable 802.11a network, use the **ap dot11 24ghz shutdown** command.

**ap dot11 24ghz shutdown**

---

### Command Default

None

---

### Command Modes

Global configuration (config)

---

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

### Examples

The following example shows how to disable the 802.11a network:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap dot11 24ghz shutdown
```

## ap dot11 5ghz channelswitch quiet

To configure the 802.11h channel switch quiet mode, use the **ap dot11 5ghz channelswitch quiet** command.

**ap dot11 5ghz channelswitch quiet**

---

### Command Default

None

---

### Command Modes

Global configuration (config)

---

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

### Examples

The following example shows how to configure the 802.11h channel switch quiet mode:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap dot11 5ghz channelswitch quiet
```

## ap dot11 5ghz cleanair

To enable CleanAir for detecting 5-GHz devices, use the **ap dot11 5ghz cleanair** command in global configuration mode.

**ap dot11 5ghz cleanair**

**Command Default** Disabled.

**Command Modes** Global configuration.

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** You must enable this CleanAir command before you configure other CleanAir commands.

This example shows how to enable CleanAir for 5-GHz devices:

```
Device(config)# ap dot11 5ghz cleanair
```



## default ap dot11 5ghz cleanair device

To configure the default state of the alarm for 5-GHz interference devices, use the **default ap dot11 5ghz cleanair device** command in global configuration mode.

**default ap dot11 5ghz cleanair device** {canopy | cont-tx | dect-like | inv | jammer | nonstd | radar | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile}

Syntax Description	Parameter	Description
	<b>canopy</b>	Configures the alarm for canopy interference devices.
	<b>cont-tx</b>	Configures the alarm for continuous transmitters.
	<b>dect-like</b>	Configures the alarm for Digital Enhanced Cordless Communication (DECT)-like phones.
	<b>inv</b>	Configures the alarm for devices using spectrally inverted Wi-Fi signals.
	<b>jammer</b>	Configures the alarm for jammer interference devices.
	<b>nonstd</b>	Configures the alarm for devices using nonstandard Wi-Fi channels.
	<b>radar</b>	Configures the alarm for radars.
	<b>report</b>	Enables interference device reports.
	<b>superag</b>	Configures the alarm for 802.11 SuperAG interference devices.
	<b>tdd-tx</b>	Configures the alarm for Time Division Duplex (TDD) transmitters.
	<b>video</b>	Configures the alarm for video cameras.
	<b>wimax-fixed</b>	Configures the alarm for WiMax fixed interference devices.
	<b>wimax-mobile</b>	Configures the alarm for WiMax mobile interference devices.

**Command Default** The alarm for Wi-Fi inverted devices is enabled. The alarm for all other interference devices is disabled.

**Command Modes** Global configuration (config).

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** You must enable CleanAir using the **ap dot11 5ghz cleanair** command before you configure this command.

This example shows how to enable CleanAir to report when a video camera interferes:

```
Device(config)# default ap dot11 5ghz cleanair device video
```

## ap dot11 5ghz power-constraint

To configure the 802.11h power constraint value, use the **ap dot11 5ghz power-constraint** command. To remove the 802.11h power constraint value, use the **no** form of this command.

```
ap dot11 5ghz power-constraint value
no ap dot11 5ghz power-constraint
```

---

### Syntax Description

*value* 802.11h power constraint value.

**Note** The range is from 0 to 30 dBm.

---



---

### Command Default

None

---

### Command Modes

Global configuration

---

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to configure the 802.11h power constraint to 5 dBm:

```
Device(config)# ap dot11 5ghz power-constraint 5
```

## ap dot11 5ghz rate

To configure 802.11a operational rates, use the **ap dot11 5ghz rate** command.

```
ap dot11 5ghz rate {RATE_12M | RATE_18M | RATE_24M | RATE_36M | RATE_48M |
RATE_54M | RATE_6M | RATE_9M} {disable | mandatory | supported}
```

### Syntax Description

**RATE\_12M** Configures the data to be transmitted at the rate of 12 Mbps

**RATE\_18M** Configures the data to be transmitted at the rate of 18 Mbps

**RATE\_24M** Configures the data to be transmitted at the rate of 24 Mbps

**RATE\_36M** Configures the data to be transmitted at the rate of 36 Mbps

**RATE\_48M** Configures the data to be transmitted at the rate of 48 Mbps

**RATE\_54M** Configures the data to be transmitted at the rate of 54 Mbps

**RATE\_6M** Configures the data to be transmitted at the rate of 6 Mbps

**RATE\_9M** Configures the data to be transmitted at the rate of 9 Mbps

**disable** Disables the data rate that you specify. Also defines that the clients specify the data rates used for communication.

**mandatory** Defines that the clients support this data rate in order to associate with an AP.

**supported** Any associated clients support this data rate can communicate with the AP using this rate. However, the clients are not required to use this rate to associate with the AP.

### Command Default

None

### Command Modes

Global configuration (config)

### Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

### Examples

The following example shows how to configure 802.11a operational rate to 24 Mbps and make it supported:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap dot11 5ghz rate RATE_24M supported
```

## ap dot11 5ghz rrm channel cleanair-event

To enable Event-Driven RRM (EDRRM) and configure the sensitivity for 5-GHz devices, use the **ap dot11 5ghz rrm channel cleanair-event** command in global configuration mode. To disable EDRRM, use the **no** form of the command.

```
ap dot11 5ghz rrm channel cleanair-event [sensitivity {high | low | medium}]
no ap dot11 5ghz rrm channel cleanair-event [sensitivity {high | low | medium}]
```

Syntax Description		
	<b>sensitivity</b>	(Optional) Configures the EDRRM sensitivity of the CleanAir event.
	<b>high</b>	(Optional) Specifies the highest sensitivity to non-Wi-Fi interference as indicated by the air quality (AQ) value.
	<b>low</b>	(Optional) Specifies the least sensitivity to non-Wi-Fi interference as indicated by the AQ value.
	<b>medium</b>	(Optional) Specifies medium sensitivity to non-Wi-Fi interference as indicated by the AQ value.

**Command Default** EDRRM is disabled and the EDRRM sensitivity is low.

**Command Modes** Global configuration (config).

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

**Usage Guidelines** You must enable EDRRM using the **ap dot11 5ghz rrm channel cleanair-event** command before you configure the sensitivity.

This example shows how to enable EDRRM and set the EDRRM sensitivity to high:

```
Device(config)# ap dot11 5ghz rrm channel cleanair-event
Device(config)# ap dot11 5ghz rrm channel cleanair-event sensitivity high
```

## ap dot11 5ghz rrm channel device

To configure persistent non-Wi-Fi device avoidance in the 802.11a channel, use the **ap dot11 5ghz rrm channel device** command in global configuration mode. To disable persistent device avoidance, use the **no** form of this command.

```
ap dot11 5ghz rrm channel device
no ap dot11 5ghz rrm channel device
```

**Syntax Description** This command has no arguments or keywords.

**Command Default** The CleanAir persistent device state is disabled.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

**Usage Guidelines** CleanAir-capable monitor mode access points collect information about persistent devices on all configured channels and stores the information in the device. Local and bridge mode access points detect interference devices on the serving channels only.

This example shows how to enable persistent device avoidance on 802.11a devices:

```
Device(config)# ap dot11 5ghz rrm channel device
```

## ap dot11 5ghz rx-sop threshold

To configure 802.11a radio receiver start-of-packet (RxSOP), use the **ap dot11 5ghz rx-sop threshold** command.

**ap dot11 5ghz rx-sop threshold** {**auto** | **high** | **low** | **medium** | **custom** *rxsop-value*}

Syntax Description	auto	Reverts RxSOP value to the default value.
	<b>high</b>	Sets the RxSOP value to high threshold (–76 dBm).
	<b>medium</b>	Sets the RxSOP value to medium threshold (–78 dBm).
	<b>low</b>	Sets the RxSOP value to low threshold (–80 dBm).
	<b>custom</b> <i>rxsop-value</i>	Sets the RxSOP value to custom threshold (–85 dBm to –60 dBm)

**Command Default** None

**Command Modes** config

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

**Usage Guidelines** RxSOP determines the Wi-Fi signal level in dBm at which an access point's radio demodulates and decodes a packet. Higher the level, less sensitive the radio is and smaller the receiver cell size. The table below shows the RxSOP threshold values for high, medium, low, and custom levels for 5-GHz band.

*Table 5: RxSOP Thresholds for 5-GHz Band*

High Threshold	Medium Threshold	Low Threshold	Custom Threshold
–76 dBm	–78 dBm	–80 dBm	–85 dBm to –60 dBm

### Examples

The following example shows how to configure 802.11b radio receiver start-of-packet (RxSOP) value to a custom value of –70 dBm:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap dot11 24ghz rx-sop threshold custom -70
```

# ap dot11 5ghz shutdown

To disable 802.11a network, use the **ap dot11 5ghz shutdown** command.

**ap dot11 5ghz shutdown**

---

**Command Default** None

---

**Command Modes** Global configuration (config)

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

## Examples

The following example shows how to disable the 802.11a network:

```
Device# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Device(config)# ap dot11 5ghz shutdown
```

## ap dot11 5ghz smart-dfs

To configure to use nonoccupancy time for radar interference channel, use the **ap dot11 5ghz smart-dfs** command.

**ap dot11 5ghz smart-dfs**

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	config
----------------------	--------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

### Examples

The following example shows how to configure to use nonoccupancy time for radar interference channel:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap dot11 5ghz smart-dfs
```



# ap dot11 beaconperiod

To change the beacon period globally for 2.4 GHz or 5 GHz bands, use the **ap dot11 beaconperiod** command.



**Note** Disable the 802.11 network before using this command. See the “Usage Guidelines” section.

**ap dot11** {24ghz | 5ghz} **beaconperiod** *time*

Syntax Description	24ghz	Specifies the settings for 2.4 GHz band.
	5ghz	Specifies the settings for 5 GHz band.
	beaconperiod	Specifies the beacon for a network globally.
	<i>time</i>	Beacon interval in time units (TU). One TU is 1024 microseconds. The range is from 20 to 1000.

**Command Default** None

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

**Usage Guidelines** In Cisco wireless LAN 802.11 networks, all Cisco lightweight access point wireless LANs broadcast a beacon at regular intervals. This beacon notifies clients that the wireless service is available and allows the clients to synchronize with the lightweight access point.

Before you change the beacon period, make sure that you have disabled the 802.11 network by using the **ap dot11** {24ghz | 5ghz} **shutdown** command. After changing the beacon period, enable the 802.11 network by using the **no ap dot11** {24ghz | 5ghz} **shutdown** command.

This example shows how to configure the 5 GHz band for a beacon period of 120 time units:

```
Device(config)# ap dot11 5ghz beaconperiod 120
```

## ap dot11 cac media-stream

To configure media stream Call Admission Control (CAC) voice and video quality parameters for 2.4 GHz and 5 GHz bands, use the **ap dot11 cac media-stream** command.

```
ap dot11 {24ghz | 5ghz} cac media-stream multicast-direct {max-retry-percent retryPercent |
min-client-rate {eighteen | eleven | fiftyFour | fivePointFive | fortyEight | nine | oneFifty |
oneFortyFourPointFour | oneThirty | oneThirtyFive | seventyTwoPointTwo | six | sixtyFive | thirtySix
| threeHundred | twelve | twentyFour | two | twoSeventy}}
```

### Syntax Description

<b>24ghz</b>	Specifies the 2.4 GHz band.
<b>5ghz</b>	Specifies the 5 GHz band.
<b>multicast-direct</b>	Specifies CAC parameters for multicast-direct media streams.
<b>max-retry-percent</b>	Specifies the percentage of maximum retries that are allowed for multicast-direct media streams.
<i>retryPercent</i>	Percentage of maximum retries that are allowed for multicast-direct media streams. <b>Note</b> The range is from 0 to 100.
<b>min-client-rate</b>	Specifies the minimum transmission data rate to the client for multicast-direct media streams (rate at which the client must transmit in order to receive multicast-direct unicast streams).  If the transmission rate is below this rate, either the video will not start or the client may be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.

---

*min-client-rate* You can choose the following rates:

- **eighteen**
- **eleven**
- **fiftyFour**
- **fivePointFive**
- **fortyEight**
- **nine**
- **one**
- **oneFifty**
- **oneFortyFourPointFour**
- **oneThirty**
- **oneThirtyFive**
- **seventyTwoPointTwo**
- **six**
- **sixtyFive**
- **thirtySix**
- **threeHundred**
- **twelve**
- **twentyFour**
- **two**
- **twoSeventy**

---

<b>Command Default</b>	The default value for the maximum retry percent is 80. If it exceeds 80, either the video will not start or the client might be classified as a bad client. The bad client video will be demoted for better effort QoS or is subject to denial.				
<b>Command Modes</b>	Global configuration				
<b>Command History</b>	<table border="0" style="width: 100%;"> <thead> <tr> <th style="text-align: left;"><b>Release</b></th> <th style="text-align: right;"><b>Modification</b></th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 16.12.1</td> <td style="text-align: right;">This command was introduced.</td> </tr> </tbody> </table>	<b>Release</b>	<b>Modification</b>	Cisco IOS XE 16.12.1	This command was introduced.
<b>Release</b>	<b>Modification</b>				
Cisco IOS XE 16.12.1	This command was introduced.				
<b>Usage Guidelines</b>	<p>CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol.</p> <p>Before you can configure CAC parameters on a network, you must complete the following prerequisites:</p> <ul style="list-style-type: none"> <li>• Disable all WLANs with WMM enabled by entering the <b>wlan wlan_name shutdown</b> command.</li> </ul>				

- Disable the radio network you want to configure by entering the **ap dot11 {24ghz | 5ghz} shutdown** command.
- Save the new configuration.
- Enable voice or video CAC for the network you want to configure by entering the **ap dot11 {24ghz | 5ghz} cac voice acm** or **ap dot11 {24ghz | 5ghz} cac video acm** commands.

This example shows how to configure the maximum retry percent for multicast-direct media streams as 90 on a 802.11a network:

```
Device(config)# ap dot11 5ghz cac media-stream multicast max-retry-percent 90
```

## ap dot11 cac multimedia

To configure multimedia Call Admission Control (CAC) voice and video quality parameters for 2.4 GHz and 5 GHz bands, use the **ap dot11 cac multimedia** command.

```
ap dot11 {24ghz | 5ghz} cac multimedia max-bandwidth bandwidth
```

Syntax Description	24ghz	Specifies the 2.4 GHz band.
	5ghz	Specifies the 5 GHz band.
	max-bandwidth	Specifies the percentage of maximum bandwidth allocated to Wi-Fi Multimedia (WMM) clients for voice and video applications on the 2.4 GHz or 5 GHz band.
	bandwidth	Percentage of the maximum bandwidth allocated to WMM clients for voice and video applications on the 802.11a or 802.11b/g network. Once the client reaches the specified value, the access point rejects new multimedia flows this radio band. The range is from 5 to 85%.

**Command Default** The default value is 75%.

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

**Usage Guidelines** CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **wlan wlan\_name shutdown** command.
- Disable the radio network you want to configure by entering the **ap dot11 {24ghz | 5ghz} shutdown** command.
- Save the new configuration.
- Enable voice or video CAC for the network you want to configure by entering the **ap dot11 {24ghz | 5ghz} cac voice acm** or **ap dot11 {24ghz | 5ghz} cac video acm** commands.

This example shows how to configure the percentage of the maximum bandwidth allocated to WMM clients for voice and video applications on the 5 GHz band:

```
Device(config)# ap dot11 5ghz cac multimedia max-bandwidth 5
```

## ap dot11 cac voice

To configure Call Admission Control (CAC) parameters for the voice category, use the **ap dot11 cac voice** command.

```
ap dot11 {24ghz | 5ghz} cac voice {acm | load-based | max-bandwidth value | roam-bandwidth value
| sip [bandwidth bw] sample-interval value | stream-size x max-streams y |
tspec-inactivity-timeout {enable | ignore}}
```

Syntax Description	
<b>24ghz</b>	Specifies the 2.4 GHz band.
<b>5ghz</b>	Specifies the 5 GHz band.
<b>acm</b>	Enables bandwidth-based voice CAC for the 2.4 GHz or 5 GHz band.  <b>Note</b> To disable bandwidth-based voice CAC for the 2.4 GHz or 5 GHz band, use the <b>no ap dot11 {24ghz   5ghz} cac voice acm</b> command.
<b>load-based</b>	Enable load-based CAC on voice access category.  <b>Note</b> To disable load-based CAC on voice access category for the 2.4 GHz or 5 GHz band, use the <b>no ap dot11 {24ghz   5ghz} cac voice load-based</b> command.
<b>max-bandwidth</b>	Sets the percentage of the maximum bandwidth allocated to clients for voice applications on the 2.4 GHz or 5 GHz band.
<i>value</i>	Bandwidth percentage value from 5 to 85%.
<b>roam-bandwidth</b>	Sets the percentage of the CAC maximum allocated bandwidth reserved for roaming voice clients on the 2.4 GHz or 5 GHz band.
<i>value</i>	Bandwidth percentage value from 0 to 85%.
<b>sip</b>	Specifies the CAC codec name and sample interval as parameters and calculates the required bandwidth per call for the 802.11 networks.

<i>bw</i>	Bandwidth in kbps. The following bandwidth values specify parameters for the SIP codecs: <ul style="list-style-type: none"> <li>• 64kbps—Specifies CAC parameters for the SIP G711 codec.</li> <li>• 8kbps—Specifies CAC parameters for the SIP G729 codec.</li> </ul> <p><b>Note</b> The default value is 64 Kbps.</p>
<b>sample-interval</b>	Specifies the packetization interval for SIP codec.
<i>value</i>	Packetization interval in msec. The sample interval for SIP codec value is 20 seconds.
<b>stream-size</b>	Specifies the number of aggregated voice Wi-Fi Multimedia (WMM) traffic specification (TSPEC) streams at a specified data rate for the 2.4 GHz or 5 GHz band.
<i>x</i>	Stream size. The range of the stream size is from 84000 to 92100.
<b>max-streams</b>	Specifies the maximum number of streams per TSPEC.
<i>y</i>	Number (1 to 5) of voice streams. <p><b>Note</b> The default number of streams is 2 and the mean data rate of a stream is 84 kbps.</p>
<b>tspec-inactivity-timeout</b>	Specifies TSPEC inactivity timeout processing mode. <p><b>Note</b> Use this keyword to process or ignore the Wi-Fi Multimedia (WMM) traffic specifications (TSPEC) inactivity timeout received from an access point. When the inactivity timeout is ignored, a client TSPEC is not deleted even if the access point reports an inactivity timeout for that client.</p>
<b>enable</b>	Processes the TSPEC inactivity timeout messages.
<b>ignore</b>	Ignores the TSPEC inactivity timeout messages. <p><b>Note</b> The default is <b>ignore</b> (disabled).</p>

**Command Default** None

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

**Usage Guidelines**

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **wlan wlan\_name shutdown** command.
- Disable the radio network you want to configure by entering the **ap dot11 {24ghz | 5ghz} shutdown** command.
- Save the new configuration.
- Enable voice or video CAC for the network you want to configure by entering the **ap dot11 {24ghz | 5ghz} cac voice acm** or **ap dot11 {24ghz | 5ghz} cac video acm** commands.

This example shows how to enable the bandwidth-based CAC:

```
Device(config)# ap dot11 24ghz cac voice acm
```

This example shows how to enable the load-based CAC on the voice access category:

```
Device(config)# ap dot11 24ghz cac voice load-based
```

This example shows how to specify the percentage of the maximum allocated bandwidth for voice applications on the selected radio band:

```
Device(config)# ap dot11 24ghz cac voice max-bandwidth 50
```

This example shows how to configure the percentage of the maximum allocated bandwidth reserved for roaming voice clients on the selected radio band:

```
Device(config)# ap dot11 24ghz cac voice roam-bandwidth 10
```

This example shows how to configure the bandwidth and voice packetization interval for the G729 SIP codec on a 2.4 GHz band:

```
Device(config)# ap dot11 24ghz cac voice sip bandwidth 8 sample-interval 40
```

This example shows how to configure the number of aggregated voice traffic specifications stream with a stream size of 85000 and with a maximum of 5 streams:

```
Device(config)# ap dot11 24ghz cac voice stream-size 85000 max-streams 5
```

This example shows how to enable the voice TSPEC inactivity timeout messages received from an access point:

```
Device(config)# ap dot11 24ghz cac voice tspec-inactivity-timeout enable
```



## ap dot11 cleanair

To configure CleanAir on 802.11 networks, use the **ap dot11 cleanair** command. To disable CleanAir on 802.11 networks, use the **no** form of this command.

```
ap dot11 {24ghz | 5ghz} cleanair
no ap dot11 {24ghz | 5ghz} cleanair
```

<b>Syntax Description</b>	<b>24ghz</b>	Specifies the 2.4 GHz band.
	<b>5ghz</b>	Specifies the 5 GHz band.
	<b>cleanair</b>	Specifies CleanAir on the 2.4 GHz or 5 GHz band.
<b>Command Default</b>	Disabled	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

This example shows how to enable the CleanAir settings on the 2.4 GHz band:

```
Device(config)# ap dot11 24ghz cleanair
```

## ap dot11 cleanair device

To configure CleanAir interference device types, use the **ap dot11 cleanair device** command.

```
ap dot11 24ghz cleanair device [{canopy | cont-tx | dect-like | inv | jammer | nonstd | report | si_fhss
| superag | tdd-tx | video | wimax-fixed | wimax-mobile}]
```

Syntax Description		
<b>canopy</b>		Specifies the Canopy devices.
<b>cont-tx</b>		Specifies the continuous transmitter.
<b>dect-like</b>		Specifies a Digital Enhanced Cordless Communication (DECT)-like phone.
<b>inv</b>		Specifies the devices using spectrally inverted Wi-Fi signals.
<b>jammer</b>		Specifies the jammer.
<b>nonstd</b>		Specifies the devices using nonstandard Wi-Fi channels.
<b>superag</b>		Specifies 802.11 SuperAG devices.
<b>tdd-tx</b>		Specifies the TDD transmitter.
<b>video</b>		Specifies video cameras.
<b>wimax-fixed</b>		Specifies a WiMax fixed device.
<b>wimax-mobile</b>		Specifies a WiMax mobile device.
<b>report</b>		Displays the device alarm report.
<b>si_fhss</b>		Specifies the QCA SI FHSS.

**Command Default** None

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to configure the device to monitor ZigBee interferences:

```
Device(config)# ap dot11 24ghz cleanair device report
```

## ap dot11 dot11n

To configure settings for an 802.11n network, use the **ap dot11 dot11n** command.

```
ap dot11 {24ghz | 5ghz} dot11n {a-mpdu tx priority {priority_value all} | scheduler timeout rt
scheduler_value} | a-msdu tx priority {priority_value all} | guard-interval {any | long} | mcs tx rate
| rifs rx}
```

Syntax	Description
<b>24ghz</b>	Specifies the 2.4-GHz band.
<b>5ghz</b>	Specifies the 5-GHz band.
<b>dot11n</b>	Enables 802.11n support.
<b>a-mpdu tx priority</b>	Specifies the traffic that is associated with the priority level that uses Aggregated MAC Protocol Data Unit (A-MPDU) transmission.
<i>priority_value</i>	Aggregated MAC protocol data unit priority level from 0 to 7.
<b>all</b>	Specifies all of the priority levels at once.
<b>a-msdu tx priority</b>	Specifies the traffic that is associated with the priority level that uses Aggregated MAC Service Data Unit (A-MSDU) transmission.
<i>priority_value</i>	Aggregated MAC protocol data unit priority level from 0 to 7.
<b>all</b>	Specifies all of the priority levels at once.
<i>scheduler_value</i>	The 802.11n A-MPDU transmit aggregation scheduler timeout value from 1 to 10000 milliseconds.
<b>guard-interval</b>	Specifies the guard interval.
<b>any</b>	Enables either a short or a long guard interval.
<b>long</b>	Enables only a long guard interval.
<b>mcs tx rate</b>	Specifies the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client.
<i>rate</i>	Specifies the modulation and coding scheme data rates. <b>Note</b> The range is from 0 to 23.
<b>rifs rx</b>	Specifies the Reduced Interframe Space (RIFS) between data frames.

**Command Default** By default, priority 0 is enabled.

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

**Usage Guidelines** Aggregation is the process of grouping packet data frames together rather than transmitting them separately. The two aggregation methods available are:

- A-MPDU—This aggregation is performed in the software.
- A-MSDU—This aggregation is performed in the hardware

Aggregated MAC Protocol Data Unit priority levels assigned per traffic type are as follows:

- 0—Best effort
- 1—Background
- 2—Spare
- 3—Excellent effort
- 4—Controlled load
- 5—Video, less than 100-ms latency and jitter
- 6—Voice, less than 10-ms latency and jitter
- 7—Network control
- all—Configure all of the priority levels at once.



**Note** Configure the priority levels to match the aggregation method used by the clients.

This example shows how to enable 802.11n support on a 2.4-GHz band:

```
Device(config)# ap dot11 24ghz dot11n
```

This example shows how to configure all the priority levels at once so that the traffic that is associated with the priority level uses A-MSDU transmission:

```
Device(config)# ap dot11 24ghz dot11n a-msdu tx priority all
```

This example shows how to enable only long guard intervals:

```
Device(config)# ap dot11 24ghz dot11n guard-interval long
```

This example shows how to specify MCS rates:

```
Device(config)# ap dot11 24ghz dot11n mcs tx 5
```

This example shows how to enable RIFS:

```
Device(config)# ap dot11 24ghz dot11n rifs rx
```

## ap dot11 dtpc

To configure Dynamic Transmit Power Control (DTPC) settings, Cisco Client eXtension (CCX) version 5 expedited bandwidth request feature, and the fragmentation threshold on an 802.11 network, use the **ap dot11 dtpc** command.

```
ap dot11 {24ghz | 5ghz} {dtpc | exp-bwreq | fragmentation threshold}
```

Syntax Description		
<b>24ghz</b>	Specifies the 2.4 GHz band.	
<b>5ghz</b>	Specifies the 5 GHz band.	
<b>dtpc</b>	Specifies Dynamic Transport Power Control (DTPC) settings.	<b>Note</b> This option is enabled by default.
<b>exp-bwreq</b>	Specifies Cisco Client eXtension (CCX) version 5 expedited bandwidth request feature.	<b>Note</b> The expedited bandwidth request feature is disabled by default.
<b>fragmentation threshold</b>	Specifies the fragmentation threshold.	<b>Note</b> This option can only be used when the network is disabled using the <b>ap dot11 {24ghz   5ghz} shutdown</b> command.
<i>threshold</i>	Threshold. The range is from 256 to 2346 bytes (inclusive).	

**Command Default** None

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

**Usage Guidelines** When the CCX version 5 expedited bandwidth request feature is enabled, the device configures all joining access points for this feature.

This example shows how to enable DTPC for the 5 GHz band:

```
Device(config)# ap dot11 5ghz dtpc
```

This example shows how to enable the CCX expedited bandwidth settings:

```
Device(config)# ap dot11 5ghz exp-bwreq
```

This example shows how to configure the fragmentation threshold on the 5 GHz band with the threshold number of 1500 bytes:

```
Device(config)# ap dot11 5ghz fragmentation 1500
```

## ap dot11 edca-parameters

To enable a specific enhanced distributed channel access (EDCA) profile on the 2.4 GHz or 5 GHz bands, use the **ap dot11 edca-parameters** command. To disable an EDCA profile on the 2.4 GHz or 5 GHz bands, use the **no** form of this command.

```
ap dot11 { 24ghz | 5ghz } edca-parameters { client-load-based | custom-voice |
optimized-video-voice | optimized-voice | svp-voice | wmm-default }
no ap dot11 { 24ghz | 5ghz } edca-parameters { client-load-based | custom-voice | fastlane
| optimized-video-voice | optimized-voice | svp-voice | wmm-default }
```

Syntax Description		
	<b>24ghz</b>	Specifies the 2.4 GHz band.
	<b>5ghz</b>	Specifies the 5 GHz band.
	<b>edca-parameters</b>	Specifies a specific enhanced distributed channel access (EDCA) profile on the 802.11 networks.
	<b>fastlane</b>	Enables Fastlane parameters for 24GHz.
	<b>client-load-based</b>	Enables client load-based EDCA configuration for 802.11 radios.
	<b>custom-voice</b>	Enables custom voice EDCA parameters.
	<b>optimized-video-voice</b>	Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network.
	<b>optimized-voice</b>	Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than SpectraLink are deployed on your network.
	<b>svp-voice</b>	Enables SpectraLink voice priority parameters. Choose this option if SpectraLink phones are deployed on your network to improve the quality of calls.
	<b>wmm-default</b>	Enables the Wi-Fi Multimedia (WMM) default parameters. Choose this option when voice or video services are not deployed on your network.

<b>Command Default</b>	<b>wmm-default</b>
------------------------	--------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.
	10.3	The <b>custom-voice</b> keyword was removed for Cisco 5700 Series WLC.
	Cisco IOS XE Bengaluru 17.5.1	The <b>client-load-based</b> keyword was added.



This example shows how to enable SpectraLink voice priority parameters:

```
Device(config)# ap dot11 24ghz edca-parameters svp-voice
```

## ap dot11 load-balancing denial

To configure the load balancing denial count, use the **ap dot11 load-balancingdenial** command. To disable load balancing denial count, use the **no** form of the command.

**ap dot11** { 24ghz | 5ghz } **load-balancingdenial** *count*

<b>Syntax Description</b>	<i>count</i> Load balancing denial count.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Global configuration (config)				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.				

### Example

The following example shows how to configure the load balancing denial count:

```
Device# configure terminal
Device(config)# ap dot11 5ghz load-balancing denial 10
```

## ap dot11 load-balancing window

To configure the number of clients for the aggressive load balancing client window, use the **ap dot11 load-balancingwindow** command. To disable the client count, use the **no** form of the command.

**ap dot11** { 24ghz | 5ghz } **load-balancingwindow** *clients*

<b>Syntax Description</b>	<i>clients</i> Number of clients. Valid range is from 0 to 20.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Global configuration (config)				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.				

### Example

The following example shows how to configure the number of clients for the aggressive load balancing client window:

```
Device# configure terminal
Device(config)# ap dot11 5ghz load-balancing window 10
```

## ap dot11 rf-profile

To configure an RF-Profile for a selected band, use the **ap dot11 rf-profile** command. To delete an RF-Profile, use the **no** form of this command.

**ap dot11** {24GHz | 5GHz} **rf-profile** *profile name*

Syntax Description	24ghz	Displays the 2.4-GHz band
	5ghz	Displays the 5-GHz band
	<i>profile name</i>	Name of the RF profile

**Command Default** None

**Command Modes** Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

**Usage Guidelines** None

This example shows how to configure an RF profile for a selected band.

```
Device#ap dot11 24GHz rf-profile doctest
```

## ap dot11 rrm

To configure basic and advanced radio resource management settings for 802.11 devices, use the **ap dot11 rrm** command.

```
ap dot11 {24ghz | 5ghz} rrm {ccx location-measurement sec | channel {cleanair-event | dca | device
| foreign | load | noise | outdoor-ap-dca} | coverage {data fail-percentage pct | data packet-count
count | data rssi-threshold threshold} | exception global percentage | level global number | voice
{fail-percentage percentage | packet-count number | rssi-threshold threshold}}
```

Syntax	Description
<b>ccx</b>	Configures Advanced (RRM) 802.11 CCX options.
<b>location-measurement</b>	Specifies 802.11 CCX Client Location Measurements in seconds. The range is between 10 and 32400 seconds.
<b>channel</b>	Configure advanced 802.11-channel assignment parameters.
<b>cleanair-event</b>	Configures cleanair event-driven RRM parameters.
<b>dca</b>	Configures 802.11-dynamic channel assignment algorithm parameters.
<b>device</b>	Configures persistent non-WiFi device avoidance in the 802.11-channel assignment.
<b>foreign</b>	Enables foreign AP 802.11-interference avoidance in the channel assignment.
<b>load</b>	Enables Cisco AP 802.11-load avoidance in the channel assignment.
<b>noise</b>	Enables non-802.11-noise avoidance in the channel assignment.
<b>outdoor-ap-dca</b>	Configures 802.11 DCA list option for outdoor AP.
<b>coverage</b>	Configures 802.11 coverage Hole-Detection.

<b>data fail-percentage</b> <i>pct</i>	Configures 802.11 coverage failure-rate threshold for uplink data packets. The range is between 1 and 100
<b>data packet-count</b> <i>count</i>	Configures 802.11 coverage minimum-failure-count threshold for uplinkdata packets.
<b>data rssi-threshold</b> <i>threshold</i>	Configures 802.11 minimum-receive-coverage level for voice packets.
<b>exception global</b> <i>percentage</i>	Configures 802.11 Cisco APs coverage-exception level. The range is between 0 and 100 percent.
<b>level global</b> <i>number</i>	Configures 802.11 Cisco AP client-minimum-exception level between 1 and 75 clients.
<b>voice</b>	Configures 802.11 coverage Hole-Detection for voice packets.
<b>fail-percentage</b> <i>percentage</i>	Configures 802.11 coverage failure rate threshold for uplink voice packets.
<b>packet-count</b> <i>number</i>	Configures 802.11 coverage minimum-uplink-failure count threshold for voice packets.
<b>rssi-threshold</b> <i>threshold</i>	Configures 802.11 minimum receive coverage level for voice packets.

**Command Default** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

**Usage Guidelines** This command applies for both 802.11a and 802.11b bands. But the appropriate commands must be chosen for configuring the parameter.

This example shows how to configure various RRM settings.

```
Device#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm ?
```

ccx	Configure Advanced(RRM) 802.11a CCX options
channel	Configure advanced 802.11a channel assignment parameters
coverage	802.11a Coverage Hole Detection
group-member	Configure members in 802.11a static RF group
group-mode	802.11a RF group selection mode
logging	802.11a event logging
monitor	802.11a statistics monitoring
ndp-type	Neighbor discovery type Protected/Transparent
profile	802.11a performance profile
tpc-threshold	Configures the Tx Power Control Threshold used by RRM for auto power assignment
txpower	Configures the 802.11a Tx Power Level

## ap dot11 rrm channel

To enable radio resource management channel for 2.4 GHz and 5GHz devices, use the **ap dot11 rrm channel** command. To disable the radio resource management for 2.4 GHz and 5 GHz devices, use the **no** form of the command.

```
ap dot11 {24ghz | 5ghz} rrm channel {cleanair-event | dca | device | foreign | load | noise}
no ap dot11 {24ghz | 5ghz} rrm channel {cleanair-event | dca | device | foreign | load | noise}
```

Syntax Description	Parameter	Description
	<b>cleanair-event</b>	Specifies the cleanair event-driven RRM parameters
	<b>dca</b>	Specifies the 802.11 dynamic channel assignment algorithm parameters
	<b>device</b>	Specifies the persistent non-WiFi device avoidance in the 802.11-channel assignment.
	<b>foreign</b>	Enables foreign AP 802.11-interference avoidance in the channel assignment.
	<b>load</b>	Enables Cisco AP 802.11-load avoidance in the channel assignment.
	<b>noise</b>	Enables non-802.11-noise avoidance in the channel assignment.

**Command Default** None.

**Command Modes** Interface configuration.

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

**Usage Guidelines** None.

This example shows all the parameters available for **Channel**.

```
Device#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#ap dot11 24ghz rrm channel ?
  cleanair-event  Configure cleanair event-driven RRM parameters
  dca              Config 802.11b dynamic channel assignment algorithm
                  parameters
  device          Configure persistent non-WiFi device avoidance in the 802.11b
                  channel assignment
  foreign         Configure foreign AP 802.11b interference avoidance in the
                  channel assignment
  load            Configure Cisco AP 802.11b load avoidance in the channel
                  assignment
  noise           Configure 802.11b noise avoidance in the channel assignment
```



## ap dot11 rrm channel dca

To configure Dynamic Channel Assignment (DCA) algorithm parameters on 802.11 networks, use the **ap dot11 rrm channel dca** command.

```
ap dot11 {24ghz | 5ghz} rrm channel dca {add value <1-14> | anchor-time value | global {auto | once} | interval value | min-metric value | remove value <1-14> | sensitivity {high | low | medium} }
```

Syntax	Description
<b>24ghz</b>	Specifies the 2.4 GHz band.
<b>5ghz</b>	Specifies the 5 GHz band.
<b>add</b>	Adds the 802.11b DCA channels to RRM allowed channel list
<b>anchor-time</b>	Specifies the anchor time for DCA.
<i>value</i>	Hour of time between 0 and 23. These values represent the hour from 12:00 a.m. to 11:00 p.m.
<b>global</b>	Specifies the global DCA mode for the access points in the 802.11 networks.
<b>auto</b>	Enables auto-RF.
<b>once</b>	Enables one-time auto-RF.
<b>interval</b>	Specifies how often the DCA is allowed to run.
<i>value</i>	Interval between the times when DCA is allowed to run. Valid values are 0, 1, 2, 3, 4, 6, 8, 12, or 24 hours. 0 is 10 minutes (600 seconds). Default value is 0 (10 minutes).
<b>min-metric</b>	Specifies the DCA minimum RSSI energy metric.
<i>value</i>	Minimum RSSI energy metric value from -100 to -60.
<b>remove</b>	Removes the 802.11b DCA channels from RRM allowed channel list.
<b>sensitivity</b>	Specifies how sensitive the DCA algorithm is to environmental changes (for example, signal, load, noise, and interference) when determining whether or not to change channels.
<b>high</b>	Specifies that the DCA algorithm is not particularly sensitive to environmental changes. See the “Usage Guidelines” section for more information.
<b>low</b>	Specifies that the DCA algorithm is moderately sensitive to environmental changes. See the “Usage Guidelines” section for more information.
<b>medium</b>	Specifies that the DCA algorithm is highly sensitive to environmental changes. See the “Usage Guidelines” section for more information.

**Command Default** None

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

### Usage Guidelines

The DCA sensitivity thresholds vary by radio band as shown in the table below.

To aid in troubleshooting, the output of this command shows an error code for any failed calls. The table below explains the possible error codes for failed calls.

**Table 6: DCA Sensitivity Threshold**

Sensitivity	2.4 Ghz DCA Sensitivity Threshold	5 Ghz DCA Sensitivity Threshold
High	5 dB	5 dB
Medium	15 dB	20 dB
Low	30 dB	35 dB

This example shows how to configure the device to start running DCA at 5 pm for the 2.4 GHz band:

```
Device(config)# ap dot11 24ghz rrm channel dca anchor-time 17
```

This example shows how to set the DCA algorithm to run every 10 minutes for the 2.4 GHz band:

```
Device(config)# ap dot11 24ghz rrm channel dca interval 0
```

This example shows how to configure the value of DCA algorithm's sensitivity to low on the 2.4 GHz band:

```
Device(config)# ap dot11 24ghz rrm channel dca sensitivity low
```

## ap dot11 rrm coverage

To enable 802.11 coverage hole detection, use the **ap dot11 rrm coverage** command.

```
ap dot11 {24ghz|5ghz} rrm coverage [{data {fail-percentage percentage | packet-count count |
 rssi-threshold threshold} | exceptional global value | level global value | voice {fail-percentage
 percentage | packet-count packet-count | rssi-threshold threshold}]
```

Syntax Description	Parameter	Description
	<b>data</b>	Specifies 802.11 coverage hole-detection data packets.
	<b>fail-percentage</b> <i>percentage</i>	Specifies 802.11 coverage failure-rate threshold for uplink data packets. The range is between 1 and 100
	<b>packet-count</b> <i>count</i>	Specifies 802.11 coverage minimum-failure-count threshold for uplink data packets.
	<b>rssi-threshold</b> <i>threshold</i>	Specifies 802.11 minimum-receive-coverage level for voice packets.
	<b>exceptional global</b> <i>value</i>	Specifies 802.11 Cisco APs coverage-exception level. The range is between 0 and 100 percent.
	<b>level global</b> <i>value</i>	Specifies 802.11 Cisco AP client-minimum-exception level between 1 and 75 clients.
	<b>voice</b>	Specifies 802.11 coverage Hole-Detection for voice packets.
	<b>fail-percentage</b> <i>percentage</i>	Specifies 802.11 coverage failure rate threshold for uplink voice packets.
	<b>packet-count</b> <i>packet-count</i>	Specifies 802.11 coverage minimum-uplink-failure count threshold for voice packets.
	<b>rssi-threshold</b> <i>threshold</i>	Specifies 802.11 minimum receive coverage level for voice packets.

**Command Default** None.

**Command Modes** Interface configuration.

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

**Usage Guidelines** If you enable coverage hole-detection, the device automatically determines, based on data that is received from the access points, whether any access points have clients that are potentially located in areas with poor coverage.

If both the number and percentage of failed packets exceed the values that you entered in the **ap dot11 {24ghz | 5ghz} rrm coverage packet-count** and **ap dot11 {24ghz | 5ghz} rrm coverage fail-percentage** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The device uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the

**ap dot11 {24ghz | 5ghz} rrm coverage level-global** and **ap dot11 {24ghz | 5ghz} rrm coverage exceptional-global** commands over a 90-second period. The device determines whether the coverage hole can be corrected and, if appropriate, mitigate the coverage hole by increasing the transmit power level for that specific access point.

This example shows how to set the RSSI-threshold for data in 5-GHz band.

```
Device#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Device(config)#ap dot11 5ghz rrm coverage data rssi-threshold -80
```

## ap dot11 rrm group-member

To configure members in an 802.11 static RF group, use the **ap dot11 rrm group-member** command. To remove members from 802.11 RF group, use the **no** form of this command.

```
ap dot11 {24ghz | 5ghz} rrm group-member controller-name controller-ip
no ap dot11 {24ghz | 5ghz} rrm group-member controller-name controller-ip
```

<b>Syntax Description</b>	<b>24ghz</b>	Specifies the 2.4 GHz band.
	<b>5ghz</b>	Specifies the 5 GHz band.
	<i>controller-name</i>	Name of the device to be added.
	<i>controller-ip</i>	IP address of the device to be added.
<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

This example shows how to add a device in the 5 GHz band RF group:

```
Device(config)# ap dot11 5ghz rrm group-member cisco-controller 192.0.2.54
```

## ap dot11 rrm group-mode

To set the 802.11 automatic RF group selection mode on, use the **ap dot11 rrm group-mode** command. To set the 802.11 automatic RF group selection mode off, use the **no** form of this command.

```
ap dot11 {5ghz | 24ghz} rrm group-mode {auto | leader | off}
no ap dot11 {5ghz | 24ghz} rrm group-mode
```

Syntax Description	
<b>5ghz</b>	Specifies the 2.4 GHz band.
<b>24ghz</b>	Specifies the 5 GHz band.
<b>auto</b>	Sets the 802.11 RF group selection to automatic update mode.
<b>leader</b>	Sets the 802.11 RF group selection to static mode, and sets this device as the group leader.
<b>off</b>	Sets the 802.11 RF group selection to off.

**Command Default** auto

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

This example shows how to turn the auto RF group selection mode on the 5 GHz band:

```
Device(config)# ap dot11 5ghz rrm group-mode auto
```

## ap dot11 rrm logging

To configure report log settings on supported 802.11 networks, use the **ap dot11 rrm logging** command.

```
ap dot11 {24ghz | 5ghz} rrm logging {channel | coverage | foreign | load | noise | performance | txpower}
```

Syntax Description	24ghz	Specifies the 2.4 GHz band.
	5ghz	Specifies the 5 GHz band.
	channel	Turns the channel change logging mode on or off. The default mode is off (Disabled).
	coverage	Turns the coverage profile logging mode on or off. The default mode is off (Disabled).
	foreign	Turns the foreign interference profile logging mode on or off. The default mode is off (Disabled).
	load	Turns the load profile logging mode on or off. The default mode is off (Disabled).
	noise	Turns the noise profile logging mode on or off. The default mode is off (Disabled).
	performance	Turns the performance profile logging mode on or off. The default mode is off (Disabled).
	txpower	Turns the transit power change logging mode on or off. The default mode is off (Disabled).
Command Default	Disabled	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

This example shows how to turn the 5 GHz logging channel selection mode on:

```
Device(config)# ap dot11 5ghz rrm logging channel
```

This example shows how to turn the 5 GHz coverage profile violation logging selection mode on:

```
Device(config)# ap dot11 5ghz rrm logging coverage
```

This example shows how to turn the 5 GHz foreign interference profile violation logging selection mode on:

```
Device(config)# ap dot11 5ghz rrm logging foreign
```

This example shows how to turn the 5 GHz load profile logging mode on:

```
Device(config)# ap dot11 5ghz rrm logging load
```

This example shows how to turn the 5 GHz noise profile logging mode on:

```
Device(config)# ap dot11 5ghz rrm logging noise
```

This example shows how to turn the 5 GHz performance profile logging mode on:

```
Device(config)# ap dot11 5ghz rrm logging performance
```

This example shows how to turn the 5 GHz transmit power change mode on:

```
Device(config)# ap dot11 5ghz rrm logging txpower
```



## ap dot11 rrm monitor

To Configure monitor settings on the 802.11 networks, use the **ap dot11 rrm monitor** command.

```
ap dot11 {24ghz | 5ghz} rrm monitor {channel-list | {all | country | dca} | coverage | load | noise | signal} seconds
```

Syntax	Description
<b>24ghz</b>	Specifies the 802.11b parameters.
<b>5ghz</b>	Specifies the 802.11a parameters.
<b>channel-list all</b>	Monitors the noise, interference, and rogue monitoring channel list for all channels.
<b>channel-list country</b>	Monitors the noise, interference, and rogue monitoring channel list for the channels used in the configured country code.
<b>channel-list dca</b>	Monitors the noise, interference, and rogue monitoring channel list for the channels used by automatic channel assignment.
<b>coverage</b>	Specifies the coverage measurement interval.
<b>load</b>	Specifies the load measurement interval.
<b>noise</b>	Specifies the noise measurement interval.
<b>signal</b>	Specifies the signal measurement interval.
<b>rsi-normalization</b>	Configure RRM Neighbor Discovery RSSI Normalization.
<i>seconds</i>	Measurement interval time from 60 to 3600 seconds.

**Command Default** None

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

This example shows how to monitor the channels used in the configured country:

```
Device(config)# ap dot11 24ghz rrm monitor channel-list country
```

This example shows how to set the coverage measurement interval to 60 seconds:

```
Device(config)# ap dot11 24ghz rrm monitor coverage 60
```

## ap dot11 rrm ndp-type

To configure the 802.11 access point radio resource management neighbor discovery protocol type, use the **ap dot11 rrm ndp-type** command.

```
ap dot11 {24ghz | 5ghz} rrm ndp-type {protected | transparent}
```

Syntax Description	24ghz	Specifies the 2.4 GHz band.
	5ghz	Specifies the 5 GHz band.
	protected	Specifies the Tx RRM protected (encrypted) neighbor discovery protocol.
	transparent	Specifies the Tx RRM transparent (not encrypted) neighbor discovery protocol.

**Command Default** None

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

**Usage Guidelines** Before you configure the 802.11 access point RRM neighbor discovery protocol type, ensure that you have disabled the network by entering the **ap dot11 {24ghz | 5ghz} shutdown** command.

This example shows how to enable the 802.11a access point RRM neighbor discovery protocol type as protected:

```
Device(config)# ap dot11 5ghz rrm ndp-type protected
```

## ap dot11 24ghz rrm tpc

To configure the tx-power control threshold used by RRM for auto power assignment, use the **ap dot11 rrm tpc** command. To disable, use the **no** form of the command.

```
ap dot11 {24ghz | 5ghz} rrm tpc{threshold | tpcv1-chan-aware}
```

<b>Syntax Description</b>	<b>tpc threshold</b>	Configures the Tx-Power Control threshold used by RRM..
	<b>tpcv1-chan-aware</b>	Configures the Tx-Power Control to be channel aware.

**Command Default** None.

**Command Modes** Interface configuration.

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** None.

This example shows how to configure the tx-power control threshold used by RRM for auto power assignment.

```
Device#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#ap dot11 24ghz rrm tpc
```

## ap dot11 rrm txpower

To configure the 802.11 tx-power level, use the **ap dot11 rrm txpower** command. To disable the 802.11 tx-power level, use the **no** form of the command.

```
ap dot11 {24ghz|5ghz} rrm txpower {powerLevel <1-5> | auto | max powerLevel | min powerLevel | oncepower-level}
```

Syntax Description		
	<i>powerLevel</i>	Configures the transmit power level.
	<b>auto</b>	Enables auto-RF.
	<b>max</b> <i>powerLevel</i>	Configures maximum auto-RF tx power. The range is between -10 to -30.
	<b>min</b> <i>powerLevel</i>	Configures minimum auto-RF tx power. The range is between -10 to -30.
	<b>once</b>	Enables one-time auto-RF.

**Command Default** None.

**Command Modes** Interface configuration.

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** None.

This example shows how to enables auto-RF once.

```
Device#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm txpower once
```

## ap dot11 rrm txpower

To configure the 802.11 tx-power level, use the **ap dot11 rrm txpower** command. To disable the 802.11 tx-power level, use the **no** form of the command.

**ap dot11** {24ghz | 5ghz} **rrm txpower** {*powerLevel* <1-5> | **auto** | **max** *powerLevel* | **min** *powerLevel* | **once***power-level*}

Syntax Description		
	<i>powerLevel</i>	Configures the transmit power level.
	<b>auto</b>	Enables auto-RF.
	<b>max</b> <i>powerLevel</i>	Configures maximum auto-RF tx power. The range is between -10 to -30.
	<b>min</b> <i>powerLevel</i>	Configures minimum auto-RF tx power. The range is between -10 to -30.
	<b>once</b>	Enables one-time auto-RF.

**Command Default** None.

**Command Modes** Interface configuration.

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** None.

This example shows how to enables auto-RF once.

```
Device#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm txpower once
```

# ap filter

To configure the AP filter and set the priority, use the **ap filter** command.

```
ap filter { { namefilter-name } | { priority priority-number | filter-name filter-name } }
```

Syntax Description	Parameter	Description
	<b>priority</b>	Set the priority for a name filter.
	<i>priority-number</i>	The valid AP filter priority range is 0 to 127.
	<i>filter-name</i>	Enter the name for the ap filter.
<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration (config)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

## Examples

The following example shows how to create a ap filter and set the priority to this filter:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap filter namep-filter-name1
Device(config-aaa-policy)# aaa-realm enable
```

# ap fra

To configure flexible radio assignment (FRA) and its parameters, use the **ap fra** command.

**ap fra** [{**interval** *no-of-hours* | **sensitivity** {**high** | **low** | **medium**} | **sensor-threshold** {**balanced** | **client-preferred** | **client-priority** | **sensor-preferred** | **sensor-priority**} | **service-priority** {**coverage** | **service-assurance**}]

Syntax Description		
<b>interval</b> <i>no-of-hours</i>		Enter the number of hours for the FRA interval. Valid range is 1 to 24 hours.
<b>sensitivity</b> { <b>high</b>   <b>low</b>   <b>medium</b> }		Configures the FRA coverage overlap sensitivity as high, low, or medium.
<b>sensor-threshold</b> { <b>balanced</b>   <b>client-preferred</b>   <b>client-priority</b>   <b>sensor-preferred</b>   <b>sensor-priority</b> }		Configures FRA sensor threshold to one of the available options.
<b>service-priority</b> { <b>coverage</b>   <b>service-assurance</b> }		Configures FRA service priority to Coverage or Service Assurance.

**Command Default** None

**Command Modes** config

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

**Usage Guidelines** Ensure that the RF group leader for 802.11b/g and 802.11a bands are same across RF domain and make sure that the RF group leader has FRA enabled.

## Examples

The following example show how to configure the FRA interval to 8 hours:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap fra interval 8
```

## ap image predownload

To instruct all APs to start image predownload, use the **ap image predownload** command.

**ap image predownload** { **abort** | **site-tag** *site-tag-name* **start** }

Syntax Description		
<b>abort</b>	Instructs all the APs to abort image predownload.	
<b>site-tag</b>	Initiates image predownload parameters.	
<i>site-tag-name</i>	Specifies the site-tag name.	
<b>start</b>	Starts image predownload.	
Command Default	None	
Command Modes	Privileged EXEC (#)	
Command History	Release	Modification
	Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

### Example

This example shows how the APs are instructed to start image predownload:

```
Device#ap image download site-tag site-tag-name start
```



## ap name antenna band mode

To configure the antenna mode, use the **ap name***ap-name* **antenna-band-mode**{ **single** | **dual** } command.

**ap name***ap-name* **antenna-band-mode**{**single** | **dual**}

---

**Syntax Description**

*ap-name* Name of the Cisco lightweight access point.

**antenna-band-mode** Instructs the access point to enable the band mode of antenna.

---

**Command Default**

None

**Example**

This example shows how to configure the antenna band mode of access point.

```
Device# ap name <ap-name> antenna-band-mode single
```

## ap name ble

To enable the able ltx state on the AP, use the **ap name** *ap name* **ble** command.

**ap name** *ap\_name* **antenna-band-mode** {**admin** | **ibeacon** | **interval** | **no-advertisement** | **sync** | **vibeacon**}

Syntax Description	ap name	AP Name
	<b>admin</b>	Enables the ble ltx admin state.
	<b>ibeacon</b>	Enables the BLE LTX iBeacon configuration.
	<b>interval</b>	Enables the BLE LTX scan configuration interval.
	<b>no-advertisement</b>	Enables the BLE LTX No Advertisement.
	<b>Sync</b>	Enables the BLE LTX synchronize.
	<b>vibeacon</b>	Enables the BLE LTX viBeacon configuration.

**Command Default** Disabled

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

### Examples

The following example shows how to enable ble on the AP:

```
Device# ap name test ble
```

## ap name clear-personal-ssid

To clear the personal SSID from a Cisco OfficeExtend Access Point (OEAP), use the **ap name clear-personal-ssid** command.

**ap name** *ap-name* **clear-personal-ssid**

<b>Syntax Description</b>	<i>ap-name</i> AP name.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

### Examples

The following example shows how to clear the personal SSID from a Cisco OEAP:

```
Device# ap name my-oeap clear-personal-ssid
```

## ap name controller

To configure the controller on the AP, use the **ap name** *ap name* **controller** command.

**ap name** *ap\_name* **controller** {**primary** | **secondary** | **tertiary**} *name* {*A.B.C.D* / *X:X:X:XX*}

### Syntax Description

<b>ap name</b>	AP Name
<b>controller</b>	Configures the controller.
<b>primary</b>	Configures the primary controller.
<b>secondary</b>	Configures the secondary controller.
<b>tertiary</b>	Configures the tertiary controller.
<i>name</i>	Specifies the name of the primary controller, secondary controller, or tertiary controller.
<i>A.B.C.D</i>	Specifies the IPv4 address of the primary controller, secondary controller, or tertiary controller.
<i>X:X:X:XX</i>	Specifies the IPv6 address of the primary controller, secondary controller, or tertiary controller.

### Command Default

Disabled

### Command Modes

Privileged EXEC (#)

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

### Examples

The following example shows how to configure the controller on the AP:

```
Device# ap name cisco-ap controller primary cisco-primary-controller 10.1.1.1
```

## ap name country

To configure the country of operation for a Cisco lightweight access point, use the **ap name country** command.

```
ap name ap-name country country-code
```

Syntax Description	
<i>ap-name</i>	Name of the Cisco lightweight access point.
<i>country-code</i>	Two-letter or three-letter country code.

Command Default	None
-----------------	------

Command History	Release	Modification
		This command was introduced.

**Usage Guidelines**

Cisco devices must be installed by a network administrator or qualified IT professional and the installer must select the proper country code. Following installation, access to the unit should be password protected by the installer to maintain compliance with regulatory requirements and to ensure proper unit functionality. See the related product guide for the most recent country codes and regulatory domains. Also, access point regulatory domains are defined during the access point manufacturing process. You can change the access point country code if the new country code matches a country that is valid within the access point regulatory domain. If you try to enter a country that is not valid to the access point regulatory domain, the command fails.

This example shows how to configure the Cisco lightweight access point's country code to DE:

```
Device# ap name AP2 country JP
```

## ap name crash-file

To manage crash data and radio core files for the Cisco access point, use the **ap name crash-file** command.

**ap name** *ap-name* **crash-file** {**get-crash-data** | **get-radio-core-dump** {**slot 0** | **slot 1**}}

### Syntax Description

<i>ap-name</i>	Name of the Cisco lightweight access point.
<b>get-crash-data</b>	Collects the latest crash data for a Cisco lightweight access point.
<b>get-radio-core-dump</b>	Gets a Cisco lightweight access point's radio core dump
<b>slot</b>	Slot ID for Cisco access point.
<b>0</b>	Specifies Slot 0.
<b>1</b>	Specifies Slot 1.

### Command Default

None

### Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

This example shows how to collect the latest crash data for access point AP3:

```
Device# ap name AP3 crash-file get-crash-data
```

This example shows how to collect the radio core dump for access point AP02 and slot 0:

```
Device# ap name AP02 crash-file get-radio-core-dump slot 0
```

## ap name dot11 24ghz slot 0 SI

To enable Spectrum Intelligence (SI) for the dedicated 2.4-GHz radio hosted on slot 0 for a specific access point, use the **ap name dot11 24ghz slot 0 SI** command.

**ap name** *ap-namedot11* { **24ghz** | **5ghz** | **dual-band** | **rx-dual-band** } *slot slot ID* **SI**

### Syntax Description

*ap\_name* Name of the Cisco Access Point.

**slot 0** Enables Spectrum Intelligence (SI) for the dedicated 2.4-GHz radio hosted on slot 0 for a specific access point.

Here, 0 refers to the Slot ID.

### Command Default

None

### Command Modes

Privileged EXEC (#)

### Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

### Example

The following example shows how to configure Spectrum Intelligence of an AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 SI
```

## ap name dot11 24ghz slot antenna

To configure the 802.11b antenna hosted on slot 0, use the **ap name dot11 24ghz slot antenna** command.

**ap name** *ap-name***dot1124ghzslot 0antenna** { **ext-ant-gain** *antenna-gain-value* | **selection** [**internal** | **external**] }

Syntax Description	
<b>ap-name</b>	Name of the AP.
<b>24ghz</b>	Configures 802.11b parameters.
<b>slot</b>	Sets the slot ID for the Cisco Access Point.
<b>antenna</b>	Configures the 802.11b Antenna.
<b>ext-ant-gain</b>	Configures the 802.11b External Antenna Gain. The value range is 0 - 4294967295. Enter External Antenna Gain value in multiple of .5 dBi units (i.e. An integer value 4 means 4 x 0.5 = 2 dBi of gain)
<b>selection</b>	Configure the 802.11b Antenna selection (internal/external)

**Command Default** None

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

### Usage Guidelines

#### Example

The following example shows how to configure the channel width of an AP.

```
Device# ap name ax1 dot11 24ghz slot 0 antenna selection external
```



## ap name dot11 24ghz slot beamforming

To configure beamforming for the 2.4-GHz radio hosted on slot 0 for a specific access point, use the **ap name dot11 24ghz slot beamforming** command.

**ap name** *ap-name***dot1124ghzslot 0beamforming**

<b>Syntax Description</b>	<b>beamforming</b> Enable 802.11b tx beamforming - 5 GHz
---------------------------	----------------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

### Usage Guidelines

#### Example

The following example shows how to configure beamforming of an AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 beamforming
```

## ap name dot11 24ghz slot channel

To configure advanced 802.11 channel assignment parameters for Cisco AP, use the **ap name dot11 24ghz slot channel** command.

```
ap name ap-name dot11 24ghz slot 0 channel { channel_number | auto }
```

Syntax Description	
<i>channel_number</i>	Advanced 802.11 channel assignment parameters for Cisco AP. Enter a channel number from 1 - 14.
<b>auto</b>	Enables auto RF.

Command Default	
	None

Command Modes	
	Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

### Usage Guidelines

#### Example

The following example shows how to configure the channel of an AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 channel auto
```

## ap name dot11 24ghz slot cleanair

To enable CleanAir for 802.11b radio hosted on slot 0 for a specific access point, use the **ap name dot11 24ghz slot cleanair** command.

**ap name** *ap-name* **dot11 24ghz slot 0 cleanair**

<b>Syntax Description</b>	<b>cleanair</b> Enables 802.11b cleanair management				
<b>Command Default</b>	None				
<b>Command Modes</b>	Privileged EXEC (#)				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE 16.12.1	This command was introduced.				

### Example

The following example shows how to configure the cleanair of an AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 cleanair
```

## ap name dot11 24ghz slot dot11n antenna

To configure 802.11n antenna for 2.4-GHz radio hosted on slot 0 for a specific access point, use the **ap name dot11 24ghz slot dot11n antenna** command.

**ap name** *ap-name* **dot11 24ghz slot 0 dot11n antenna** { **A** | **B** | **C** | **D** }

<b>Syntax Description</b>	<b>dot11n</b> Configures 802.11n antenna for 2.4-GHz radio hosted on slot 0 for a specific access point.
	<b>antenna</b> Configures the 802.11n - 2.4 GHz antenna selection from antenna ports A, B, C, and D.

**Command Default** None

**Command Modes** Privileged EXEC (#)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

### Example

The following example shows how to configure the channel width of an AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 dot11n antenna A
```

## ap name dot11 24ghz slot dot11ax bss-color

To set the BSS color on the 2.4 GHz, 5 GHz, or dual-band radio, for a specific access point, use the **ap name dot11 24ghz slot dot11ax bss-color** command.

**ap name** *ap-name* **dot11 24ghz slot 0 dot11ax bss-color** <1-63>

<b>Syntax Description</b>	<b>bss-color</b> Configures 802.11ax-2.4GHz BSS color				
<b>Command Default</b>	None				
<b>Command Modes</b>	Privileged EXEC (#)				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE 16.12.1	This command was introduced.				

### Example

The following example shows how to disable 802.11b radio on Cisco AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 dot11ax bss-color 3
```

## ap name dot11 24ghz slot shutdown

To disable 802.11b radio hosted on slot 0 for a specific access point, use the **ap name dot11 24ghz slot shutdown** command.

**ap name** *ap-name* **dot11 24ghz slot 0 shutdown**

<b>Syntax Description</b>	<b>shutdown</b> Disables 802.11b radio on Cisco AP				
<b>Command Default</b>	None				
<b>Command Modes</b>	Privileged EXEC (#)				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE 16.12.1	This command was introduced.				

### Example

The following example shows how to disable 802.11b radio on Cisco AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 shutdown
```

## ap name dot11 dual-band cleanair

To configure CleanAir for a dual band radio, use the **ap name dot11 dual-band cleanair** command.

```
ap name ap-name dot11 dual-band cleanair
ap name ap-name no dot11 dual-band cleanair
```

<b>Syntax Description</b>	<i>ap-name</i> Name of the Cisco AP.				
	<b>cleanair</b> Specifies the CleanAir feature.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Privileged EXEC				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.				

This example shows how to enable CleanAir for a dual band radio of the access point AP01:

```
Device# ap name AP01 dot11 dual-band cleanair
```

## ap name dot11 dual-band shutdown

To disable dual band radio on a Cisco AP, use the **ap name dot11 dual-band shutdown** command.

**ap name** *ap-name* **dot11 dual-band shutdown**  
**ap name** *ap-name* **no dot11 dual-band shutdown**

<b>Syntax Description</b>	<i>ap-name</i> Name of the Cisco AP.
	<b>shutdown</b> Disables the dual band radio on the Cisco AP.
<b>Command Default</b>	None
<b>Command Modes</b>	Privileged EXEC
<b>Command History</b>	<b>Release</b>
	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1 This command was introduced.

This example shows how to disable dual band radio on the Cisco access point AP01:

```
Device# ap name AP01 dot11 dual-band shutdown
```



## ap name dot11 rrm profile

To configure Radio Resource Management (RRM) performance profile settings for a Cisco lightweight access point, use the **ap name dot11 rrm profile** command.

```
ap name ap-name dot11 {24ghz | 5ghz} rrm profile {clients value | customize | foreign value |
noise value | throughput value | utilization value}
```

Syntax	Description
<i>ap-name</i>	Name of the Cisco lightweight access point.
<b>24ghz</b>	Specifies the 2.4 GHz band.
<b>5ghz</b>	Specifies the 5 GHz band.
<b>clients</b>	Sets the access point client threshold.
<i>value</i>	Access point client threshold from 1 to 75 clients. <b>Note</b> The default client threshold is 12.
<b>customize</b>	Turns on performance profile customization for an access point. <b>Note</b> Performance profile customization is off by default.
<b>foreign</b>	Sets the foreign 802.11 transmitter interference threshold.
<i>value</i>	Foreign 802.11 transmitter interference threshold from 0 to 100 percent. <b>Note</b> The default is 10 percent.
<b>noise</b>	Sets the 802.11 foreign noise threshold.
<i>value</i>	802.11 foreign noise threshold between -127 and 0 dBm. <b>Note</b> The default is -70 dBm.
<b>throughput</b>	Sets the data-rate throughput threshold.
<i>value</i>	802.11 throughput threshold from 1000 to 10000000 bytes per second. <b>Note</b> The default is 1,000,000 bytes per second.
<b>utilization</b>	Sets the RF utilization threshold. <b>Note</b> The operating system generates a trap when this threshold is exceeded.
<i>value</i>	802.11 RF utilization threshold from 0 to 100 percent. <b>Note</b> The default is 80 percent.

---

**Command Default**      None

---

**Command History**

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

---

This example shows how to set the AP1 clients threshold to 75 clients:

```
Device# ap name AP1 dot11 24ghz rrm profile clients 75
```

This example shows how to turn performance profile customization on for 802.11a Cisco lightweight access point AP1:

```
Device# ap name AP1 dot11 5ghz rrm profile customize
```

This example shows how to set the foreign 802.11a transmitter interference threshold for AP1 to 0 percent:

```
Device# ap name AP1 dot11 5ghz rrm profile foreign 0
```

This example shows how to set the 802.11a foreign noise threshold for AP1 to 0 dBm:

```
Device# ap name AP1 dot11 5ghz rrm profile noise 0
```

This example shows how to set the AP1 data-rate threshold to 10000000 bytes per second:

```
Device# ap name AP1 dot11 5ghz rrm profile throughput 10000000
```

This example shows how to set the RF utilization threshold for AP1 to 100 percent:

```
Device# ap name AP1 dot11 5ghz rrm profile utilization 100
```

## ap name image

To configure an image on a specific access point, use the **ap name image** command.

```
ap name ap-name image {predownload | swap}
```

<b>Syntax Description</b>	<i>ap-name</i>	Name of the Cisco lightweight access point.
	<b>predownload</b>	Instructs the access point to start the image predownload.
	<b>swap</b>	Instructs the access point to swap the image.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
		This command was introduced.

This example shows how to predownload an image to an access point:

```
Device# ap name AP2 image predownload
```

This example shows how to swap an access point's primary and secondary images:

```
Device# ap name AP2 image swap
```

## ap name indoor

To enable the access point in the indoor mode, use the **ap name** *ap name* **indoor** command.

**ap name** *ap\_name* **indoor**

<b>Syntax Description</b>	<b>ap name</b> AP Name
	<b>indoor</b> Enables the access point in the indoor mode.

**Command Default** None

**Command Modes** Privileged EXEC (#)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

### Examples

The following example shows how to enable the access point in the indoor mode:

```
Device# ap name test indoor
```

## ap name ipsla

To configure ipsla on the AP, use the **ap name** *ap\_name* **ipsla** command.

**ap name** *ap\_name* **ipsla**

<b>Syntax Description</b>	<b>ap name</b> AP Name
	<b>ipsla</b> Enables the ipsla on the access point.

**Command Default** None

**Command Modes** Privileged EXEC (#)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

### Examples

The following example shows how to configure ipsla on the access point:

```
Device# ap name test ipsla
```

## ap name keepalive

To enable the keepalive option on the AP, use the **ap name** *ap\_name* **keepalive** command.

**ap name** *ap\_name* **keepalive**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 17.03.1	This command was introduced.

### Examples

The following example shows how to enable the keepalive option on the AP:

```
Device# ap name test keepalive
```

## ap name lan

To configure LAN port configurations for APs, use the **ap name lan** command. To remove LAN port configurations for APs, use the **ap name no lan** command.

**ap name** *ap-name* [ **no** ] **lan port-id** *port-id* { **shutdown** | **vlan-access** }

Syntax Description		
<b>no</b>		Removes LAN port configurations.
<b>port-id</b>		Configures the port.
<i>port-id</i>		The ID of the port. The range is 1-4
<b>shutdown</b>		Disables the Port.
<b>vlan-access</b>		Enables VLAN access to Port.

**Command Default** None

**Command Modes** Privileged EXEC(#)

This example shows how to enable VLAN access to port:

```
Device# ap name AP1 lan port-id 1 vlan-access
```

## ap name led

To enable the LED state for an access point, use the **ap name led** command. To disable the LED state for an access point, use the **no** form of this command.

```
ap name ap-name led
no ap name ap-name [led] led
```

### Syntax Description

*ap-name* Name of the Cisco lightweight access point.

**led** Enables the access point's LED state.

### Command Default

None

### Command History

#### Release

#### Modification

This command was introduced.

This example shows how to enable the LED state for an access point:

```
Device# ap name AP2 led
```

This example shows how to disable the LED state for an access point:

```
Device# ap name AP2 no led
```



## ap name led-brightness-level

To configure the LED brightness level on the AP, use the **ap name** *ap\_name* **led-brightness-level** command.

**ap name** *ap\_name* **led-brightness-level** {1–8}

<b>Syntax Description</b>	<b>ap name</b>	AP Name
	<b>led brightness level</b>	Configures the led brightness level.
	<b>Note</b>	Valid led brightness level is from 1 to 8.
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC (#)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

### Examples

The following example shows the LED brightness level on the access point:

```
Device# ap name cisco-ap led-brightness-level2
```

## ap name location

To modify the descriptive location of a Cisco lightweight access point, use the **ap name location** command.

**ap name** *ap-name* **location** *location*

### Syntax Description

*ap-name* Name of the Cisco lightweight access point.

*location* Location name of the access point (enclosed by double quotation marks).

### Command Default

None

### Command History

#### Release

#### Modification

This command was introduced.

### Usage Guidelines

The Cisco lightweight access point must be disabled before changing this parameter.

This example shows how to configure the descriptive location for access point AP1:

```
Device# ap name AP1 location Building1
```

## ap name mdsn-ap

To configure mdsn-ap on the AP, use the **ap name** *ap name* **mdsn-ap** command.

**ap name** *ap\_name* **mdsn-ap** {**disable** | **enable** | **vlan**} *add delete*

Syntax Description	
<b>ap name</b>	AP Name
<b>disable</b>	Disables the mDNS access point.
<b>enable</b>	Enables the mDNS access point.
<b>vlan</b>	Adds or deletes the VLAN from mDNS access point.
<i>add</i>	Adds vlan to mDNS AP.
<i>delete</i>	Deletes vlan from the mDNS AP.

**Command Default** None

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

### Examples

The following example shows how to enable mdns on the AP:

```
Device# Device# ap name test mdns enable
```

## ap name name new-ap-name

To configure the new Cisco AP name, use the **ap name** *ap\_name* **name** *new-ap-name* command.

**ap name** *ap\_name* **name** *new-ap-name*

Syntax Description	
<b>ap name</b>	AP Name
<b>name</b>	Specifies the new Cisco AP name.

**Command Default** None

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

### Examples

The following example shows how to configure the new Cisco AP:

```
Device# ap name test name test2
```

## ap name no

To negate a command or set its defaults on the AP, use the **no** command.

**ap name** *ap\_name* **no**

<b>Syntax Description</b>	<b>ap name</b> AP Name
	<b>no</b> Negate a command or set its defaults.

**Command Default** None

**Command Modes** Privileged EXEC (#)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

### Examples

The following example shows how to negate a command or set its defaults on the AP:

```
Device# ap name test no
```

## ap name monitor-mode dot11b

To configure 802.11b scanning channels for a monitor-mode access point, use the **ap name monitor-mode dot11b** command.

**ap name** *ap-name* **monitor-mode dot11b fast-channel** *channel1* [*channel2*] [*channel3*] [*channel4*]

### Syntax Description

<i>ap-name</i>	Name of the access point.
<b>fast-channel</b>	Specifies the 2.4 GHz band scanning channel (or channels) for a monitor-mode access point.
<i>channel1</i>	Scanning channel1.
<i>channel2</i>	(Optional) Scanning channel2.
<i>channel3</i>	(Optional) Scanning channel3.
<i>channel4</i>	(Optional) Scanning channel4.

### Command Default

None

### Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

This example shows how to configure an access point in tracking optimized mode to listen to channels 1, 6, and 11:

```
Device# ap name AP01 monitor-mode dot11b fast-channel 1 6 11
```

## ap name name

To modify the name of a Cisco lightweight access point, use the **ap name name** command.

```
ap name ap-name name new-name
```

---

### Syntax Description

*ap-name* Current Cisco lightweight access point name.

*new-name* Desired Cisco lightweight access point name.

---

### Command Default

None

---

### Command History

#### Release

#### Modification

This command was introduced.

---

This example shows how to modify the name of access point AP1 to AP2:

```
Device# ap name AP1 name AP2
```

## ap name network-diagnostics

To trigger network diagnostics on an OfficeExtend AP, use the **ap name network-diagnostics** command.

**ap name** *ap-name* **network-diagnostics**

<b>Syntax Description</b>	<i>ap-name</i> Name of the access point.
<b>Command Default</b>	None
<b>Command Modes</b>	Privileged EXEC (#)
<b>Command History</b>	<b>Release</b>
	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.5.1 This command was introduced.

### Example

The following example shows how to trigger network diagnostics on an OfficeExtend AP.

```
Device# ap name ap18 network-diagnostics
```



## ap name priority

To configure the priority of an access point, use the **ap name priority** command.

**ap name** *ap-name* **priority** *priority-value*

<b>Syntax Description</b>	<i>priority-value</i> Priority value for the AP. Valid range is 1 to 4.
---------------------------	-------------------------------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

### Examples

The following example shows how to configure the priority for an access point:

```
Device# ap name my-ap priority 1
```

## ap name reset

To reset a specific Cisco lightweight access point, use the **ap name reset** command.

**ap name** *ap-name* **reset**

<b>Syntax Description</b>	<i>ap-name</i> Name of the Cisco lightweight access point.				
<b>Command Default</b>	None				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td></td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification		This command was introduced.
Release	Modification				
	This command was introduced.				

This example shows how to reset a Cisco lightweight access point named AP2:

```
Device# ap name AP2 reset
```

## ap name reset-button

To configure the Reset button for an access point, use the **ap name reset-button** command.

**ap name** *ap-name* **reset-button**

<b>Syntax Description</b>	<i>ap-name</i> Name of the Cisco lightweight access point.
<b>Command Default</b>	None
<b>Command History</b>	<b>Release Modification</b> This command was introduced.

This example shows how to enable the Reset button for access point AP03:

```
Device# ap name AP03 reset-button
```

## ap name role

To configure the role of operation for an AP, use the **ap name role** command.

```
ap name ap-name role {mesh-ap | root-ap}
```

<b>Syntax Description</b>	<i>ap-name</i> Name of the AP.	
	<b>mesh-ap</b> Configures mesh AP role for the AP.	
	<b>root-ap</b> Configures root AP role for the AP.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

### Examples

The following example shows how to configure the role of operation as mesh AP for an AP:

```
Device# ap name mymeshap role mesh-ap
```

## ap name slot

To configure various slot parameters, use the **ap name slot** command. To disable a slot on a Cisco lightweight access point, use the **no** form of this command.

```
ap name ap-name slot slot-number {channel {global | number channel-number | width channel-width}
| rtsthreshold value | shutdown | txpower {globalchannel-level}}
ap name ap-name no slot {0 | 1 | 2 | 3} shutdown
```

Syntax Description					
<i>ap-name</i>	Name of the Cisco access point.				
<i>slot-number</i>	Slot downlink radio to which the channel is assigned. You can specify the following slot numbers: <ul style="list-style-type: none"> <li>• <b>0</b>—Enables slot number 0 on a Cisco lightweight access point.</li> <li>• <b>1</b>—Enables slot number 1 on a Cisco lightweight access point.</li> <li>• <b>2</b>—Enables slot number 2 on a Cisco lightweight access point.</li> <li>• <b>3</b>—Enables slot number 3 on a Cisco lightweight access point.</li> </ul>				
<b>channel</b>	Specifies the channel for the slot.				
<b>global</b>	Specifies channel global properties for the slot.				
<b>number</b>	Specifies the channel number for the slot.				
<i>channel-number</i>	Channel number from 1 to 169.				
<b>width</b>	Specifies the channel width for the slot.				
<i>channel-width</i>	Channel width from 20 to 40.				
<b>rtsthreshold</b>	Specifies the RTS/CTS threshold for an access point.				
<i>value</i>	RTS/CTS threshold value from 0 to 65535.				
<b>shutdown</b>	Shuts down the slot.				
<b>txpower</b>	Specifies Tx power for the slot.				
<b>global</b>	Specifies auto-RF for the slot.				
<i>channel-level</i>	Transmit power level for the slot from 1 to 7.				
<b>Command Default</b>	None				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td></td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification		This command was introduced.
Release	Modification				
	This command was introduced.				

This example shows how to enable slot 3 for the access point abc:

```
Device# ap name abc slot 3
```

This example shows how to configure RTS for the access point abc:

```
Device# ap name abc slot 3 rtsthreshold 54
```

## ap name static-ip

**ap name** *Cisco-ap-name***static-ipip-address** { **A.B.C.D***netmask**netmask*  
| **X:X:X:X::X***prefix**prefix-length* } **gateway***gateway*

Syntax Description	ap name	Name of the Cisco access point.
	static-ip	Sets the Cisco AP static IP address configuration.
	ip-address	Adds the Cisco AP static IP address.
	A.B.C.D	Indicates the IPv4 address.
	X:X:X:X::X	Indicates the IPv6 address.
	netmask	<i>netmask</i> Specifies the Cisco AP static-IP netmask.
	prefix	<i>prefix-length</i> Specifies the Cisco AP static-IP prefix length.
	gateway	<i>gateway</i> Specifies the Cisco AP static-IP gateway.

**Command Default** None

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

The following example shows how to enable or disable static-ip for an access point:

```
Device#ap name cisco-ap-name static-ip ip-address 9.9.9.2 netmask 255.0.0.0 gateway 9.9.9.2
```

## ap name static-ip

To configure lightweight access point static IP settings, use the **ap name static-ip** command. To disable the Cisco lightweight access point static IP address, use the **no** form of this command.

```
ap name ap-name static-ip {domain domain-name | ip-address ip-address netmask netmask gateway
gateway | nameserver ip-address}
ap name ap-name no static-ip
```

Syntax Description		
	<i>ap-name</i>	Name of the access point.
	<b>domain</b>	Specifies the Cisco access point domain name.
	<i>domain-name</i>	Domain to which a specific access point belongs.
	<b>ip-address</b>	Specifies the Cisco access point static IP address.
	<i>ip-address</i>	Cisco access point static IP address.
	<b>netmask</b>	Specifies the Cisco access point static IP netmask.
	<i>netmask</i>	Cisco access point static IP netmask.
	<b>gateway</b>	Specifies the Cisco access point gateway.
	<i>gateway</i>	IP address of the Cisco access point gateway.
	<b>nameserver</b>	Specifies a DNS server so that a specific access point can discover the device using DNS resolution.
	<i>ip-address</i>	IP address of the DNS server.

**Command Default** None

Command History	Release	Modification
		This command was introduced.

**Usage Guidelines** An access point cannot discover the device using Domain Name System (DNS) resolution if a static IP address is configured for the access point unless you specify a DNS server and the domain to which the access point belongs.

This example shows how to configure an access point static IP address:

```
Device# ap name AP2 static-ip ip-address 192.0.2.54 netmask 255.255.255.0 gateway 192.0.2.1
```



## ap name shutdown

To disable a Cisco lightweight access point, use the **ap name shutdown** command. To enable a Cisco lightweight access point, use the **no** form of this command.

```
ap name ap-name shutdown
ap name ap-name no shutdown
```

---

### Syntax Description

*ap-name* Name of the Cisco lightweight access point.

---

### Command Default

None

---

### Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

---

This example shows how to disable a specific Cisco lightweight access point:

```
Device# ap name AP2 shutdown
```

## ap name usb-module

To enable the USB port on the access point (AP), use the **ap name** *ap-name* **usb-module**. To disable the feature, use the **no** form of this command.

**ap name** *ap-name* **usb-module**

**no ap name** *ap-name* **usb-module**

<b>Syntax Description</b>	<b>usb-module</b> Enables the USB port on the AP.
---------------------------	---------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC mode
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.4.1	This command was introduced.

<b>Usage Guidelines</b>	None
-------------------------	------

### Example

This example shows you how to enable the USB port on the AP:

```
Device# ap name ap-name usb-module
```

## ap name usb-module override

To enable access point (AP) USB override, use the **ap name *ap-name* usb-module override** command. To disable the feature, use the **no** form of this command.

**ap name *ap-name* usb-module override**

**no ap name *ap-name* usb-module override**

<b>Syntax Description</b>	<b>usb-module override</b> Overrides USB status of the AP profile and considers the local AP configuration. You can configure the USB status for an AP only if you enable USB override for it.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Privileged EXEC mode				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Bengaluru 17.4.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Bengaluru 17.4.1	This command was introduced.
Release	Modification				
Cisco IOS XE Bengaluru 17.4.1	This command was introduced.				
<b>Usage Guidelines</b>	None				

### Example

This example shows you how to override USB status of the AP:

```
Device# ap name ap-name usb-module override
```

## ap name vlan-tag

To configure VLAN tagging for a nonbridge AP, use the **ap name vlan-tag** command.

**ap name** *ap-name* **vlan-tag** *vlan-id*

Syntax Description	
	<i>ap-name</i> Access point name.
	<i>vlan-id</i> VLAN identifier.

**Command Default** VLAN tagging is not enabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

### Example

The following example shows how to configure VLAN tagging for a nonbridge AP:

```
Device# ap name AP1 vlan-tag 12
```

## ap name write tag-config

To write the existing configuration to an AP, use the **ap name write tag-config** command in privileged EXEC mode

**ap name** *ap-name* **write tag-config**

<b>Syntax Description</b>	<i>ap-name</i> Name of the access point.	
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.
<b>Usage Guidelines</b>	Use this command to write the existing configuration to an AP.	

### Example

This example shows how to write the existing configuration to an AP:

```
Device# ap name AP40CE.2485.D594 write tag-config
```

## ap name-regex

To configure filter based on AP name regular expression to match with, use the **ap name-regex** command.

**ap name-regex** *regular-expression*

<b>Syntax Description</b>	<i>regular-expression</i> Enter the filter string.
---------------------------	----------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

### Examples

The following example shows how to configure filter based on AP name regular expression match with:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap filter name filter--name
Device(config-ap-filter)# ap name-regex regular-expression-string
```

# ap profile

To configure access point profile, use the **ap profile** command.

```
ap profile profile-name
```

---

<b>Syntax Description</b>	<i>profile-name</i> Enter the name of the AP profile.
---------------------------	-------------------------------------------------------

---

---

<b>Command Default</b>	By default, the AP profile name is default-ap-profile.
------------------------	--------------------------------------------------------

---

---

<b>Command Modes</b>	Global configuration (config)
----------------------	-------------------------------

---

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

---

## Examples

The following example shows how to configure AP profile name:

```
Device# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Device(config)# ap profile my-ap-profile
```

## ap remote-lan profile-name

To configure remote LAN profile, use the **ap remote-lan profile-name** command.

**ap remote-lan profile-name** *remote-lan-profile-name rlan-id*

Syntax Description	remote-lan-profile-name
	Is the remote LAN profile name. Range is from 1 to 32 alphanumeric characters.
rlan-id	Is the remote LAN identifier. Range is from 1 to 128.
	<p><b>Note</b> You can create a maximum of 128 RLANs. You cannot use the <i>rlan-id</i> of an existing RLAN while creating another RLAN.</p> <p>Both RLAN and WLAN profile cannot have the same names. Similarly, RLAN and WLAN policy profile cannot have the same names.</p>

**Command Default** None

**Command Modes** Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

This example shows how to configure remote LAN profile:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap remote-lan profile-name rlan_profile_name 3
```



# ap remote-lan shutdown

To enable or disable all RLANs, use the **ap remote-lan shutdown** command.

**ap remote-lan shutdown**

---

**Command Default**      None

---

**Command Modes**        Global configuration (config)

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

---

## Example

This example shows how to enable or disable all RLANs:

```
Device# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Device(config)# [no] ap remote-lan shutdown  
Device(config)# end
```

## ap remote-lan-policy policy-name

To configure RLAN policy profile, use the **ap remote-lan-policy policy-name** command.

**ap remote-lan-policy policy-name** *profile-name*

---

**Command Default**      None

---

**Command Modes**      Global configuration (config)

---

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

---

### Example

This example shows how to configure RLAN policy profile:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap remote-lan-policy policy-name rlan_policy_prof_name
```

## ap tag-source-priority

To configure ap tag source priority, use the **ap tag-source-priority** command.

**ap tag-source-priority** *source-priority* **source** { **filter** | **ap** }

<b>Syntax Description</b>	<i>source-priority</i>	Enter the ap tag source priority. Valid range is 2 to 3.
	<b>source</b>	Specify the source for which priority is been set.
	<b>filter</b>	AP filter as tag source.
	<b>ap</b>	AP as tag source.
<b>Command Default</b>	None	
<b>Command Modes</b>	config	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

### Examples

The following example shows how to set AP as a tag source:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap tag-source-priority priority-value source ap
```

## ap tag-sources revalidate

To revalidate the access point tag sources, use the **ap tag-sources revalidate** command.

**ap tag-sources revalidate**

<b>Syntax Description</b>	<b>tag-sources</b> Tag Sources.
	<b>revalidate</b> Revalidate access point tag sources.

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

### Examples

The following example shows how to revalidate the access point tag sources:

```
Device# ap tag-sources revalidate
```

## ap vlan-tag

To configure VLAN tagging for all nonbridge APs, use the **ap vlan-tag** command.

```
ap vlan-tag vlan-id
```

<b>Syntax Description</b>	<i>vlan-id</i> VLAN identifier.				
<b>Command Default</b>	VLAN tagging is not enabled for nonbridge APs.				
<b>Command Modes</b>	Privileged EXEC				
<b>Command History</b>	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE 16.12.1</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE 16.12.1	This command was introduced.				

### Example

The following example shows how to configure VLAN tagging for all non-bridge APs:

```
Device# ap vlan-tag 1000
```

# assisted-roaming

To configure assisted roaming using 802.11k on a WLAN, use the **assisted-roaming** command. To disable assisted roaming, use the **no** form of this command.

**assisted-roaming** {**dual-list** | **neighbor-list** | **prediction**}

**no assisted-roaming** {**dual-list** | **neighbor-list** | **prediction**}

<b>Syntax Description</b>	<b>dual-list</b>	Configures a dual band 802.11k neighbor list for a WLAN. The default is the band that the client is currently associated with.
	<b>neighbor-list</b>	Configures an 802.11k neighbor list for a WLAN.
	<b>prediction</b>	Configures assisted roaming optimization prediction for a WLAN.
<b>Command Default</b>	Neighbor list and dual band support are enabled by default. The default is the band that the client is currently associated with.	
<b>Command Modes</b>	WLAN configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
<b>Usage Guidelines</b>	When you enable the assisted roaming prediction list, a warning appears and load balancing is disabled for the WLAN if load balancing is already enabled on the WLAN. To make changes to the WLAN, the WLAN must be in disabled state.	

## Example

The following example shows how to configure a 802.11k neighbor list on a WLAN:

```
Device(config-wlan)#assisted-roaming neighbor-list
```

The following example shows the warning message when load balancing is enabled on a WLAN.

Load balancing must be disabled if it is already enabled when configuring assisted roaming:

```
Device(config)#wlan test-prediction 2 test-prediction
Device(config-wlan)#client vlan 43
Device(config-wlan)#no security wpa
Device(config-wlan)#load-balance
Device(config-wlan)#assisted-roaming prediction
WARNING: Enabling neighbor list prediction optimization may slow association and impact
VOICE client perform.
Are you sure you want to continue? (y/n)[y]: y
% Request aborted - Must first disable Load Balancing before enabling Assisted Roaming
Prediction Optimization on this WLAN.
```

## avg-packet-size packetsize

To configure the wireless media-stream's average packet size, use the **avg-packet-size** command.

**avg-packet-size** *packetsize-value*

<b>Syntax Description</b>	<i>packetsize-value</i> Average Packet Size. Valid range is 100 to 1500.				
<b>Command Default</b>	None				
<b>Command Modes</b>	media-stream				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE 16.12.1	This command was introduced.				

### Examples

The following example shows how to configure wireless media-stream's average packet size:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless media-stream group doc-grp 224.0.0.0 224.0.0.223
Device(config-media-stream)# avg-packet-size500
```

# band-select client

To configure the client threshold minimum dB for the selected band, use the **band-select client** command. To reset the client threshold minimum dB for the selected band, use the **no** form of this command.

**band-select client** { **mid-rssi** | **rssi** } *dBm value*

Syntax Description	Parameter	Description
	<b>mid-rssi</b>	Minimum dBm of a client RSSI start to respond to probe
	<b>rssi</b>	Minimum dBm of a client RSSI to respond to probe
	<i>dBm value</i>	Minimum dBm of a client RSSI to respond to probe. Valid range is between -90 and -20 dBm.

**Command Default** None

**Command Modes** config-rf-profile

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

**Usage Guidelines** This command is enabled only for 2.4-GHz band.

This example shows how to set the client threshold to minimum dB for a selected band.

```
Device(config-rf-profile)#band-select client rssi -50
```



# band-select cycle

To configure the band cycle parameters, use the **band-select cycle** command. To reset the threshold value, use the **no** form of this command.

**band-select cycle** { **count** | **threshold** } *value*

Syntax Description	Parameter	Description
	<b>count</b>	Sets the Band Select probe cycle count.
	<i>value</i>	Maximum number of cycles not responding. The range is between 1 and 10.
	<b>threshold</b>	Sets the time threshold for a new scanning cycle.
	<i>value</i>	Set the threshold value in milliseconds. The valid is between 1 and 1000.

**Command Default** None

**Command Modes** config-rf-profile

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

**Usage Guidelines** None

This example shows how to configure the probe cycle count in an RF profile for a selected band.

```
Device(config-rf-profile)#band-select cycle count 5
```

# band-select expire

To configure the expiry time for the RF profile for the selected band, use the **band-select expire** command. To reset the value, use the **no** form of this command.

```
band-select expire { dual-band | suppression } value
no band-select expire { dual-band | suppression }
```

Syntax Description		
	<b>dual-band</b>	Configures the RF Profile Band Select Expire Dual Band.
	<i>value</i>	Setting the time to expire for pruning previously known dual-band clients. The range is between 10 and 300.
	<b>suppression</b>	Configures the RF Profile Band Select Expire Suppression.
	<i>value</i>	Setting the time to expire for pruning previously known 802.11b/g clients. The range is between 10 and 200.

**Command Default** None

**Command Modes** config-rf-profile

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

**Usage Guidelines** None

This example shows how to configure the time to expire for a dual-band of an RF profile in a selected band.

```
Device(config-rf-profile)#band-select expire dual-band 15
```

## band-select probe-response

To configure the probe responses to the clients for a selected band, use the **band-select probe-response** command. To disable the probe-response, use the **no** form of this command.

### band-select probe-response

<b>Syntax Description</b>	<b>probe-response</b>	Probe responses to clients.
<b>Command Default</b>	None	
<b>Command Modes</b>	config-rf-profile	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Denali 16.3.1	This command was introduced.
<b>Usage Guidelines</b>	None	
	This example shows how to enable probe response to the clients.	
	Device(config-rf-profile)# <b>band-select probe-response</b>	

## bss-transition

To configure BSS transition per WLAN, use the **bss-transition** command.

**bss-transition** [**disassociation-imminent**]

<b>Syntax Description</b>	<b>disassociation-imminent</b> BSS transition disassociation Imminent per WLAN.
---------------------------	---------------------------------------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	config-wlan
----------------------	-------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

### Example

The following example shows how to configure BSS transition per WLAN:

```
Device(config-wlan)# bss-transition
```

# call-snoop

**call-snoop**

**no call-snoop**

<b>Syntax Description</b>	This command has no keywords or arguments.	
<b>Command Default</b>	VoIP snooping is disabled by default.	
<b>Command Modes</b>	WLAN configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
<b>Usage Guidelines</b>	You must disable the WLAN before using this command. The WLAN on which call snooping is configured must be configured with Platinum QoS. You must disable quality of service before using this command.	

## Example

This example shows how to enable VoIP on a WLAN:

```
Device# configure terminal
Device(config)# wireless profile policy policy-name
Device(config-wireless-policy)#service-policy input platinum-up
Device(config-wireless-policy)#service-policy output platinum
Device(config-wireless-policy)#call-snoop
Device(config-wireless-policy)#no shutdown
Device(config-wireless-policy)#end
```

# captive-bypass-portal

To configure captive bypassing, use the **captive-bypass-portal** command.

## captive-bypass-portal

<b>Command Default</b>	None
<b>Command Modes</b>	Global configuration (config)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

## Example

This example shows how to configure captive bypassing for WLAN in LWA and CWA:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# parameter-map type webauth WLAN1_MAP
Device(config)# captive-bypass-portal
Device(config)# wlan WLAN1_NAME 4 WLAN1_NAME
Device(config-wlan)# security web-auth
Device(config-wlan)# security web-auth parameter-map WLAN1_MAP
Device(config-wlan)# end
```

# capwap-discovery

To set CAPWAP discovery response method as to whether a capwap-discovery response contains the public or private IP of the controller, use the **capwap-discovery** command.

**capwap-discovery** { **private** | **public** }

Syntax Description	
<b>private</b>	Includes private IP in CAPWAP discovery response.
<b>public</b>	Includes public IP in CAPWAP discovery response.

**Command Default** None

**Command Modes** Management Interface Configuration(config-mgmt-interface)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Usage Guidelines

### Example

The following example shows how to configure a CAPWAP discovery response method:

```
Device# configure terminal
Device(config)# wireless management interface Vlan1
Device(config-mgmt-interface)# capwap-discovery public
```

## capwap backup

To configure a primary or secondary backup device for all access points that are joined to a specific device, use the **capwap backup** command.

**capwap backup** {**primary** *primary-controller-name primary-controller-ip-address* | **secondary** *secondary-controller-name secondary-controller-ip-address*}

Syntax Description		
<b>primary</b>		Specifies the primary backup device.
<i>primary-controller-name</i>		Primary backup device name.
<i>primary-controller-ip-address</i>		Primary backup device IP address.
<b>secondary</b>		Specifies the secondary backup device.
<i>secondary-controller-name</i>		Secondary backup device name.
<i>secondary-controller-ip-address</i>		Secondary backup device IP address.

**Command Default** None

**Command Modes** AP profile configuration (config-ap-profile)

Command History	Release	Modification
	Cisco IOS XE 16.12.1	This command was introduced.

This example shows how to configure a primary backup device for all access points that are joined to a specific device:

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# capwap backup primary controller1 192.0.2.51
```

This example shows how to configure a secondary backup device for all access points that are joined to a specific device:

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# capwap backup secondary controller1 192.0.2.52
```



## cco-password (image-download-mode cco)

To configure the CCO server password for image download, use the **cco-password** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
cco-password {0 | 8} <Enter password> <Re-enter password>
```

```
no cco-password {0 | 8} <Enter password> <Re-enter password>
```

<b>Syntax Description</b>	<b>0</b>	Specifies that an unencrypted password will follow.
	<b>8</b>	Specifies that an AES encrypted password will follow.
	<i>password</i>	Specifies the CCO server password.
	<i>re-enter password</i>	Indicates that the user must re-enter the CCO server password.
<b>Command Default</b>	None	
<b>Command Modes</b>	Wireless image download profile CCO configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

### Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode cco
Device(config-wireless-image-download-profile-cco)# cco-password 0 xxxxxxxx
```

## cco-username (image-download-mode cco)

To configure the CCO username for image download, use the **cco-username** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
cco-username Username
```

```
no cco-username Username
```

<b>Syntax Description</b>	<i>username</i> Specifies the CCO username.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Wireless image download profile CCO configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Amsterdam 17.1.1s</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.
Release	Modification				
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.				

### Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode cco
Device(config-wireless-image-download-profile-cco)# cco-username cco-server-username
```

## cco-version (image-download-mode cco)

To configure and download the latest or the suggested version of the software image from CCO, use the **cco-version** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
cco-version {latest| suggested}
```

```
no cco-version {latest| suggested}
```

<b>Syntax Description</b>	<b>latest</b>	Configures and downloads the <b>latest</b> version of software image from CCO.
	<b>suggested</b>	Configures and downloads the <b>suggested</b> version of software image from CCO. By default <b>suggested</b> version is selected.
<b>Command Default</b>	None	
<b>Command Modes</b>	Wireless image download profile CCO configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

### Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode cco
Device(config-wireless-image-download-profile-cco)# cco-version suggested
```

## cco-auto-check (image-download-mode cco)

To enable automatic check of the new software version on CCO, use the **cco-auto-check** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
cco-auto-check
```

```
no cco-auto-check
```

<b>Syntax Description</b>	<b>cco-auto-check</b> Enables the automatic check of the new software version at CCO every 30 days. This is applicable to Image Upgrade or Predownload only. By default the command is enabled.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Wireless image download profile CCO configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Amsterdam 17.1.1s</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.
Release	Modification				
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.				

### Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode cco
Device(config-wireless-image-download-profile-cco)# cco-auto-check
```

## ccx aironet-iesupport

To configure the support of Aironet IE CCX option, use the following command:

```
ccx aironet-iesupport
```

<b>Syntax Description</b>	<b>ccx</b>	Configures the Cisco Client Extension options.
	<b>aironet-iesupport</b>	Sets the support of Aironet IE on WLAN.
<b>Command Default</b>	None	
<b>Command Modes</b>	WLAN configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

### Example

This example shows how to configure Aironet IE support:

```
Device(config-wlan)#ccx aironet-iesupport
```

# cdp

To enable the Cisco Discovery Protocol (CDP) on a Cisco lightweight access point under the AP profile, use the **cdp** command. To disable the Cisco Discovery Protocol (CDP) on a Cisco lightweight access point, use the **no** form of this command.

```
ap profile default-ap-profile
```

```
cdp
no cdp
```

---

**Command Default** Disabled on all access points.

---

**Command Modes** AP profile mode (config-ap-profile)

---

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

---



---

**Usage Guidelines** The **no cdp** command disables CDP on all access points that are joined to the device and all access points that join in the future. CDP remains disabled on both current and future access points even after the device or access point reboots. To enable CDP, enter the **cdp** command.




---

**Note** CDP over Ethernet/radio interfaces is available only when CDP is enabled. After you enable CDP on all access points joined to the device, you can disable and then reenables CDP on individual access points using the **ap name Cisco-AP cdp** command. After you disable CDP on all access points joined to the device, you can enable and then disable CDP on individual access points.

---

This example shows how to enable CDP on all access points:

```
Device(config)# ap profile default-ap-profile
```

```
Device(config-ap-profile)# cdp
```

# central association

To enable central association for locally switched clients, use the **central association** command.

## **central association**

<b>Syntax Description</b>	This command has no keywords or arguments.	
<b>Command Default</b>	None	
<b>Command Modes</b>	config-wireless-policy	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

## **Example**

The following example shows how to enable enable central association for locally switched clients:

```
Device(config-wireless-policy)# central association
```

# central authentication

To enable or disable central authentication, use the **central authentication** command.

## central authentication

<b>Syntax Description</b>	This command has no keywords or arguments.	
<b>Command Default</b>	None	
<b>Command Modes</b>	config-wireless-policy	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

### Example

The following example shows how to enable central authentication:

```
Device(config-wireless-policy)# central authentication
```



# central dhcp

To enable central dhcp for locally switched clients, use the **central dhcp** command.

## central dhcp

<b>Syntax Description</b>	This command has no keywords or arguments.	
<b>Command Default</b>	None	
<b>Command Modes</b>	config-wireless-policy	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

## Example

The following example shows how to enable central dhcp for locally switched clients:

```
Device(config-wireless-policy)# central dhcp
```

# central-webauth

To configure central-webauth for an ACL, use the **central-webauth** command.

## central-webauth

<b>Syntax Description</b>	This command has no keywords or arguments.	
<b>Command Default</b>	None	
<b>Command Modes</b>	config-wireless-policy	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

## Example

The following example shows how to configure central-webauth for an ACL:

```
Device(config-wireless-policy)# central-webauth
```

# chassis redundancy keep-alive

To configure peer keep-alive retries and time interval before claiming peer is down, use the **chassis redundancy keep-alive** command.

```
chassis redundancy keep-alive { retries retries | timer timer }
```

## Syntax Description

*retries* Chassis peer keep-alive retries before claiming peer is down.

Valid values range from 5 to 10, enter 5 for default.

*timer* Chassis peer keep-alive time interval in multiple of 100 ms.

Valid values range from 1 to 10, enter 1 for default.

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to configure peer keep-alive retries and time interval:

```
Device# chassis redundancy keep-alive retries 6
```

```
Device# chassis redundancy keep-alive timer 6
```

# chassis renumber

To renumber the local chassis id assignment, use the **chassis renumber** command.

**chassis** *chassis-num* **renumber** *renumber-id*

---

## Syntax Description

*chassis-num* Chassis number.

*renumber-id* Local chassis id.

---



---

## Command Default

None

---

## Command Modes

Privileged EXEC(#)

---

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

## Examples

The following example shows how to renumber the local chassis id assignment:

```
Device# chassis 1 renumber 1
```

# chassis transport

To enable or disable chassis transport, use the **chassis transport** command.

**chassis** *chassis-num* **transport** { **enable** | **disable** }

---

## Syntax Description

*chassis-num* Chassis number.

---



---

## Command Default

None

---

## Command Modes

Privileged EXEC(#)

---

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

## Examples

The following example shows how to enable chassis transport:

```
Device# chassis 1 transport enable
```

# class

To define a traffic classification match criteria for the specified class-map name, use the **class** command in policy-map configuration mode. Use the **no** form of this command to delete an existing class map.

```
class {class-map-name | class-default}
no class {class-map-name | class-default}
```

## Syntax Description

*class-map-name* The class map name.

**class-default** Refers to a system default class that matches unclassified packets.

## Command Default

No policy map class-maps are defined.

## Command Modes

Policy-map configuration

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

## Usage Guidelines

Before using the **class** command, you must use the **policy-map** global configuration command to identify the policy map and enter policy-map configuration mode. After specifying a policy map, you can configure a policy for new classes or modify a policy for any existing classes in that policy map. You attach the policy map to a port by using the **service-policy** interface configuration command.

After entering the **class** command, you enter the policy-map class configuration mode. These configuration commands are available:

- **exit**—Exits the policy-map class configuration mode and returns to policy-map configuration mode.
- **no**—Returns a command to its default setting.
- **police**—Defines a policer or aggregate policer for the classified traffic. The policer specifies the bandwidth limitations and the action to take when the limits are exceeded. For more information about this command, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com.
- **set**—Specifies a value to be assigned to the classified traffic. For more information, see [set, on page 448](#)

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

The **class** command performs the same function as the **class-map** global configuration command. Use the **class** command when a new classification, which is not shared with any other ports, is needed. Use the **class-map** command when the map is shared among many ports.

You can configure a default class by using the **class class-default** policy-map configuration command. Unclassified traffic (traffic that does not meet the match criteria specified in the traffic classes) is treated as default traffic.

You can verify your settings by entering the **show policy-map** privileged EXEC command.

## Examples

This example shows how to create a policy map called policy1. When attached to the ingress direction, it matches all the incoming traffic defined in class1, sets the IP Differentiated Services Code Point (DSCP) to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic exceeding the profile is marked down to a DSCP value gotten from the policed-DSCP map and then sent.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police 1000000 20000 conform-action
Device(config-pmap-c)# police 1000000 20000 exceed-action
Device(config-pmap-c)# exit
```

This example shows how to configure a default traffic class to a policy map. It also shows how the default traffic class is automatically placed at the end of policy-map pm3 even though **class-default** was configured first:

```
Device# configure terminal
Device(config)# class-map cm-3
Device(config-cmap)# match ip dscp 30
Device(config-cmap)# exit

Device(config)# class-map cm-4
Device(config-cmap)# match ip dscp 40
Device(config-cmap)# exit

Device(config)# policy-map pm3
Device(config-pmap)# class class-default
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# exit

Device(config-pmap)# class cm-3
Device(config-pmap-c)# set dscp 4
Device(config-pmap-c)# exit

Device(config-pmap)# class cm-4
Device(config-pmap-c)# set precedence 5
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device# show policy-map pm3
Policy Map pm3
  Class cm-3
    set dscp 4
  Class cm-4
    set precedence 5
  Class class-default
    set dscp af11
```

# classify

To classify a rule for rogue devices, use the **classify** command.

```
classify {friendly | malicious | delete}
```

## Syntax Description

**friendly** Classifies devices matching this rule as friendly.

**malicious** Classifies devices matching this rule as malicious.

**delete** Devices matching this rule are ignored.

## Command Default

None

## Command Modes

config-rule

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to classify rogue devices as friendly:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless wps rogue rule my-rogue-rule priority 3
Device(config-rule)# classify friendly
```



# class-map

To create a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode, use the **class-map** command in global configuration mode. Use the **no** form of this command to delete an existing class map and to return to global or policy map configuration mode.

```
class-map [{match-anytype}][{match-alltype}] class-map-name
no class-map [{match-anytype}][{match-alltype}] class-map-name
```

Syntax Description	
<b>match-any</b>	(Optional) Performs a logical-OR of the matching statements under this class map. One or more criteria must be matched.
<b>match-all</b>	(Optional) Performs a logical-AND all matching statements under this classmap.
<b>type</b>	(Optional) Configures the CPL class map.
<i>class-map-name</i>	The class map name.

**Command Default** No class maps are defined.

**Command Modes** Global configuration  
Policy map configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** Use this command to specify the name of the class for which you want to create or modify class-map match criteria and to enter class-map configuration mode.

The **class-map** command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally named service policy applied on a per-port basis.

After you are in quality of service (QoS) class-map configuration mode, these configuration commands are available:

- **description**—Describes the class map (up to 200 characters). The **show class-map** privileged EXEC command displays the description and the name of the class map.
- **exit**—Exits from QoS class-map configuration mode.
- **match**—Configures classification criteria.
- **no**—Removes a match statement from a class map.

If you enter the **match-any** keyword, you can only use it to specify an extended named access control list (ACL) with the **match access-group** class-map configuration command.

To define packet classification on a physical-port basis, only one **match** command per class map is supported.

The ACL can have multiple access control entries (ACEs).

---

**Examples**

This example shows how to configure the class map called class1 with one match criterion, which is an access list called 103:

```
Device(config)# access-list 103 permit ip any any dscp 10  
Device(config)# class-map class1  
Device(config-cmap)# match access-group 103  
Device(config-cmap)# exit
```

This example shows how to delete the class map class1:

```
Device(config)# no class-map class1
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

# clear chassis redundancy

To clear high-availability (HA) configuration, use the **clear chassis redundancy** command.

**clear chassis redundancy**

---

**Syntax Description**

This command has no keywords or arguments.

---

---

**Command Default**

None

---

**Command Modes**

Privileged EXEC(#)

---

---

**Command History**

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

## Examples

The following example shows how to clear HA configuration:

```
Device# clear chassis redundancy
```

## clear mdns-sd cache

To clear mDNS cache details, use the **clear mdns-sd cache** command.

```
clear mdns-sd cache { ap-mac mac-address (H.H.H) | client-mac client-mac-address (H.H.H) |
detail | glan-id <1 - 5> | location-group <0 - 4096> | mdns-ap mdns-ap mac address (H.H.H)
| rlan-id <1 - 128> | udn { <1 - 4294967295> | shared } | wired | wlan-id <0 -
4096> }
```

Syntax Description		
<b>ap-mac</b> <i>mac-address (H.H.H)</i>		Clears the AP Ethernet MAC address.
<b>client-mac</b> <i>client-mac-address (H.H.H)</i>		Clears the client MAC address.
<b>detail</b>		Clears the cache details.
<b>glan-id</b> <i>&lt;1 - 5&gt;</i>		Clears the GLAN ID. The value range is from 1 to 5.
<b>location-group</b> <i>&lt;0 - 4096&gt;</i>		Clears the location group. The value range is from 0 to 4096.
<b>mdns-ap</b> <i>mdns-ap mac address (H.H.H)</i>		Clears cached services from mDNS AP.
<b>rlan-id</b> <i>&lt;1 - 128&gt;</i>		Clears the RLAN ID. The value range is from 1 - 128.
<b>udn</b> <i>&lt;1 - 4294967295&gt;</i>		Clears the UDN ID. The value range is from 1 to 4294967295.
<b>shared</b>		Clears the UDN shared services.
<b>wired</b>		Clears the mDNS services from wired clients.
<b>wlan-id</b> <i>&lt;0 - 4096&gt;</i>		Clears the WLAN ID. The value range is from 1 to 4096.

**Command Default** None

**Command Modes** Privileged EXEC mode

Command History	Release	Modification
	Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

**Usage Guidelines** None

### Example

The following example shows how to clear the mDNS cache details:

```
Device# clear mdns-sd cache
```

## clear mdns-sd statistics

To clear mDNS statistics, use the **clear mdns-sd statistics** command.

```
clear mdns-sd statistics { debug | glan-id <1 - 5> | rlan-id <1 - 128> wired | wlan-id <1 - 4096> }
```

Syntax Description	Parameter	Description
	<b>debug</b>	Clears the mDNS debug statistics.
	<b>glan-id</b> <1 - 5>	Clears the GLAN ID. The value range is from 1 to 5.
	<b>rlan-id</b> <1 - 128>	Clears the RLAN ID. The value range is from 1 to 128.
	<b>wired</b>	Clears the mDNS wired statistics.
	<b>wlan-id</b> <1 - 4096>	Clears the WLAN ID. The value range is from 1 to 4096.

**Command Default** None

**Command Modes** Privileged EXEC mode

Command History	Release	Modification
	Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

**Usage Guidelines** None

### Example

The following example shows how to clear the mDNS statistics:

```
Device# clear mdns-sd statistics
```

# clear platform condition all

To clear all conditional debug and packet-trace configuration and data, use the **clear platform condition all** command.

**clear platform condition all**

---

## Command Default

None

---

## Command Modes

Privileged EXEC

---

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to clear all conditional debug and packet-trace configuration and data:

```
Device# clear platform condition all
```

# clear wireless wps rogue ap

To clear all rogue APs or rogue APs with specific MAC addresses, use the **clear wireless wps rogue ap** command.

```
clear wireless wps rogue ap { all | mac-address <MAC Address> }
```

<b>Syntax Description</b>	<b>all</b> Clears all the rogue APs.				
	<b>mac-address &lt;MAC Address&gt;</b> Clears the rogue APs with specific MAC addresses.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Privileged EXEC (#)				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Amsterdam 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Amsterdam 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.				
<b>Usage Guidelines</b>	None				

## Example

The following example shows you how to clear all rogue APs or rogue APs with specific MAC addresses:

```
Device# clear wireless wps rogue ap all
```

```
Device# clear wireless wps rogue ap mac-address 10.10.1
```

# clear wireless wps rogue client

To clear all rogue clients or client with specific MAC addresses, use the **clear wireless wps rogue client** command.

**clear wireless wps rogue client** { **all** | **mac-address** <MAC Address> }

Syntax Description	
<b>all</b>	Clears all the rogue clients.
<b>mac-address</b> <MAC Address>	Clears the rogue clients with specific MAC addresses.

**Command Default** None

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

**Usage Guidelines** None

## Example

The following example shows you how to clear all rogue clients or rogue clients with specific MAC addresses:

```
Device# clear wireless wps rogue client all
Device# clear wireless wps rogue client mac-address 10.10.1
```



# clear wireless wps rogue stats

To clear rogue statistics, use the **clear wireless wps rogue stats** command.

**clear wireless wps rogue stats**

---

**Syntax Description**

This command has no arguments.

---

---

**Command Default**

None

---

**Command Modes**

Privileged EXEC (#)

---

**Command History**

Release	Modification
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

---

---

**Usage Guidelines**

None

**Example**

The following example shows you how to clear rogue statistics:

```
Device# clear wireless wps rogue stats
```

# client association limit

To configure the maximum number of client connections on a WLAN, use the **client association limit** command. To disable clients association limit on the WLAN, use the **no** form of this command.

**client association limit** {*association-limit*}

**no client association limit** {*association-limit*}

<b>Syntax Description</b>	<i>association-limit</i>	Number of client connections to be accepted. The range is from 0 to . A value of zero (0) indicates no set limit.
---------------------------	--------------------------	----------------------------------------------------------------------------------------------------------------------

**Command Default** The maximum number of client connections is set to 0 (no limit).

**Command Modes** WLAN configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to configure a client association limit on a WLAN and configure the client limit to 200:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# client association limit 200
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

This example shows how to disable a client association limit on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# no client association limit
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

This example shows how to configure a client association limit per radio on a WLAN and configure the client limit to 200:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# client association limit radio 200
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

This example shows how to configure a client association limit per AP on a WLAN and configure the client limit to 300:

```
Device# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Device(config)# wlan wlan1  
Device(config-wlan)# client association limit ap 300  
Device(config-wlan)# no shutdown  
Device(config-wlan)# end
```

## channel foreign

To configure the RF Profile DCA foreign AP contribution, use the **channel foreign** command. To disable the DCA Foreign AP Contribution, use the **no** form of this command.

### channel foreign

<b>Syntax Description</b>	<b>foreign</b>	Configures the RF Profile DCA foreign AP contribution.
<b>Command Default</b>	None	
<b>Command Modes</b>	config-rf-profile	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Denali 16.3.1	This command was introduced.
<b>Usage Guidelines</b>	None	

This example shows how to configure the RF profile DCA foreign AP contribution.

```
Device (config-rf-profile) #channel foreign
```

## client-l2-vnid

To configure the client l2-vnid on a wireless fabric profile, use the **client-l2-vnid** command.

**client-l2-vnid** *vnid*

---

### Syntax Description

*vnid* Configures client l2-vnid. Valid range is 0 to 16777215.

---

### Command Default

None

### Command Modes

config-wireless-fabric

---

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

### Examples

The following example shows how to configure the client l2-vnid value on a wireless fabric profile:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile fabric fabric-profile-name
Device(config-wireless-fabric)# client-l2-vnid 10
```

## convergence

To configure mesh convergence method, use the **convergence** command.

**convergence** { **fast** | **noise-tolerant-fast** | **standard** | **very-fast** }

Syntax Description	fast	Configures fast convergence method.
	noise-tolerant-fast	Configures noise-tolerant fast convergence method method to handle unstable RF environment.
	standard	Configures standard convergence method.
	very-fast	Configures very fast convergence method.
Command Default	Standard	
Command Modes	config-wireless-mesh-profile	
Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

### Examples

The following example shows how to configure the fast convergence method for a mesh AP profile:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile mesh mesh-profile
Device(config-wireless-mesh-profile)# convergence fast
```

## coverage

To configure the voice and data coverage, use the **coverage** command. To reset the minimum RSSI value use the **no** form of this command.

**coverage** {**data** | **voice**} **rsi threshold** *value*

<b>Syntax Description</b>	<b>data</b>	Configure Coverage Hole Detection for data packets.
	<b>voice</b>	Configure Coverage Hole Detection for voice packets.
	<i>value</i>	Minimum RSSI value for the packets received by the access point. The valid range is between -90 and -60 dBm.
<b>Command Default</b>	None	
<b>Command Modes</b>	config-rf-profile	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Denali 16.3.1 This command was introduced.	
<b>Usage Guidelines</b>	None	

This example shows how to configure the coverage hole detection for data packets.

```
Device(config-rf-profile)#coverage data rssi threshold -85
```

## crypto key generate rsa

To generate Rivest, Shamir, and Adelman (RSA) key pairs, use the **crypto key generate rsa** command in global configuration mode.

```
crypto key generate rsa [{general-keys | usage-keys | signature | encryption}] [label key-label]
[exportable] [modulus modulus-size] [storage devicename :] [redundancy] [on devicename :]
```

### Syntax Description

<b>general-keys</b>	(Optional) Specifies that a general-purpose key pair will be generated, which is the default.
<b>usage-keys</b>	(Optional) Specifies that two RSA special-usage key pairs, one encryption pair and one signature pair, will be generated.
<b>signature</b>	(Optional) Specifies that the RSA public key generated will be a signature special usage key.
<b>encryption</b>	(Optional) Specifies that the RSA public key generated will be an encryption special usage key.
<b>label</b> <i>key-label</i>	(Optional) Specifies the name that is used for an RSA key pair when they are being exported.  If a key label is not specified, the fully qualified domain name (FQDN) of the router is used.
<b>exportable</b>	(Optional) Specifies that the RSA key pair can be exported to another Cisco device, such as a router.
<b>modulus</b> <i>modulus-size</i>	(Optional) Specifies the IP size of the key modulus.  By default, the modulus of a certification authority (CA) key is 1024 bits. The recommended modulus for a CA key is 2048 bits. The range of a CA key modulus is from 350 to 4096 bits.  <b>Note</b> Effective with Cisco IOS XE Release 2.4 and Cisco IOS Release 15.1(1)T, the maximum key size was expanded to 4096 bits for private key operations. The maximum for private key operations prior to these releases was 2048 bits.
<b>storage</b> <i>devicename</i> :	(Optional) Specifies the key storage location. The name of the storage device is followed by a colon (:).
<b>redundancy</b>	(Optional) Specifies that the key should be synchronized to the standby CA.
<b>on</b> <i>devicename</i> :	(Optional) Specifies that the RSA key pair will be created on the specified device, including a Universal Serial Bus (USB) token, local disk, or NVRAM. The name of the device is followed by a colon (:).  Keys created on a USB token must be 2048 bits or less.

### Command Default

RSA key pairs do not exist.



**Command Modes**

Global configuration

**Command History**

Release	Modification
11.3	This command was introduced.
12.2(8)T	The <i>key-label</i> argument was added.
12.2(15)T	The <b>exportable</b> keyword was added.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(4)T	The <b>storage</b> keyword and <i>devicename</i> : argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The <b>storage</b> keyword and <i>devicename</i> : argument were implemented on the Cisco 7200VXR NPE-G2 platform. The <b>signature</b> , <b>encryption</b> and <b>on</b> keywords and <i>devicename</i> : argument were added.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.
XE 2.4	The maximum RSA key size was expanded from 2048 to 4096 bits for private key operations.
15.0(1)M	This command was modified. The <b>redundancy</b> keyword was introduced.
15.1(1)T	This command was modified. The range value for the <b>modulus</b> keyword value is extended from 360 to 2048 bits to 360 to 4096 bits.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

**Usage Guidelines**

**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the [Next Generation Encryption \(NGE\)](#) white paper.

Use this command to generate RSA key pairs for your Cisco device (such as a router).

RSA keys are generated in pairs--one public RSA key and one private RSA key.

If your router already has RSA keys when you issue this command, you will be warned and prompted to replace the existing keys with new keys.



**Note** Before issuing this command, ensure that your router has a hostname and IP domain name configured (with the **hostname** and **ip domain-name** commands). You will be unable to complete the **crypto key generate rsa** command without a hostname and IP domain name. (This situation is not true when you generate only a named key pair.)



**Note** Secure Shell (SSH) may generate an additional RSA key pair if you generate a key pair on a router having no RSA keys. The additional key pair is used only by SSH and will have a name such as `{router_FQDN}.server`. For example, if a router name is “router1.cisco.com,” the key name is “router1.cisco.com.server.”

This command is not saved in the router configuration; however, the RSA keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.



**Note** If the configuration is not saved to NVRAM, the generated keys are lost on the next reload of the router.

There are two mutually exclusive types of RSA key pairs: special-usage keys and general-purpose keys. When you generate RSA key pairs, you will be prompted to select either special-usage keys or general-purpose keys.

### Special-Usage Keys

If you generate special-usage keys, two pairs of RSA keys will be generated. One pair will be used with any Internet Key Exchange (IKE) policy that specifies RSA signatures as the authentication method, and the other pair will be used with any IKE policy that specifies RSA encrypted keys as the authentication method.

A CA is used only with IKE policies specifying RSA signatures, not with IKE policies specifying RSA-encrypted nonces. (However, you could specify more than one IKE policy and have RSA signatures specified in one policy and RSA-encrypted nonces in another policy.)

If you plan to have both types of RSA authentication methods in your IKE policies, you may prefer to generate special-usage keys. With special-usage keys, each key is not unnecessarily exposed. (Without special-usage keys, one key is used for both authentication methods, increasing the exposure of that key.)

### General-Purpose Keys

If you generate general-purpose keys, only one pair of RSA keys will be generated. This pair will be used with IKE policies specifying either RSA signatures or RSA encrypted keys. Therefore, a general-purpose key pair might get used more frequently than a special-usage key pair.

### Named Key Pairs

If you generate a named key pair using the *key-label* argument, you must also specify the **usage-keys** keyword or the **general-keys** keyword. Named key pairs allow you to have multiple RSA key pairs, enabling the Cisco IOS software to maintain a different key pair for each identity certificate.

### Modulus Length

When you generate RSA keys, you will be prompted to enter a modulus length. The longer the modulus, the stronger the security. However a longer modulus takes longer to generate (see the table below for sample times) and takes longer to use.

**Table 7: Sample Times by Modulus Length to Generate RSA Keys**

Router	360 bits	512 bits	1024 bits	2048 bits (maximum)
Cisco 2500	11 seconds	20 seconds	4 minutes, 38 seconds	More than 1 hour
Cisco 4700	Less than 1 second	1 second	4 seconds	50 seconds

Cisco IOS software does not support a modulus greater than 4096 bits. A length of less than 512 bits is normally not recommended. In certain situations, the shorter modulus may not function properly with IKE, so we recommend using a minimum modulus of 2048 bits.



**Note** As of Cisco IOS Release 12.4(11)T, peer *public* RSA key modulus values up to 4096 bits are automatically supported. The largest private RSA key modulus is 4096 bits. Therefore, the largest RSA private key a router may generate or import is 4096 bits. However, RFC 2409 restricts the private key size to 2048 bits or less for RSA encryption. The recommended modulus for a CA is 2048 bits; the recommended modulus for a client is 2048 bits.

Additional limitations may apply when RSA keys are generated by cryptographic hardware. For example, when RSA keys are generated by the Cisco VPN Services Port Adapter (VSPA), the RSA key modulus must be a minimum of 384 bits and must be a multiple of 64.

#### Specifying a Storage Location for RSA Keys

When you issue the **crypto key generate rsa** command with the **storage devicename** : keyword and argument, the RSA keys will be stored on the specified device. This location will supersede any **crypto key storage** command settings.

#### Specifying a Device for RSA Key Generation

As of Cisco IOS Release 12.4(11)T and later releases, you may specify the device where RSA keys are generated. Devices supported include NVRAM, local disks, and USB tokens. If your router has a USB token configured and available, the USB token can be used as cryptographic device in addition to a storage device. Using a USB token as a cryptographic device allows RSA operations such as key generation, signing, and authentication of credentials to be performed on the token. The private key never leaves the USB token and is not exportable. The public key is exportable.

RSA keys may be generated on a configured and available USB token, by the use of the **on devicename** : keyword and argument. Keys that reside on a USB token are saved to persistent token storage when they are generated. The number of keys that can be generated on a USB token is limited by the space available. If you attempt to generate keys on a USB token and it is full you will receive the following message:

```
% Error in generating keys:no available resources
```

Key deletion will remove the keys stored on the token from persistent storage immediately. (Keys that do not reside on a token are saved to or deleted from nontoken storage locations when the **copy** or similar command is issued.)

For information on configuring a USB token, see “ Storing PKI Credentials ” chapter in the Cisco IOS Security Configuration Guide, Release 12.4T. For information on using on-token RSA credentials, see the “ Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment ” chapter in the Cisco IOS Security Configuration Guide , Release 12.4T.

#### Specifying RSA Key Redundancy Generation on a Device

You can specify redundancy for existing keys only if they are exportable.

### Examples

The following example generates a general-usage 1024-bit RSA key pair on a USB token with the label “ms2” with crypto engine debugging messages shown:

```
Router(config)# crypto key generate rsa label ms2 modulus 2048 on usbtoken0:
```

```

The name for the keys will be: ms2
% The key modulus size is 2048 bits
% Generating 1024 bit RSA keys, keys will be on-token, non-exportable...
Jan 7 02:41:40.895: crypto_engine: Generate public/private keypair [OK]
Jan 7 02:44:09.623: crypto_engine: Create signature
Jan 7 02:44:10.467: crypto_engine: Verify signature
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_CREATE_PUBKEY(hw) (ipsec)
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_PUB_DECRYPT(hw) (ipsec)

```

Now, the on-token keys labeled “ms2” may be used for enrollment.

The following example generates special-usage RSA keys:

```

Router(config)# crypto key generate rsa usage-keys
The name for the keys will be: myrouter.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
Choose the size of the key modulus in the range of 360 to 2048 for your Encryption Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].

```

The following example generates general-purpose RSA keys:




---

**Note**

You cannot generate both special-usage and general-purpose keys; you can generate only one or the other.

---

```

Router(config)# crypto key generate rsa general-keys
The name for the keys will be: myrouter.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].

```

The following example generates the general-purpose RSA key pair “exampleCAkeys”:

```

crypto key generate rsa general-keys label exampleCAkeys
crypto ca trustpoint exampleCAkeys
  enroll url
http://exampleCAkeys/certsrv/mscep/mscep.dll
  rsakeypair exampleCAkeys 1024 1024

```

The following example specifies the RSA key storage location of “usbtoken0:” for “tokenkey1”:

```
crypto key generate rsa general-keys label tokenkey1 storage usbtoken0:
```

The following example specifies the **redundancy** keyword:

```
Router(config)# crypto key generate rsa label MYKEYS redundancy
```

The name for the keys will be: MYKEYS

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]:

% Generating 512 bit RSA keys, keys will be non-exportable with redundancy...[OK]

Related Commands	Command	Description
	copy	Copies any file from a source to a destination, use the copy command in privileged EXEC mode.
	<b>crypto key storage</b>	Sets the default storage location for RSA key pairs.
	<b>debug crypto engine</b>	Displays debug messages about crypto engines.
	<b>hostname</b>	Specifies or modifies the hostname for the network server.
	<b>ip domain-name</b>	Defines a default domain name to complete unqualified hostnames (names without a dotted-decimal domain name).
	<b>show crypto key mypubkey rsa</b>	Displays the RSA public keys of your router.
	show crypto pki certificates	Displays information about your PKI certificate, certification authority, and any registration authority certificates.

# crypto pki trustpoint

To create a new TrustPoint dedicated for a single CA certificate, use the **crypto pki trustpoint** command.

## crypto pki trustpoint

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Global Configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

### Usage Guidelines

This example shows how to create a new TrustPoint dedicated for a single CA certificate:

```
Device# configure terminal
Device(config)# crypto pki trustpoint <tp_name>
Device(ca-trustpoint)# enrollment terminal
Device(ca-trustpoint)# exit
Device(config)# crypto pki authenticate <tp_name>
<<< PASTE CA-CERT in PEM format followed by quit >>>
```

# crypto pki trust pool import terminal

To import the root certificate by pasting the CA certificate from the [digicert.com](https://www.digicert.com), use the **crypto pki trust pool import terminal** command.

**crypto pki trust pool import terminal**

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Global Configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

## Usage Guidelines

This example shows how to import the root certificate by pasting the CA certificate from the [digicert.com](https://www.digicert.com):

```
Device# configure terminal
Device(config)# crypto pki trust pool import terminal
Device(config)# end
```

# crypto pki trustpool clean

To erase the downloaded CA certificate bundles, use the **crypto pki trustpool clean** command.

## crypto pki trustpool clean

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Global Configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

### Usage Guidelines

This example shows how to erase the downloaded CA certificate bundles:

```
Device# configure terminal
Device(config)# crypto pki trustpool clean
Device(config)# end
```



# cts inline-tagging

To configure Cisco TrustSec (CTS) inline tagging, use the **cts inline-tagging** command.

## cts inline-tagging

<b>Syntax Description</b>	This command has no keywords or arguments.	
<b>Command Default</b>	Inline tagging is not configured.	
<b>Command Modes</b>	wireless policy configuration (config-wireless-policy)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

## Example

This example shows how to configure CTS inline tagging.

```
Device(config-wireless-policy)# cts inline-tagging
```

## cts role-based enforcement

To configure Cisco TrustSec (CTS) SGACL enforcement, use the **cts role-based enforcement** command.

### cts role-based enforcement

<b>Syntax Description</b>	This command has no keywords or arguments.	
<b>Command Default</b>	SGACL is not enforced.	
<b>Command Modes</b>	wireless policy configuration (config-wireless-policy)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

### Example

This example shows how to configure CTS SGACL enforcement.

```
Device(config-wireless-policy)# cts role-based enforcement
```

## cts sgt

To set the Cisco TrustSec (CTS) default security group tag (SGT), use the **cts sgt** command.

**cts sgt** *sgt-value*

---

### Syntax Description

*sgt-value* Security group tag value.

---



---

### Command Default

SGT tag is not set.

---

### Command Modes

wireless policy configuration (config-wireless-policy)

---

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

---

### Example

This example shows how to set the default SGT.

```
Device(config-wireless-policy)# cts sgt 100
```

## custom-page login device

To configure a customized login page, use the **custom-page login device** command.

**custom-page login device** *html-filename*

<b>Syntax Description</b>	<i>html-filename</i> Enter the HTML filename of the login page.
---------------------------	-----------------------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	config-params-parameter-map
----------------------	-----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

### Examples

The following example shows how to configure a customized login page:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# parameter-map type webauth parameter-map-name
Device(config-params-parameter-map)# custom-page login device bootflash:login.html
```

# default

To set the parameters to their default values, use the **default** command.

**default** {aaa-override | accounting-list | band-select | broadcast-ssid | call-snoop | ccx | channel-scan | parameters | chd | client | datalink | diag-channel | dtim | exclusionlist | ip | ipv6 | load-balance | local-auth | mac-filtering | media-stream | mfp | mobility | nac | passive-client | peer-blocking | radio | roamed-voice-client | security | service-policy | session-timeout | shutdown | sip-cac | static-ip | uapsd | wgb | wmm }

Syntax	Description
<b>aaa-override</b>	Sets the AAA override parameter to its default value.
<b>accounting-list</b>	Sets the accounting parameter and its attributes to their default values.
<b>band-select</b>	Sets the band selection parameter to its default values.
<b>broadcast-ssid</b>	Sets the broadcast Service Set Identifier (SSID) parameter to its default value.
<b>call-snoop</b>	Sets the call snoop parameter to its default value.
<b>ccx</b>	Sets the Cisco client extension (Cisco Aironet IE) parameters and attributes to their default values.
<b>channel-scan</b>	Sets the channel scan parameters and attributes to their default values.
<b>chd</b>	Sets the coverage hold detection parameter to its default value.
<b>client</b>	Sets the client parameters and attributes to their default values.
<b>datalink</b>	Sets the datalink parameters and attributes to their default values.
<b>diag-channel</b>	Sets the diagnostic channel parameters and attributes to their default values.
<b>dtim</b>	Sets the Delivery Traffic Indicator Message (DTIM) parameter to its default value.
<b>exclusionlist</b>	Sets the client exclusion timeout parameter to its default value.
<b>ip</b>	Sets the IP parameters to their default values.
<b>ipv6</b>	Sets the IPv6 parameters and attributes to their default values.
<b>load-balance</b>	Sets the load-balancing parameter to its default value.
<b>local-auth</b>	Sets the Extensible Authentication Protocol (EAP) profile parameters and attributes to their default values.
<b>mac-filtering</b>	Sets the MAC filtering parameters and attributes to their default values.
<b>media-stream</b>	Sets the media stream parameters and attributes to their default values.

<b>mfp</b>	Sets the Management Frame Protection (MPF) parameters and attributes to their default values.
<b>mobility</b>	Sets the mobility parameters and attributes to their default values.
<b>nac</b>	Sets the RADIUS Network Admission Control (NAC) parameter to its default value.
<b>passive-client</b>	Sets the passive client parameter to its default value.
<b>peer-blocking</b>	Sets the peer to peer blocking parameters and attributes to their default values.
<b>radio</b>	Sets the radio policy parameters and attributes to their default values.
<b>roamed-voice-client</b>	Sets the roamed voice client parameters and attributes to their default values.
<b>security</b>	Sets the security policy parameters and attributes to their default values.
<b>service-policy</b>	Sets the WLAN quality of service (QoS) policy parameters and attributes to their default values.
<b>session-timeout</b>	Sets the client session timeout parameter to its default value.
<b>shutdown</b>	Sets the shutdown parameter to its default value.
<b>sip-cac</b>	Sets the Session Initiation Protocol (SIP) Call Admission Control (CAC) parameters and attributes to their default values.
<b>static-ip</b>	Sets the static IP client tunneling parameters and their attributes to their default values.
<b>uapsd</b>	Sets the Wi-Fi Multimedia (WMM) Unscheduled Automatic Power Save Delivery (UAPSD) parameters and attributes to their default values.
<b>wgb</b>	Sets the Workgroup Bridges (WGB) parameter to its default value.
<b>wmm</b>	Sets the WMM parameters and attributes to their default values.

**Command Default** None.

**Command Modes** WLAN configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to set the Cisco Client Extension parameter to its default value:

```
Device(config-wlan)# default ccx aironet-iesupport
```

## description

To configure a description for a flow monitor, flow exporter, or flow record, use the **description** command in the appropriate configuration mode. To remove a description, use the **no** form of this command.

**description** *description*  
**no description** *description*

---

### Syntax Description

*description* Text string that describes the flow monitor, flow exporter, or flow record.

---



---

### Command Default

The default description for a flow sampler, flow monitor, flow exporter, or flow record is "User defined."

---

### Command Modes

The following command modes are supported:

Flow exporter configuration

Flow monitor configuration

Flow record configuration

---

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

---



---

### Usage Guidelines

To return this command to its default setting, use the **no description** or **default description** command in the appropriate configuration mode.

The following example configures a description for a flow monitor:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# description Monitors traffic to 172.16.0.1 255.255.0.0
```



# destination

To configure an export destination for a flow exporter, use the **destination** command in flow exporter configuration mode. To remove an export destination for a flow exporter, use the **no** form of this command.

**destination** *{hostnameip-address}*  
**no destination** *{hostnameip-address}*

## Syntax Description

*hostname* Hostname of the device to which you want to send the NetFlow information.

*ip-address* IPv4 address of the workstation to which you want to send the NetFlow information.

## Command Default

An export destination is not configured.

## Command Modes

Flow exporter configuration

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

## Usage Guidelines

Each flow exporter can have only one destination address or hostname.

When you configure a hostname instead of the IP address for the device, the hostname is resolved immediately and the IPv4 address is stored in the running configuration. If the hostname-to-IP-address mapping that was used for the original Domain Name System (DNS) name resolution changes dynamically on the DNS server, the device does not detect this, and the exported data continues to be sent to the original IP address, resulting in a loss of data.

To return this command to its default setting, use the **no destination** or **default destination** command in flow exporter configuration mode.

The following example shows how to configure the networking device to export the cache entry to a destination system:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# destination 10.0.0.4
```

## destination stealthwatch-cloud

To configure the export destination as Cisco Stealthwatch Cloud, use the **destination stealthwatch-cloud** command. To disable the command, use the **no** form of this command.

**destination stealthwatch-cloud**

**no destination stealthwatch-cloud**

Syntax Description	destination	Configures the export destination.
	<b>stealthwatch-cloud</b>	Configures export to Cisco Stealthwatch Cloud.

**Command Default** None

**Command Modes** Flow Exporter Configuration

Command History	Release	Modification
	Cisco IOS XE Bengaluru 17.4.1	This command was introduced.

**Usage Guidelines** None

### Example

This example shows how to configure the export destination as Cisco Stealthwatch Cloud:

```
Device(config-flow-exporter)# destination stealthwatch-cloud
```

# device-tracking binding vlan

To configure IPv4 or IPv6 static entry, use the **device-tracking binding vlan** command.

**device-tracking binding vlan** *vlan-id* {*ipv4-addr* *ipv6-addr* } **interface** **gigabitEthernet** *ge-intf-num* *hardware-or-mac-address*

Syntax Description		
<i>vlan-id</i>	VLAN ID. Valid range is 1 to 4096.	
<i>ipv4-addr</i>	IPv4 address of the device.	
<b>interface</b> <b>gigabitEthernet</b>	GigabitEthernet IEEE 802.3z.	
<i>ge-intf-num</i>	GigabitEthernet interface number. Valid range is 1 to 32.	
<i>hardware-or-mac-address</i>	The 48-bit hardware address or the MAC address of the device.	
Command Default	None	
Command Modes	Global configuration (config)	
Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to configure IPv4 static entry:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# device-tracking binding vlan 20 20.20.20.5 interface gigabitEthernet 1
0000.1111.2222
```

# dhcp-tlv-caching

To configure DHCP TLV caching on a WLAN, use the **dhcp-tlv-caching** command.

## dhcp-tlv-caching

### Command Default

None

### Command Modes

config-wireless-policy

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

### Example

This example shows how to configure DHCP TLV caching on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy rr-xyz-policy-1
Device(config-wireless-policy)# dhcp-tlv-caching
Device(config-wireless-policy)# radius-profiling
Device(config-wireless-policy)# end
```

# dnscrypt

To enable or disable DNSCrypt, use the **dnscrypt** command.

## dnscrypt

### Command Default

None

### Command Modes

config-profile

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

### Usage Guidelines

By default, the DNSCrypt option is enabled.

This example shows how to enable or disable DNSCrypt:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# parameter-map type umbrella global
Device(config-profile)# token 57CC80106C087FB1B2A7BAB4F2F4373C00247166
Device(config-profile)# local-domain dns_wl
Device(config-profile)# no dnscrypt
Device(config-profile)# end
```

## domain-name (DHCP)

To specify the domain name for a Dynamic Host Configuration Protocol (DHCP) client, use the **domain-name** command in DHCP pool configuration mode. To remove the domain name, use the no form of this command.

**domain-name** *domain*  
**no domain-name**

### Syntax Description

<i>domain</i>	Specifies the domain name string of the client.
---------------	-------------------------------------------------

### Command Default

No default behavior or values.

### Command Modes

DHCP pool configuration

### Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

### Examples

The following example specifies cisco.com as the domain name of the client:

```
domain-name cisco.com
```

### Related Commands

Command	Description
<b>dns-server</b>	Specifies the DNS IP servers available to a DHCP client.
<b>ip dhcp pool</b>	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

## dot11ax twt-broadcast-support

To configure TWT broadcast support on WLAN, use the **dot11ax twt-broadcast-support** command. To disable the feature, use the **no** command of the command.

**dot11ax twt-broadcast-support**

**[no] dot11ax twt-broadcast-support**

<b>Syntax Description</b>	<b>dot11ax twt-broadcast-support</b> Configures the TWT broadcast support on WLAN	
<b>Command Default</b>	None	
<b>Command Modes</b>	WLAN configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

### Example

This example shows how to configure target wakeup time on WLAN:

```
Device(config-wlan)# dot11ax twt-broadcast-support
```

## dot11 5ghz reporting-interval

To configure the client report interval sent from AP for clients on 802.11a radio, use the **dot11 5ghz reporting-interval** command.

**dot11 5ghz reporting-interval** *reporting-interval*

<b>Syntax Description</b>	<i>reporting-interval</i> Interval at which client report needs to be sent in seconds.	
<b>Command Default</b>	None	
<b>Command Modes</b>	config-ap-profile	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

### Examples

The following example shows how to set the client report interval in seconds:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap profile profile-name
Device(config-ap-profile)# dot11 5ghz reporting-interval 8
```



# dot11 reporting-interval

To set the volume metering interval, use the **dot11 reporting-interval** command.

```
dot11 {24ghz | 5ghz }reporting-interval
```

<b>Syntax Description</b>	<i>reporting-interval</i> Interval to send client accounting statistics.				
<b>Command Default</b>	Interval is configured at the default level of 90 seconds.				
<b>Command Modes</b>	config-ap-profile				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.				

**Usage Guidelines**

Though the CLI allows you to configure range from 5 to 90 seconds, we recommend that you use 60 to 90 seconds range for Volume Metering.

This CLI can also be used to configure the interval when smart roam is enabled, which has a range of 5 to 90 seconds.

Though you can set two different values for volume metering and smart roam, only one value takes effect based on the order of execution. So, we recommend that you use the same reporting interval for both.

## Example

The following example shows how to configure volume metering:

```
Device(config-ap-profile)# dot11 24ghz 60
```

# dot1x system-auth-control

To globally enable 802.1X SystemAuthControl (port-based authentication), use the **dot1x system-auth-control** command in global configuration mode. To disable SystemAuthControl, use the **no** form of this command.

**dot1x system-auth-control**  
**no dot1x system-auth-control**

**Syntax Description** This command has no arguments or keywords.

**Command Default** System authentication is disabled by default. If this command is disabled, all ports behave as if they are force authorized.

**Command Modes** Global configuration (config)

## Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

## Usage Guidelines

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN before making available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol (EAP) over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

The **no** form of the command removes any 802.1X-related configurations.

You must enable Authentication, Authorization, and Accounting (AAA) and specify the authentication method list before enabling 802.1X. A method list describes the sequence and authentication methods to be queried to authenticate a user.

## Examples

The following example shows how to enable SystemAuthControl:

```
Router(config)# dot1x system-auth-control
```

Related Commands	Command	Description
	<b>aaa authentication dot1x</b>	Specifies one or more AAA methods for use on interfaces running IEEE 802.1X.
	<b>aaa new-model</b>	Enables the AAA access-control model.
	<b>debug dot1x</b>	Displays 802.1X debugging information.
	<b>description</b>	Specifies a description for an 802.1X profile.
	<b>device</b>	Statically authorizes or rejects individual devices.
	<b>dot1x initialize</b>	Initializes 802.1X state machines on all 802.1X-enabled interfaces.
	<b>dot1x max-req</b>	Sets the maximum number of times that a router or Ethernet switch network module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.
	<b>dot1x port-control</b>	Enables manual control of the authorized state of a controlled port.
	<b>dot1x re-authenticate</b>	Manually initiates a reauthentication of the specified 802.1X-enabled ports.
	<b>dot1x reauthentication</b>	Globally enables periodic reauthentication of the client PCs on the 802.1X interface.
	<b>dot1x timeout</b>	Sets retry timeouts.
	<b>identity profile</b>	Creates an identity profile and enters identity profile configuration mode.
	<b>show dot1x</b>	Displays details and statistics for an identity profile.
	<b>template</b>	Specifies a virtual template from which commands may be cloned.

# eap profile

To configure an EAP profile, use the **eap profile** command.

**eap profile** *profile-name*

---

<b>Syntax Description</b>	<i>profile-name</i> Name of the EAP profile. Maximum number of allowed characters is 63.
---------------------------	------------------------------------------------------------------------------------------

---

<b>Command Default</b>	None
------------------------	------

---

<b>Command Modes</b>	Global configuration (config)
----------------------	-------------------------------

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

## Examples

The following example shows how to configure an EAP profile name:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# eap profile eap-profile-name
```

# exclusionlist

To configure an exclusion list on a wireless LAN, use the **exclusionlist** command. To disable an exclusion list, use the **no** form of this command.

```
exclusionlist [timeout seconds]  
no exclusionlist [timeout]
```

<b>Syntax Description</b>	<b>timeout</b> <i>seconds</i> (Optional) Specifies an exclusion list timeout in seconds. The range is from 0 to 2147483647. A value of zero (0) specifies no timeout.				
<b>Command Default</b>	The exclusion list is set to 60 seconds.				
<b>Command Modes</b>	WLAN configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.				
<b>Usage Guidelines</b>	<p>You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.</p> <p>This example shows how to configure a client exclusion list for a WLAN:</p> <pre>Device# <b>configure terminal</b> Enter configuration commands, one per line. End with CNTL/Z. Device(config)# <b>wlan wlan1</b> Device(config-wlan)# <b>exclusionlist timeout 345</b></pre> <p>This example shows how to disable a client exclusion list on a WLAN:</p> <pre>Device# <b>configure terminal</b> Enter configuration commands, one per line. End with CNTL/Z. Device(config)# <b>wlan wlan1</b> Device(config-wlan)# <b>no exclusionlist timeout 345</b></pre>				

## exporter default-flow-exporter

To add an exporter to use to export records, use the **exporter default-flow-exporter** command. Use the **no** form of this command to disable the feature.

**exporter default-flow-exporter**

**[no] exporter default-flow-exporter**

<b>Syntax Description</b>	There are no arguments to this command.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Flow monitor configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

### Example

This example shows how to add an exporter to use to export records:

```
Device(config-flow-monitor)#exporter default-flow-exporter
```

# fallback-radio-shut

To configure shutdown of the radio interface, use the **fallback-radio-shut** command.

## fallback-radio-shut

<b>Command Default</b>	None
<b>Command Modes</b>	config-wireless-flex-profile

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to configure shutdown of the radio interface:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile flex flex-profile-name
Device(config-wireless-flex-profile)# fallback-radio-shut
```

# flex

To configure flex related parameters, use the **flex** command.

**flex** {**nat-pat** | **split-mac-acl** *split-mac-acl-name* | **vlan-central-switching** }

## Syntax Description

<b>nat-pat</b>	Enables NAT-PAT.
<b>split-mac-acl</b>	Configures split-mac-acl name.
<i>split-mac-acl-name</i>	Name of split MAC ACL.
<b>vlan-central-switching</b>	VLAN based central switching.

## Command Default

None

## Command Modes

config-wireless-policy

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to configure flex related VLAN central-switching:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy profile-name
Device(config-wireless-policy)# flex vlan-central-switching
```



# flow exporter

To create a flow exporter, or to modify an existing flow exporter, and enter flow exporter configuration mode, use the **flow exporter** command in global configuration mode. To remove a flow exporter, use the **no** form of this command.

**flow exporter** *exporter-name*  
**no flow exporter** *exporter-name*

<b>Syntax Description</b>	<i>exporter-name</i> Name of the flow exporter that is being created or modified.
---------------------------	-----------------------------------------------------------------------------------

<b>Command Default</b>	flow exporters are not present in the configuration.
------------------------	------------------------------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

<b>Usage Guidelines</b>	Flow exporters export the data in the flow monitor cache to a remote system, such as a server running NetFlow collector, for analysis and storage. Flow exporters are created as separate entities in the configuration. Flow exporters are assigned to flow monitors to provide data export capability for the flow monitors. You can create several flow exporters and assign them to one or more flow monitors to provide several export destinations. You can create one flow exporter and apply it to several flow monitors.
-------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>Examples</b>	The following example creates a flow exporter named FLOW-EXPORTER-1 and enters flow exporter configuration mode:
-----------------	------------------------------------------------------------------------------------------------------------------

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)#
```

# flow monitor

To create a flow monitor, or to modify an existing flow monitor, and enter flow monitor configuration mode, use the **flow monitor** command in global configuration mode. To remove a flow monitor, use the **no** form of this command.

**flow monitor** *monitor-name*  
**no flow monitor** *monitor-name*

<b>Syntax Description</b>	<i>monitor-name</i> Name of the flow monitor that is being created or modified.
---------------------------	---------------------------------------------------------------------------------

<b>Command Default</b>	flow monitors are not present in the configuration.
------------------------	-----------------------------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

<b>Usage Guidelines</b>	Flow monitors are the component that is applied to interfaces to perform network traffic monitoring. Flow monitors consist of a flow record and a cache. You add the record to the flow monitor after you create the flow monitor. The flow monitor cache is automatically created at the time the flow monitor is applied to the first interface. Flow data is collected from the network traffic during the monitoring process based on the key and nonkey fields in the flow monitor's record and stored in the flow monitor cache.
-------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>Examples</b>	The following example creates a flow monitor named FLOW-MONITOR-1 and enters flow monitor configuration mode:
-----------------	---------------------------------------------------------------------------------------------------------------

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)#
```

# flow record

To create a flow record, or to modify an existing flow record, and enter flow record configuration mode, use the **flow record** command in global configuration mode. To remove a record, use the **no** form of this command.

```
flow record record-name
no flow record record-name
```

<b>Syntax Description</b>	<i>record-name</i> Name of the flow record that is being created or modified.
---------------------------	-------------------------------------------------------------------------------

<b>Command Default</b>	A flow record is not configured.
------------------------	----------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

<b>Usage Guidelines</b>	A flow record defines the keys that uses to identify packets in the flow, as well as other fields of interest that gathers for the flow. You can define a flow record with any combination of keys and fields of interest. The supports a rich set of keys. A flow record also defines the types of counters gathered per flow. You can configure 64-bit packet or byte counters.
-------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>Examples</b>	The following example creates a flow record named FLOW-RECORD-1, and enters flow record configuration mode:
-----------------	-------------------------------------------------------------------------------------------------------------

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)#
```

## ftp-path

To configure the path at the FTP server for trace log export, use the **ftp-path** command. Use the **no** form of the command to negate the command or to set the command to its default.

```
ftp-path ftp-path
```

```
no ftp-path ftp-path
```

<b>Syntax Description</b>	<i>ftp-path</i> Specifies the path at the FTP server.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Wireless trace export profile FTP configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.2s</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.				

### Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode ftp
Device(config-wireless-trace-export-profile-ftp)# ftp-path
ip-address/download/object/stream/images/ap-images
```

## ftp-password

To configure the FTP server password for trace export, use the **ftp-password** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
ftp-password} <Enter password> <Re-enter password>
```

```
no ftp-password <Enter password> <Re-enter password>
```

<b>Syntax Description</b>	<i>password</i>	Specifies the FTP server password.
	<i>re-enter password</i>	Indicates that the user must re-enter the FTP server password.
<b>Command Default</b>	None	
<b>Command Modes</b>	Wireless trace export profile FTP configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

### Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode ftp
Device(config-wireless-trace-export-profile-ftp)# ftp-password xxxxxxxx xxxxxxxx
```

## ftp-server

To configure the FTP server address for trace export, use the **ftp-server** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
ftp-server {A.B.C.D | X:X:X:X::X}
```

```
no ftp-server {A.B.C.D | X:X:X:X::X}
```

Syntax Description	
<i>A.B.C.D</i>	Specifies the FTP IPv4 server address.
<i>X:X:X:X::X</i>	Specifies the FTP IPv6 server address.

Command Default	None
-----------------	------

Command Modes	Wireless trace export profile FTP configuration
---------------	-------------------------------------------------

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

### Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode ftp
Device(config-wireless-trace-export-profile-ftp)# ftp-server 10.1.1.1
```

## ftp-username

To configure the FTP server username for trace export, use the **ftp-username** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
ftp-username Username
```

```
no ftp-username Username
```

<b>Syntax Description</b>	<i>username</i> Specifies the FTP server username.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Wireless trace export profile FTP configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.2s</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.				

### Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode ftp
Device(config-wireless-trace-export-profile-ftp)# ftp-username ftp-server-username
```

ftp-username





## Configuration Commands: g to z

---

- `idle-timeout` , on page 261
- `image-download-mode` , on page 262
- `inactive-timeout`, on page 263
- `install add file tftp`, on page 264
- `install add profile default`, on page 265
- `install activate`, on page 267
- `install activate auto-abort-timer`, on page 268
- `install activate file`, on page 269
- `install auto-abort-timer stop`, on page 270
- `install commit`, on page 271
- `install remove file backup_image`, on page 272
- `install remove profile default` , on page 273
- `install deactivate` , on page 274
- `install rollback`, on page 275
- `interface vlan`, on page 276
- `ip access-group`, on page 277
- `ip access-list extended` , on page 278
- `ip address`, on page 279
- `ip dhcp pool`, on page 281
- `ip dhcp-relay information option server-override`, on page 282
- `ip dhcp-relay source-interface`, on page 284
- `ip domain-name` , on page 285
- `ip flow monitor`, on page 286
- `ip flow-export destination`, on page 287
- `ip helper-address`, on page 288
- `ip http client secure-ciphersuite`, on page 291
- `ip http secure-ciphersuite`, on page 292
- `ip http secure-server`, on page 294
- `ip http server`, on page 296
- `ip ssh`, on page 298
- `ip ssh version`, on page 300
- `ip tftp blocksize`, on page 302
- `ip verify source`, on page 303

- [ipv4 acl](#), on page 304
- [ipv4 dhcp](#) , on page 305
- [ipv4 flow monitor](#) , on page 306
- [ipv4 flow monitor output](#), on page 307
- [ipv6 flow monitor input](#), on page 308
- [ipv6 flow monitor output](#), on page 309
- [ipv6 access-list](#), on page 310
- [ipv6 acl](#), on page 312
- [ipv6-address-type](#), on page 313
- [ipv6 address](#), on page 314
- [ipv6 dhcp pool](#), on page 316
- [ipv6 enable](#), on page 319
- [ipv6 mld snooping](#), on page 321
- [ipv6 nd managed-config-flag](#) , on page 322
- [ipv6 nd other-config-flag](#) , on page 323
- [ipv6 nd ra throttler attach-policy](#) , on page 324
- [ipv6 nd rguard policy](#), on page 325
- [ipv6 snooping policy](#), on page 327
- [ipv6 traffic-filter](#) , on page 328
- [key chain](#), on page 329
- [key config-key](#), on page 330
- [key config-key password-encrypt](#), on page 331
- [license air level](#), on page 332
- [license smart \(global config\)](#), on page 336
- [license smart \(privileged EXEC\)](#), on page 346
- [local-admin-mac deny](#) , on page 352
- [local-auth ap eap-fast](#) , on page 353
- [local-site](#) , on page 354
- [location expiry](#) , on page 355
- [location notify-threshold](#), on page 356
- [log-export-mode](#) , on page 357
- [mab request format attribute](#), on page 358
- [mac-filtering](#) , on page 359
- [match activated-service-template](#), on page 360
- [match any](#) , on page 362
- [match message-type](#), on page 363
- [match non-client-nrt](#), on page 364
- [match protocol](#), on page 365
- [match service-instance](#), on page 368
- [match service-type](#), on page 369
- [match user-role](#) , on page 370
- [match username](#), on page 371
- [match \(access-map configuration\)](#), on page 372
- [match \(class-map configuration\)](#), on page 374
- [match wlan user-priority](#), on page 377
- [max-bandwidth](#) , on page 378

- max-through, on page 379
- mdns-sd, on page 380
- mdns-sd-interface, on page 381
- mdns-sd flex-profile, on page 382
- mdns-sd profile, on page 383
- method fast , on page 384
- mgmtuser username , on page 385
- mop sysid, on page 386
- nac, on page 387
- nas-id option2 , on page 388
- network , on page 389
- nmsp cloud-services enable , on page 390
- nmsp cloud-services http-proxy , on page 391
- nmsp cloud-services server token , on page 392
- nmsp cloud-services server url, on page 393
- nmsp notification interval, on page 394
- nmsp strong-cipher, on page 396
- option, on page 397
- parameter-map type subscriber attribute-to-service , on page 399
- password encryption aes, on page 400
- peer-blocking, on page 401
- policy, on page 402
- police, on page 403
- police cir, on page 405
- policy-map, on page 406
- policy-map, on page 408
- port, on page 410
- priority priority-value, on page 411
- public-ip, on page 412
- qos video, on page 413
- radius server, on page 414
- radius-server attribute wireless accounting call-station-id, on page 415
- radius-server attribute wireless authentication call-station-id, on page 417
- range, on page 419
- record wireless avc basic, on page 420
- redirect , on page 421
- redirect portal , on page 422
- remote-lan, on page 423
- request platform software trace archive, on page 424
- rf tag, on page 425
- rrc-evaluation, on page 426
- security , on page 427
- security dot1x authentication-list, on page 428
- security ft, on page 429
- security pmf, on page 431
- security static-wep-key , on page 433

- security web-auth, on page 434
- security wpa akm, on page 435
- security wpa akm owe, on page 437
- security wpa akm psk, on page 438
- security wpa akm sae, on page 439
- sensor-name, on page 440
- service-key, on page 441
- service-policy (WLAN), on page 442
- service-policy qos , on page 443
- service-template, on page 444
- service timestamps, on page 445
- session-timeout, on page 447
- set, on page 448
- sftp-image-path (image-download-mode sftp), on page 455
- sftp-image-server (image-download-mode sftp), on page 456
- sftp-password (image-download-mode sftp), on page 457
- sftp-password (trace-export), on page 458
- sftp-path, on page 459
- sftp-server, on page 460
- sftp-username (image-download-mode sftp), on page 461
- sftp-username (trace-export), on page 462
- software auto-upgrade enable, on page 463
- statistics ap-system-monitoring alarm-enable, on page 464
- statistics ap-system-monitoring alarm-hold-time, on page 465
- statistics ap-system-monitoring alarm-retransmit-time, on page 466
- statistics ap-system-monitoring cpu-threshold, on page 467
- statistics ap-system-monitoring enable, on page 468
- statistics ap-system-monitoring mem-threshold, on page 469
- statistics ap-system-monitoring sampling-interval, on page 470
- statistics ap-system-monitoring stats-interval, on page 471
- stealthwatch-cloud-monitor, on page 472
- tag rf, on page 473
- tag site, on page 474
- tftp-image-path (image-download-mode tftp), on page 475
- tftp-image-server (image-download-mode tftp), on page 476
- tftp-path, on page 477
- tftp-server, on page 478
- trapflags ap ap-stats, on page 479
- udp-timeout, on page 480
- umbrella-param-map, on page 481
- update-timer, on page 482
- url, on page 483
- urlfilter list, on page 484
- usb-enable, on page 485
- username, on page 486
- violation, on page 488

- wgb broadcast-tagging, on page 489
- wgb vlan, on page 490
- whitelist acl, on page 491
- wired-vlan-range, on page 492
- config wlan assisted-roaming, on page 493
- wireless aaa policy, on page 494
- wireless aaa policy, on page 495
- wireless autoqos policy-profile , on page 496
- wireless broadcast vlan, on page 497
- wireless client, on page 498
- wireless client mac-address, on page 500
- wireless config validate , on page 505
- wireless country, on page 507
- wireless exclusionlist mac address, on page 508
- wireless ipv6 ra wired, on page 509
- wireless load-balancing, on page 510
- wireless macro-micro steering transition-threshold , on page 511
- wireless macro-micro steering probe-suppression, on page 512
- wireless management certificate, on page 513
- wireless management interface, on page 514
- wireless management trustpoint, on page 515
- wireless ewc-ap ap ap-type, on page 516
- wireless ewc-ap ap capwap, on page 517
- wireless ewc-ap ap reload, on page 518
- wireless ewc-ap ap shell , on page 519
- wireless ewc-ap ap shell username, on page 520
- wireless ewc-ap preferred-master, on page 521
- wireless ewc-ap factory-reset, on page 522
- wireless ewc-ap vrrp vrid, on page 523
- wireless profile flex, on page 524
- wireless profile image-download default, on page 525
- wireless profile policy, on page 526
- wireless profile transfer, on page 527
- wireless rfid, on page 528
- wireless security dot1x, on page 529
- wireless security dot1x radius accounting mac-delimiter, on page 531
- wireless security dot1x radius accounting username-delimiter, on page 532
- wireless security dot1x radius callStationIdCase, on page 533
- wireless security dot1x radius mac-authentication call-station-id, on page 534
- wireless security dot1x radius mac-authentication mac-delimiter, on page 535
- wireless security web-auth retries, on page 536
- wireless tag policy, on page 537
- wireless tag site, on page 538
- wireless wps ap-authentication threshold, on page 539
- wireless wps client-exclusion, on page 540
- wireless wps mfp ap-impersonation, on page 542

- [wireless wps rogue network-assurance enable](#), on page 543
- [wireless wps rogue ap aaa](#) , on page 544
- [wireless wps rogue ap aaa polling-interval](#), on page 545
- [wireless wps rogue ap init-timer](#), on page 546
- [wireless wps rogue ap mac-address rldp initiate](#) , on page 547
- [wireless wps rogue ap notify-min-rssi](#), on page 548
- [wireless wps rogue ap notify-rssi-deviation](#), on page 549
- [wireless wps rogue ap rldp alarm-only](#), on page 550
- [wireless wps rogue ap rldp alarm-only monitor-ap-only](#), on page 551
- [wireless wps rogue ap rldp auto-contain](#), on page 552
- [wireless wps rogue ap rldp retries](#), on page 553
- [wireless wps rogue ap rldp schedule](#), on page 554
- [wireless wps rogue ap rldp schedule day](#), on page 555
- [wireless wps rogue ap timeout](#), on page 556
- [wireless wps rogue auto-contain](#) , on page 557
- [wireless wps rogue client aaa](#), on page 558
- [wireless wps rogue client mse](#), on page 559
- [wireless wps rogue client client-threshold](#) , on page 560
- [wireless wps rogue client notify-min-rssi](#), on page 561
- [wireless wps rogue client notify-rssi-deviation](#), on page 562
- [wireless wps rogue rule](#), on page 563
- [wireless wps rogue security-level](#), on page 565
- [wireless-default radius server](#), on page 566
- [wlan policy](#) , on page 567

# idle-timeout

To configure the idle-timeout value in seconds for a wireless profile policy, use the **idle-timeout** command.

**idle-timeout** *value*

<b>Syntax Description</b>	<i>value</i> Sets the idle-timeout value. Valid range is 15 to 100000 seconds.	
<b>Command Default</b>	None	
<b>Command Modes</b>	config-wireless-policy	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to set the idle-timeout in a wireless profile policy:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy policy-profile-name
Device(config-wireless-policy)# idle-timeout 100
```

# image-download-mode

To configure image download using the HTTP, SFTP, TFTP, or CCO modes, use the **image-download-mode** command.

**image-download-mode** { **http** | **sftp** | **tftp** | **cco** }

<b>Syntax Description</b>	<b>http</b> Configures image download using the HTTP mode.						
	<b>sftp</b> Configures image download using the SFTP mode.						
	<b>tftp</b> Configures image download using the TFTP mode.						
	<b>cco</b> Configures image download using the CCO mode.						
<b>Command Default</b>	None						
<b>Command Modes</b>	Wireless image download profile configuration mode						
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.2s</td> <td>This command was introduced.</td> </tr> <tr> <td>Cisco IOS XE Amsterdam 17.1.1s</td> <td>The <b>image-download-mode cco</b> was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.	Cisco IOS XE Amsterdam 17.1.1s	The <b>image-download-mode cco</b> was introduced.
Release	Modification						
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.						
Cisco IOS XE Amsterdam 17.1.1s	The <b>image-download-mode cco</b> was introduced.						

## Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode http
```



# inactive-timeout

To enable in-active timer, use the **inactive-timeout** command.

**inactive-timeout** *timeout-in-seconds*

<b>Syntax Description</b>	<i>timeout-in-seconds</i> Specifies the inactive flow timeout value. The range is from 1 to 604800.				
<b>Command Default</b>	None				
<b>Command Modes</b>	ET-Analytics configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.				

This example shows how to enable in-active timer in the ET-Analytics configuration mode:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# et-analytics
Device(config-et-analytics)# inactive-timeout 15
Device(config-et-analytics)# end
```

# install add file tftp

To install a package file to the system, use the **install add file tftp** command.

**install add file tftp:** *tftp file path*

<b>Syntax Description</b>	<b>install add file tftp:</b> The <b>install add</b> command copies the file from the external server to the backup_image directory on the embedded wireless controller.
---------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC mode
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

## Example

This example shows how to install a package file to the system:

```
Device#install add file tftp://<server-ip>/<path>/<smu-filename>
```

# install add profile default

To download the embedded wireless controller image from the external server, use the **install add profile default** command.

**install add profile** *profile\_name***activatecommitprompt-level none**

Syntax Description	add	Installs a package file to the system.
	<b>profile</b>	Selects a profile.
	<i>profile_name</i>	Adds a profile name with a maximum of 15 characters. Specify <b>default</b> to trigger the default behaviour.
	<b>activate</b>	Activates the installed profile.
	<b>commit</b>	Commits the changes to the loadpath.
	<b>prompt-level</b>	Sets the prompt-level to none.

**Command Default** None

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

**Usage Guidelines** Ensure that you have the *image-download-profile* configured on embedded wireless controller. Extract the contents of the image bundle (.zip archive) to an external TFTP or HTTP(S) server. The .zip archive contains the controller image and various compatible AP images (apXgY).

## Example

The following example shows how to download the embedded wireless controller image:

```
Device#install add profile default

install_add: START Thu Jan 24 20:08:01 UTC 2019
Jan 24 20:08:03.389: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
add
Jan 24 20:08:03.389 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
add
install_add: Default profile addition successful
SUCCESS: install_add Thu Jan 24 20:08:03 UTC 2019
Jan 24 20:08:04.358: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install add
Jan 24 20:08:04.358 %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install add
WLC#
*Jan 24 20:08:03.350: %INSTALL-5-INSTALL_START_INFO: Chassis 1 R0/0: install_engine: Started
install add
```

```
*Jan 24 20:08:04.335: %INSTALL-5-INSTALL_COMPLETED_INFO: Chassis 1 R0/0: install_engine:  
Completed install add
```



---

**Note** The log `Completed install add` means that the command is successful and the download will start soon.

---

The following example verifies the the image download status:

```
Device#sh wireless ewc-ap predownload status
```

# install activate

To activate an installed package, use the **install activate** command.

**install activate** { **auto-abort-timer** | **file** | **profile** | **prompt-level** }

<b>Syntax Description</b>	<b>auto-abort-timer</b>	Sets the cancel timer. The time range is between 30 and 1200 minutes.
	<b>file</b>	Specifies the package to be activated.
	<b>profile</b>	Specifies the profile to be activated.
	<b>prompt-level</b>	Sets the prompt level.
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC (#)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

## Example

The following example shows how to activate the installed package:

```
Device# install activate profile default
install_activate: START Thu Nov 24 20:14:53 UTC 2019

System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q] y
Building configuration...
[OK]Modified configuration has been saved
Jan 24 20:15:02.745: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
activate
Jan 24 20:15:02.745 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
activate
install_activate: Activating PACKAGE
```

## install activate auto-abort-timer

To set the abort timer, use the **install activate auto-abort-timer** command.

**install activate auto-abort-timer** *<30-1200>* **prompt-level none**

Syntax Description	auto-abort-timer	Sets the cancel timer. The time range is between 30 and 1200 minutes.
	<i>&lt;30-1200&gt;</i>	Specifies the cancel timer time in minutes.
	<b>prompt-level</b>	Specifies the prompt level.
	<b>none</b>	Specifies no prompting.

**Command Default** None

**Command Modes** Privileged EXEC (#)

Task ID	Task ID	Operation
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

### Example

The following example shows how to activate the cancel timer:

```
Device#install activate auto-abort-timer 30 prompt-level none
```

# install activate file

To activate an installed package, use the **install activate file** command.

**install activate file** *file-name*

<b>Syntax Description</b>	<i>file-name</i> Specifies the package name. Options are: bootflash:, flash:, and webui:.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC (#)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

## Example

The following example shows how to use an auto cancel timer while activating an install package on a standby location:

```
Device# install activate file vwlc_aps_16.11.1.0_74.bin
```

# install auto-abort-timer stop

To stop the auto abort timer, use the **install auto-abort-timer stop** command.

## install auto-abort-timer stop

<b>Syntax Description</b>	<b>auto-abort-timer stop</b> Stops the auto-abort-timer	
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC (#)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

## Example

This example shows how to stop the auto abort timer:

```
Device#install auto-abort-timer stop
```



# install commit

To commit the changes to the loadpath, use the **install commit** command.

**install commit**

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

## Example

The following example shows how to commit the changes to the loadpath:

```
Device# install commit
```

# install remove file backup\_image

To remove installed packages, use the **install remove file backup\_image** command.

**install remove file backup\_image** *filename*

<b>Syntax Description</b>	<i>filename</i> Specifies the file that needs to be removed.
---------------------------	--------------------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

## Example

This example shows how a file is removed from the package:

```
Device#install remove file backup_image: file_name
```

# install remove profile default

To specify an install package that is to be removed, use the **install remove profile default** command.

## install remove profile default

<b>Syntax Description</b>	<b>remove</b> Removes the install package.				
	<b>profile</b> Specifies the profile to be removed.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Privileged EXEC (#)				
<b>Command History</b>	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Gibraltar 16.11.1</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE Gibraltar 16.11.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.				

### Example

The following example shows how to remove a default profile:

```
Device# install remove profile default
```

# install deactivate

To specify an install package that is to be deactivated, use the **install deactivate file** command.

**install deactivate file** *file-name*

<b>Syntax Description</b>	<i>file-name</i> Specifies the package name. Options are: bootflash:, flash:, and webui:.
---------------------------	-------------------------------------------------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

## Example

The following example shows how to deactivate an install package:

```
Device# install deactivate file vwlc_aps_16.11.1.0_74.bin
```

# install rollback

To roll back to a particular installation point, use the **install rollback** command.

**install rollback to** { **base** | **committed** | **id** *id* | **label** *label* } [**prompt-level** **none**]

Syntax Description	base	Rolls back to the base image.
	<b>prompt-level none</b>	Sets the prompt level as none.
	<b>committed</b>	Rolls back to the last committed installation point.
	<b>id</b>	Rolls back to a specific install point ID.
	<b>label</b>	Rolls back to a specific install point label.

**Command Default** None

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

## Example

The following example shows how to specify the ID of the install point to roll back to:

```
Device# install rollback to id 1
```

# interface vlan

To create or access a dynamic switch virtual interface (SVI) and to enter interface configuration mode, use the **interface vlan** command in global configuration mode. To delete an SVI, use the **no** form of this command.

**interface vlan** *vlan-id*  
**no interface vlan** *vlan-id*

<b>Syntax Description</b>	<i>vlan-id</i>	VLAN number. The range is 1 to 4094.
<b>Command Default</b>	The default VLAN interface is VLAN 1.	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
<b>Usage Guidelines</b>	SVIs are created the first time you enter the <b>interface vlan</b> <i>vlan-id</i> command for a particular VLAN. The <i>vlan-id</i> corresponds to the VLAN-tag associated with data frames on an IEEE 802.1Q encapsulated trunk or the VLAN ID configured for an access port.	



**Note** When you create an SVI, it does not become active until it is associated with a physical port.

If you delete an SVI using the **no interface vlan** *vlan-id* command, it is no longer visible in the output from the **show interfaces** privileged EXEC command.



**Note** You cannot delete the VLAN 1 interface.

You can reinstate a deleted SVI by entering the **interface vlan** *vlan-id* command for the deleted interface. The interface comes back up, but the previous configuration is gone.

The interrelationship between the number of SVIs configured on a and the number of other features being configured might have an impact on CPU utilization due to hardware limitations. You can use the **sdm prefer** global configuration command to reallocate system hardware resources based on templates and feature tables.

You can verify your setting by entering the **show interfaces** and **show interfaces vlan** *vlan-id* privileged EXEC commands.

This example shows how to create a new SVI with VLAN ID 23 and enter interface configuration mode:

```
Device(config)# interface vlan 23
Device(config-if)#
```

## ip access-group

To configure WLAN access control group (ACL), use the **ip access-group** command. To remove a WLAN ACL group, use the **no** form of the command.

```
ip access-group [web] acl-name
no ip access-group [web]
```

<b>Syntax Description</b>	<p><b>web</b> (Optional) Configures the IPv4 web ACL.</p> <p><i>acl-name</i> Specify the preauth ACL used for the WLAN with the security type value as webauth.</p>				
<b>Command Default</b>	None				
<b>Command Modes</b>	WLAN configuration				
<b>Usage Guidelines</b>	You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.				

This example shows how to configure a WLAN ACL:

```
Device#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#wlan wlan1
Device(config-wlan)#ip access-group test-acl
```

This example shows how to configure an IPv4 WLAN web ACL:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# ip access-group web test
Device(config-wlan)#
```

## ip access-list extended

To configure extended access list, use the **ip access-list extended** command.

```
ip access-list extended {<100-199> | <2000-2699>} access-list-name
```

<b>Syntax Description</b>	<100-199> Extended IP access-list number.
	<2000-2699> Extended IP access-list number (expanded range).
<b>Command Default</b>	None
<b>Command Modes</b>	Global configuration (config)
<b>Command History</b>	<b>Release</b>
	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1 This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

### Examples

The following example shows how to configure extended access list:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ip access-list extended access-list-name
```



# ip address

To set a primary or secondary IP address for an interface, use the **ip address** command in interface configuration mode. To remove an IP address or disable IP processing, use the no form of this command.

```
ip address ip-address mask [secondary [vrf vrf-name]]
no ip address ip-address mask [secondary [vrf vrf-name]]
```

Syntax Description	
<i>ip-address</i>	IP address.
<i>mask</i>	Mask for the associated IP subnet.
<b>secondary</b>	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.  <b>Note</b> If the secondary address is used for a VRF table configuration with the <b>vrf</b> keyword, the <b>vrf</b> keyword must be specified also.
<b>vrf</b>	(Optional) Name of the VRF table. The <i>vrf-name</i> argument specifies the VRF name of the ingress interface.

**Command Default** No IP address is defined for the interface.

**Command Modes** Interface configuration (config-if)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the Cisco IOS software always use the primary IP address. Therefore, all devices and access servers on a segment should share the same primary network number.

Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) mask request message. Devices respond to this request with an ICMP mask reply message.

You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command. If the software detects another host using one of its IP addresses, it will print an error message on the console.

The optional **secondary** keyword allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.

Secondary IP addresses can be used in a variety of situations. The following are the most common applications:

- There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need 300 host addresses. Using

secondary IP addresses on the devices or access servers allows you to have two logical subnets using one physical subnet.

- Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnetted, device-based network. Devices on an older, bridged segment can be easily made aware that many subnets are on that segment.
- Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is *extended*, or layered on top of the second network using secondary addresses.



#### Note

- If any device on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.
- When you are routing using the Open Shortest Path First (OSPF) algorithm, ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.
- If you configure a secondary IP address, you must disable sending ICMP redirect messages by entering the **no ip redirects** command, to avoid high CPU utilization.

#### Examples

In the following example, 192.108.1.27 is the primary address and 192.31.7.17 is the secondary address for GigabitEthernet interface 1/0/1:

```
Device# enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 192.108.1.27 255.255.255.0
Device(config-if)# ip address 192.31.7.17 255.255.255.0 secondary
```

#### Related Commands

Command	Description
<b>match ip route-source</b>	Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.
<b>route-map</b>	Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
<b>set vrf</b>	Enables VPN VRF selection within a route map for policy-based routing VRF selection.
<b>show ip arp</b>	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.
<b>show ip interface</b>	Displays the usability status of interfaces configured for IP.
<b>show route-map</b>	Displays static and dynamic route maps.

# ip dhcp pool

To configure a Dynamic Host Configuration Protocol (DHCP) address pool on a DHCP server and enter DHCP pool configuration mode, use the **ip dhcp pool** command in global configuration mode. To remove the address pool, use the no form of this command.

**ip dhcp pool** *name*  
**no ip dhcp pool** *name*

<b>Syntax Description</b>	<i>name</i>	Name of the pool. Can either be a symbolic string (such as engineering) or an integer (such as 0).
---------------------------	-------------	----------------------------------------------------------------------------------------------------

**Command Default** DHCP address pools are not configured.

**Command Modes** Global configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(1)T	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

**Usage Guidelines** During execution of this command, the configuration mode changes to DHCP pool configuration mode, which is identified by the (config-dhcp)# prompt. In this mode, the administrator can configure pool parameters, like the IP subnet number and default router list.

**Examples** The following example configures pool1 as the DHCP address pool:

```
ip dhcp pool pool1
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>host</b>	Specifies the IP address and network mask for a manual binding to a DHCP client.
	<b>ip dhcp excluded-address</b>	Specifies IP addresses that a Cisco IOS DHCP server should not assign to DHCP clients.
	<b>network (DHCP)</b>	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.

## ip dhcp-relay information option server-override

To enable the system to globally insert the server ID override and link selection suboptions into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a Dynamic Host Configuration Protocol (DHCP) server, use the **ip dhcp-relay information option server-override** command in global configuration mode. To disable inserting the server ID override and link selection suboptions into the DHCP relay agent information option, use the **no** form of this command.

**ip dhcp-relay information option server-override**  
**no ip dhcp-relay information option server-override**

**Syntax Description** This command has no arguments or keywords.

**Command Default** The server ID override and link selection suboptions are not inserted into the DHCP relay agent information option.

**Command Modes** Global configuration (config)

### Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

### Usage Guidelines

The **ip dhcp-relay information option server-override** command adds the following suboptions into the relay agent information option when DHCP broadcasts are forwarded by the relay agent from clients to a DHCP server:

- Server ID override suboption
- Link selection suboption

When this command is configured, the gateway address (giaddr) will be set to the IP address of the outgoing interface, which is the interface that is reachable by the DHCP server.

If the **ip dhcp relay information option server-id-override** command is configured on an interface, it overrides the global configuration on that interface only.

### Examples

In the following example, the DHCP relay will insert the server ID override and link selection suboptions into the relay information option of the DHCP packet. The loopback interface IP address is configured to be the source IP address for the relayed messages.

```
Device(config)# ip dhcp-relay information option server-override
Device(config)# ip dhcp-relay source-interface loopback 0
Device(config)# interface Loopback 0
Device(config-if)# ip address 10.2.2.1 255.255.255.0
```

Related Commands	Command	Description
	<b>ip dhcp relay information option server-id-override</b>	Enables the system to insert the server ID override and link selection suboptions on a specific interface into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.

## ip dhcp-relay source-interface

To globally configure the source interface for the relay agent to use as the source IP address for relayed messages, use the **ip dhcp-relay source-interface** command in global configuration mode. To remove the source interface configuration, use the **no** form of this command.

**ip dhcp-relay source-interface** *type number*  
**no ip dhcp-relay source-interface** *type number*

Syntax Description	Parameter	Description
	<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
	<i>number</i>	Interface or subinterface number. For more information about the numbering system for your networking device, use the question mark (?) online help function.

**Command Default** The source interface is not configured.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
	12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
	15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

**Usage Guidelines** The **ip dhcp-relay source-interface** command allows the network administrator to specify a stable, hardware-independent IP address (such as a loopback interface) for the relay agent to use as a source IP address for relayed messages.

If the **ip dhcp-relay source-interface** global configuration command is configured and the **ip dhcp relay source-interface** command is also configured, the **ip dhcp relay source-interface** command takes precedence over the global configuration command. However, the global configuration is applied to interfaces without the interface configuration.

### Examples

In the following example, the loopback interface IP address is configured to be the source IP address for the relayed messages:

```
Device(config)# ip dhcp-relay source-interface loopback 0
Device(config)# interface loopback 0
Device(config-if)# ip address 10.2.2.1 255.255.255.0
```

Related Commands	Command	Description
	<b>ip dhcp relay source-interface</b>	Configures the source interface for the relay agent to use as the source IP address for relayed messages.

# ip domain-name

To configure the host domain on the device, use the **ip domain-name** command.

**ip domain-name** *domain-name* [**vrf** *vrf-name*]

## Syntax Description

*domain-name* Default domain name.

*vrf-name* Specifies the virtual routing and forwarding (VRF) to use to resolve the domain name.

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to configure a host domain in a device:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ip domain-name domain-name
```

## ip flow monitor

To configure IP NetFlow monitoring, use the **ip flow monitor** command. To remove IP NetFlow monitoring, use the **no** form of this command.

```
ip flow monitor ip-monitor-name {input | output}
no ip flow monitor ip-monitor-name {input | output}
```

<b>Syntax Description</b>	<i>ip-monitor-name</i> Flow monitor name.				
<b>input</b>	Enables a flow monitor for ingress traffic.				
<b>output</b>	Enables a flow monitor for egress traffic.				
<b>Command Default</b>	None				
<b>Command Modes</b>	WLAN configuration				
<b>Usage Guidelines</b>	You must disable the WLAN before using this command.				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.				

This example shows how to configure an IP flow monitor for the ingress traffic:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# ip flow monitor test input
```

This example shows how to disable an IP flow monitor:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no ip flow monitor test input
```



## ip flow-export destination

To configure ETA flow export destination, use the **ip flow-export destination** command.

**ip flow-export destination** *ip\_address port\_number*

<b>Syntax Description</b>	<i>port_number</i> Port number. The range is from 1 to 65535.
---------------------------	---------------------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	ET-Analytics configuration
----------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to configure ETA flow export destination in the ET-Analytics configuration mode:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# et-analytics
Device(config-et-analytics)# ip flow-export
destination 120.0.0.1 2055
Device(config-et-analytics)# end
```

## ip helper-address

To enable forwarding of User Datagram Protocol (UDP) broadcasts, including Bootstrap Protocol (BOOTP), received on an interface, use the **ip helper-address** command in interface configuration mode. To disable forwarding of broadcast packets to specific addresses, use the **no** form of this command.

```
ip helper-address [{vrf name | global}] address {[redundancy vrg-name]}
no ip helper-address [{vrf name | global}] address {[redundancy vrg-name]}
```

### Syntax Description

<b>vrf</b> <i>name</i>	(Optional) Enables the VPN routing and forwarding (VRF) instance and the VRF name.
<b>global</b>	(Optional) Configures a global routing table.
<i>address</i>	Destination broadcast or host address to be used when forwarding UDP broadcasts. There can be more than one helper address per interface.
<b>redundancy</b> <i>vrg-name</i>	(Optional) Defines the Virtual Router Group (VRG) name.

### Command Default

UDP broadcasts are not forwarded.

### Command Modes

Interface configuration (config-if)

### Command History

Release	Modification
10.0	This command was introduced.
12.2(4)B	This command was modified. The <b>vrf name</b> keyword and argument pair and the <b>global</b> keyword were added.
12.2(15)T	This command was modified. The <b>redundancy vrg-name</b> keyword and argument pair was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

### Usage Guidelines

The **ip forward-protocol** command along with the **ip helper-address** command allows you to control broadcast packets and protocols that are forwarded.

One common application that requires helper addresses is DHCP, which is defined in RFC 1531. To enable BOOTP or DHCP broadcast forwarding for a set of clients, configure a helper address on the router interface connected to the client. The helper address must specify the address of the BOOTP or DHCP server. If you have multiple servers, configure one helper address for each server.

The following conditions must be met for a UDP or IP packet to be able to use the **ip helper-address** command:

- The MAC address of the received frame must be all-ones broadcast address (ffff.ffff.ffff).

- The IP destination address must be one of the following: all-ones broadcast (255.255.255.255), subnet broadcast for the receiving interface, or major-net broadcast for the receiving interface if the **no ip classless** command is also configured.
- The IP time-to-live (TTL) value must be at least 2.
- The IP protocol must be UDP (17).
- The UDP destination port must be for TFTP, Domain Name System (DNS), Time, NetBIOS, ND, BOOTP or DHCP packet, or a UDP port specified by the **ip forward-protocol udp** command in global configuration mode.

If the DHCP server resides in a VPN or global space that is different from the interface VPN, then the **vrf name** or the **global** option allows you to specify the name of the VRF or global space in which the DHCP server resides.

The **ip helper-address vrfname address** option uses the address associated with the VRF name regardless of the VRF of the incoming interface. If the **ip helper-address vrfname address** command is configured and later the VRF is deleted from the configuration, then all IP helper addresses associated with that VRF name will be removed from the interface configuration.

If the **ip helper-address address** command is already configured on an interface with no VRF name configured, and later the interface is configured with the **ip helper-address vrf name address** command, then the previously configured **ip helper-address address** command is considered to be global.



**Note** The **ip helper-address** command does not work on an X.25 interface on a destination router because the router cannot determine if the packet was intended as a physical broadcast.

The **service dhcp** command must be configured on the router to enable IP helper statements to work with DHCP. If the command is not configured, the DHCP packets will not be relayed through the IP helper statements. The **service dhcp** command is configured by default.

## Examples

The following example shows how to define an address that acts as a helper address:

```
Router(config)# interface ethernet 1
Router(config-if)# ip helper-address 10.24.43.2
```

The following example shows how to define an address that acts as a helper address and is associated with a VRF named host1:

```
Router(config)# interface ethernet 1/0
Router(config-if)# ip helper-address vrf host1 10.25.44.2
```

The following example shows how to define an address that acts as a helper address and is associated with a VRG named group1:

```
Router(config)# interface ethernet 1/0
Router(config-if)# ip helper-address 10.25.45.2 redundancy group1
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ip forward-protocol</b>	Specifies which protocols and ports the router forwards when forwarding broadcast packets.
<b>service dhcp</b>	Enables the DHCP server and relay agent features on the router.

## ip http client secure-ciphersuite

To specify the CipherSuite that should be used for encryption over the secure HTTP connection from the client to a remote server, use the **ip http client secure-ciphersuite** command in global configuration mode. To remove a previously configured CipherSuite specification for the client, use the **no** form of this command.

```
ip http client secure-ciphersuite [3des-ede-cbc-sha] [rc4-128-sha] [rc4-128-md5] [des-cbc-sha]
no ip http client secure-ciphersuite
```

Syntax Description	
<b>3des-ede-cbc-sha</b>	SSL_RSA_WITH_3DES_EDE_CBC_SHA--Rivest, Shamir, and Adleman (RSA) key exchange with 3DES and DES-EDE3-CBC for message encryption and Secure Hash Algorithm (SHA) for message digest.
<b>rc4-128-sha</b>	SSL_RSA_WITH_RC4_128_SHA--RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and SHA for message digest.
<b>rc4-128-md5</b>	SSL_RSA_WITH_RC4_128_MD5--RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and Message Digest 5 (MD5) for message digest.
<b>des-cbc-sha</b>	SSL_RSA_WITH_DES_CBC_SHA--RSA key exchange with DES-CBC for message encryption and SHA for message digest.

**Command Default** The client and server negotiate the best CipherSuite that they both support from the list of available CipherSuites.

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE

**Usage Guidelines** This command allows you to restrict the list of CipherSuites (encryption algorithms) that the client offers when connecting to a secure HTTP server. For example, you may want to allow only the most secure CipherSuites to be used.

Unless you have a reason to specify the CipherSuites that should be used, or you are unfamiliar with the details of these CipherSuites, you should leave this command unconfigured and let the server and client negotiate the CipherSuite that they both support (this is the default). The **no** form of this command returns the list of available CipherSuites to the default (that is, all CipherSuites supported on your device are available for negotiation).

### Examples

The following example shows how to configure the HTTPS client to use only the SSL\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA CipherSuite:

```
Router(config)# ip http client secure-ciphersuite 3des-ede-cbc-sha
```

## ip http secure-ciphersuite

To specify the CipherSuites that should be used by the secure HTTP server when negotiating a connection with a remote client, use the **ip http secure-ciphersuite** command in global configuration mode. To return the configuration to the default set of CipherSuites, use the **no** form of this command.

```
ip http secure-ciphersuite [3des-ede-cbc-sha] [rc4-128-sha] [rc4-128-md5] [des-cbc-sha]
no ip http secure-ciphersuite
```

### Syntax Description

<b>3des-ede-cbc-sha</b>	SSL_RSA_WITH_3DES_EDE_CBC_SHA--Rivest, Shamir, and Adleman (RSA) key exchange with 3DES and DES-EDE3-CBC for message encryption and Secure Hash Algorithm (SHA) for message digest.
<b>rc4-128-sha</b>	SSL_RSA_WITH_RC4_128_SHA --RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and SHA for message digest.
<b>rc4-128-md5</b>	SSL_RSA_WITH_RC4_128_MD5 --RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and Message Digest 5 (MD5) for message digest.
<b>des-cbc-sha</b>	SSL_RSA_WITH_DES_CBC_SHA--RSA key exchange with DES-CBC for message encryption and SHA for message digest.

### Command Default

The HTTPS server negotiates the best CipherSuite using the list received from the connecting client.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE

### Usage Guidelines

This command is used to restrict the list of CipherSuites (encryption algorithms) that should be used for encryption over the HTTPS connection. For example, you may want to allow only the most secure CipherSuites to be used.

Unless you have a reason to specify the CipherSuites that should be used, or you are unfamiliar with the details of these CipherSuites, you should leave this command unconfigured and let the server and client negotiate the CipherSuite that they both support (this is the default).

The supported CipherSuites vary by Cisco IOS software image. For example, “IP Sec56” (“k8”) images support only the SSL\_RSA\_WITH\_DES\_CBC\_SHA CipherSuite in Cisco IOS Release 12.2(15)T.

In terms of router processing load (speed), the following list ranks the CipherSuites from fastest to slowest (slightly more processing time is required for the more secure and more complex CipherSuites):

1. SSL\_RSA\_WITH\_DES\_CBC\_SHA
2. SSL\_RSA\_WITH\_RC4\_128\_MD5
3. SSL\_RSA\_WITH\_RC4\_128\_SHA

#### 4. SSL\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

Additional information about these CipherSuites can be found online from sources that document the Secure Sockets Layer (SSL) 3.0 protocol.

#### Examples

The following example shows how to restrict the CipherSuites offered to a connecting secure web client:

```
Router(config)# ip http secure-ciphersuite rc4-128-sha rc4-128-md5
```

## ip http secure-server

To enable a secure HTTP (HTTPS) server, enter the **ip http secure-server** command in global configuration mode. To disable the HTTPS server, use the **no** form of this command..

**ip http secure-server**  
**no ip http secure-server**

**Syntax Description** This command has no arguments or keywords.

**Command Default** The HTTPS server is disabled.

**Command Modes** Global configuration (config)

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** The HTTPS server uses the Secure Sockets Layer (SSL) version 3.0 protocol.



### Caution

When enabling an HTTPS server, you should always disable the standard HTTP server to prevent unsecured connections to the same services. Disable the standard HTTP server using the **no ip http server** command in global configuration mode (this step is precautionary; typically, the HTTP server is disabled by default).

If a certificate authority (CA) is used for certification, you should declare the CA trustpoint on the routing device before enabling the HTTPS server.

To close HTTP/TCP port 8090, you must disable both the HTTP and HTTPS servers. Enter the **no http server** and the **no http secure-server** commands, respectively.

### Examples

In the following example the HTTPS server is enabled, and the (previously configured) CA trustpoint CA-trust-local is specified:

```
Device#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#ip http secure-server
Device(config)#ip http secure-trustpoint CA-trust-local
Device(config)#end

Device#show ip http server secure status
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint: CA-trust-local
```



**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ip http secure-trustpoint</b>	Specifies the CA trustpoint that should be used for obtaining signed certificates for the HTTPS server.
<b>ip http server</b>	Enables the HTTP server on an IP or IPv6 system, including the Cisco web browser user interface.
<b>show ip http server secure status</b>	Displays the configuration status of the HTTPS server.

# ip http server

To enable the HTTP server on your IP or IPv6 system, including the Cisco web browser user interface, enter the **ip http server** command in global configuration mode. To disable the HTTP server, use the **no** form of this command..

**ip http server**  
**no ip http server**

**Syntax Description** This command has no arguments or keywords.

**Command Default** The HTTP server uses the standard port 80 by default.  
 HTTP/TCP port 8090 is open by default.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

**Usage Guidelines** The command enables both IPv4 and IPv6 access to the HTTP server. However, an access list configured with the **ip http access-class** command is applied only to IPv4 traffic. IPv6 traffic filtering is not supported.



**Caution**

The standard HTTP server and the secure HTTP (HTTPS) server can run on a system at the same time. If you enable the HTTPS server using the **ip http secure-server** command, disable the standard HTTP server using the **no ip http server** command to ensure that secure data cannot be accessed through the standard HTTP connection.

To close HTTP/TCP port 8090, you must disable both the HTTP and HTTPS servers. Enter the **no http server** and the **no http secure-server** commands, respectively.

**Examples**

The following example shows how to enable the HTTP server on both IPv4 and IPv6 systems.

After enabling the HTTP server, you can set the base path by specifying the location of the HTML files to be served. HTML files used by the HTTP web server typically reside in system flash memory. Remote URLs can be specified using this command, but use of remote path names (for example, where HTML files are located on a remote TFTP server) is not recommended.

```
Device(config)#ip http server
Device(config)#ip http path flash:
```

**Related Commands**

Command	Description
<b>ip http access-class</b>	Specifies the access list that should be used to restrict access to the HTTP server.
<b>ip http path</b>	Specifies the base path used to locate files for use by the HTTP server.

Command	Description
ip http secure-server	Enables the HTTPS server.

# ip ssh

To configure Secure Shell (SSH) control parameters on your router, use the **ip ssh** command in global configuration mode. To restore the default value, use the **no** form of this command.

```
ip ssh [{timeout seconds | authentication-retries integer}]
no ip ssh [{timeout seconds | authentication-retries integer}]
```

## Syntax Description

<b>timeout</b>	(Optional) The time interval that the router waits for the SSH client to respond.  This setting applies to the SSH negotiation phase. Once the EXEC session starts, the standard timeouts configured for the vty apply. By default, there are 5 vtys defined (0-4), therefore 5 terminal sessions are possible. After the SSH executes a shell, the vty timeout starts. The vty timeout defaults to 10 minutes.
<i>seconds</i>	(Optional) The number of seconds until timeout disconnects, with a maximum of 120 seconds. The default is 120 seconds.
<b>authentication- retries</b>	(Optional) The number of attempts after which the interface is reset.
<i>integer</i>	(Optional) The number of retries, with a maximum of 5 authentication retries. The default is 3.

## Command Default

SSH control parameters are set to default router values.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1) T.
12.2(17a)SX	This command was integrated into Cisco IOS Release 12.2(17a)SX.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

## Usage Guidelines

Before you configure SSH on your router, you must enable the SSH server using the **crypto key generate rsa** command.

## Examples

The following examples configure SSH control parameters on your router:

```
ip ssh timeout 120  
ip ssh authentication-retries 3
```

## ip ssh version

To specify the version of Secure Shell (SSH) to be run on a router, use the **ip ssh version** command in global configuration mode. To disable the version of SSH that was configured and to return to compatibility mode, use the **no** form of this command.

```
ip ssh version [{1 | 2}]
no ip ssh version [{1 | 2}]
```

Syntax Description	
	<b>1</b> (Optional) Router runs only SSH Version 1.
	<b>2</b> (Optional) Router runs only SSH Version 2.

**Command Default** If this command is not configured, SSH operates in compatibility mode, that is, Version 1 and Version 2 are both supported.

**Command Modes** Global configuration

Command History	Release	Modification
	12.3(4)T	This command was introduced.
	12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
	12.3(7)JA	This command was integrated into Cisco IOS Release 12.3(7)JA.
	12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
	12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
	15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

**Usage Guidelines** You can use this command with the **2** keyword to ensure that your router will not inadvertently establish a weaker SSH Version 1 connection.

### Examples

The following example shows that only SSH Version 1 support is configured:

```
Router (config)# ip ssh version 1
```

The following example shows that only SSH Version 2 is configured:

```
Router (config)# ip ssh version 2
```

The following example shows that SSH Versions 1 and 2 are configured:

```
Router (config)# no ip ssh version
```

**Related Commands**

<b>Command</b>	<b>Description</b>
debug ip ssh	Displays debug messages for SSH.
disconnect ssh	Terminates a SSH connection on your router.
<b>ip ssh</b>	Configures SSH control parameters on your router.
ip ssh rsa keypair-name	Specifies which RSA key pair to use for a SSH connection.
show ip ssh	Displays the SSH connections of your router.

# ip tftp blocksize

To specify TFTP client blocksize, use the **ip tftp blocksize** command.

**ip tftp blocksize** *blocksize-value*

---

<b>Syntax Description</b>	<i>blocksize-value</i> Blocksize value. Valid range is from 512-8192 Kbps.
---------------------------	----------------------------------------------------------------------------

---

<b>Command Default</b>	TFTP client blocksize is not configured.
------------------------	------------------------------------------

<b>Command Modes</b>	Global configuration (config)
----------------------	-------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

<b>Usage Guidelines</b>	Use this command to change the default blocksize to decrease the image download time.
-------------------------	---------------------------------------------------------------------------------------

## Example

The following example shows how to specify TFTP client blocksize:

```
Device(config)# ip tftp blocksize 512
```



# ip verify source

To enable IP source guard on an interface, use the **ip verify source** command in interface configuration mode. To disable IP source guard, use the **no** form of this command.

**ip verify source**  
**no ip verify source**

**Command Default** IP source guard is disabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** To enable IP source guard with source IP address filtering, use the **ip verify source** interface configuration command.

## Examples

This example shows how to enable IP source guard with source IP address filtering on an interface:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip verify source
```

You can verify your settings by entering the **show ip verify source** privileged EXEC command.

# ipv4 acl

To create ACL configuration for wireless IPv4, use the **ipv4 acl** command configuration.

**ipv4 acl** *ipv4-acl-name*

<b>Syntax Description</b>	<b>ipv4 acl</b>	Creates ACL configuration for wireless IPv4.
	<i>ipv4-acl-name</i>	Specifies the IPv4 ACL name.
<b>Command Default</b>	None	
<b>Command Modes</b>	Wireless policy configuration mode	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

## Example

This example shows how to create an ACL configuration for wireless IPv4:

```
Device(config-wireless-policy)#ipv4 acl ipv4-acl-name
```

# ipv4 dhcp

To configure the DHCP parameters for a WLAN, use the **ipv4 dhcp** command.

**ipv4 dhcp** {**opt82** | {**ascii** | **rid** | **format** | {**ap\_ethmac** | **ap\_location** | **apmac** | **apname** | **policy\_tag** | **ssid** | **vlan\_id** }} | **required** | **server** *dhcp-ip-addr*}

Syntax Description		
<b>opt82</b>	Sets DHCP option 82 for wireless clients on this WLAN	
<b>required</b>	Specifies whether DHCP address assignment is required	
<b>server</b>	Configures the WLAN's IPv4 DHCP Server	
<b>ascii</b>	Supports ASCII for DHCP option 82	
<b>rid</b>	Supports adding Cisco 2 byte RID for DHCP option 82	
<b>format</b>	Sets RemoteID format	
<b>ap_ethmac</b>	Enables DHCP AP Ethernet MAC address	
<b>ap_location</b>	Enables AP location	
<b>apmac</b>	Enables AP MAC address	
<b>apname</b>	Enables AP name	
<b>policy_tag</b>	Enables Policy tag	
<b>ssid</b>	Enables SSID	
<b>vlan_id</b>	Enables VLAN ID	
<i>dhcp-ip-addr</i>	Enter the override DHCP server's IP Address.	

**Command Default** None

**Command Modes** config-wireless-policy

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to configure DHCP address assignment as a requirement:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy demo-profile-name
Device(config-wireless-policy)# ipv4 dhcp required
```

# ipv4 flow monitor

To configure the IPv4 traffic ingress flow monitor for a WLAN profile policy, use the **ipv4 flow monitor input** command.

**ipv4 flow monitor** *monitor-name* **input**

Syntax Description	
	<i>monitor-name</i> Flow monitor name.
	<b>input</b> Enables flow monitor on ingress traffic.

**Command Default** None

**Command Modes** config-wireless-policy

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to configure the IPv4 traffic ingress flow monitor for a WLAN profile policy:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy policy-profile-name
Device(config-wireless-policy)# ipv4 flow monitor flow-monitor-name input
```

# ipv4 flow monitor output

To configure the IPv4 traffic egress flow monitor for a WLAN profile policy, use the **ipv4 flow monitor output** command.

**ipv4 flow monitor** *monitor-name* **output**

<b>Syntax Description</b>	<i>monitor-name</i> Flow monitor name.
	<b>output</b> Enables flow monitor on egress traffic.
<b>Command Default</b>	None
<b>Command Modes</b>	config-wireless-policy
<b>Command History</b>	<b>Release</b>
	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.2.1 This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.2.1.

## Examples

The following example shows how to configure the IPv4 traffic egress flow monitor for a WLAN profile policy:

```
Device(config-wireless-policy)#ipv4 flow monitor flow-monitor-name output
```

## ipv6 flow monitor input

To configure the IPv6 traffic ingress flow monitor for a WLAN profile policy, use the **ipv6 flow monitor input** command.

**ipv6 flow monitor** *monitor-name* **input**

<b>Syntax Description</b>	<i>monitor-name</i>	Flow monitor name.
	<b>input</b>	Enables flow monitor on ingress traffic.
<b>Command Default</b>	None	
<b>Command Modes</b>	config-wireless-policy	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.2.1	This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.2.1.

### Examples

The following example shows how to configure the IPv6 traffic ingress flow monitor for a WLAN profile policy:

```
Device(config-wireless-policy)#ipv6 flow monitor flow-monitor-name input
```

# ipv6 flow monitor output

To configure the IPv6 traffic egress flow monitor for a WLAN profile policy, use the **ipv6 flow monitor output** command.

**ipv6 flow monitor** *monitor-name* **output**

<b>Syntax Description</b>	<i>monitor-name</i> Flow monitor name.	
	<b>output</b> Enables flow monitor on egress traffic.	
<b>Command Default</b>	None	
<b>Command Modes</b>	config-wireless-policy	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.2.1	This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.2.1.

## Examples

The following example shows how to configure the IPv6 traffic egress flow monitor for a WLAN profile policy:

```
Device(config-wireless-policy)#ipv6 flow monitor flow-monitor-name output
```

## ipv6 access-list

To define an IPv6 access list and to place the device in IPv6 access list configuration mode, use the **ipv6 access-list** command in global configuration mode. To remove the access list, use the **no** form of this command.

**ipv6 access-list** *access-list-name* | **match-local-traffic** | **log-update threshold** *threshold-in-msgs* | **role-based** *list-name*  
**noipv6 access-list** *access-list-name* | **client** *permit-control-packets* | **log-update** *threshold* | **role-based** *list-name*

### Syntax Description

<b>ipv6</b> <i>access-list-name</i>	Creates a named IPv6 ACL (up to 64 characters in length) and enters IPv6 ACL configuration mode.  <i>access-list-name</i> - Name of the IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeric.
<b>match-local-traffic</b>	Enables matching for locally-generated traffic.
<b>log-update threshold</b> <i>threshold-in-msgs</i>	Determines how syslog messages are generated after the initial packet match.  <i>threshold-in-msgs</i> - Number of packets generated.
<b>role-based</b> <i>list-name</i>	Creates a role-based IPv6 ACL.

### Command Default

No IPv6 access list is defined.

### Command Modes

Global configuration

### Command History

Release	Modification

### Usage Guidelines

IPv6 ACLs are defined by using the **ipv6 access-list** command in global configuration mode and their permit and deny conditions are set by using the **deny** and **permit** commands in IPv6 access list configuration mode. Configuring the **ipv6 access-list** command places the device in IPv6 access list configuration mode--the device prompt changes to Device(config-ipv6-acl)#. From IPv6 access list configuration mode, permit and deny conditions can be set for the defined IPv6 ACL.



### Note

IPv6 ACLs are defined by a unique name (IPv6 does not support numbered ACLs). An IPv4 ACL and an IPv6 ACL cannot share the same name.

IPv6 is automatically configured as the protocol type in **permit any any** and **deny any any** statements that are translated from global configuration mode to IPv6 access list configuration mode.

Every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect. The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default,



IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Use the **ipv6 traffic-filter** interface configuration command with the *access-list-name* argument to apply an IPv6 ACL to an IPv6 interface. Use the **ipv6 access-class** line configuration command with the *access-list-name* argument to apply an IPv6 ACL to incoming and outgoing IPv6 virtual terminal connections to and from the device.

An IPv6 ACL applied to an interface with the **ipv6 traffic-filter** command filters traffic that is forwarded, not originated, by the device.

## Examples

The example configures the IPv6 ACL list named list1 and places the device in IPv6 access list configuration mode.

```
Device(config)# ipv6 access-list list1
Device(config-ipv6-acl)#
```

The following example configures the IPv6 ACL named list2 and applies the ACL to outbound traffic on Ethernet interface 0. Specifically, the first ACL entry keeps all packets from the network FEC0:0:0:2::/64 (packets that have the site-local prefix FEC0:0:0:2 as the first 64 bits of their source IPv6 address) from exiting out of Ethernet interface 0. The second entry in the ACL permits all other traffic to exit out of Ethernet interface 0. The second entry is necessary because an implicit deny all condition is at the end of each IPv6 ACL.

```
Device(config)# ipv6 access-list list2 deny FEC0:0:0:2::/64 any
Device(config)# ipv6 access-list list2 permit any any
Device(config)# interface ethernet 0
Device(config-if)# ipv6 traffic-filter list2 out
```

# ipv6 acl

To create ACL configuration for wireless IPv6, use the **ipv6 acl** command configuration.

**ipv6 acl** *ipv6-acl-name*

<b>Syntax Description</b>	<b>ipv6 acl</b>	Creates ACL configuration for wireless IPv6.
	<i>ipv6-acl-name</i>	Specifies the IPv6 ACL name.
<b>Command Default</b>	None	
<b>Command Modes</b>	Wireless policy configuration mode	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

## Example

This example shows how to create an ACL configuration for wireless IPv6:

```
Device(config-wireless-policy)#ipv6 acl ipv6-acl-name
```

## ipv6-address-type

To configure the 802.11u IPv6 address type, use the **ipv6-address-type** command. To remove the address type, use the **no** form of the command.

**ipv6-address-type** { **available** | **not-available** | **not-known** }

<b>Syntax Description</b>	<b>available</b>	Sets IPv6 address type as available.
	<b>not-available</b>	Sets IPv6 address type as not available.
	<b>not-known</b>	Sets IPv6 address type availability as not known.
<b>Command Default</b>	None	
<b>Command Modes</b>	Wireless ANQP Server Configuration (config-wireless-anqp-server)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

### Example

The following example shows how to configure a 802.11u IPv6 address type:

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# ipv4-address-type available
```

## ipv6 address

To configure an IPv6 address based on an IPv6 general prefix and enable IPv6 processing on an interface, use the **ipv6 address** command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

**ipv6 address** {*ipv6-prefix/prefix-length* | *prefix-name sub-bits/prefix-length*}  
**no ipv6 address** {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*}

### Syntax Description

<i>ipv6-address</i>	The IPv6 address to be used.
<i>/ prefix-length</i>	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
<i>prefix-name</i>	A general prefix, which specifies the leading bits of the network to be configured on the interface.
<i>sub-bits</i>	The subprefix bits and host bits of the address to be concatenated with the prefixes provided by the general prefix specified with the <i>prefix-name</i> argument.  The <i>sub-bits</i> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

### Command Default

No IPv6 addresses are defined for any interface.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco ASR 1000 Series devices.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

**Usage Guidelines**

The **ipv6 address** command allows multiple IPv6 addresses to be configured on an interface in various different ways, with varying options. The most common way is to specify the IPv6 address with the prefix length.

Addresses may also be defined using the general prefix mechanism, which separates the aggregated IPv6 prefix bits from the subprefix and host bits. In this case, the leading bits of the address are defined in a general prefix, which is globally configured or learned (for example, through use of Dynamic Host Configuration Protocol-Prefix Delegation (DHCP-PD)), and then applied using the *prefix-name* argument. The subprefix bits and host bits are defined using the *sub-bits* argument.

Using the **no ipv6 address autoconfig** command without arguments removes all IPv6 addresses from an interface.

IPv6 link-local addresses must be configured and IPv6 processing must be enabled on an interface by using the **ipv6 address link-local** command.

**Examples**

The following example shows how to enable IPv6 processing on the interface and configure an address based on the general prefix called my-prefix and the directly specified bits:

```
Device(config-if) ipv6 address my-prefix 0:0:0:7272::72/64
```

Assuming the general prefix named my-prefix has the value of 2001:DB8:2222::/48, then the interface would be configured with the global address 2001:DB8:2222:7272::72/64.

**Related Commands**

Command	Description
<b>ipv6 address anycast</b>	Configures an IPv6 anycast address and enables IPv6 processing on an interface.
<b>ipv6 address eui-64</b>	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
<b>ipv6 address link-local</b>	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
<b>ipv6 unnumbered</b>	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
<b>no ipv6 address autoconfig</b>	Removes all IPv6 addresses from an interface.
<b>show ipv6 interface</b>	Displays the usability status of interfaces configured for IPv6.

## ipv6 dhcp pool

To configure a Dynamic Host Configuration Protocol (DHCP) for IPv6 server configuration information pool and enter DHCP for IPv6 pool configuration mode, use the **ipv6 dhcp pool** command in global configuration mode. To delete a DHCP for IPv6 pool, use the **no** form of this command.

**ipv6 dhcp pool** *poolname*  
**no ipv6 dhcp pool** *poolname*

### Syntax Description

<i>poolname</i>	User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).
-----------------	----------------------------------------------------------------------------------------------------------------------------------------

### Command Default

DHCP for IPv6 pools are not configured.

### Command Modes

Global configuration

### Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

### Usage Guidelines

Use the **ipv6 dhcp pool** command to create a DHCP for IPv6 server configuration information pool. When the **ipv6 dhcp pool** command is enabled, the configuration mode changes to DHCP for IPv6 pool configuration mode. In this mode, the administrator can configure pool parameters, such as prefixes to be delegated and Domain Name System (DNS) servers, using the following commands:

- **address prefix** *IPv6-prefix* [**lifetime** {*valid-lifetime preferred-lifetime* | **infinite**}] sets an address prefix for address assignment. This address must be in hexadecimal, using 16-bit values between colons.
- **link-address** *IPv6-prefix* sets a link-address IPv6 prefix. When an address on the incoming interface or a link-address in the packet matches the specified IPv6-prefix, the server uses the configuration information pool. This address must be in hexadecimal, using 16-bit values between colons.
- **vendor-specific** *vendor-id* enables DHCPv6 vendor-specific configuration mode. Specify a vendor identification number. This number is the vendor IANA Private Enterprise Number. The range is 1 to 4294967295. The following configuration command is available:
  - **suboption** *number* sets vendor-specific suboption number. The range is 1 to 65535. You can enter an IPv6 address, ASCII text, or a hex string as defined by the suboption parameters.



**Note** The **hex** value used under the **suboption** keyword allows users to enter only hex digits (0-f). Entering an invalid **hex** value does not delete the previous configuration.

Once the DHCP for IPv6 configuration information pool has been created, use the **ipv6 dhcp server** command to associate the pool with a server on an interface. If you do not configure an information pool, you need to use the **ipv6 dhcp server interface** configuration command to enable the DHCPv6 server function on an interface.

When you associate a DHCPv6 pool with an interface, only that pool services requests on the associated interface. The pool also services other interfaces. If you do not associate a DHCPv6 pool with an interface, it can service requests on any interface.

Not using any IPv6 address prefix means that the pool returns only configured options.

The **link-address** command allows matching a link-address without necessarily allocating an address. You can match the pool from multiple relays by using multiple link-address configuration commands inside a pool.

Since a longest match is performed on either the address pool information or the link information, you can configure one pool to allocate addresses and another pool on a subprefix that returns only configured options.

## Examples

The following example specifies a DHCP for IPv6 configuration information pool named `cisco1` and places the router in DHCP for IPv6 pool configuration mode:

```
Router(config)# ipv6 dhcp pool cisco1
Router(config-dhcpv6)#
```

The following example shows how to configure an IPv6 address prefix for the IPv6 configuration pool `cisco1`:

```
Router(config-dhcpv6)# address prefix 2001:1000::0/64
Router(config-dhcpv6)# end
```

The following example shows how to configure a pool named `engineering` with three link-address prefixes and an IPv6 address prefix:

```
Router# configure terminal
Router(config)# ipv6 dhcp pool engineering
Router(config-dhcpv6)# link-address 2001:1001::0/64
Router(config-dhcpv6)# link-address 2001:1002::0/64
Router(config-dhcpv6)# link-address 2001:2000::0/48
Router(config-dhcpv6)# address prefix 2001:1003::0/64
Router(config-dhcpv6)# end
```

The following example shows how to configure a pool named `350` with vendor-specific options:

```
Router# configure terminal
Router(config)# ipv6 dhcp pool 350
Router(config-dhcpv6)# vendor-specific 9
Router(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Router(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Router(config-dhcpv6-vs)# end
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ipv6 dhcp server</b>	Enables DHCP for IPv6 service on an interface.
<b>show ipv6 dhcp pool</b>	Displays DHCP for IPv6 configuration pool information.



# ipv6 enable

To enable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **ipv6 enable** command in interface configuration mode. To disable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **no** form of this command.

**ipv6 enable**  
**no ipv6 enable**

**Syntax Description** This command has no arguments or keywords.

**Command Default** IPv6 is disabled.

**Command Modes** Interface configuration (config-if)

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

**Usage Guidelines** The **ipv6 enable** command automatically configures an IPv6 link-local unicast address on the interface while also enabling the interface for IPv6 processing. The **no ipv6 enable** command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

**Examples** The following example enables IPv6 processing on Ethernet interface 0/0:

## ipv6 enable

```
Device(config)# interface ethernet 0/0
Device(config-if)# ipv6 enable
```

### Related Commands

Command	Description
<b>ipv6 address link-local</b>	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
<b>ipv6 address eui-64</b>	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
<b>ipv6 unnumbered</b>	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
<b>show ipv6 interface</b>	Displays the usability status of interfaces configured for IPv6.

# ipv6 mld snooping

To enable Multicast Listener Discovery version 2 (MLDv2) protocol snooping globally, use the **ipv6 mld snooping** command in global configuration mode. To disable the MLDv2 snooping globally, use the **no** form of this command.

**ipv6 mld snooping**  
**no ipv6 mld snooping**

**Syntax Description** This command has no arguments or keywords.

**Command Default** This command is enabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

**Usage Guidelines** MLDv2 snooping is supported on the Supervisor Engine 720 with all versions of the Policy Feature Card 3 (PFC3).  
 To use MLDv2 snooping, configure a Layer 3 interface in the subnet for IPv6 multicast routing or enable the MLDv2 snooping querier in the subnet.

**Examples** This example shows how to enable MLDv2 snooping globally:

```
Router(config)# ipv6 mld snooping
```

Related Commands	Command	Description
	<b>show ipv6 mld snooping</b>	Displays MLDv2 snooping information.

## ipv6 nd managed-config-flag

To set the managed address configuration flag in IPv6 router advertisements, use the **ipv6 nd managed-config-flag** command in an appropriate configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

```
ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag
```

<b>Syntax Description</b>	This command has no keywords or arguments.	
<b>Command Default</b>	The managed address configuration flag is not set in IPv6 router advertisements.	
<b>Command Modes</b>	Interface configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

**Usage Guidelines**

Setting the managed address configuration flag in IPv6 router advertisements indicates to attached hosts whether they should use stateful autoconfiguration to obtain addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain addresses. If the flag is not set, the attached hosts should not use stateful autoconfiguration to obtain addresses.

Hosts may use stateful and stateless address autoconfiguration simultaneously.

### Examples

This example shows how to configure the managed address configuration flag in IPv6 router advertisements:

```
Device(config)# interface
Device(config-if)# ipv6 nd managed-config-flag
```

## ipv6 nd other-config-flag

To set the other stateful configuration flag in IPv6 router advertisements, use the **ipv6 nd other-config-flag** command in an appropriate configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

**ipv6 nd other-config-flag**

### Syntax Description

This command has no keywords or arguments.

### Command Default

The other stateful configuration flag is not set in IPv6 router advertisements.

### Command Modes

Interface configuration

Dynamic template configuration

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

### Usage Guidelines

The setting of the other stateful configuration flag in IPv6 router advertisements indicates to attached hosts how they can obtain autoconfiguration information other than addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain the other (nonaddress) information.



#### Note

If the managed address configuration flag is set using the **ipv6 nd managed-config-flag** command, then an attached host can use stateful autoconfiguration to obtain the other (nonaddress) information regardless of the setting of the other stateful configuration flag.

### Examples

This example (not applicable for BNG) configures the “other stateful configuration” flag in IPv6 router advertisements:

```
Device(config)# interface
Device(config-if)# ipv6 nd other-config-flag
```

## ipv6 nd ra throttler attach-policy

To configure a IPv6 policy for feature RA throttler, use the **ipv6 nd ra-throttler attach-policy** command.

**ipv6 nd ra-throttler attach-policy** *policy-name*

<b>Syntax Description</b>	<b>ipv6</b>	IPv6 root chain.
	<b>ra-throttler</b>	Configure RA throttler on the VLAN.
	<b>attach-policy</b>	Apply a policy for feature RA throttler.
	<i>policy-name</i>	Policy name for feature RA throttler
<b>Command Default</b>	None	
<b>Command Modes</b>	config-vlan	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

### Examples

The following example shows how to configure configure a IPv6 policy for feature RA throttler:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# vlan configuration vlan-id
Device(config-vlan-config)# ipv6 nd ra-throttler attach-policy
```

## ipv6 nd rguard policy

To define the router advertisement (RA) guard policy name and enter RA guard policy configuration mode, use the **ipv6 nd rguard policy** command in global configuration mode.

**ipv6 nd rguardpolicy** *policy-name*

Syntax Description	
	<i>policy-name</i> IPv6 RA guard policy name.

**Command Default** An RA guard policy is not configured.

**Command Modes** Global configuration (config)#

Command History	Release	Modification
	12.2(50)SY	This command was introduced.
	15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
	15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
	Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

**Usage Guidelines** Use the **ipv6 nd rguard policy** command to configure RA guard globally on a router. Once the device is in ND inspection policy configuration mode, you can use any of the following commands:

- **device-role**
- **drop-unsecure**
- **limit address-count**
- **sec-level minimum**
- **trusted-port**
- **validate source-mac**

After IPv6 RA guard is configured globally, you can use the **ipv6 nd rguard attach-policy** command to enable IPv6 RA guard on a specific interface.

### Examples

The following example shows how to define the RA guard policy name as policy1 and place the device in policy configuration mode:

```
Device(config)# ipv6 nd rguard policy policy1
Device(config-ra-guard)#
```

**Related Commands***Table 8:*

<b>Command</b>	<b>Description</b>
<b>device-role</b>	Specifies the role of the device attached to the port.
<b>drop-unsecure</b>	Drops messages with no or invalid options or an invalid signature.
<b>ipv6 nd rguard attach-policy</b>	Applies the IPv6 RA guard feature on a specified interface.
<b>limit address-count</b>	Limits the number of IPv6 addresses allowed to be used on the port.
<b>sec-level minimum</b>	Specifies the minimum security level parameter value when CGA options are used.
<b>trusted-port</b>	Configures a port to become a trusted port.
<b>validate source-mac</b>	Checks the source MAC address against the link layer address.



# ipv6 snooping policy



**Note** All existing IPv6 Snooping commands (prior to ) now have corresponding SISF-based device-tracking commands that allow you to apply your configuration to both IPv4 and IPv6 address families.

To configure an IPv6 snooping policy and enter IPv6 snooping configuration mode, use the **ipv6 snooping policy** command in global configuration mode. To delete an IPv6 snooping policy, use the **no** form of this command.

**ipv6 snooping policy** *snooping-policy*  
**no ipv6 snooping policy** *snooping-policy*

<b>Syntax Description</b>	<i>snooping-policy</i> User-defined name of the snooping policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).				
<b>Command Default</b>	An IPv6 snooping policy is not configured.				
<b>Command Modes</b>	Global configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td></td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification		This command was introduced.
Release	Modification				
	This command was introduced.				

**Usage Guidelines** Use the **ipv6 snooping policy** command to create an IPv6 snooping policy. When the **ipv6 snooping policy** command is enabled, the configuration mode changes to IPv6 snooping configuration mode. In this mode, the administrator can configure the following IPv6 first-hop security commands:

- The **device-role** command specifies the role of the device attached to the port.
- The **limit address-count** *maximum* command limits the number of IPv6 addresses allowed to be used on the port.
- The **protocol** command specifies that addresses should be gleaned with Dynamic Host Configuration Protocol (DHCP) or Neighbor Discovery Protocol (NDP).
- The **security-level** command specifies the level of security enforced.
- The **tracking** command overrides the default tracking policy on a port.
- The **trusted-port** command configures a port to become a trusted port; that is, limited or no verification is performed when messages are received.

This example shows how to configure an IPv6 snooping policy:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)#
```

## ipv6 traffic-filter

This command enables IPv6 traffic filter.

To enable the filtering of IPv6 traffic on an interface, use the **ipv6 traffic-filter** command. To disable the filtering of IPv6 traffic on an interface, use the **no** form of the command.

Use the **ipv6 traffic-filter** interface configuration command on the switch stack or on a standalone switch to filter IPv6 traffic on an interface. The type and direction of traffic that you can filter depends on the feature set running on the switch stack. Use the **no** form of this command to disable the filtering of IPv6 traffic on an interface.

**ipv6 traffic-filter** [**web**] *acl-name*

**no ipv6 traffic-filter** [**web**]

<b>Syntax Description</b>	<p><b>web</b> (Optional) Specifies an IPv6 access name for the WLAN Web ACL.</p> <p><i>acl-name</i> Specifies an IPv6 access name.</p>				
<b>Command Default</b>	Filtering of IPv6 traffic on an interface is not configured.				
<b>Command Modes</b>	wlan				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td></td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification		This command was introduced.
Release	Modification				
	This command was introduced.				
<b>Usage Guidelines</b>	<p>To configure the dual IPv4 and IPv6 template, enter the <b>sdm prefer dual-ipv4-and-ipv6 {default   vlan}</b> global configuration command and reload the switch.</p> <p>You can use the <b>ipv6 traffic-filter</b> command on physical interfaces (Layer 2 or Layer 3 ports), Layer 3 port channels, or switch virtual interfaces (SVIs).</p> <p>You can apply an ACL to outbound or inbound traffic on Layer 3 interfaces (port ACLs), or to inbound traffic on Layer 2 interfaces (router ACLs).</p> <p>If <b>any</b> port ACL (IPv4, IPv6, or MAC) is applied to an interface, that port ACL is used to filter packets, and any router ACLs attached to the SVI of the port VLAN are ignored.</p> <p>This example shows how to filter IPv6 traffic on an interface:</p> <pre>Device(config-wlan)# ipv6 traffic-filter TestDocTrafficFilter</pre>				

# key chain

To create or modify a keychain, use the **key chain** command. To disable this feature, use the **no** form of this command.

**key chain***key-chain name* { **macsec** | **tcp** }  
**no key chain***key-chain name* { **macsec** | **tcp** }

Syntax Description		
	<i>key-chain name</i>	Specifies the name of the key chain.
	<b>macsec</b>	Specifies a MacSEC key chain.
	<b>tcp</b>	Specifies the tcp key chain.

**Command Default** No default.

**Command Modes** Global configuration mode.

**Examples** The following example shows how to specify a key chain to identify authentication on a key-chain:

```
Device(config)# key chain key-chain-name macsec
```

Related Commands	Command	Description
	<b>key config-key</b>	Sets a private configuration key for general use.
	<b>show key chain</b>	Displays authentication key information.

## key config-key

To set a private configuration key for private use, use the **key config-key** command. To disable this feature, use the **no** form of this command.

**key config-key** { 1 LINE | **newpass** *config-key* | **password-encrypt** LINE }  
**no key config-key** { 1 LINE | **newpass** *config-key* | **password-encrypt** LINE }

Syntax Description		
<b>1</b>		Sets a private configuration key for private use.
<b>newpass</b>		Specifies a new password without space or tabs.
<i>config-key</i>		Specifies the config key, with a minimum of 8 characters, and not beginning with the IOS special characters - !, #, and ;.
<b>password-encrypt</b>		Sets a private configuration key for password encryption.

**Command Default** None

**Command Modes** Global configuration mode.

**Examples** The following example shows how to specify a config-key:

```
Device(config)# key config-key password-encrypt config-key
```

# key config-key password-encrypt

To set a private configuration key for password encryption, use the **key config-key password-encrypt** command. To disable this feature, use the **no** form of this command.

**key config-key password-encrypt** <config-key>

<b>Syntax Description</b>	<i>config-key</i> Enter a value with minimum 8 characters.	
	<b>Note</b>	The value must not begin with the following special characters:  !, #, and ;
<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration mode	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 17.6.1	This command was introduced.

## Examples

The following example shows how to set a username and password for AP management:

```
Device# enable
Device# configure terminal
Device(config)# key config-key password-encryption 12345678
Device(config-ap-profile)# password encryption aes
Device(config-ap-profile)# end
```

# license air level

To configure AIR licenses on a wireless controller, enter the **license air level** command in global configuration mode. To revert to the default setting, use the **no** form of this command.

```
license air level { air-network-advantage [ addon air-dna-advantage ] | air-network-essentials [ addon air-dna-essentials ] }
```

**no license air level**

## Syntax Description

<b>air-network-advantage</b>	Configures the AIR Network Advantage license level.
<b>addon air-dna-advantage</b>	(Optional) Configures the add-on AIR DNA Advantage license level. This add-on option is available with the AIR Network Advantage license.
<b>air-network-essentials</b>	Configures the AIR Network Essentials license level.
<b>addon air-dna-essentials</b>	(Optional) Configures the add-on AIR DNA Essentials license level. This add-on option is available with the AIR Network Essential license.

## Command Default

For all Cisco Catalyst 9800 Wireless controllers the default license is AIR DNA Advantage.

For EWC-APs:

- Prior to Cisco IOS XE Bengaluru 17.4.1, the default license is AIR DNA Essentials.
- Starting with Cisco IOS XE Bengaluru 17.4.1, the default license is AIR Network Essentials

## Command Modes

Global configuration (config)

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	This command continues to be available and applicable with the introduction of Smart Licensing Using Policy.
Cisco IOS XE Bengaluru 17.4.1	Only for EWC-APs, the default license was changed from AIR DNA Essentials to AIR Network Essentials.

## Usage Guidelines

In the Smart Licensing Using Policy environment, you can use the **license air level** command to change the license level being used on the product instance, or to additionally configure an add-on license on the product instance. The change is effective after a reload.

The licenses that can be configured are:

- AIR Network Essential
- AIR Network Advantage
- AIR DNA Essential

- AIR DNA Advantage

You can configure AIR DNA Essential or AIR DNA Advantage license level and on term expiry, you can move to the Network Advantage or Network Essentials license level, if you do not want to renew the DNA license.

Every connecting AP requires a Cisco DNA Center License to leverage the unique value properties of the controller.

### Specifics for EWC-APs

Starting with Cisco IOS XE Bengaluru 17.4.1, *only for EWC-APs*, you can opt-out of purchasing an AIR DNA license. The option to opt-out of AIR DNA licenses is available only through the [Cisco Commerce](#) portal. When you opt-out, Smart Licensing Using Policy functionality is disabled.

For a new product instance, this means:

Condition	Required Action	Outcome or Result
You opt-out of AIR DNA licenses	None.	Use only AIR Network Essentials. Smart Licensing Using Policy functionality is disabled on the product instance and for your Smart Account and Virtual Account in CSSM. License usage is not recorded, and no reporting requirements apply.
You purchase AIR DNA licenses	Enter the <b>license air level</b> command in global configuration mode and configure the corresponding AIR DNA license. Reload to use the corresponding license.  Implement one of the supported topologies and fulfill reporting requirements. For information about implementing a topology, For information about implementing a topology, see the Supported Topologies section in the <a href="#">software configuration guide</a> of the required release.	Use the purchased AIR DNA and AIR Network license.  Smart Licensing Using Policy functionality is enabled on the product instance and for your Smart Account and Virtual Account in CSSM.

For an existing product instance, this means:

Condition	Required Action	Outcome or Result
You are using an AIR DNA license	None.	No change. You are already in the Smart Licensing Using Policy environment.

Condition	Required Action	Outcome or Result
You do not want to renew the DNA license on term expiry	On term expiry, enter the <b>license air level</b> command in global configuration mode and configure AIR Network Essentials or AIR Network Advantage. Reload to use the corresponding license.	If you had AIR DNA Essentials, you now use AIR Network Essentials. If you had AIR DNA Advantage, you now use AIR Network Advantage. Smart Licensing Using Policy functionality is disabled on the product instance and for your Smart Account and Virtual Account in CSSM. License usage is not recorded, and no reporting requirements apply.

### Examples

The following example show how to configure the AIR DNA Essential license level:

```
Device# configure terminal
Device(config)# license air level network-essentials addon air-dna-essentials
```

The following example shows how the AIR DNA Advantage license level is configured to begin with and then changed to AIR DNA Essentials:

Current configuration as AIR DNA Advantage:

```
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2,
RELEASE SOFTWARE
<output truncated>
AIR License Level: AIR DNA Advantage
Next reload AIR license Level: AIR DNA Advantage
```

```
Smart Licensing Status: Registration Not Applicable/Not Applicable
<output truncated>
```

Configuration of AIR DNA Essentials :

```
Device# configure terminal
Device(config)# license air level air-network-essentials addon air-dna-essentials

Device# exit
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2,
RELEASE SOFTWARE
<output truncated>
AIR License Level: AIR DNA Advantage
Next reload AIR license Level: AIR DNA Essentials
Smart Licensing Status: Registration Not Applicable/Not Applicable
<output truncated>
```

```
Device# write memory
Device# reload
```

After reload:

```
Device# show version
Cisco IOS XE Software, Version 17.03.02
```



```
Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2,  
RELEASE SOFTWARE  
<output truncated>  
AIR License Level: AIR DNA Essentials  
Next reload AIR license Level: AIR DNA Essentials  
  
Smart Licensing Status: Registration Not Applicable/Not Applicable  
<output truncated>
```

## license smart (global config)

To configure licensing-related settings such as the mode of transport and the URL that the product instance uses to communicate with Cisco Smart Software Manager (CSSM), or Cisco Smart Licensing Utility (CSLU), or Smart Software Manager On-Prem (SSM On-Prem), to configure the usage reporting interval, to configure the information that must be excluded or included in a license usage report (RUM report), enter the **license smart** command in global configuration mode. Use the **no** form of the command to revert to default values.

```
license smart { custom_id ID | enable | privacy { all | hostname | version } | proxy { address
address_hostname | port port } | reservation | server-identity-check | transport { automatic | callhome
| cslu | off | smart } | url { url | cslu cslu_or_on-prem_url | default | smart smart_url | utility secondary_url
} | usage { customer-tags { tag1 | tag2 | tag3 | tag4 } tag_value | interval interval_in_days } | utility [
customer_info { city city | country country | postalcode postalcode | state state | street street } ] }
```

```
no license smart { custom_id | enable | privacy { all | hostname | version } | proxy { address
address_hostname | port port } | reservation | server-identity-check | transport | url { url | cslu
cslu_or_on-prem_url | default | smart smart_url | utility secondary_url } | usage { customer-tags { tag1
| tag2 | tag3 | tag4 } tag_value | interval interval_in_days } | utility [ customer_info { city city | country
country | postalcode postalcode | state state | street street } ] }
```

### Syntax Description

<b>custom_id</b> <i>ID</i>	Although available on the CLI, this option is not supported.
<b>enable</b>	Although visible on the CLI, configuring this keyword has no effect. Smart licensing is always enabled.
<b>privacy</b> { <b>all</b>   <b>hostname</b>   <b>version</b> }	Enables you to <i>leave out</i> certain information from the usage reports that are sent to CSSM. Choose from the following options: <ul style="list-style-type: none"> <li>• <b>all</b>: Sends only the minimal licensing information in any communication.</li> <li>• <b>hostname</b>: Excludes the hostname from any communication.</li> <li>• <b>version</b>: Excludes the product instance agent version from any communication.</li> </ul>

---

**proxy** { **address** *address\_hostname* | **port** *port* } Configures a proxy for license usage synchronization with CSLU or CSSM. This means that you can use this option to configure a proxy only if the transport mode is **license smart transport smart** (CSSM), or **license smart transport cslu** (CSLU).

However, you cannot configure a proxy for license usage synchronization in an SSM On-Prem deployment, which also uses **license smart transport cslu** as the transport mode.

Configure the following options:

- **address** *address\_hostname*: Configures the proxy address.  
For *address\_hostname*, enter the IP address or hostname of the proxy.
- **port***port*: Configures the proxy port.  
For *port*, enter the proxy port number.

---

**reservation** Enables or disables a license reservation feature.

**Note** Although available on the CLI, this option is not applicable because license *reservation* is not applicable in the Smart Licensing Using Policy environment.

---

**server-identity-check** Enables or disables the HTTP secure server identity check.

---

**transport** { **automatic** | **callhome** | **cslu** | **off** | **smart** } Configures the mode of transport the product instance uses to communicate with CSSM. Choose from the following options:

- **automatic**: Sets the transport mode **cslu**.  
**Note** The **automatic** keyword is not supported on Cisco Catalyst Wireless Controllers.
  - **callhome**: Enables Call Home as the transport mode.
  - **cslu**: Enables CSLU as the transport mode. This is the default transport mode.  
The same keyword applies to both CSLU *and* SSM On-Prem, but the URLs are different. See **cslu***cslu\_or\_on-prem\_url* in the following row.
  - **off**: Disables all communication from the product instance.
  - **smart**: Enables Smart transport.
-

---

```
url { url | cslu cslu_url | default | smart
      smart_url | utility secondary_url }
```

---

Sets URL that is used for the configured transport mode. Choose from the following options:

- **url**: If you have configured the transport mode as **callhome**, configure this option. Enter the CSSM URL exactly as follows:

```
https://tools.cisco.com/its/service/odbe/services/DDCEService
```

The **no license smart url url** command reverts to the default URL.

- **cslu cslu\_or\_on-prem\_url**: If you have configured the transport mode as **cslu**, configure this option, with the URL for CSLU or SSM On-Prem, as applicable:

- If you are using CSLU, enter the URL as follows:

```
http://<cslu_ip_or_host>:8182/cslu/v1/pi
```

For <cslu\_ip\_or\_host>, enter the hostname or the IP address of the windows host where you have installed CSLU. 8182 is the port number and it is the only port number that CSLU uses.

The **no license smart url cslu cslu\_or\_on-prem\_url** command reverts to

```
http://cslu-local:8182/cslu/v1/pi
```

- If you are using SSM On-Prem, enter the URL as follows:

```
http://<ip>/cslu/v1/pi/<tenant ID>
```

For <ip>, enter the hostname or the IP address of the server where you have installed SSM On-Prem. The <tenantID> must be the default local virtual account ID.

**Tip** You can retrieve the entire URL from SSM On-Prem. In the software configuration guide (17.3.x and later), see Smart Licensing Using Policy > Task Library for Smart Licensing Using Policy > Retrieving the Transport URL (SSM On-Prem UI).

The **no license smart url cslu cslu\_or\_on-prem\_url** command reverts to

```
http://cslu-local:8182/cslu/v1/pi
```

- **default**: Depends on the configured transport mode. Only the **smart** and **cslu** transport modes are supported with this option.

If the transport mode is set to **cslu**, and you configure **license smart url default**, the CSLU URL is configured automatically

(<https://cslu-local:8182/cslu/v1/pi>).

If the transport mode is set to **smart**, and you configure **license smart url default**, the Smart URL is configured automatically

(<https://smartreceiver.cisco.com/licservice/license>).

- **smart** *smart\_url*: If you have configured the transport type as **smart**, configure this option. Enter the URL exactly as follows:

<https://smartreceiver.cisco.com/licservice/license>

When you configure this option, the system automatically creates a duplicate of the URL in **license smart url url**. You can ignore the duplicate entry, no further action is required.

The **no license smart url smartsmart\_url** command reverts to the default URL.

- **utility** *smart\_url*: Although available on the CLI, this option is not supported.
-

**usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag\_value* | **interval** *interval\_in\_days* } Configures usage reporting settings. You can set the following options:

- **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag\_value*: Defines strings for inclusion in data models, for telemetry. Up to 4 strings (or tags) may be defined.  
For *tag\_value*, enter the string value for each tag that you define.
- **interval** *interval\_in\_days*: Sets the reporting interval in days. By default the RUM report is sent every 30 days. The valid value range is 1 to 3650.

If you set the value to zero, RUM reports are not sent, regardless of what the applied policy specifies - this applies to topologies where CSLU or CSSM may be on the receiving end.

If you set a value that is greater than zero and the transport type is set to **off**, then, between the *interval\_in\_days* and the policy value for `Ongoing reporting frequency(days) :`, the lower of the two values is applied. For example, if *interval\_in\_days* is set to 100, and the value in the in the policy says `Ongoing reporting frequency (days):90`, RUM reports are sent every 90 days.

If you do not set an interval, and the default is effective, the reporting interval is determined entirely by the policy value. For example, if the default value is effective and only unenforced licenses are in use, if the policy states that reporting is not required, then RUM reports are not sent.

**utility** [ **customer\_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* } ] Although visible on the CLI, this option is not supported.

#### Command Default

Cisco IOS XE Amsterdam 17.3.1 or earlier: Smart Licensing is enabled by default.

Cisco IOS XE Amsterdam 17.3.2a and later: Smart Licensing Using Policy is enabled by default.

#### Command Modes

Global config (config)

#### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Release	Modification
Cisco IOS XE Amsterdam 17.3.2a	<p>The following keywords and variables were introduced with Smart Licensing Using Policy:</p> <ul style="list-style-type: none"> <li>Under the <b>url</b> keyword, these options were introduced:           <pre>{ <b>cslu</b> <i>cslu_url</i>   <b>smart</b> <i>smart_url</i> }</pre> </li> <li>Under the <b>transport</b> keyword, these options were introduced:           <pre>{ <b>cslu</b>   <b>off</b> }</pre> <p>Further, the default transport type was changed from <b>callhome</b>, to <b>cslu</b>.</p> </li> <li><b>usage</b> { <b>customer-tags</b> { <b>tag1</b>   <b>tag2</b>   <b>tag3</b>   <b>tag4</b> } <i>tag_value</i>   <b>interval</b> <i>interval_in_days</i> }</li> </ul> <p>The following keywords and variables under the <b>license smart</b> command are deprecated and no longer available on the CLI: <b>enable</b> and <b>conversion automatic</b>.</p>
Cisco IOS XE Amsterdam 17.3.3	<p>SSM On-Prem support was introduced. For product instance-initiated communication in an SSM On-Prem deployment, the existing [<b>no</b>] <b>license smart url cslu</b> <i>cslu_or_on-prem_url</i> command supports the configuration of a URL for SSM On-Prem as well. But the required URL format for SSM On-Prem is:  <pre>http://&lt;ip&gt;/cslu/v1/pi/&lt;tenant ID&gt;.</pre> </p> <p>The corresponding transport mode that must be configured is also an existing command (<b>license smart transport cslu</b>).</p>

## Usage Guidelines

The reporting interval that you configure (**license smart usage interval** *interval\_in\_days* command), determines the date and time at which the product instance sends out the RUM report. If the scheduled interval coincides with a communication failure, the product instance attempts to send out the RUM report for up to four hours after the scheduled time has expired. If it is still unable to send out the report (because the communication failure persists), the system resets the interval to 15 minutes. Once the communication failure is resolved, the system reverts the reporting interval to the value that you last configured.

The system message you may see in case of a communication failure is %SMART\_LIC-3-COMM\_FAILED. For information about resolving this error and restoring the reporting interval value, in the software configuration guide of the required release (17.3.x onwards), see *System Configuration > Smart Licensing Using Policy > Troubleshooting Smart Licensing Using Policy*.

## Examples

- [Examples for Data Privacy, on page 343](#)
- [Examples for Transport Type and URL, on page 343](#)
- [Examples for Usage Reporting Options, on page 344](#)



## Examples for Data Privacy

The following examples show how to configure data privacy related information using **license smart privacy** command in global configuration mode. The accompanying **show license status** output displays configured information.

No private information is sent:

```
Device# configure terminal
Device(config)# license smart privacy all
Device(config)# license smart transport callhome
Device(config)# license smart url
https://tools.cisco.com/its/service/odcce/services/DDCEService
Device(config)# exit
Device# show license status
<output truncated>
Data Privacy:
  Sending Hostname: no
  Callhome hostname privacy: ENABLED
  Smart Licensing hostname privacy: ENABLED
  Version privacy: ENABLED

Transport:
  Type: Callhome
<output truncated>
```

Agent version on the product instance is not sent:

```
Device# configure terminal
Device(config)# license smart privacy version
Device(config)# license smart transport callhome
Device(config)# license smart url
https://tools.cisco.com/its/service/odcce/services/DDCEService
Device(config)# exit
Device# show license status
<output truncated>
Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: ENABLED

Transport:
  Type: Callhome
<output truncated>
```

## Examples for Transport Type and URL

The following examples show how to configure some of the transport types using the **license smart transport** and the **license smart url** commands in global configuration mode. The accompanying **show license all** output displays configured information.

Transport cslu:

```
Device# configure terminal
Device(config)# license smart transport cslu
Device(config)# license smart url default
Device(config)# exit
Device# show license all
<output truncated>
```

```

Transport:
  Type: cslu
  Cslu address: http://192.168.0.1:8182/cslu/v1/pi
  Proxy:
    Not Configured
<output truncated>

```

#### Transport smart:

```

Device# configure terminal
Device(config)# license smart transport smart
Device(config)# license smart url smart https://smartreceiver.cisco.com/licservice/license
Device(config)# exit
Device# show license all
<output truncated>
Transport:
  Type: Smart
  URL: https://smartreceiver-stage.cisco.com/licservice/license
  Proxy:
    Not Configured
<output truncated>

```

### Examples for Usage Reporting Options

The following examples show how to configure some of the usage reporting settings using the **license smart usage** command in global configuration mode. The accompanying **show running-config** output displays configured information.

#### Configuring the **customer-tag** option:

```

Device# configure terminal
Device(config)# license smart usage customer-tags tag1 SA/VA:01
Device(config)# exit
Device# show running-config | include tag1
license smart usage customer-tags tag1 SA/VA:01

```

#### Configuring a narrower reporting interval than the currently applied policy:

```

Device# show license status
<output truncated>
Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Dec 21 12:02:21 2020 PST
Reporting push interval: 30 days
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 22 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
Last report file write: <none>
<output truncated>

```

```

Device# configure terminal
Device(config)# license smart usage interval 20
Device(config)# exit
Device# show license status
<output truncated>

```

```

Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Nov 22 12:02:21 2020 PST
Reporting push interval: 20 days
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 12 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST

```

```
Last report file write: <none>  
<output truncated>
```

## license smart (privileged EXEC)

To configure licensing functions such as requesting or returning authorization codes, saving Resource Utilization Measurement reports (RUM reports), importing a file on to a product instance, establishing trust with Cisco Smart Software Manager (CSSM), synchronizing the product instance with CSSM, or Cisco Smart License Utility (CSLU), or Smart Software Manager On-Prem (SSM On-Prem), and removing licensing information from the product instance, enter the **license smart** command in privileged EXEC mode with the corresponding keyword or argument.

```
license smart { authorization { request { add | replace } feature_name { all | local } | return { all | local } { offline [ path ] | online } } | clear eventlog | export return { all | local } feature_name | factory reset | import file_path | save { trust-request filepath_filename | usage { all | days days | rum-id rum-ID | unreported } { file file_path } } | sync { all | local } | trust idtoken id_token_value { local | all } { force } }
```

Syntax Description	smart	Provides options for Smart Licensing.
	<b>authorization</b>	Provides the option to request for, or return, authorization codes.  Authorization codes are required <i>only</i> if you use licenses with enforcement type: export-controlled or enforced.
	<b>request</b>	Requests an authorization code from CSSM, CSLU (CSLU in-turn fetches it from CSSM), or SSM On-Prem and installs it on the product instance.
	<b>add</b>	Adds the requested license to the existing authorization code. The new authorization code will contain all the licenses of the existing authorization code and the requested license.
	<b>replace</b>	Replaces the existing authorization code. The new authorization code will contain only the requested license. All licenses in the current authorization code are returned.  When you enter this option, the product instance verifies if licenses that correspond to the authorization codes that will be removed, are in-use. If licenses are being used, an error message tells you to first disable the corresponding features.
	<i>feature_name</i>	Name of the license for which you are requesting an authorization code.
	<b>all</b>	Performs the action for all product instances in a High Availability configuration.
	<b>local</b>	Performs the action for the <i>active</i> product instance. This is the default option.
	<b>return</b>	Returns an authorization code back to the license pool in CSSM.
	<b>offline</b> <i>file_path</i>	Means the product instance is not connected to CSSM. The authorization code is returned offline. This option requires you to print the return code to a file.  Optionally, you can also specify a path to save the file. The file format can be any readable format, such as <code>.txt</code>  If you choose the offline option, you must complete the additional step of copying the return code from the CLI or the saved file and entering it in CSSM.

<b>online</b>	Means that the product instance is in a connected mode. The authorization code is returned to CSLU or CSSM directly.
<b>clear eventlog</b>	Clears all event log files from the product instance.
<b>export return</b>	Returns the authorization key for an export-controlled license.
<b>factory reset</b>	Clears all saved licensing information from the product instance.
<b>import</b> <i>filepath_filename</i>	Imports a file on to the product instance. The file may be that of an authorization code, a trust code, or, or a policy.  For <i>filepath_filename</i> , specify the location, including the filename.
<b>save</b>	Provides options to save RUM reports or trust code requests.
<b>trust-request</b> <i>filepath_filename</i>	Saves the trust code request for the active product instance in the specified location.  For <i>filepath_filename</i> , specify the absolute path to the file, including the filename.
<b>usage</b> { <b>all</b>   <b>days</b> <i>days</i>   <b>rum-id</b> <i>rum-ID</i>   <b>unreported</b> } { <b>file</b> <i>file_path</i> }	Saves RUM reports (license usage information) in the specified location. You must specify one of these options: <ul style="list-style-type: none"> <li>• <b>all</b>: Saves all RUM reports.</li> <li>• <b>days</b> <i>days</i>: Saves RUM report for the last <i>n</i> number of days (excluding the current day). Enter a number. The valid range is 0 to 4294967295.  For example, if you enter 3, RUM reports of the last three days are saved.</li> <li>• <b>rum-Id</b> <i>rum-ID</i>: Saves a specified RUM ID. The valid value range is 0 to 18446744073709551615.</li> <li>• <b>unreported</b>: Saves all unreported RUM reports.</li> </ul> <p><b>file</b> <i>filepath_filename</i>: Saves the specified usage information to a file. Specify the absolute path to the file, including the filename.</p>
<b>sync</b> { <b>all</b>   <b>local</b> }	Synchronizes with CSSM or CSLU, or SSM On-Prem, to send and receive any pending data. This includes uploading pending RUM reports, downloading the ACK response, any pending authorization codes, trust codes, and policies for the product instance.  Specify the product instance by entering one of these options: <ul style="list-style-type: none"> <li>• <b>all</b>: Performs synchronization for all the product instances in a High Availability set-up. If you choose this option, the product instance also sends the list of all the UDIs in the synchronization request.</li> <li>• <b>local</b>: Performs synchronization only for the active product instance sending the request, that is, its own UDI. This is the default option.</li> </ul>
<b>trust idtoken</b> <i>id_token_value</i>	Establishes a trusted connection with CSSM.  To use this option, you must first generate a token in the CSSM portal. Provide the generated token value for <i>id_token_value</i> .

---

**force** Submits a trust code request even if a trust code already exists on the product instance.

A trust code is node-locked to the UDI of a product instance. If the UDI is already registered, CSSM does not allow a new registration for the same UDI. Entering the **force** keyword overrides this behavior.

---

**Command Default**

Cisco IOS XE Amsterdam 17.3.1 or earlier: Smart Licensing is enabled by default.

Cisco IOS XE Amsterdam 17.3.2a and later: Smart Licensing Using Policy is enabled by default.

**Command Modes**

Privileged EXEC

**Command History**

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	<p>The following keywords and variables were introduced with Smart Licensing Using Policy:</p> <ul style="list-style-type: none"> <li>• <b>authorization</b> { <b>request</b> { <b>add</b>   <b>replace</b> } <i>feature_name</i> { <b>all</b>   <b>local</b> }   <b>return</b> { <b>all</b>   <b>local</b> } { <b>offline</b> [ <i>path</i> ]   <b>online</b> } }</li> <li>• <b>import</b> <i>file_path</i></li> <li>• <b>save</b> { <b>trust-request</b> <i>filepath_filename</i>   <b>usage</b> { <b>all</b>   <b>days</b> <i>days</i>   <b>rum-id</b> <i>rum-ID</i>   <b>unreported</b> } { <b>file</b> <i>file_path</i> } }</li> <li>• <b>sync</b> { <b>all</b>   <b>local</b> }</li> <li>• <b>trust idtoken</b> <i>id_token_value</i> { <b>local</b>   <b>all</b> } [ <b>force</b> ]</li> </ul> <p>The following keywords and variables under the <b>license smart</b> command are deprecated and no longer available on the CLI:</p> <ul style="list-style-type: none"> <li>• <b>register idtoken</b> <i>token_id</i> [ <b>force</b> ]</li> <li>• <b>renew id</b> { <b>ID</b>   <b>auth</b> }</li> <li>• <b>debug</b> { <b>error</b>   <b>debug</b>   <b>trace</b>   <b>all</b> }</li> <li>• <b>reservation</b> { <b>cancel</b> [ <b>all</b>   <b>local</b> ]   <b>install</b> [ <b>file</b> ] <i>key</i>   <b>request</b> { <b>all</b>   <b>local</b>   <b>universal</b> }   <b>return</b> [ <b>all</b>   <b>authorization</b> { <i>auth_code</i>   <b>file</b> <i>filename</i> }   <b>Local</b> ] <i>key</i> }</li> <li>• <b>mfg reservation</b> { <b>request</b>   <b>install</b>   <b>install file</b>   <b>cancel</b> }</li> <li>• <b>conversion</b> { <b>start</b>   <b>stop</b> }</li> </ul>
Cisco IOS XE Amsterdam 17.3.3	Support for SSM On-Prem was introduced. You can perform licensing-related tasks such as saving Resource Utilization Measurement reports (RUM reports), importing a file on to a product instance, synchronizing the product instance, returning authorization codes, and removing licensing information from the product instance in an SSM On-Prem deployment.

**Usage Guidelines****Overwriting a Trust Code**

Use case for the **force** option when configuring the **license smart trust idtoken** command: You use same token for all the product instances that are part of one Virtual Account. If the product instance has moved from one account to another (for instance, because it was added to a High Availability set-up, which is part of another Virtual Account), then there may be an existing trust code you have to overwrite.

**Removing Licensing Information**

Entering the **licence smart factory reset** command removes all licensing information (except the licenses in-use) from the product instance, including any authorization codes, RUM reports etc. Therefore, we recommend the use of this command only if the product instance is being returned (Return Material Authrization, or RMA), or being decommissioned permanently. We also recommend that you send a RUM report to CSSM, before you remove licensing information from the product instance - this is to ensure that CSSM has up-to-date usage information.

**Authorization Codes and License Reservations:**

Options relating to authorization codes and license reservations:

- Since there are no export-controlled or enforced licenses on any of the Cisco Catalyst Wireless Controllers, and the notion of reserved licenses is not applicable in the Smart Licensing Using Policy environment, the following commands are not applicable:
  - **license smart authorization request { add | replace } *feature\_name* { all | local }**
  - **license smart export return**
- The following option is applicable and required for any SLR authorization codes you may want to return:

```
license smart authorization return { all | local } { offline [ path ] | online }
```

**Examples**

- [Example for Saving Licensing Usage Information, on page 349](#)
- [Example for Installing a Trust Code, on page 350](#)
- [Example for Returning an SLR Authorization Code, on page 350](#)

**Example for Saving Licensing Usage Information**

The following example shows how you can save license usage information on the product instance. You can use this option to fulfil reporting requirements in an air-gapped network. In the example, the file is first save to flash memory and then copied to a TFTP location:

```
Device> enable
Device# license smart save usage unreported file flash:RUM-unrep.txt
Device# dir
Directory of bootflash:/
33      -rw-                5994   Nov 2 2020 03:58:04 +05:00  RUM-unrep.txt

Device# copy flash:RUM-unrep.txt tftp://192.168.0.1//auto/tftp-user/user01/
Address or name of remote host [192.168.0.1]?
Destination filename [//auto/tftp-user/user01/RUM-unrep.txt]?
```

```
!!
15128 bytes copied in 0.161 secs (93963 bytes/sec)
```

After you save RUM reports to a file, you must upload it to CSSM (from a workstation that has connectivity to the internet, and Cisco).

### Example for Installing a Trust Code

The following example shows how to install a trust code even if one is already installed on the product instance. This requires connectivity to CSSM. The accompanying **show license status** output shows sample output after successful installation:

Before you can install a trust code, you must generate a token and download the corresponding file from CSSM.

Use the **show license status** command (Trust Code Installed:) to verify results.

```
Device> enable
Device# license smart trust idtoken
NGMwMjk5mYtNZaxMS00NzMZmtgWm local force

Device# show license status
<output truncated>
Trust Code Installed:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
         INSTALLED on Nov 02 05:19:05 2020 IST
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
         INSTALLED on Nov 02 05:19:05 2020 IST
<output truncated>
```

### Example for Returning an SLR Authorization Code

The following example shows how to remove and return an SLR authorization code. Here the code is returned offline (no connectivity to CSSM). The accompanying **show license all** output shows sample output after successful return:

```
Device> enable
Device# show license all
<output truncated>
License Authorizations
=====
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
         Status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
         Last Confirmation code: 102fc949
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
         Status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
         Last Confirmation code: ad4382fe
<output truncated>

Device# license smart authorization return local offline
Enter this return code in Cisco Smart Software Manager portal:
UDI: PID:C9800-CL-K9,SN:93BBAH93MGS
     Return code: CqaUPW-WSPYiq-ZNU2ci-SnWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h
UDI: PID:C9800-CL-K9,SN:9XECPSUU4XN
     Return code: CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA

Device# show license all
<output truncated>
```



```
License Authorizations
=====
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        Status: NOT INSTALLED
        Last return code: CqaUPW-WSPYiq-ZNU2ci-SnWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        Status: NOT INSTALLED
        Last return code: CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA
<output truncated>
```

If you choose the **offline** option, you must complete the additional step of copying the return code from the CLI or the saved file and entering it in CSSM.

## local-admin-mac deny

To deny association of clients using Locally Administered Addresses, use the **local-admin-mac deny** command. Use the **no** form of this command to disable the feature.

**local-admin-mac deny**

**no local-admin-mac deny**

<b>Syntax Description</b>	<b>local-admin-mac</b>	Specifies the locally administered MAC addresses.
	<b>deny</b>	Denies the association of clients using Locally Administered Addresses
<b>Command Default</b>	None	
<b>Command Modes</b>	WLAN configuration mode (config-wlan)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

### Example

The following example shows how to deny association of clients using Locally Administered Addresses:

```
Device# configure terminal
Device(config)# wlan wlan-test 3 ssid-test
Device(config-wlan)# shutdownDevice(config-wlan)# [no] local-admin-mac deny
Device(config-wlan)# no shutdown
```

# local-auth ap eap-fast

To configure Flex policy local authentication using EAP Fast method, use the **local-auth ap eap-fast** command.

**local-auth ap eap-fast** *profile-name*

---

## Syntax Description

*profile-name* Enter eap-fast profile name.

---



---

## Command Default

None

---

## Command Modes

config-wireless-flex-profile

---

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

## Examples

The following example shows how to configure EAP Fast method authentication on a Flex policy:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile flex profile-name
Device(config-wireless-flex-profile)# local-auth ap eap-fast eap-fast-profile-name
```

# local-site

To configure the site as local site, use the **local-site** command.

## local-site

<b>Syntax Description</b>	<b>local-site</b> Configure this site as local site.				
<b>Command Default</b>	None				
<b>Command Modes</b>	config-site-tag				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.
Release	Modification				
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.				

## Examples

The following example shows how to set the current site as local site:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless tag site tag-name
Device(config-site-tag)# local-site
```

# location expiry

To configure the location expiry duration, use the **location expiry** command in global configuration mode.

**location expiry** { **calibrating-client** | **client** | **tags** } *timeout-duration*

Syntax Description		
<b>calibrating-client</b>	Timeout value for calibrating clients.	
<b>client</b>	Timeout value for clients.	
<b>tags</b>	Timeout value for RFID tags.	
<i>timeout-duration</i>	Timeout duration, in seconds.	
Command Default	Timeout value is not configured.	
Command Modes	Global configuration (config)	
Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

## Example

This example shows how to configure the location expiry duration:

```
Device(config)# location expiry tags 50
```

## location notify-threshold

To configure the NMSP notification threshold for RSSI measurements, use the **location notify-threshold** command in global configuration mode. To remove the NMSP notification threshold for RSSI measurements, use the **no** form of this command.

```
location notify-threshold {client | rogue-aps | tags } db
no location notify-threshold {client | rogue-aps | tags }
```

Syntax Description	
<b>client</b>	Specifies the NMSP notification threshold (in dB) for clients and rogue clients. The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.
<b>rogue-aps</b>	Specifies the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.
<b>tags</b>	Specifies the NMSP notification threshold (in dB) for RFID tags. The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.
<b>db</b>	The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.

**Command Default** No default behavior or values.

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to configure the NMSP notification threshold to 10 dB for clients. A notification NMSP message is sent to MSE as soon as the client RSSI changes by 10 dB:

```
Device# configure terminal
Device(config)# location notify-threshold client 10
Device(config)# end
```

# log-export-mode

To configure the log export using FTP, STP and TFTP, use the **log-export-mode** command. Use the **no** command to negate the command or to set the command to its default.

**log-export-mode** { **ftp** | **stp** | **tftp** }

**no log-export-mode** { **ftp** | **stp** | **tftp** }

Syntax Description	
<b>ftp</b>	Configures the log export using FTP.
<b>stp</b>	Configures the log export using STP.
<b>tftp</b>	Configures the log export using TFTP.

Command Default	None
-----------------	------

Command Modes	Wireless trace export profile configuration
---------------	---------------------------------------------

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

## Example

```
Device(config)# wireless profile transfer trace-export trace-export-name
Device(config-wireless-trace-export-profile)# log-export-mode tftp
```

# mab request format attribute

To configure the delimiter while configuring MAC filtering on a WLAN, use the mab request format attribute command.

**mab request format attribute** *username password nas-identifier* ]

## Syntax Description

<i>username</i>	Username format used for MAB requests
<i>password</i>	Global Password used for all MAB requests
<i>Nas-identifier</i>	NAS-Identifier attribute

## Command Default

Global Configuration

## Command Modes

MAC is sent without any delimiter.

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Usage Guidelines

MAC is sent without any delimiter.

## Example

The following example shows how to configure delimiter while configuring MAC filtering:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# mab request format attribute 1 groupsize 4
```



# mac-filtering

To enable MAC filtering on a WLAN, use the **mac-filtering** command.

**mac-filtering** [*mac-authorization-list* ]

<b>Syntax Description</b>	<i>mac-authorization-list</i> Name of the Authorization list.				
<b>Command Default</b>	None				
<b>Command Modes</b>	config-wlan				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.
Release	Modification				
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.				

## Examples

The following example shows how to enable MAC filtering on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan-name wlan-index SSID-name
Device(config-wlan)# mac-filtering
```

## match activated-service-template

To create a condition that evaluates true based on the service template activated on a session, use the **match activated-service-template** command in control class-map filter configuration mode. To create a condition that evaluates true if the service template activated on a session does not match the specified template, use the **no-match activated-service-template** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

**match activated-service-template** *template-name*

**no-match activated-service-template** *template-name*

**no** {**match** | **no-match**} **activated-service-template** *template-name*

<b>Syntax Description</b>	<i>template-name</i> Name of a configured service template as defined by the <b>service-template</b> command.
---------------------------	---------------------------------------------------------------------------------------------------------------

**Command Default** The control class does not contain a condition based on the service template.

**Command Modes** Control class-map filter configuration (config-filter-control-classmap)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.2SE	This command was introduced.

**Usage Guidelines** The **match activated-service-template** command configures a match condition in a control class based on the service template applied to a session. A control class can contain multiple conditions, each of which will evaluate as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true for the actions of the control policy to be executed.

The **no-match** form of this command specifies a value that results in an unsuccessful match. All other values of the specified match criterion result in a successful match. For example, if you configure the **no-match activated-service-template SVC\_1** command, all template values except SVC\_1 are accepted as a successful match.

The **class** command associates a control class with a control policy.

### Examples

The following example shows how to configure a control class that evaluates true if the service template named VLAN\_1 is activated on the session:

```
class-map type control subscriber match-all CLASS_1
 match activated-service-template VLAN_1
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>activate</b> (policy-map action)	Activates a control policy or service template on a subscriber session.
	<b>class</b>	Associates a control class with one or more actions in a control policy.
	<b>match service-template</b>	Creates a condition that evaluates true based on an event's service template.

Command	Description
<b>service-template</b>	Defines a template that contains a set of service policy attributes to apply to subscriber sessions.

# match any

To perform a match on any protocol that passes through the device, use the **match any** command.

## match any

---

### Command Default

None

---

### Command Modes

config-cmap

---

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to match any packet passing through the device:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# class-map cmap-name
Device(config-cmap)# match any
```

# match message-type

To set a message type to match a service list, use the **match message-type** command.

```
match message-type {announcement | any | query}
```

Syntax Description	
<b>announcement</b>	Allows only service advertisements or announcements for the Device.
<b>any</b>	Allows any match type.
<b>query</b>	Allows only a query from the client for a certain Device in the network.

**Command Default** None

**Command Modes** Service list configuration.

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** Multiple service maps of the same name with different sequence numbers can be created, and the evaluation of the filters will be ordered on the sequence number. Service lists are an ordered sequence of individual statements, with each one having a permit or deny result. The evaluation of a service list consists of a list scan in a predetermined order, and an evaluation of the criteria of each statement that matches. A list scan is stopped once the first statement match is found and a permit/deny action associated with the statement match is performed. The default action after scanning through the entire list is to deny.



**Note** It is not possible to use the **match** command if you have used the **service-list mdns-sd service-list-name query** command. The **match** command can be used only for the **permit** or **deny** option.

## Example

The following example shows how to set the announcement message type to be matched:

```
Device(config-mdns-sd-sl) # match message-type announcement
```

## match non-client-nrt

To match non-client NRT (non-real-time), use the **match non-client-nrt** command in class-map configuration mode. Use the **no** form of this command to return to the default setting.

**match non-client-nrt**  
**no match non-client-nrt**

<b>Syntax Description</b>	This command has no arguments or keywords.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Class-map	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
<b>Usage Guidelines</b>	None	

This example show how you can configure non-client NRT:

```
Device(config)# class-map test_1000
Device(config-cmap)# match non-client-nrt
```

# match protocol

To configure the match criterion for a class map on the basis of a specified protocol, use the **match protocol** command in class-map configuration or policy inline configuration mode. To remove the protocol-based match criterion from the class map, use the **no** form of this command. For more information about the **match protocol** command, refer to the *Cisco IOS Quality of Service Solutions Command Reference*.

**match protocol** {*protocol-name* | **attribute category** *category-name* | **attribute sub-category** *sub-category-name* | **attribute application-group** *application-group-name*}

<b>Syntax Description</b>	<i>protocol-name</i>	Name of the protocol (for example, bgp) used as a matching criterion.
	<i>category-name</i>	Name of the application category used as a matching criterion.
	<i>sub-category-name</i>	Name of the application subcategory used as a matching criterion.
	<i>application-group-name</i>	Name of the application group as a matching criterion. When the application name is specified, the application is configured as the match criterion instead of the application group.
<b>Command Default</b>	No match criterion is configured.	
<b>Command Modes</b>	Class-map configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to create class maps with apply match protocol filters for application name, category, and sub category:

```
Device# configure terminal
Device(config)# class-map cat-browsing
Device(config-cmap)# match protocol attribute category browsing
Device(config-cmap)#end

Device# configure terminal
Device(config)# class-map cat-fileshare
Device(config-cmap)# match protocol attribute category file-sharing
Device(config-cmap)#end

Device# configure terminal
Device(config)# class-map match-any subcat-terminal
Device(config-cmap)# match protocol attribute sub-category terminal
Device(config-cmap)#end

Device# configure terminal
Device(config)# class-map match-any webex-meeting
Device(config-cmap)# match protocol webex-meeting
Device(config-cmap)#end
```

This example shows how to create policy maps and define existing class maps for upstream QoS:

```

Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class cat-browsing
Device(config-pmap-c)# police 150000
Device(config-pmap-c)# set dscp 12
Device(config-pmap-c)#end

```

```

Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class cat-fileshare
Device(config-pmap-c)# police 1000000
Device(config-pmap-c)# set dscp 20
Device(config-pmap-c)#end

```

```

Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class subcat-terminal
Device(config-pmap-c)# police 120000
Device(config-pmap-c)# set dscp 15
Device(config-pmap-c)#end

```

```

Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class webex-meeting
Device(config-pmap-c)# police 50000000
Device(config-pmap-c)# set dscp 21
Device(config-pmap-c)#end

```

This example shows how to create policy maps and define existing class maps for downstream QoS:

```

Device# configure terminal
Device(config)# policy-map test-avc-down
Device(config-pmap)# class cat-browsing
Device(config-pmap-c)# police 200000
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)#end

```

```

Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class cat-fileshare
Device(config-pmap-c)# police 300000
Device(config-pmap-c)# set wlan user-priority 2
Device(config-pmap-c)# set dscp 20
Device(config-pmap-c)#end

```

```

Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class subcat-terminal
Device(config-pmap-c)# police 100000
Device(config-pmap-c)# set dscp 25
Device(config-pmap-c)#end

```

```

Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class webex-meeting
Device(config-pmap-c)# police 60000000

```



```
Device(config-pmap-c) # set dscp 41
Device(config-pmap-c) #end
```

This example shows how to apply defined QoS policy on a WLAN:

```
Device# configure terminal
Device(config)#wlan alpha
Device(config-wlan)#shut
Device(config-wlan)#end
Device(config-wlan)#service-policy client input test-avc-up
Device(config-wlan)#service-policy client output test-avc-down
Device(config-wlan)#no shut
Device(config-wlan)#end
```

## match service-instance

To set a service instance to match a service list, use the **match service-instance** command.

**match service-instance** *line*

<b>Syntax Description</b>	<i>line</i> Regular expression to match the service instance in packets.
---------------------------	--------------------------------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Service list configuration
----------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

<b>Usage Guidelines</b>	It is not possible to use the <b>match</b> command if you have used the <b>service-list mdns-sd</b> <i>service-list-name</i> <b>query</b> command. The <b>match</b> command can be used only for the <b>permit</b> or <b>deny</b> option.
-------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### Example

The following example shows how to set the service instance to match:

```
Device(config-mdns-sd-sl)# match service-instance servInst 1
```

## match service-type

To set the value of the mDNS service type string to match, use the **match service-type** command.

**match service-type** *line*

<b>Syntax Description</b>	<i>line</i> Regular expression to match the service type in packets.
---------------------------	----------------------------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Service list configuration
----------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

<b>Usage Guidelines</b>	It is not possible to use the <b>match</b> command if you have used the <b>service-list mdns-sd service-list-name query</b> command. The <b>match</b> command can be used only for the <b>permit</b> or <b>deny</b> option.
-------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### Example

The following example shows how to set the value of the mDNS service type string to match:

```
Device(config-mdns-sd-sl)# match service-type _ipp._tcp
```

## match user-role

To configure the class-map attribute filter criteria, use the **match user-role** command.

**match user-role** *user-role*

<b>Command Default</b>	None	
<b>Command Modes</b>	config-filter-control-classmap	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

### Examples

The following example shows how to configure a class-map attribute filter criteria:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# class-map type control subscriber match-any map-name
Device(config-filter-control-classmap)# match user-role user-role
```

# match username

To create a condition that evaluates true based on an event's username, use the **match username** command in control class-map filter configuration mode. To create a condition that evaluates true if an event's username does not match the specified username, use the **no-match username** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

**match username** *username*  
**no-match username** *username*  
**no** {**match** | **no-match**} **username** *username*

<b>Syntax Description</b>	<i>username</i> Username.
---------------------------	---------------------------

**Command Default** The control class does not contain a condition based on the event's username.

**Command Modes** Control class-map filter configuration (config-filter-control-classmap)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.2SE	This command was introduced.

**Usage Guidelines** The **match username** command configures a match condition in a control class based on the username. A control class can contain multiple conditions, each of which will evaluate as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true to execute the actions of the control policy.

The **no-match** form of this command specifies a value that results in an unsuccessful match. All other values of the specified match criterion result in a successful match. For example, if you configure the **no-match username josmithe** command, the control class accepts any username value except josmithe as a successful match.

The **class** command associates a control class with a control policy.

## Examples

The following example shows how to configure a control class that evaluates true if the username is josmithe:

```
class-map type control subscriber match-all CLASS_1
 match username josmithe
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>class</b>	Associates a control class with one or more actions in a control policy.
	<b>policy-map type control subscriber</b>	Defines a control policy for subscriber sessions

## match (access-map configuration)

To set the VLAN map to match packets against one or more access lists, use the **match** command in access-map configuration mode. Use the **no** form of this command to remove the match parameters.

```
{match ip address {namenumber} [{namenumber}] [{namenumber}]. . . | mac address name [name]
[name]. . .}
{no match ip address {namenumber} [{namenumber}] [{namenumber}]. . . | mac address name
[name] [name]. . .}
```

Syntax Description	
<b>ip address</b>	Set the access map to match packets against an IP address access list.
<b>mac address</b>	Set the access map to match packets against a MAC address access list.
<b>name</b>	Name of the access list to match packets against.
<b>number</b>	Number of the access list to match packets against. This option is not valid for MAC access lists.

**Command Default** The default action is to have no match parameters applied to a VLAN map.

**Command Modes** Access-map configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** You enter access-map configuration mode by using the **vlan access-map** global configuration command.

You must enter one access list name or number; others are optional. You can match packets against one or more access lists. Matching any of the lists counts as a match of the entry.

In access-map configuration mode, use the **match** command to define the match conditions for a VLAN map applied to a VLAN. Use the **action** command to set the action that occurs when the packet matches the conditions.

Packets are matched only against access lists of the same protocol type; IP packets are matched against IP access lists, and all other packets are matched against MAC access lists.

Both IP and MAC addresses can be specified for the same map entry.

### Examples

This example shows how to define and apply a VLAN access map *vmap4* to VLANs 5 and 6 that will cause the interface to drop an IP packet if the packet matches the conditions defined in access list *a12*.

```
Device(config)# vlan access-map vmap4
Device(config-access-map)# match ip address a12
Device(config-access-map)# action drop
Device(config-access-map)# exit
```

```
Device(config)# vlan filter vmap4 vlan-list 5-6
```

You can verify your settings by entering the **show vlan access-map** privileged EXEC command.

## match (class-map configuration)

To define the match criteria to classify traffic, use the **match** command in class-map configuration mode. Use the **no** form of this command to remove the match criteria.

### Cisco IOS XE Everest 16.5.x and Earlier Releases

```
match {access-group {name acl-name acl-index} | class-map class-map-name | cos cos-value | dscp
dscp-value | [ip] dscp dscp-list | [ip] precedence ip-precedence-list | precedence
precedence-value1...value4 | qos-group qos-group-value | vlan vlan-id}
no match {access-group {name acl-name acl-index} | class-map class-map-name | cos cos-value | dscp
dscp-value | [ip] dscp dscp-list | [ip] precedence ip-precedence-list | precedence
precedence-value1...value4 | qos-group qos-group-value | vlan vlan-id}
```

### Cisco IOS XE Everest 16.6.x and Later Releases

```
match {access-group {name acl-name acl-index} | cos cos-value | dscp dscp-value | [ip] dscp dscp-list
| [ip] precedence ip-precedence-list | mpls experimental-value | non-client-nrt | precedence
precedence-value1...value4 | protocol protocol-name | qos-group qos-group-value | vlan vlan-id | wlan
wlan-id}
no match {access-group {name acl-name acl-index} | cos cos-value | dscp dscp-value | [ip] dscp
dscp-list | [ip] precedence ip-precedence-list | mpls experimental-value | non-client-nrt | precedence
precedence-value1...value4 | protocol protocol-name | qos-group qos-group-value | vlan vlan-id | wlan
wlan-id}
```

Syntax Description		
<b>access-group</b>		Specifies an access group.
<b>name</b> <i>acl-name</i>		Specifies the name of an IP standard or extended access control list (ACL) or MAC ACL.
<i>acl-index</i>		Specifies the number of an IP standard or extended access control list (ACL) or MAC ACL. For an IP standard ACL, the ACL index range is 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index range is 100 to 199 and 2000 to 2699.
<b>class-map</b> <i>class-map-name</i>		Uses a traffic class as a classification policy and specifies a traffic class name to use as the match criterion.
<b>cos</b> <i>cos-value</i>		Matches a packet on the basis of a Layer 2 class of service (CoS)/Inter-Switch Link (ISL) marking. The cos-value is from 0 to 7. You can specify up to four CoS values in one <b>match cos</b> statement, separated by a space.
<b>dscp</b> <i>dscp-value</i>		Specifies the parameters for each DSCP value. You can specify a value in the range 0 to 63 specifying the differentiated services code point value.



<b>ip dscp</b> <i>dscp-list</i>	Specifies a list of up to eight IP Differentiated Services Code Point (DSCP) values to match against incoming packets. Separate each value with a space. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value.
<b>ip precedence</b> <i>ip-precedence-list</i>	Specifies a list of up to eight IP-precedence values to match against incoming packets. Separate each value with a space. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.
<b>precedence</b> <i>precedence-value1...value4</i>	Assigns an IP precedence value to the classified traffic. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.
<b>qos-group</b> <i>qos-group-value</i>	Identifies a specific QoS group value as a match criterion. The range is 0 to 31.
<b>vlan</b> <i>vlan-id</i>	Identifies a specific VLAN as a match criterion. The range is 1 to 4094.
<b>mpls</b> <i>experimental-value</i>	Specifies Multi Protocol Label Switching specific values.
<b>non-client-nrt</b>	Matches a non-client NRT (non-real-time).
<b>protocol</b> <i>protocol-name</i>	Specifies the type of protocol.
<b>wlan</b> <i>wlan-id</i>	Identifies 802.11 specific values.

**Command Default** No match criteria are defined.

**Command Modes** Class-map configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** The **match** command is used to specify which fields in the incoming packets are examined to classify the packets. Only the IP access group or the MAC access group matching to the Ether Type/Len are supported. If you enter the **class-map match-any***class-map-name* global configuration command, you can enter the following **match** commands:

- **match access-group name** *acl-name*



**Note** The ACL must be an extended named ACL.

- **match ip dscp** *dscp-list*
- **match ip precedence** *ip-precedence-list*

The **match access-group** *acl-index* command is not supported.

To define packet classification on a physical-port basis, only one **match** command per class map is supported. In this situation, the **match-any** keyword is equivalent.

For the **match ip dscp** *dscp-list* or the **match ip precedence** *ip-precedence-list* command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **match ip dscp af11** command, which is the same as entering the **match ip dscp 10** command. You can enter the **match ip precedence critical** command, which is the same as entering the **match ip precedence 5** command. For a list of supported mnemonics, enter the **match ip dscp ?** or the **match ip precedence ?** command to see the command-line help strings.

Use the **input-interface** *interface-id-list* keyword when you are configuring an interface-level class map in a hierarchical policy map. For the *interface-id-list*, you can specify up to six entries.

## Examples

This example shows how to create a class map called class2, which matches all the incoming traffic with DSCP values of 10, 11, and 12:

```
Device(config)# class-map class2
Device(config-cmap)# match ip dscp 10 11 12
Device(config-cmap)# exit
```

This example shows how to create a class map called class3, which matches all the incoming traffic with IP-precedence values of 5, 6, and 7:

```
Device(config)# class-map class3
Device(config-cmap)# match ip precedence 5 6 7
Device(config-cmap)# exit
```

This example shows how to delete the IP-precedence match criteria and to classify traffic using acl1:

```
Device(config)# class-map class2
Device(config-cmap)# match ip precedence 5 6 7
Device(config-cmap)# no match ip precedence
Device(config-cmap)# match access-group acl1
Device(config-cmap)# exit
```

This example shows how to specify a list of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Device(config)# class-map match-any class4
Device(config-cmap)# match cos 4
Device(config-cmap)# exit
```

This example shows how to specify a range of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Device(config)# class-map match-any class4
Device(config-cmap)# match cos 4
Device(config-cmap)# exit
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

## match wlan user-priority

To match 802.11 specific values, use the **match wlan user-priority** command in class-map configuration mode. Use the **no** form of this command to return to the default setting.

```
match wlan user-priority wlan-value [wlan-value] [wlan-value] [wlan-value]
no match wlan user-priority wlan-value [wlan-value] [wlan-value] [wlan-value]
```

<b>Syntax Description</b>	<i>wlan-value</i> The 802.11-specific values. Enter the user priority 802.11 TID user priority (0-7). (Optional) Enter up to three user priority values separated by white-spaces.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Class-map configuration (config-cmap)				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.				
<b>Usage Guidelines</b>	None				

This example show how you can configure user-priority values:

```
Device(config)# class-map test_1000
Device(config-cmap)# match wlan user-priority 7
```

# max-bandwidth

To configure the wireless media-stream's maximum expected stream bandwidth in Kbps, use the **max-bandwidth** command.

**max-bandwidth** *bandwidth*

<b>Syntax Description</b>	<i>bandwidth</i> Maximum Expected Stream Bandwidth in Kbps. Valid range is 1 to 35000 Kbps.
---------------------------	---------------------------------------------------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	media-stream
----------------------	--------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to configure wireless media-stream bandwidth in Kbps:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless media-stream group doc-grp 224.0.0.0 224.0.0.223
Device(config-media-stream)# max-bandwidth 3500
```

# max-through

To limit multicast router advertisements (RAs) per VLAN per throttle period, use the **max-through** command in IPv6 RA throttle policy configuration mode. To reset the command to its defaults, use the **no** form of this command.

**max-through** {*mt-value* | **inherit** | **no-limit**}

## Syntax Description

**mt-value** Number of multicast RAs allowed on the VLAN before throttling occurs. The range is from 0 through 256.

**inherit** Merges the setting between target policies.

**no-limit** Multicast RAs are not limited on the VLAN.

## Command Default

10 RAs per VLAN per 10 minutes

## Command Modes

IPv6 RA throttle policy configuration (config-nd-ra-throttle)

## Command History

Release	Modification
Cisco IOS XE Release 3.2XE	This command was introduced.

## Usage Guidelines

The **max-through** command limits the amount of multicast RAs that are passed through to the VLAN per throttle period. This command can be configured only on a VLAN.

## Example

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)# max-through 25
```

# mdns-sd

To configure the mDNS service discovery gateway, use the **mdns-sd** command. To disable the configuration, use the **no** form of this command.

**mdns-sd** { **gateway** | **service-definition** *service-definition-name* | **service-list** *service-list-name* { **IN** | **OUT** } | **service-policy** *service-policy-name* }

**no mdns-sd** { **gateway** | **service-definition** *service-definition-name* | **service-list** *service-list-name* { **IN** | **OUT** } | **service-policy** *service-policy-name* }

Syntax Description	Command	Description
	<b>mdns-sd</b>	Configures the mDNS service discovery gateway.
	<b>gateway</b>	Configures mDNS gateway.
	<b>service-definition</b>	Configures mDNS service definition.
	<i>service-definition-name</i>	Specifies the mDNS service definition name.
	<b>service-list</b>	Configures mDNS service list.
	<i>service-list-name</i>	Specifies the mDNS service definition name.
	<b>IN</b>	Specifies the inbound filtering.
	<b>OUT</b>	Specifies the outbound filtering.
	<b>service-policy</b>	Configures mDNS service policy.
	<i>service-policy-name</i>	Specifies the mDNS service policy name.

**Command Default** None

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

**Usage Guidelines** None

## Example

The following example shows how to configure the mDNS service discovery gateway:

```
Device(config)# mdns-sd gateway
```

## mdns-sd-interface

To configure the mDNS service discovery per WLAN, use the **mdns-sd-interface** command. To disable the command, use the **no** form of this command.

```
mdns-sd-interface { drop | gateway }
```

```
no mdns-sd-interface { drop | gateway }
```

Syntax Description	
<b>mdns-sd-interface</b>	Configures the mDNS service discovery per WLAN
<b>drop</b>	Disables mDNS gateway and bridging for WLAN.
<b>gateway</b>	Enables mDNS gateway for WLAN.

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	WLAN configuration
----------------------	--------------------

Command History	Release	Modification
	Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

<b>Usage Guidelines</b>	None
-------------------------	------

### Example

The following example shows how to configure the mDNS service discovery per WLAN:

```
Device(config-wlan)# mdns-sd-interface gateway
```

# mdns-sd flex-profile

To configure the mDNS service discovery flex profile, use the **mdns-sd flex-profile** command. To disable the command, use the **no** form of this command.

**mdns-sd flex-profile** *flex-profile-name*

**no mdns-sd flex-profile** *flex-profile-name*

Syntax Description	Command	Description
	<b>mdns-sd flex-profile</b>	Configures the mDNS service discovery flex profile.
	<i>flex-profile-name</i>	Specifies the mDNS flex profile name.

**Command Default** None

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

**Usage Guidelines** None

## Example

The following example shows how to configure the mDNS service discovery flex profile:

```
Device(config)# mdns-sd flex-profile mdns-flex-profile
```



# mdns-sd profile

To apply the mDNS flex profile to the wireless flex profile, use the **mdns-sd profile** command in the wireless flex profile mode. To disable the command, use the **no** form of this command.

**mdns-sd profile** *flex-profile-name*

**no mdns-sd profile** *flex-profile-name*

<b>Syntax Description</b>	<b>mdns-sd profile</b>	Configures the mDNS flex profile in the wireless flex profile.
	<i>flex-profile-name</i>	Specifies the mDNS flex profile name.

**Command Default** None

**Command Modes** Wireless flex profile configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

**Usage Guidelines** None

## Example

The following example shows how to apply the mDNS flex profile to the wireless flex profile:

```
Device(config-wireless-flex-profile)# mdns-sd profile mdns-flex-profile
```

## method fast

To configure EAP profile to support EAP-FAST method, use the **method fast** command.

**method fast** [**profile** *profile-name*]

<b>Syntax Description</b>	<i>profile-name</i> Specify the method profile.
---------------------------	-------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	config-eap-profile
----------------------	--------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

### Examples

The following example shows how to enable EAP Fast method on a EAP profile:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# eap profile profile-name
Device(config-eap-profile)# method fast
```

## mgmtuser username

To set a username and password for AP management, use the **mgmtuser username** command. To disable this feature, use the **no** form of this command.

**mgmtuser username** *username* **password** {0 | 8} *password*

Syntax Description	
	<i>username</i> Enter a username for AP management.
	0 Specifies an UNENCRYPTED password.
	8 Specifies an AES encrypted password.
	<i>password</i> Configures the encryption password (key).

**Command Default** None

**Command Modes** AP Profile Configuration (config-ap-profile)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 17.6.1	This command was introduced.

### Examples

The following example shows how to set a username and password for AP management:

```
Device# enable
Device# configure terminal
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# mgmtuser username myusername password 0
Device(config-ap-profile)# end
```

# mop sysid

To enable an interface to send out periodic Maintenance Operation Protocol (MOP) system identification messages, use the **mopsysid** command in interface configuration mode. To disable MOP message support on an interface, use the **no** form of this command.

**mop sysid**  
**no mop sysid**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Enabled

**Command Modes** Interface configuration

## Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

## Usage Guidelines

You can still run MOP without having the background system ID messages sent. This command lets you use the MOP remote console, but does not generate messages used by the configurator.

## Examples

The following example enables serial interface 0 to send MOP system identification messages:

```
Router(config)# interface serial 0
Router(config-if)# mop sysid
```

## Related Commands

Command	Description
<b>mop device-code</b>	Identifies the type of device sending MOP sysid messages and request program messages.
<b>mop enabled</b>	Enables an interface to support the MOP.

## nac

To enable RADIUS Network Admission Control (NAC) support for a WLAN, use the **nac** command. To disable NAC out-of-band support, use the **no** form of this command.

**nac**  
**no nac**

**Syntax Description** This command has no keywords or arguments.

**Command Default** NAC is disabled.

**Command Modes** WLAN configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** You should enable AAA override before you enable the RADIUS NAC state.

This example shows how to configure RADIUS NAC on the WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# aaa-override
Device(config-wlan)# nac
```

This example shows how to disable RADIUS NAC on the WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no nac
Device(config-wlan)# no aaa-override
```

## nas-id option2

To configure option 2 parameters for a NAS-ID, use the **nas-id option2** command.

**nas-id option2** {**sys-ip** | **sys-name** | **sys-mac** }

<b>Syntax Description</b>	<b>sys-ip</b> System IP Address.				
	<b>sys-name</b> System Name.				
	<b>sys-mac</b> System MAC address.				
<b>Command Default</b>	None				
<b>Command Modes</b>	config-aaa-policy				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.
Release	Modification				
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.				

### Examples

The following example shows how to configure the system IP address for the NAS-ID:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless aaa policy profile-name
Device(config-aaa-policy)# nas-id option2 sys-ip
```

# network

To configure the network number in decimal notation, use the **network** command.

**network** *network-number* [{*network-mask* | **secondary** }]

## Syntax Description

*ipv4-address* Network number in dotted-decimal notation.

*network-mask* Network mask or prefix length.

**secondary** Configure as secondary subnet.

## Command Default

None

## Command Modes

dhcp-config

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to configure network number and the mask address:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ip dhcp pool name
Device(dhcp-config)# network 209.165.200.224 255.255.255.0
```

## nmsp cloud-services enable

To configure NMSP cloud services, use the **nmsp cloud-services enable** command.

### **nmsp cloud-services enable**

---

#### Command Default

None

---

#### Command Modes

Global configuration (config)

---

#### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

### Examples

The following example shows how to enable NMSP cloud services:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# nmsp cloud-services enable
```



## nmosp cloud-services http-proxy

To configure the proxy for NMSP cloud server, use the **nmosp cloud-services http-proxy** command.

**nmosp cloud-services http-proxy** *proxy-server port*

### Syntax Description

*proxy-server* Enter the hostname or the IP address of the proxy server for NMSP cloud services.

*port* Enter the proxy server port number for NMSP cloud services.

### Command Default

None

### Command Modes

Global configuration (config)

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

### Examples

The following example shows how to configure the proxy for NMSP cloud server:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# nmosp cloud-services http-proxy host-name port-number
```

## nmsp cloud-services server token

To configure the NMSP cloud services server parameters, use the **nmsp cloud-services server token** command.

**nmsp cloud-services server token** *token*

---

<b>Syntax Description</b>	<i>token</i> Authentication token for the NMSP cloud services.
---------------------------	----------------------------------------------------------------

---



---

<b>Command Default</b>	None
------------------------	------

---



---

<b>Command Modes</b>	config
----------------------	--------

---



---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

### Examples

The following example shows how to configure the for the NMSP cloud services server parameters:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# nmsp cloud-services server token authentication-token
```

## nmosp cloud-services server url

To configure NMSP cloud services server URL, use the **nmosp cloud-services server url** command.

```
nmosp cloud-services server url url
```

---

**Syntax Description**

*url* URL of the NMSP cloud services server.

---

---

**Command Default**

None

---

**Command Modes**

Global configuration (config)

---

---

**Command History**

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

### Examples

The following example shows how to configure a URL for NMSP cloud services server:

```
Device(config)# nmosp cloud-services server url http://www.example.com
```

## nmosp notification interval

To modify the Network Mobility Services Protocol (NMSP) notification interval value on the controller to address latency in the network, use the **nmosp notification interval** command in global configuration mode.

```
nmosp notification interval { attachment | location | rssi { clients | rfid | rogues { ap | client } } }
```

Syntax Description		
	<b>attachment</b>	Specifies the time used to aggregate attachment information.
	<b>location</b>	Specifies the time used to aggregate location information.
	<b>rssi</b>	Specifies the time used to aggregate RSSI information.
	<b>clients</b>	Specifies the time interval for clients.
	<b>rfid</b>	Specifies the time interval for rfid tags.
	<b>rogues</b>	Specifies the time interval for rogue APs and rogue clients .
	<b>ap</b>	Specifies the time used to aggregate rogue APs .
	<b>client</b>	Specifies the time used to aggregate rogue clients.

**Command Default** No default behavior or values.

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to set the NMSP notification interval for the active RFID tags to 25 seconds:

```
Device# configure terminal
Device(config)# nmosp notification-interval rfid 25
Device(config)# end
```

This example shows how to modify NMSP notification intervals for device attachment (connecting to the network or disconnecting from the network) every 10 seconds:

```
Device# configure terminal
Device(config)# nmosp notification-interval attachment 10
Device(config)# end
```

This example shows how to configure NMSP notification intervals for location parameters (location change) every 20 seconds:

```
Device# configure terminal  
Device(config)# nmosp notification-interval location 20  
Device(config)# end
```

# nmsp strong-cipher

To enable the new ciphers, use the **nmsp strong-cipher** command in global configuration mode. To disable, use the **no** form of this command.

**nmsp strong-cipher**  
**no nmsp strong-cipher**

**Syntax Description** This command has no arguments or keywords.

**Command Default** The new ciphers are not enabled.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	15.2(2)E	This command was introduced.

**Usage Guidelines** The **nmsp strong-cipher** command enables strong ciphers for new Network Mobility Service Protocol (NMSP) connections.



**Note** The existing NMSP connections will use the default cipher.

**Examples** The following example shows how to enable a strong-cipher for NMSP:

```
Device> enable
Device> configure terminal
Device(config)# nmsp strong-cipher
```

Related Commands	Command	Description
	<b>show nmsp status</b>	Displays the status of active NMSP connections.

# option

To configure optional data parameters for a flow exporter for , use the **option** command in flow exporter configuration mode. To remove optional data parameters for a flow exporter, use the **no** form of this command.

**option** {**exporter-stats** | **interface-table** | **sampler-table**} [{**timeout** *seconds*}]  
**no option** {**exporter-stats** | **interface-table** | **sampler-table**}

Syntax Description	Option	Description
	<b>exporter-stats</b>	Configures the exporter statistics option for flow exporters.
	<b>interface-table</b>	Configures the interface table option for flow exporters.
	<b>sampler-table</b>	Configures the export sampler table option for flow exporters.
	<b>timeout</b> <i>seconds</i>	(Optional) Configures the option resend time in seconds for flow exporters. The range is 1 to 86400. The default is 600.

**Command Default** The timeout is 600 seconds. All other optional data parameters are not configured.

**Command Modes** Flow exporter configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** The **option exporter-stats** command causes the periodic sending of the exporter statistics, including the number of records, bytes, and packets sent. This command allows the collector to estimate packet loss for the export records it receives. The optional timeout alters the frequency at which the reports are sent.

The **option interface-table** command causes the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names. The optional timeout can alter the frequency at which the reports are sent.

The **option sampler-table** command causes the periodic sending of an options table, which details the configuration of each sampler and allows the collector to map the sampler ID provided in any flow record to a configuration that it can use to scale up the flow statistics. The optional timeout can alter the frequency at which the reports are sent.

To return this command to its default settings, use the **no option** or **default option** flow exporter configuration command.

The following example shows how to enable the periodic sending of the sampler option table, which allows the collector to map the sampler ID to the sampler type and rate:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option sampler-table
```

The following example shows how to enable the periodic sending of the exporter statistics, including the number of records, bytes, and packets sent:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option exporter-stats
```

The following example shows how to enable the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names:

```
Device(config)# flow exporter FLOW-EXPORTER-1  
Device(config-flow-exporter)# option interface-table
```



# parameter-map type subscriber attribute-to-service

To configure parameter map type and name, use the **parameter-map type subscriber attribute-to-service** command.

**parameter-map type subscriber attribute-to-service** *parameter-map-name*

<b>Syntax Description</b>	<p><b>attribute-to-service</b> Name the attribute to service.</p> <p><i>parameter-map-name</i> Name of the parameter map. The map name is limited to 33 characters.</p>				
<b>Command Default</b>	None				
<b>Command Modes</b>	Global configuration (config)				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.
Release	Modification				
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.				

## Examples

The following example shows how to configure parameter map type and name:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# parameter-map type subscriber attribute-to-service parameter-map-name
```

## password encryption aes

To enable strong (AES) password encryption, use the **password encryption aes** command. To disable this feature, use the **no** form of this command.

```
password encryption aes
no password encryption aes
```

### Syntax Description

**password** Configures the encryption password (key).

**encryption** Encrypts system passwords.

**aes** Enables stronger (AES) password encryption.

### Command Default

None

### Command Modes

Global configuration mode.

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

### Example

The following example shows how to enable AES password encryption :

```
Device(config)#password encryption aes
```

# peer-blocking

To configure peer-to-peer blocking on a WLAN, use the **peer-blocking** command. To disable peer-to-peer blocking, use the **no** form of this command.

```
peer-blocking {drop | forward-upstream}
no peer-blocking
```

<b>Syntax Description</b>	<b>drop</b>	Specifies the device to discard the packets.
	<b>forward-upstream</b>	Specifies the packets to be forwarded on the upstream VLAN. The device next in the hierarchy to the device decides what action to take regarding the packets.
<b>Command Default</b>	Peer blocking is disabled.	
<b>Command Modes</b>	WLAN configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
		This command was introduced.

**Usage Guidelines** You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to enable the drop and forward-upstream options for peer-to-peer blocking:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1

Device(config-wlan)# peer-blocking drop
Device(config-wlan)# peer-blocking forward-upstream
```

This example shows how to disable the drop and forward-upstream options for peer-to-peer blocking:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1

Device(config-wlan)# no peer-blocking drop
Device(config-wlan)# no peer-blocking forward-upstream
```

# policy

To configure media stream admission policy, use the **policy** command.

**policy** {**admit** | **deny**}

---

## Syntax Description

**admit** Allows traffic for a media stream group.

**deny** Denies traffic for a media stream group.

---



---

## Command Default

None

---

## Command Modes

media-stream

---

## Command History

### Release

### Modification

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

## Examples

The following example shows how to allow traffic for a media stream group:

```
Device # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless media-stream group ms-group 224.0.0.0 224.0.0.223
Device(media-stream)# policy admit
```

# police

To define a policer for classified traffic, use the **police** command in policy-map class configuration mode. Use the **no** form of this command to remove an existing policer.

```
police rate-bps burst-byte [conform-action transmit]
no police rate-bps burst-byte [conform-action transmit]
```

Syntax Description		
	<i>rate-bps</i>	Specify the average traffic rate in bits per second (b/s). The range is 1000000 to 1000000000.
	<i>burst-byte</i>	Specify the normal burst size in bytes. The range is 8000 to 1000000.
	<b>conform-action transmit</b>	(Optional) When less than the specified rate, specify that the switch transmits the packet.

**Command Default** No policers are defined.

**Command Modes** Policy-map class configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** A policer defines a maximum permissible rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded.

When configuring hierarchical policy maps, you can only use the **police** policy-map command in a secondary interface-level policy map.

The port ASIC device, which controls more than one physical port, supports 256 policers on the switch (255 user-configurable policers plus 1 policer reserved for internal use). The maximum number of configurable policers supported per port is 63. Policers are allocated on demand by the software and are constrained by the hardware and ASIC boundaries. You cannot reserve policers per port. There is no guarantee that a port will be assigned to any policer.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

## Examples

This example shows how to configure a policer that transmits packets if traffic is less than 1 Mb/s average rate with a burst size of 20 KB. There is no packet modification.

```
Device(config)# class-map class1
Device(config-cmap)# exit
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# police 1000000 20000 conform-action transmit
Device(config-pmap-c)# exit
```

This example shows how to configure a policer that transmits packets if traffic is less than 1 Mb/s average rate with a burst size of 20 KB. There is no packet modification. This example uses an abbreviated syntax:

```
Device(config)# class-map class1
Device(config-cmap)# exit
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# police 1m 20000 conform-action transmit
Device(config-pmap-c)# exit
```

This example shows how to configure a policer, which marks down the DSCP values with the values defined in policed-DSCP map and sends the packet:

```
Device(config)# policy-map policy2
Device(config-pmap)# class class2
Device(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Device(config-pmap-c)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

# police cir

To set the policing of committed information rate, use the **police cir** command.

**police cir** <target bit rate>

<b>Syntax Description</b>	<b>police cir</b>	Polices committed information rate.
	<i>8000-10000000000</i>	Sets the target bit rate at bits per second. The range is between 8000 and 10000000000.
<b>Command Default</b>	None	
<b>Command Modes</b>	Policy map class configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

## Example

This example shows how to set the committed information rate:

```
Device(config-pmap-c)#police cir 8000
```

# policy-map

To create or modify a policy map that can be attached to multiple physical ports or switch virtual interfaces (SVIs) and to enter policy-map configuration mode, use the **policy-map** command in global configuration mode. Use the **no** form of this command to delete an existing policy map and to return to global configuration mode.

**policy-map** *policy-map-name*  
**no policy-map** *policy-map-name*

## Syntax Description

*policy-map-name* Name of the policy map.

## Command Default

No policy maps are defined.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

## Usage Guidelines

After entering the **policy-map** command, you enter policy-map configuration mode, and these configuration commands are available:

- **class**—Defines the classification match criteria for the specified class map.
- **description**—Describes the policy map (up to 200 characters).
- **exit**—Exits policy-map configuration mode and returns you to global configuration mode.
- **no**—Removes a previously defined policy map.
- **sequence-interval**—Enables sequence number capability.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Before configuring policies for classes whose match criteria are defined in a class map, use the **policy-map** command to specify the name of the policy map to be created, added to, or modified. Entering the **policy-map** command also enables the policy-map configuration mode in which you can configure or modify the class policies for that policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. To configure the match criteria for a class, use the **class-map** global configuration and **match** class-map configuration commands. You define packet classification on a physical-port basis.

Only one policy map per ingress port is supported. You can apply the same policy map to multiple physical ports.

You can apply a nonhierarchical policy maps to physical ports. A nonhierarchical policy map is the same as the port-based policy maps in the device.

A hierarchical policy map has two levels in the format of a parent-child policy. The parent policy cannot be modified but the child policy (port-child policy) can be modified to suit the QoS configuration.



In VLAN-based QoS, a service policy is applied to an SVI interface.



**Note** Not all MQC QoS combinations are supported for wired ports. For information about these restrictions, see chapters "Restrictions for QoS on Wired Targets" in the QoS configuration guide.

## Examples

This example shows how to create a policy map called policy1. When attached to the ingress port, it matches all the incoming traffic defined in class1, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic less than the profile is sent.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police 1000000 20000 conform-action transmit
Device(config-pmap-c)# exit
```

This example show you how to configure hierarchical polices:

```
Device# configure terminal
Device(config)# class-map c1
Device(config-cmap)# exit

Device(config)# class-map c2
Device(config-cmap)# exit

Device(config)# policy-map child
Device(config-pmap)# class c1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class c2
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit

Device(config-pmap)# class class-default
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device(config)# policy-map parent
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 1000000
Device(config-pmap-c)# service-policy child
Device(config-pmap-c)# end
```

This example shows how to delete a policy map:

```
Device(config)# no policy-map policymap2
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

# policy-map

To create or modify a policy map that can be attached to multiple physical ports or switch virtual interfaces (SVIs) and to enter policy-map configuration mode, use the **policy-map** command in global configuration mode. Use the **no** form of this command to delete an existing policy map and to return to global configuration mode.

**policy-map** *policy-map-name*  
**no policy-map** *policy-map-name*

## Syntax Description

*policy-map-name* Name of the policy map.

## Command Default

No policy maps are defined.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

## Usage Guidelines

After entering the **policy-map** command, you enter policy-map configuration mode, and these configuration commands are available:

- **class**—Defines the classification match criteria for the specified class map.
- **description**—Describes the policy map (up to 200 characters).
- **exit**—Exits policy-map configuration mode and returns you to global configuration mode.
- **no**—Removes a previously defined policy map.
- **sequence-interval**—Enables sequence number capability.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Before configuring policies for classes whose match criteria are defined in a class map, use the **policy-map** command to specify the name of the policy map to be created, added to, or modified. Entering the **policy-map** command also enables the policy-map configuration mode in which you can configure or modify the class policies for that policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. To configure the match criteria for a class, use the **class-map** global configuration and **match** class-map configuration commands. You define packet classification on a physical-port basis.

Only one policy map per ingress port is supported. You can apply the same policy map to multiple physical ports.

You can apply a nonhierarchical policy maps to physical ports. A nonhierarchical policy map is the same as the port-based policy maps in the device.

A hierarchical policy map has two levels in the format of a parent-child policy. The parent policy cannot be modified but the child policy (port-child policy) can be modified to suit the QoS configuration.

In VLAN-based QoS, a service policy is applied to an SVI interface.



**Note** Not all MQC QoS combinations are supported for wired ports. For information about these restrictions, see chapters "Restrictions for QoS on Wired Targets" in the QoS configuration guide.

## Examples

This example shows how to create a policy map called policy1. When attached to the ingress port, it matches all the incoming traffic defined in class1, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic less than the profile is sent.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police 1000000 20000 conform-action transmit
Device(config-pmap-c)# exit
```

This example show you how to configure hierarchical polices:

```
Device# configure terminal
Device(config)# class-map c1
Device(config-cmap)# exit

Device(config)# class-map c2
Device(config-cmap)# exit

Device(config)# policy-map child
Device(config-pmap)# class c1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class c2
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit

Device(config-pmap)# class class-default
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device(config)# policy-map parent
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 1000000
Device(config-pmap-c)# service-policy child
Device(config-pmap-c)# end
```

This example shows how to delete a policy map:

```
Device(config)# no policy-map policymap2
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

# port

To configure the port number to use when configuring the custom application, use the **port** command.

**port** *port-no*

---

## Syntax Description

*port-no* Port number.

---

## Command Default

None

## Command Modes

config-custom

---

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

## Examples

The following example shows how to configure the port number to use when configuring the custom application:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ip nbar custom custom-protocol http host host-string
Device(config-custom)# http host hostname
Device(config-custom)# port port-no
```

# priority priority-value

To configure media stream priority, use the **priority** *priority-value* command.

**priority** *priority-value*

<b>Syntax Description</b>	<i>priority-value</i> Media stream priority value. Valid range is 1 to 8, with 1 being lowest priority and 8 being highest priority.				
<b>Command Default</b>	None				
<b>Command Modes</b>	config-media-stream				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.
Release	Modification				
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.				

## Examples

The following example shows how to set the media stream priority value to the highest, that is 8:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# priority 8
```

# public-ip

To configure the NAT public IP address of the controller, use the **public-ip** command.

**public-ip** { *ipv4-address* | *ipv6-address* }

## Syntax Description

*ipv4-address* Sets IPv4 address.

*ipv6-address* Sets IPv6 address.

## Command Default

None

## Command Modes

Management Interface Configuration(config-mgmt-interface)

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Usage Guidelines

### Example

The following example shows how to configure the NAT public IP address of the controller:

```
Device# configure terminal
Device(config)# wireless management interface Vlan1
Device(config-mgmt-interface)# public-ip 192.168.172.100
```

# qos video

To configure over-the-air QoS class to video only, use the **qos video** command.

## qos video

---

### Command Default

None

---

### Command Modes

config-media-stream

---

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

## Examples

The following example shows how to configure over-the-air QoS class to video only:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# qos video
```

# radius server

To configure the RADIUS server, use the **radius server** command in global configuration mode.

**radius server** *server-name*

<b>Syntax Description</b>	<i>server-name</i> RADIUS server name.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Global configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.				
<b>Usage Guidelines</b>	None				

The following example shows how to configure a radius server:

```
Device(config)# radius server ISE
```



# radius-server attribute wireless accounting call-station-id

To configure call station identifier sent in the RADIUS accounting messages, use the **radius-server attribute wireless accounting call-station-id** command. To remove the call station identifier from the radius accounting messages, use the **no** form of the command.

```
radius-server attribute wireless authentication call-station-id { ap-ethmac-only | ap-ethmac-ssid |
ap-ethmac-ssid-flexprofilename | ap-ethmac-ssid-policytagname | ap-ethmac-ssid-sitetagname |
ap-group-name | ap-label-address | ap-label-address-ssid | ap-location | ap-macaddress |
ap-macaddress-ssid | ap-macaddress-ssid-flexprofilename | ap-macaddress-ssid-policytagname |
ap-macaddress-ssid-sitetagname | ap-name | ap-name-ssid | flex-profile-name | ipaddress | macaddress
| policy-tag-name | site-tag-name | vlan-id }
```

Syntax Description		
<b>ap-ethmac-only</b>		Sets the call station identifier type to be AP's radio MAC address.
<b>ap-ethmac-ssid</b>		Sets the call station identifier type AP's radio MAC address with SSID.
<b>ap-ethmac-ssid-flexprofilename</b>		Sets the call station identifier type AP's radio MAC address with SSID and flex profile name.
<b>ap-ethmac-ssid-policytagname</b>		Sets the call station identifier type AP's radio MAC address with SSID and policy tag name.
<b>ap-ethmac-ssid-sitetagname</b>		Sets the call station identifier type AP's radio MAC address with SSID and site tag name.
<b>ap-group-name</b>		Sets the call station identifier type to use the AP group name.
<b>ap-label-address</b>		Sets the call station identifier type to the AP's radio MAC address that is printed on the AP label.
<b>ap-label-address-ssid</b>		Sets the call station identifier type to the AP's radio MAC address and SSID that is printed on the AP label.
<b>ap-location</b>		Sets the call station identifier type to the AP location.
<b>ap-macaddress</b>		Sets the call station identifier type to the AP's radio MAC address.
<b>ap-macaddress-ssid</b>		Sets the call station identifier type to the AP's radio MAC address with SSID.
<b>ap-macaddress-ssid-flexprofilename</b>		Sets the call station identifier type to the AP's radio MAC address with SSID and flex profile name.
<b>ap-macaddress-ssid-policytagname</b>		Sets the call station identifier type to the AP's radio MAC address with SSID and policy tag name.
<b>ap-macaddress-ssid-sitetagname</b>		Sets the call station identifier type to the AP's radio MAC address with SSID and site tag name.
<b>ap-name</b>		Sets the call station identifier type to the AP name.

<b>ap-name-ssid</b>	Sets the call station identifier type to the AP name with SSID.
<b>flex-profile-name</b>	Sets the call station identifier type to the flex profile name.
<b>ipaddress</b>	Sets the call station identifier type to the IP address of the system.
<b>macaddress</b>	Sets the call station identifier type to the MAC address of the system.
<b>policy-tag-name</b>	Sets the call station identifier type to the policy tag name.
<b>site-tag-name</b>	Sets the call station identifier type to the site tag name.
<b>vlan-id</b>	Sets the call station identifier type to the system's VLAN ID.

**Command Default** Call station identifier is not configured.

**Command Modes** Global Configuration(config)

#### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
Cisco IOS XE Bengaluru 17.4.1	This command was modified. The <b>policy-tag-name</b> , <b>flex-profile-name</b> , <b>ap-macaddress-ssid-flexprofile-name</b> , <b>ap-macaddress-ssid-policytagname</b> , <b>ap-macaddress-ssid-sitetagname</b> , <b>ap-ethmac-ssid-flexprofile-name</b> , <b>ap-ethmac-ssid-policytagname</b> , and <b>ap-ethmac-ssid-sitetagname</b> keywords were introduced.

#### Usage Guidelines

##### Example

The following example shows how to configure a call station identifier sent in the RADIUS accounting messages:

```
Device(config)# radius-server attribute wireless accounting call-station-id site-tag-name
```

# radius-server attribute wireless authentication call-station-id

To configure call station identifier sent in the RADIUS authentication messages, use the **radius-server attribute wireless authentication call-station-id** command. To remove the call station identifier from the radius accounting messages, use the **no** form of the command.

```
radius-server attribute wireless authentication call-station-id { ap-ethmac-only | ap-ethmac-ssid |
ap-ethmac-ssid-flexprofilename | ap-ethmac-ssid-policytagname | ap-ethmac-ssid-sitetagname |
ap-group-name | ap-label-address | ap-label-address-ssid | ap-location | ap-macaddress |
ap-macaddress-ssid | ap-macaddress-ssid-flexprofilename | ap-macaddress-ssid-policytagname |
ap-macaddress-ssid-sitetagname | ap-name | ap-name-ssid | flex-profile-name | ipaddress | macaddress
| policy-tag-name | site-tag-name | vlan-id }
```

## Syntax Description

<b>ap-ethmac-only</b>	Sets the call station identifier type to be AP's radio MAC address.
<b>ap-ethmac-ssid</b>	Sets the call station identifier type AP's radio MAC address with SSID.
<b>ap-ethmac-ssid-flexprofilename</b>	Sets the call station identifier type AP's radio MAC address with SSID and flex profile name.
<b>ap-ethmac-ssid-policytagname</b>	Sets the call station identifier type AP's radio MAC address with SSID and policy tag name.
<b>ap-ethmac-ssid-sitetagname</b>	Sets the call station identifier type AP's radio MAC address with SSID and site tag name.
<b>ap-group-name</b>	Sets the call station identifier type to use the AP group name.
<b>ap-label-address</b>	Sets the call station identifier type to the AP's radio MAC address that is printed on the AP label.
<b>ap-label-address-ssid</b>	Sets the call station identifier type to the AP's radio MAC address and SSID that is printed on the AP label.
<b>ap-location</b>	Sets the call station identifier type to the AP location.
<b>ap-macaddress</b>	Sets the call station identifier type to the AP's radio MAC address.
<b>ap-macaddress-ssid</b>	Sets the call station identifier type to the AP's radio MAC address with SSID.
<b>ap-macaddress-ssid-flexprofilename</b>	Sets the call station identifier type to the AP's radio MAC address with SSID and flex profile name.
<b>ap-macaddress-ssid-policytagname</b>	Sets the call station identifier type to the AP's radio MAC address with SSID and policy tag name.
<b>ap-macaddress-ssid-sitetagname</b>	Sets the call station identifier type to the AP's radio MAC address with SSID and site tag name.
<b>ap-name</b>	Sets the call station identifier type to the AP name.

<b>ap-name-ssid</b>	Sets the call station identifier type to the AP name with SSID.
<b>flex-profile-name</b>	Sets the call station identifier type to the flex profile name.
<b>ipaddress</b>	Sets the call station identifier type to the IP address of the system.
<b>macaddress</b>	Sets the call station identifier type to the MAC address of the system.
<b>policy-tag-name</b>	Sets the call station identifier type to the policy tag name.
<b>site-tag-name</b>	Sets the call station identifier type to the site tag name.
<b>vlan-id</b>	Sets the call station identifier type to the system's VLAN ID.

**Command Default** Call station identifier is not configured.

**Command Modes** Global Configuration(config)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
	Cisco IOS XE Bengaluru 17.4.1	This command was modified. The <b>policy-tag-name</b> , <b>flex-profile-name</b> , <b>ap-macaddress-ssid-flexprofilename</b> , <b>ap-macaddress-ssid-policytagname</b> , <b>ap-macaddress-ssid-sitetagname</b> , <b>ap-ethmac-ssid-flexprofilename</b> , <b>ap-ethmac-ssid-policytagname</b> , and <b>ap-ethmac-ssid-sitetagname</b> keywords were introduced.

### Usage Guidelines

#### Example

The following example shows how to configure a call station identifier sent in the RADIUS authentication messages:

```
Device(config)# radius-server attribute wireless authentication call-station-id site-tag-name
```

# range

To configure range from MAP to RAP bridge, use the **range** command.

**range** *range-in-feet*

<b>Syntax Description</b>	<i>range-in-feet</i> Configure the range value in terms of feet. Valid range is from 150 feet to 132000 feet.	
<b>Command Default</b>	1200	
<b>Command Modes</b>	config-wireless-mesh-profile	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to configure range from MAP to RAP bridge for a mesh AP profile:

```
Device # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# range 300
```

## record wireless avc basic

To apply the *wireless avc basic* AVC flow record to a flow monitor, use the **record wireless avc basic** command.

**record wireless avc basic**

---

### Command Default

None

---

### Command Modes

config-flow-monitor

---

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

### Usage Guidelines

This command specifies the basic wireless AVC template. When you are configuring AVC, you will need to create a flow monitor using the **record wireless avc basic** command.

### Examples

The following example shows how to apply the *wireless avc basic* AVC flow record to a flow monitor named *test-flow*:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# flow monitor test-flow
Device(config-flow-monitor)# record wireless avc basic
```

# redirect

To configure a redirect to an external portal, use the **redirect** command.

**redirect** {**for-login** | **on-failure** | **on-success**} *redirect-url-name*

## Syntax Description

<b>for-login</b>	To login, redirect to this URL.
<b>on-failure</b>	If login fails, redirect to this URL.
<b>on-success</b>	If login is successful, redirect to this URL.
<i>redirect-url-name</i>	Redirect URL name.

## Command Default

None

## Command Modes

config-params-parameter-map

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to configure an redirect to an external IPv4 URL to login:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# parameter-map type webauth parameter-name
Device(config-params-parameter-map)# redirect for-login cisco.com
```

# redirect portal

To configure external IPv4 or IPv6 portal, use the **redirect portal** command.

**redirect portal** {**ipv4** | **ipv6**} *ip-addr*

## Syntax Description

**ipv4** IPv4 portal address

**ipv6** IPv6 portal address

## Command Default

None

## Command Modes

config-params-parameter-map

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to configure an external IPv4 portal address:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# parameter-map type webauth parameter-name
Device(config-params-parameter-map)# redirect portal ipv4 192.168.1.100
```



# remote-lan

To map an RLAN policy profile to an RLAN profile, use the **remote-lan** command.

**remote-lan** *remote-lan-profile-name* **policy** *rlan-policy-profile-name* **port-id** *port-id*

<b>Syntax Description</b>	<i>remote-lan-profile-name</i>	Remote LAN profile name.
	<i>rlan-policy-profile-name</i>	Remote LAN policy profile name.
	<i>port-id</i>	Port ID.
<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration (config)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

## Example

This example shows how to map an RLAN policy profile to an RLAN profile:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless tag policy remote-lan-policy-tag
Device(config-policy-tag)# remote-lan rlan_profile_name policy rlan_policy_profile port-id
2
Device(config-policy-tag)# end
```

# request platform software trace archive

To archive all the trace logs relevant to all the processes running on a system since the last reload on the and to save this in the specified location, use the **request platform software trace archive** command in privileged EXEC or user EXEC mode.

**request platform software trace archive** [**last** *number-of-days* [**days** [**target** *location*]] | **target** *location*]

Syntax Description		
<b>last</b> <i>number-of-days</i>		Specifies the number of days for which the trace files have to be archived.
<b>target</b> <i>location</i>		Specifies the location and name of the archive file.

Command Modes	
	User EXEC (>)
	Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** This archive file can be copied from the system, using the tftp or scp commands.

**Examples** This example shows how to archive all the trace logs of the processes running on the since the last 5 days:

```
Device# request platform software trace archive last 5 days target flash:test_archive
```

# rf tag

To configure an RF tag to the AP, use the **rf tag** command.

**rf tag** *rf-tag-name*

<b>Syntax Description</b>	<i>rf-tag-name</i> RF tag name.	
<b>Command Default</b>	None	
<b>Command Modes</b>	config-ap-tag	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
<b>Usage Guidelines</b>	The AP will disconnect and rejoin after running this command.	

## Example

The following example shows how to configure an RF tag:

```
Device(config-ap-tag)# rf-tag rftag1
```

## rrc-evaluation

To configure Resource Reservation Control (RRC) reevaluation admission, use the **rrc-evaluation** command.

**rrc-evaluation** {**initial** | **periodic**}

<b>Syntax Description</b>	<b>initial</b> Configures initial admission evaluation.
	<b>periodic</b> Configures periodic admission evaluation.

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	config-media-stream
----------------------	---------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

### Examples

The following example shows how to configure the RRC reevaluation admission to initial admission evaluation.

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# rrc-evaluation initial
```

# security

To configure mesh security, use the **security** command.

```
security { eap | psk }
```

## Syntax Description

**ep** Configure mesh security EAP for Mesh AP.

**psk** Configure mesh security PSK for Mesh AP

## Command Default

EAP

## Command Modes

config-wireless-mesh-profile

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to configure mesh security with EAP protocol on an Mesh AP:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile mesh profile-name
Device(config-wireless-mesh-profile)# security eap
```

## security dot1x authentication-list

To configure security authentication list for IEEE 802.1x, use the **security dot1x authentication-list *auth-list-name*** command.

**security dot1x authentication-list *auth-list-name***

Syntax Description	Parameter	Description
	<i>auth-list-name</i>	Authentication list name.
Command Default	None	
Command Modes	config-wlan	
Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

### Examples

The following example shows how to configure security authentication list for IEEE 802.1x:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan-name
Device(config-wlan)# security dot1x authentication-list auth-list-realm
```

# security ft

To configure 802.11r fast transition parameters, use the **security ft** command. To configure fast transition **over the air**, use the **no security ft over-the-ds** command.

**security ft** [{over-the-ds | reassociation-timeout *timeout-jn-seconds*}]

**no security ft** [{over-the-ds | reassociation-timeout}]

<b>Syntax Description</b>	<b>over-the-ds</b>	(Optional) Specifies that the 802.11r fast transition occurs over a distributed system. The no form of the command with this parameter configures security ft over the air.
	<b>reassociation-timeout</b>	(Optional) Configures the reassociation timeout interval.
	<i>timeout-in-seconds</i>	(Optional) Specifies the reassociation timeout interval in seconds. The valid range is between 1 to 100. The default value is 20.
<b>Command Default</b>	The feature is disabled.	
<b>Command Modes</b>	WLAN configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
<b>Usage Guidelines</b>	None WLAN Security must be enabled.	

## Example

The following example configures security FT configuration for an open WLAN:

```
Device#wlan test
Device(config-wlan)# client vlan 0140
Device(config-wlan)# no mobility anchor sticky
Device(config-wlan)# no security wpa
Device(config-wlan)# no security wpa akm dot1x
Device(config-wlan)# no security wpa wpa2
Device(config-wlan)# no security wpa wpa2 ciphers aes
Device(config-wlan)# security ft
Device(config-wlan)# shutdown
```

The following example shows a sample security FT on a WPA-enabled WLAN:

```
Device# wlan test
Device(config-wlan)# client vlan 0140
Device(config-wlan)# no security wpa akm dot1x
Device(config-wlan)# security wpa akm ft psk
Device(config-wlan)# security wpa akm psk set-key ascii 0 test-test
```

```
Device(config-wlan)# security ft
Device(config-wlan)# no shutdown
```



## security pmf

To configure 802.11w Management Frame Protection (PMF) on a WLAN, use the **security pmf** command. To disable management frame protection, use the **no** form of the command.

```
security pmf {association-comeback association-comeback-time-seconds | mandatory | optional |
saquery-retry-time saquery-retry-time-milliseconds}
no security pmf [{association-comeback association-comeback-time-seconds | mandatory | optional |
saquery-retry-time saquery-retry-time-milliseconds}]
```

Syntax Description		
<b>association-comeback</b>		Configures the 802.11w association comeback time.
<i>association-comeback-time-seconds</i>		Association comeback interval in seconds. Time interval that an associated client must wait before the association is tried again after it is denied with a status code 30. The status code 30 message is "Association request rejected temporarily; Try again later."  The range is from 1 through 20 seconds.
<b>mandatory</b>		Specifies that clients are required to negotiate 802.1w PMF protection on the WLAN.
<b>optional</b>		Specifies that the WLAN does not mandate 802.11w support on clients. Clients with no 802.11w capability can also join.
<b>saquery-retry-time</b>		Time interval identified before which the SA query response is expected. If the device does not get a response, another SA query is tried.
<i>saquery-retry-time-milliseconds</i>		The saquery retry time in milliseconds. The range is from 100 to 500 ms. The value must be specified in multiples of 100 milliseconds.

**Command Default** PMF is disabled.

**Command Modes** WLAN configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** You must have WPA (Wi-Fi Protected Access) and AKM (Authentication Key Management) configured to use this feature. See Related Command section for more information on configuring the security parameters.

802.11w introduces an Integrity Group Temporal Key (IGTK) that is used to protect broadcast or multicast robust management frames. IGTK is a random value, assigned by the authenticator station (device) used to protect MAC management protocol data units (MMPDUs) from the source STA. The 802.11w IGTK key is

derived using the four-way handshake and is used only on WLANs that are configured with WPA2 security at Layer 2.

This example shows how to enable the association comeback value at 15 seconds.

```
Device(config-wlan)# security pmf association-comeback 15
```

This example shows how to configure mandatory 802.11w MPF protection for clients on a WLAN:

```
Device(config-wlan)# security pmf mandatory
```

This example shows how to configure optional 802.11w MPF protection for clients on a WLAN:

```
Device(config-wlan)# security pmf optional
```

This example shows how to configure the saquery parameter:

```
Device(config-wlan)# security pmf saquery-retry-time 100
```

This example shows how to disable the PMF feature:

```
Device(config-wlan)# no security pmf
```

# security static-wep-key

To configure static WEP keys on a WLAN, use the **security static-wep-key** command.

```
security static-wep-key {authentication {open | sharedkey } | encryption {104 | 40 } {ascii | hex | {0 | 8 }wep-key | wep-index }}
```

Syntax Description	open	Open system authentication.
	sharedkey	Shared key authentication.
	0	Specifies an UNENCRYPTED password is used.
	8	Specifies an AES encrypted password is used.
	wep-key	Enter the name of the WEP key.
Command Default	None	
Command Modes	config-wlan	
Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to authenticate 802.11 using shared key:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan profile-name wlan-id
Device(config-wlan)# security static-wep-key authentication sharedkey
```

## security web-auth

To change the status of web authentication used on a WLAN, use the **security web-auth** command. To disable web authentication on a WLAN, use the **no** form of the command.

```
security web-auth [{authentication-list authentication-list-name | on-macfilter-failure | parameter-map
parameter-map-name}]
no security web-auth [{authentication-list [authentication-list-name] | on-macfilter-failure |
parameter-map [parameter-name]]]
```

Syntax Description		
<b>authentication-list</b> <i>authentication-list-name</i>	Sets the authentication list for IEEE 802.1x.	
<b>on-macfilter-failure</b>	Enables web authentication on MAC failure.	
<b>parameter-map</b> <i>parameter-map-name</i>	Configures the parameter map.	

**Command Default** Web authentication is disabled.

**Command Modes** WLAN configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

### Examples

The following example shows how to configure the authentication-list web authentication on a WLAN:

```
Device(config-wlan)# security web-auth authentication-list test
```

## security wpa akm

To configure authentication key management using Cisco Centralized Key Management (CCKM), use the **security wpa akm** command. To disable the authentication key management for Cisco Centralized Key Management, use the **no** form of the command.

```
security wpa [{akm {cckm | dot1x | ft | pmf | psk} | wpa1 [ciphers {aes | tkip}]] | wpa2 [ciphers {aes | tkip}]}
```

```
no security wpa [{akm {cckm | dot1x | ft | pmf | psk} | wpa1 [ciphers {aes | tkip}]] | wpa2 [ciphers {aes | tkip}]}
```

Syntax	Description
<b>akm</b>	Configures the Authentication Key Management (AKM) parameters.
<b>aes</b>	Configures AES (Advanced Encryption Standard) encryption support.
<b>cckm</b>	Configures Cisco Centralized Key Management support.
<b>ciphers</b>	Configures WPA ciphers.
<b>dot1x</b>	Configures 802.1x support.
<b>ft</b>	Configures fast transition using 802.11r.
<b>pmf</b>	Configures 802.11w management frame protection.
<b>psk</b>	Configures 802.11r fast transition pre-shared key (PSK) support.
<b>tkip</b>	Configures Temporal Key Integrity Protocol (TKIP) encryption support.
<b>wpa2</b>	Configures Wi-Fi Protected Access 2 (WPA2) support.

**Command Default** By default Wi-Fi Protected Access2, 802.1x are enabled. WPA2, PSK, CCKM, FT dot1x, FT PSK, PMF dot1x, PMF PSK, FT Support are disabled. The FT Reassociation timeout is set to 20 seconds, PMF SA Query time is set to 200.

**Command Modes** WLAN configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Example**

The following example shows how to configure CCKM on the WLAN.

```
Device(config-wlan)#security wpa akm cckm
```

## security wpa akm owe

To enable Auth Key Management (AKM) Opportunistic Wireless Encryption (OWE), use the **security wpa akm owe** command. Use the **no** form of this command to disable the feature.

**security wpa akm owe**

**no security wpa akm owe**

Syntax Description		
<b>security</b>	Configures the security policy for a WLAN.	
<b>wpa</b>	Configures WPA/WPA2 Support for a WLAN.	
<b>akm</b>	Configures Auth Key Management.	
<b>owe</b>	Configures OWE support.	
Command Default	None	
Command Modes	WLAN configuration mode (config-wlan)	
Command History	Release	Modification
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

The following example shows how to enable Auth Key Management (AKM) Opportunistic Wireless Encryption (OWE):

```
Device# configure terminal
Device(config)# wlan wlan-test 3 ssid-test
Device(config-wlan)# security wpa akm owe
```

## security wpa akm psk

To enable Auth Key Management (AKM) pre-shared key (PSK), use the **security wpa akm psk** command. Use the **no** form of this command to disable the feature.

**security wpa akm psk**

**no security wpa akm psk**

Syntax Description	
<b>security</b>	Configures the security policy for a WLAN.
<b>wpa</b>	Configures WPA/WPA2 Support for a WLAN.
<b>akm</b>	Configures Auth Key Management.
<b>psk</b>	Configures PSK support.

**Command Default** None

**Command Modes** WLAN configuration mode (config-wlan)

Command History	Release	Modification
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

The following example shows how to enable Auth Key Management (AKM) pre-shared key (PSK):

```
Device# configure terminal
Device(config)# wlan wlan-test 3 ssid-test
Device(config-wlan)# security wpa akm psk
```



## security wpa akm sae

To enable Auth Key Management (AKM) Secure Agile Exchange (SAE), use the **security wpa akm sae** command. Use the **no** form of this command to disable the feature.

**security wpa akm sae**

**no security wpa akm sae**

Syntax Description	
<b>security</b>	Configures the security policy for a WLAN.
<b>wpa</b>	Configures WPA/WPA2 Support for a WLAN.
<b>akm</b>	Configures Auth Key Management.
<b>sae</b>	Configures SAE support.

**Command Default** None

**Command Modes** WLAN configuration mode (config-wlan)

Command History	Release	Modification
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

The following example shows how to enable Auth Key Management (AKM) Secure Agile Exchange (SAE):

```
Device# configure terminal
Device(config)# wlan wlan-test 3 ssid-test
Device(config-wlan)# security wpa akm sae
```

## sensor-name

To set the sensor name for Stealthwatch Cloud registration, use the **sensor-name** *swc-sensor-name* command. To disable the command, use the **no** form of this command.

**sensor-name** *swc-sensor-name*

**no sensor-name** *swc-sensor-name*

Syntax Description		
	<b>sensor-name</b>	Sets the sensor name for Stealthwatch Cloud registration.
	<i>swc-sensor-name</i>	Specifies the Stealthwatch service key. The device serial number is the default value.

**Command Default** None

**Command Modes** Stealthwatch Cloud monitor configuration mode

Command History	Release	Modification
	Cisco IOS XE Bengaluru 17.4.1	This command was introduced.

**Usage Guidelines** None

### Example

This example shows how to set the sensor name for Stealthwatch Cloud registration:

```
Device(config-stealthwatch-cloud-monitor)# sensor-name SwC-sensor-name
```

# service-key

To set the Stealthwatch Cloud service key, use the **service-key** *swc-service-key*. To disable the command, use the **no** form of this command.

**service-key** *swc-service-key*

**no service-key** *swc-service-key*

<b>Syntax Description</b>	<b>service-key</b>	Sets the Stealthwatch Cloud service key.  Service-key is provided by the Stealthwatch Cloud portal. The alternative to service-key is the authentication through the IP address allowed list.
	<i>swc-service-key</i>	Specifies the Stealthwatch service key.

**Command Default** None

**Command Modes** Stealthwatch Cloud monitor configuration mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
		Cisco IOS XE Bengaluru 17.4.1

**Usage Guidelines** None

## Example

This example shows how to set the Stealthwatch Cloud service key:

```
Device(config-stealthwatch-cloud-monitor)# service-key xxxxxxxxxxxxxxxxxxxxxxxx
```

## service-policy (WLAN)

To configure the WLAN quality of service (QoS) service policy, use the **service-policy** command. To disable a QoS policy on a WLAN, use the **no** form of this command.

```
service-policy [client] {input | output} policy-name
no service-policy [client] {input | output} policy-name
```

### Syntax Description

<b>client</b>	(Optional) Assigns a policy map to all clients in the WLAN.
<b>input</b>	Assigns an input policy map.
<b>output</b>	Assigns an output policy map.
<i>policy-name</i>	The policy name.

### Command Default

No policies are assigned and the state assigned to the policy is None.

### Command Modes

WLAN configuration

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

### Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

### Examples

This example shows how to configure the input QoS service policy on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# service-policy input policy-test
```

This example shows how to disable the input QoS service policy on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no service-policy input policy-test
```

This example shows how to configure the output QoS service policy on a WLAN to platinum (precious metal policy):

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# service-policy output platinum
```

## service-policy qos

To configure a QoS service policy, use the **service-policy qos** command.

**service-policy qos** {**input** | **output**}*policy-name*

<b>Syntax Description</b>	<b>input</b>	Input QoS policy.
	<b>output</b>	Output QoS policy.
	<i>policy-name</i>	Policy name.
<b>Command Default</b>	None	
<b>Command Modes</b>	config-service-template	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

### Examples

The following example shows how to configure an output QoS policy:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# service-template fabric-profile-name
Device(config-service-template)# service-policy qos output policy-name
```

# service-template

To configure service template, use the **service-template** command.

```
service-template service-template-name { access-group acl_list | vlan vlan_id | absolute-timer seconds
| service-policy qos { input | output } }
```

Syntax Description		
<i>service-template-name</i>	Name of the service template.	
<i>acl_list</i>	Access list name to be applied.	
<i>vlan_id</i>	VLAN ID. The VLAN ID value ranges from 1 to 4094.	
<i>seconds</i>	Session timeout value for service template. The session timeout value ranges from 1 to 65535 seconds.	
<b>service-policy qos</b> { <b>input</b>   <b>output</b> }	QoS policies for client.	

**Command Default** None

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** None

The following example shows how to configure service template:

```
Device#configure terminal
Device(config)#service-template cisco-phone-template
Device(config-service-template)#access-group foo-acl
Device(config-service-template)#vlan 100
Device(config-service-template)#service-policy qos input foo-qos
Device(config-service-template)#end
```

## service timestamps

To configure the system to time-stamp debugging or logging messages, use the **service timestamps** command in global configuration commands. Use the **no** form of this command to disable this service.

```
service timestamps debug log {datetime | uptime localtime msec show-timezone year}
no service timestamps debuglog
```

Syntax	Description
<b>debug</b>	Debug as the timestamp message type.
<b>log</b>	Log as the timestamp message type.
<b>datetime</b>	<b>datetime</b>
<b>uptime</b>	(Optional) Time stamp with time since the system was rebooted.
<b>localtime</b>	(Optional) Time stamp relative to the local time zone.
<b>msec</b>	(Optional) Include milliseconds in the date and time stamp.
<b>show-timezone</b>	(Optional) Include the time zone name in the time stamp.
<b>year</b>	(Optional) Include year in timestamp.

Command Default	Description
	No time-stamping.
	If <b>service timestamps</b> is specified with no arguments or keywords, default is <b>service timestamps debug uptime</b> .
	The default for <b>service timestamps debug datetime</b> is to format the time in UTC, with no milliseconds and no time zone name.
	The command <b>no service timestamps</b> by itself disables time stamps for both debug and log messages.

Command Modes	Description
	Global configuration

Command History	Release	Modification
	Cisco IOS XE Amsterdam 17.1.1s	This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.1.1s.

Usage Guidelines	Description
	Time stamps can be added to either debugging or logging messages independently. The uptime form of the command adds time stamps in the format HHHH:MM:SS, indicating the time since the system was rebooted. The datetime form of the command adds time stamps in the format MMM DD HH:MM:SS, indicating the date and time according to the system clock. If the system clock has not been set, the date and time are preceded by an asterisk (*) to indicate that the date and time are probably not correct.

### Example

The following example enables time stamps on debugging messages, showing the time since reboot:

```
Device(config)# service timestamps debug uptime
```

The following example enables time stamps on logging messages, showing the current time and date relative to the local time zone, with the time zone name included:

```
Device(config)# service timestamps log datetime localtime show-timezone
```



## session-timeout

To configure session timeout for clients associated to a WLAN, use the **session-timeout** command. To disable a session timeout for clients that are associated to a WLAN, use the **no** form of this command.

**session-timeout seconds**  
**no session-timeout**

<b>Syntax Description</b>	<i>seconds</i> Timeout or session duration in seconds. The range is from 300 to 86400.  Configuring 86400 is equivalent to max timeout. And value 0 is not recommended.				
<b>Command Default</b>	The client timeout is set to 1800 seconds for WLANs that are configured with dot1x security. The client timeout is set to 0 for open WLANs.				
<b>Command Modes</b>	WLAN configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.				

This example shows how to configure a session timeout to 300 seconds:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# session-timeout 300
```

This example shows how to disable a session timeout:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no session-timeout
```

## set

To classify IP traffic by setting a Differentiated Services Code Point (DSCP) or an IP-precedence value in the packet, use the **set** command in policy-map class configuration mode. Use the **no** form of this command to remove traffic classification.

**set**

**cos | dscp | precedence | ip | qos-group | wlan**

**set cos**

*{cos-value}* | **{cos | dscp | precedence | qos-group | wlan}** [**{table table-map-name}**]

**set dscp**

*{dscp-value}* | **{cos | dscp | precedence | qos-group | wlan}** [**{table table-map-name}**]

**set ip {dscp | precedence}**

**set precedence** *{precedence-value}* | **{cos | dscp | precedence | qos-group}** [**{table table-map-name}**]

**set qos-group**

*{qos-group-value}* | **dscp** [**{table table-map-name}**] | **precedence** [**{table table-map-name}**]

**set wlan user-priority**

*user-priority-value* | **costable** *table-map-name* | **dscptable** *table-map-name* | **qos-groupstable** *table-map-name* | **wlantable** *table-map-name*

---

**Syntax Description**    **cos**

Sets the Layer 2 class of service (CoS) value or user priority of an outgoing packet. You can specify these values:

- *cos-value*—CoS value from 0 to 7. You also can enter a mnemonic name for a commonly used value.
- Specify a packet-marking category to set the CoS value of the packet. If you also configure a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords:
  - **cos**—Sets a value from the CoS value or user priority.
  - **dscp**—Sets a value from packet differentiated services code point (DSCP).
  - **precedence**—Sets a value from packet precedence.
  - **qos-group**—Sets a value from the QoS group.
  - **wlan**—Sets the WLAN user priority values.
- (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map are used to set the CoS value. Enter the name of the table map used to specify the CoS value. The table map name can be a maximum of 64 alphanumeric characters.

If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the CoS value. For example, if you enter the **set cos precedence** command, the precedence (packet-marking category) value is copied and used as the CoS value.

---

---

**dscp**

Sets the differentiated services code point (DSCP) value to mark IP(v4) and IPv6 packets. You can specify these values:

- *cos-value*—Number that sets the DSCP value. The range is from 0 to 63. You also can enter a mnemonic name for a commonly used value.
- Specify a packet-marking category to set the DSCP value of the packet. If you also configure a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords:
  - **cos**—Sets a value from the CoS value or user priority.
  - **dscp**—Sets a value from packet differentiated services code point (DSCP).
  - **precedence**—Sets a value from packet precedence.
  - **qos-group**—Sets a value from the QoS group.
  - **wlan**—Sets a value from WLAN.
- (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the DSCP value. Enter the name of the table map used to specify the DSCP value. The table map name can be a maximum of 64 alphanumeric characters.

If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the DSCP value. For example, if you enter the **set dscp cos** command, the CoS value (packet-marking category) is copied and used as the DSCP value.

---

**ip**

Sets IP values to the classified traffic. You can specify these values:

- **dscp**—Specify an IP DSCP value from 0 to 63 or a packet marking category.
  - **precedence**—Specify a precedence-bit value in the IP header; valid values are from 0 to 7 or specify a packet marking category.
-

---

**precedence**

Sets the precedence value in the packet header. You can specify these values:

- *precedence-value*— Sets the precedence bit in the packet header; valid values are from 0 to 7. You also can enter a mnemonic name for a commonly used value.
- Specify a packet marking category to set the precedence value of the packet.
  - **cos**—Sets a value from the CoS or user priority.
  - **dscp**—Sets a value from packet differentiated services code point (DSCP).
  - **precedence**—Sets a value from packet precedence.
  - **qos-group**—Sets a value from the QoS group.
- (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the precedence value. Enter the name of the table map used to specify the precedence value. The table map name can be a maximum of 64 alphanumeric characters.

If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the precedence value. For example, if you enter the **set precedence cos** command, the CoS value (packet-marking category) is copied and used as the precedence value.

---

---

**qos-group**

Assigns a QoS group identifier that can be used later to classify packets.

- *qos-group-value*—Sets a QoS value to the classified traffic. The range is 0 to 31. You also can enter a mnemonic name for a commonly used value.
- **dscp**—Sets the original DSCP field value of the packet as the QoS group value.
- **precedence**—Sets the original precedence field value of the packet as the QoS group value.
- (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the DSCP or precedence value. Enter the name of the table map used to specify the value. The table map name can be a maximum of 64 alphanumeric characters.

If you specify a packet-marking category (**dscp** or **precedence**) but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the QoS group value. For example, if you enter the **set qos-group precedence** command, the precedence value (packet-marking category) is copied and used as the QoS group value.

---

**wlan user-priority** *wlan-user-priority*

Assigns a WLAN user-priority to the classified traffic. You can specify these values:

- *wlan-user-priority*—Sets a WLAN user priority to the classified traffic. The range is 0 to 7.
- **cos**—Sets the Layer 2 CoS field value as the WLAN user priority.
- **dscp**—Sets the DSCP field value as the WLAN user priority.
- **precedence**—Sets the precedence field value as the WLAN user priority.
- **wlan**—Sets the WLAN user priority field value as the WLAN user priority.
- (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the WLAN user priority value. Enter the name of the table map used to specify the value. The table map name can be a maximum of 64 alphanumeric characters.

If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the WLAN user priority. For example, if you enter the **set wlan user-priority cos** command, the cos value (packet-marking category) is copied and used as the WLAN user priority.

**Command Default**

No traffic classification is defined.

**Command Modes**

Policy-map class configuration

**Command History**

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines**

For the **set dscp** *dscp-value* command, the **set cos** *cos-value* command, and the **set ip precedence** *precedence-value* command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **set dscp af11** command, which is the same as entering the **set dscp 10** command. You can enter the **set ip precedence critical** command, which is the same as entering the **set ip precedence 5** command. For a list of supported mnemonics, enter the **set dscp ?** or the **set ip precedence ?** command to see the command-line help strings.

When you configure the **set dscp cos** command, note the following: The CoS value is a 3-bit field, and the DSCP value is a 6-bit field. Only the three bits of the CoS field are used.

When you configure the **set dscp qos-group** command, note the following:

- The valid range for the DSCP value is a number from 0 to 63. The valid value range for the QoS group is a number from 0 to 99.
- If a QoS group value falls within both value ranges (for example, 44), the packet-marking value is copied and the packets is marked.
- If QoS group value exceeds the DSCP range (for example, 77), the packet-marking value is not be copied and the packet is not marked. No action is taken.

The **set qos-group** command cannot be applied until you create a service policy in policy-map configuration mode and then attach the service policy to an interface or ATM virtual circuit (VC).

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

## Examples

This example shows how to assign DSCP 10 to all FTP traffic without any policers:

```
Device(config)# policy-map policy_ftp
Device(config-pmap)# class-map ftp_class
Device(config-cmap)# exit
Device(config)# policy policy_ftp
Device(config-pmap)# class ftp_class
Device(config-pmap-c)# set dscp 10
Device(config-pmap)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.



## sftp-image-path (image-download-mode sftp)

To configure the image path of the SFTP server for image download, use the **sftp-image-path** command. Use the **no** form of the command to negate the command or to set the command to its default.

```
sftp-image-path sftp-image-path
```

```
no sftp-image-path sftp-image-path
```

<b>Syntax Description</b>	<i>sftp-image-path</i> Specifies the image path of the SFTP server.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Wireless image download profile SFTP configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.2s</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.				

### Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode sftp
Device(config-wireless-image-download-profile-sftp)# sftp-image-path
/download/object/stream/images/ap-images
```

## sftp-image-server (image-download-mode sftp)

To configure the SFTP server address for image download, use the **sftp-image-server** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
sftp-image-server {A.B.C.D | X:X:X:X::X}
```

```
no sftp-image-server {A.B.C.D | X:X:X:X::X}
```

<b>Syntax Description</b>	<i>A.B.C.D</i>	Specifies the SFTP IPv4 server address.
	<i>X:X:X:X::X</i>	Specifies the SFTP IPv6 server address.
<b>Command Default</b>	None	
<b>Command Modes</b>	Wireless image download profile SFTP configuration mode.	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

### Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode sftp
Device(config-wireless-image-download-profile-sftp)# sftp-image-server 10.1.1.1
```

## sftp-password (image-download-mode sftp)

To configure the SFTP server password for image download, use the **sftp-password** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
sftp-password {0| 8}<Enter password> <Re-enter password>
```

```
no sftp-password {0 | 8}<Enter password> <Re-enter password>
```

<b>Syntax Description</b>	<b>0</b>	Specifies that an unencrypted password will follow.
	<b>8</b>	Specifies that an AES encrypted password will follow.
	<i>password</i>	Specifies the SFTP server password.
	<i>re-enter password</i>	Indicates that the user must re-enter the SFTP server password.
<b>Command Default</b>	None	
<b>Command Modes</b>	Wireless image download profile SFTP configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

### Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode sftp
Device(config-wireless-image-download-profile-sftp)# sftp-password 0 xxxxxxxx
```

## sftp-password (trace-export)

To configure the SFTP server password for trace export, use the **sftp-password** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
sftp-password<Enter password> <Re-enter password>
```

```
no sftp-password<Enter password> <Re-enter password>
```

<b>Syntax Description</b>	<i>password</i>	Specifies the SFTP server password.
	<i>re-enter password</i>	Indicates that the user must re-enter the SFTP server password.
<b>Command Default</b>	None	
<b>Command Modes</b>	Wireless trace export profile SFTP configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

### Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode sftp
Device(config-wireless-trace-export-profile-sftp)# sftp-password xxxxxxxx xxxxxxxx
```

## sftp-path

To configure the path at the SFTP server for trace log export, use the **sftp-path** command. Use the **no** form of the command to negate the command or to set the command to its default.

```
sftp-path sftp-path
```

```
no sftp-path sftp-path
```

<b>Syntax Description</b>	<i>sftp-path</i> Specifies the path at the SFTP server.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Wireless trace export profile SFTP configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.2s</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.				

### Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode sftp
Device(config-wireless-trace-export-profile-sftp)# sftp-path
/download/object/stream/images/ap-images
```

## sftp-server

To configure the SFTP server address for trace export, use the **sftp-server** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
sftp-server {A.B.C.D | X:X:X:X::X}
```

```
no sftp-server {A.B.C.D | X:X:X:X::X}
```

Syntax Description	
<i>A.B.C.D</i>	Specifies the SFTP IPv4 server address.
<i>X:X:X:X::X</i>	Specifies the SFTP IPv6 server address.

Command Default	None
-----------------	------

Command Modes	Wireless trace export profile SFTP configuration
---------------	--------------------------------------------------

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

### Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode sftp
Device(config-wireless-trace-export-profile-sftp)# sftp-server 10.1.1.1
```

## sftp-username (image-download-mode sftp)

To configure the SFTP server username for image download, use the **sftp-username** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
sftp-username Username
```

```
no sftp-username Username
```

<b>Syntax Description</b>	<i>username</i> Specifies the SFTP server username.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Wireless image download profile SFTP configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.2s</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.				

### Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode sftp
Device(config-wireless-image-download-profile-sftp)# sftp-username sftp-server-username
```

## sftp-username (trace-export)

To configure the SFTP server username for trace export, use the **sftp-username** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
sftp-username Username
```

```
no sftp-username Username
```

<b>Syntax Description</b>	<i>username</i> Specifies the SFTP server username.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Wireless trace export profile SFTP configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.2s</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.				

### Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode sftp
Device(config-wireless-trace-export-profile-sftp)# sftp-username sftp-server-username
```



# software auto-upgrade enable

To enable Auto-Upgrade feature, use the **software auto-upgrade enable** command.



**Note** If you disable this feature using the **no** form of the command, you need to manually auto-upgrade using the **install autoupgrade** command in privileged EXEC mode.

---

## software auto-upgrade enable

---

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Global Configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

---

## Usage Guidelines

This example shows how to enable Auto-Upgrade feature:

```
Device# configure terminal
Device(config)# software auto-upgrade enable
Device(config)# end
```

## statistics ap-system-monitoring alarm-enable

To enable alarms for AP real-time statistics (CPU and Memory), use the **statistics ap-system-monitoring alarm-enable** command. Use the **no** form of this command to disable the feature.

**[no] statistics ap-system-monitoring alarm-enable**

<b>Syntax Description</b>	<b>statistics</b>	Configures the AP statistics.
	<b>ap-system-monitoring alarm-enable</b>	Enables alarms for AP real-time statistics (CPU and Memory).
<b>Command Default</b>	None	
<b>Command Modes</b>	AP Profile Configuration (config-ap-profile)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

### Example

The following example shows how to enable alarms for AP real-time statistics (CPU and Memory):

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring alarm-enable
```

## statistics ap-system-monitoring alarm-hold-time

To define the hold time interval before triggering the alarm, use the **statistics ap-system-monitoring alarm-hold-time** command.

```
statistics ap-system-monitoring alarm-hold-time 0-3600
```

<b>Syntax Description</b>	<b>statistics</b>	Configures the AP statistics.
	<b>ap-system-monitoring alarm-hold-time</b>	Enables alarms for AP real-time statistics (CPU and Memory).
	<i>0-3600</i>	Specifies the alarm hold time interval in seconds.
<b>Command Default</b>	None	
<b>Command Modes</b>	AP Profile Configuration (config-ap-profile)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

### Example

The following example shows how to define the hold time interval before triggering the alarm:

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring alarm-hold-time 60
```

## statistics ap-system-monitoring alarm-retransmit-time

To define the interval between retransmissions of the trap alarm, use the **statistics ap-system-monitoring alarm-retransmit-time**

**statistics ap-system-monitoring alarm-retransmit-time** *0-65535*

<b>Syntax Description</b>	<b>statistics</b>	Configures the AP statistics.
	<b>ap-system-monitoring alarm-retransmit-time</b>	Define the interval between retransmissions of the trap alarm.
	<i>0-65535</i>	Specifies the interval between retransmissions of the trap alarm, in seconds.
<b>Command Default</b>	None	
<b>Command Modes</b>	AP Profile Configuration (config-ap-profile)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

### Example

The following example shows how to define the interval between retransmissions of the trap alarm:

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring alarm-retransmit-time 60
```

## statistics ap-system-monitoring cpu-threshold

To define the threshold percentage for CPU usage on the AP to trigger alarms, use the **statistics ap-system-monitoring cpu-threshold** command.

**statistics ap-system-monitoring cpu-threshold** *0-100*

<b>Syntax Description</b>	<b>statistics</b>	Configures the AP statistics.
	<b>ap-system-monitoring cpu-threshold</b>	Defines the threshold for CPU usage on AP to trigger alarms.
	<i>0-100</i>	Specifies the percentage of threshold for CPU usage on AP to trigger alarms.
<b>Command Default</b>	None	
<b>Command Modes</b>	AP Profile Configuration (config-ap-profile)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

### Example

The following example shows how to define the threshold percentage for CPU usage on the AP to trigger alarms:

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring cpu-threshold 70
```

## statistics ap-system-monitoring enable

To enable monitoring of AP real-time statistics (CPU and Memory), use the **statistics ap-system-monitoring enable** command. Use the **no** form of this command to disable the feature.

**[no] statistics ap-system-monitoring enable**

<b>Syntax Description</b>	<b>statistics</b>	Configures the AP statistics.
	<b>ap-system-monitoring enable</b>	Enables monitoring of AP real-time statistics (CPU and Memory).
<b>Command Default</b>	None	
<b>Command Modes</b>	AP Profile Configuration (config-ap-profile)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

### Example

The following example shows how to enable monitoring of AP real-time statistics (CPU and Memory):

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring enable
```

## statistics ap-system-monitoring mem-threshold

To define the threshold percentage for memory usage on the AP, to trigger alarms.

**statistics ap-system-monitoring mem-threshold** *0-100*

<b>Syntax Description</b>	<b>statistics</b>	Configures the AP statistics.
	<b>ap-system-monitoring mem-threshold</b>	Defines the threshold for memory usage on AP to trigger alarms.
	<i>0-100</i>	Specifies the percentage of threshold for memory usage on AP to trigger alarms.
<b>Command Default</b>	None	
<b>Command Modes</b>	AP Profile Configuration (config-ap-profile)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

### Example

The following example shows how to define the threshold percentage for memory usage on the AP to trigger alarms:

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring mem-threshold 60
```

## statistics ap-system-monitoring sampling-interval

To define the sampling interval, use the **statistics ap-system-monitoring sampling-interval**

**statistics ap-system-monitoring sampling-interval** 2-900

<b>Syntax Description</b>	<b>statistics</b>	Configures the AP statistics.
	<b>ap-system-monitoring sampling-interval</b>	Defines the sampling interval.
	2-900	Specifies the sampling interval, in seconds.
<b>Command Default</b>	None	
<b>Command Modes</b>	AP Profile Configuration (config-ap-profile)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

### Example

The following example shows how to define the sampling interval:

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring sampling-interval 100
```



## statistics ap-system-monitoring stats-interval

To define the statistics interval, which gives more weight in the calculations to the statistics received in the last statistic interval seconds, use the **statistics ap-system-monitoring stats-interval**

**statistics ap-system-monitoring stats-interval** *120-900*

<b>Syntax Description</b>	<b>statistics</b>	Configures the AP statistics.
	<b>ap-system-monitoring stats-interval</b>	Defines the statistics interval, which gives more weight in the calculations to the statistics received in the last statistic interval seconds.
	<i>120-900</i>	Specifies the statistics interval, in seconds.
<b>Command Default</b>	None	
<b>Command Modes</b>	AP Profile Configuration (config-ap-profile)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

### Example

The following example shows how to define the statistics interval:

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring stats-interval 120
```

# stealthwatch-cloud-monitor

To configure Stealthwatch Cloud monitor and enter the Stealthwatch Cloud Monitor configuration mode, use the **stealthwatch-cloud-monitor** command. To disable the command, use the **no** form of this command.

**stealthwatch-cloud-monitor**

**no stealthwatch-cloud-monitor**

---

## Command Default

None

---

## Command Modes

Global Configuration

---

## Syntax Description

**stealthwatch-cloud-monitor** Configures Stealthwatch Cloud monitor.

---



---

## Command History

Release	Modification
Cisco IOS XE Bengaluru 17.4.1	This command was introduced.

---



---

## Usage Guidelines

None

## Example

This example shows how to configure Stealthwatch Cloud monitor:

```
Device(config)# stealthwatch-cloud-monitor
```

# tag rf

To configure a policy tag for an AP filter, use the **tag rf** command.

```
tag rf rf-tag
```

<b>Syntax Description</b>	<i>rf-tag</i> RF tag name.				
<b>Command Default</b>	None				
<b>Command Modes</b>	config-ap-filter				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.
Release	Modification				
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.				

## Examples

The following example shows how to configure a policy tag for an AP filter:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap filter name ap-filter-name
Device(config-ap-filter)# rf tag rf-tag-name
```

## tag site

To configure a site tag for an AP filter, use the **tag site** *site-tag* command.

**tag site** *site-tag*

<b>Syntax Description</b>	<i>site-tag</i>	Name of the site tag.
<b>Command Default</b>	None	
<b>Command Modes</b>	config-ap-filter	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

### Examples

The following example shows how to configure a site tag for an AP filter:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap filter name ap-filter-name
Device(config-ap-filter)# site tag site-tag-name
```

## tftp-image-path (image-download-mode tftp)

To configure the image path at the TFTP server for image download, use the **tftp-image-path** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
tftp-image-path tftp-image-path
```

```
no tftp-image-path tftp-image-path
```

<b>Syntax Description</b>	<i>tftp-image-path</i> Specifies the image path of the TFTP server.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Wireless image download profile TFTP configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.2s</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.				

### Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode tftp
Device(config-wireless-image-download-profile-tftp)# tftp-image-path
/download/object/stream/images/ap-images
```

## tftp-image-server (image-download-mode tftp)

To configure the TFTP server address for image download, use the **tftp-image-server** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
image-download-mode tftp
```

```
tftp-image-server {A.B.C.D | X:X:X:X::X}
```

```
no tftp-image-server {A.B.C.D | X:X:X:X::X}
```

Syntax Description	
	<i>A.B.C.D</i> Specifies the TFTP IPv4 server address.
	<i>X:X:X:X::X</i> Specifies the TFTP IPv6 server address.

Command Default	
	None

Command Modes	
	Wireless image download profile TFTP configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

### Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode tftp
Device(config-wireless-image-download-profile-tftp)# tftp-image-server 10.1.1.1
```

## tftp-path

To configure the path at the TFTP server for trace log export, use the **tftp-path** command. Use the **no** form of the command to negate the command or to set the command to its default.

```
tftp-path tftp-path
```

```
no tftp-path tftp-path
```

<b>Syntax Description</b>	<i>tftp-path</i> Specifies the path at the TFTP server.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Wireless trace export profile TFTP configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.2s</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.				

### Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode tftp
Device(config-wireless-trace-export-profile-tftp)# tftp-path
/download/object/stream/images/ap-images
```

## tftp-server

To configure the TFTP server address for trace export, use the **tftp-server** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
tftp-server {A.B.C.D | X:X:X:X::X}
```

```
no tftp-server {A.B.C.D | X:X:X:X::X}
```

Syntax Description	
<i>A.B.C.D</i>	Specifies the TFTP IPv4 server address.
<i>X:X:X:X::X</i>	Specifies the TFTP IPv6 server address.

Command Default	None
-----------------	------

Command Modes	Wireless trace export profile TFTP configuration
---------------	--------------------------------------------------

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

### Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode tftp
Device(config-wireless-trace-export-profile-tftp)# tftp-server 10.1.1.1
```



## trapflags ap ap-stats

To enable or disable the transmission of AP related traps, which are to be sent when the statistics are past the threshold, use the **trapflags ap ap-stats**. Use the **no** form of this command to disable the feature.

**[no] trapflags ap ap-stats**

Syntax Description	
<b>trapflags</b>	Enables or disables the transmission of AP related trapflags.
<b>ap ap-stats</b>	Specifies the traps to be sent when the stats are past the threshold.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

### Example

The following example shows how to enable or disable the transmission of AP related traps:

```
Device# configure terminal
Device(config)# trapflags ap ap-stats
```

# udp-timeout

To configure timeout value for UDP sessions, use the **udp-timeout** command.

**udp-timeout** *timeout\_value*

---

## Syntax Description

*timeout\_value* Is the timeout value for UDP sessions.

The range is from 1 to 30 seconds.

**Note** The *public-key* and *resolver* parameter-map options are automatically populated with the default values. So, you need not change them.

---

## Command Default

None

## Command Modes

Profile configuration

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

---

## Example

This example shows how to configure timeout value for UDP sessions:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# parameter-map type umbrella global
Device(config-profile)# token 57CC80106C087FB1B2A7BAB4F2F4373C00247166
Device(config-profile)# local-domain dns_w1
Device(config-profile)# udp-timeout 2
Device(config-profile)# end
```

# umbrella-param-map

To configure the Umbrella OpenDNS feature for WLAN, use the **umbrella-param-map** command.

**umbrella-param-map** *umbrella-name*

<b>Syntax Description</b>	<i>umbrella-name</i>				
<b>Command Default</b>	None				
<b>Command Modes</b>	config-wireless-policy				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.				

## Example

This example shows how to configure the Umbrella OpenDNS feature for WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# umbrella-param-map global
Device(config-wireless-policy)# end
```

# update-timer

To configure the mDNS update timers for flex profile, use the **update-timer** command. To disable the command, use the **no** form of this command.

```
update-timer { service-cache <1-100> | statistics <1-100> }
```

```
update-timer { service-cache <1-100> | statistics <1-100> }
```

Syntax Description	update-timer	Configures the mDNS update timers for flex profile.
	<b>service-cache</b> <1-100>	Specifies the mDNS update service-cache timer for flex profile. The default value is one minute,
	<b>statistics</b> <1-100>	Specifies the mDNS update statistics timer for flex profile. The default value is one minute,

**Command Default** None

**Command Modes** mDNS flex profile configuration

Command History	Release	Modification
	Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

**Usage Guidelines** None

## Example

The following example shows how to configure the mDNS update timers for flex profile:

```
Device(config-mdns-flex-prof)# update-timer service-cache 20
```

# url

To configure the Stealthwatch Cloud server URL, use the **url** *swc-server-url* command. To disable the command, use the **no** form of this command.

**url** *swc-server-url*

**no url** *swc-server-url*

<b>Syntax Description</b>	<b>url</b>	Sets the Stealthwatch Cloud server URL.
	<i>swc-server-url</i>	Stealthwatch Cloud URL.

**Command Default** None

**Command Modes** Stealthwatch Cloud Monitor Configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.4.1	This command was introduced.

**Usage Guidelines** None

## Example

This example shows how to configure the Stealthwatch Cloud server URL:

```
Device(config-stealthwatch-cloud-monitor)# url https://sensors.eu-2.obsrvbl.com
```

## urlfilter list

To configure Flex URL filtering commands for ACL binding, use the **urlfilter list** c in the wireless flex profile ACL mode. To disable the feature, use the **no** form of the command.

**urlfilter list** *urlfilter-list-name*

**[no] urlfilter list** *urlfilter-list-name*

<b>Syntax Description</b>	<b>urlfilter list</b>	Configures the Flex URL filtering commands for ACL binding.
	<i>urlfilter-list-name</i>	Specifies the URL filter list name.
<b>Command Default</b>	None	
<b>Command Modes</b>	Wireless Flex Profile ACL configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.1.1	This command was introduced.

### Example

This example shows how the Flex URL filtering commands for ACL binding, is configured:

```
Device(config-wireless-flex-profile-acl)# urlfilter list urlfilter-list-name
```

# usb-enable

To enable USB for Cisco access points (APs), use the **usb-enable** command. To disable the command, use the **no** form of this command.

**usb-enable**

**no usb-enable**

<b>Syntax Description</b>	<b>usb-enable</b> Enables USB for Cisco APs.				
<b>Command Default</b>	None				
<b>Command Modes</b>	AP profile configuration mode				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Bengaluru 17.4.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Bengaluru 17.4.1	This command was introduced.
Release	Modification				
Cisco IOS XE Bengaluru 17.4.1	This command was introduced.				
<b>Usage Guidelines</b>	None				

## Example

This example shows how to enable USB for Cisco APs:

```
Device(config-ap-profile)# usb-enable
```

# username

To add a user who can access the Cisco ISE-3315 using SSH, use the **username** command in configuration mode. If the user already exists, the password, the privilege level, or both change with this command. To delete the user from the system, use the **no** form of this command.

**[no] username** *username* **password** {**hash** | **plain**} *password* **role** {**admin** | **user**} [**disabled** [**email** *email-address*]] [**email** *email-address*]

For an existing user, use the following command option:

**username** *username* **password** **role** {**admin** | **user**} *password*

## Syntax Description

<i>username</i>	You should enter only one word which can include hyphen (-), underscore (_) and period (.). <b>Note</b> Only alphanumeric characters are allowed at an initial setup.
<b>password</b>	The command to use specify password and user role.
<i>password</i>	Password character length up to 40 alphanumeric characters. You must specify the password for all new users.
<b>hash</b>   <b>plain</b>	Type of password. Up to 34 alphanumeric characters.
<b>role</b> <b>admin</b>   <b>user</b>	Sets the privilege level for the user.
<b>disabled</b>	Disables the user according to the user's email address.
<b>email</b> <i>email-address</i>	The user's email address. For example, user1@example.com.
<b>wlan-profile-name</b>	Displays details of the WLAN profile.

## Command Default

The initial user during setup.

## Command Modes

Configuration

## Usage Guidelines

The **username** command requires that the username and password keywords precede the hash / plain and the admin / user options.

### Example 1

```
ncs/admin(config)# username admin password hash ##### role admin
ncs/admin(config)#
```

### Example 2

```
ncs/admin(config)# username admin password plain Secr3tp@swd role admin
ncs/admin(config)#
```



### Example 3

```
ncs/admin(config)# username admin password plain Secr3tp@swd role admin email  
admin123@example.com  
ncs/admin(config)#
```

# violation

To configure stream violation policy on periodic reevaluation, use the **violation** command.

**violation** {**drop** | **fallback**}

Syntax Description	Parameter	Description
	<b>drop</b>	Stream will be dropped on periodic reevaluation.
	<b>fallback</b>	Stream will be demoted to BestEffort class on periodic reevaluation.
Command Default	None	
Command Modes	config-media-stream	
Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to configure stream violation policy on periodic reevaluation:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# violation drop
```

# wgb broadcast-tagging

To configure WGB broadcast tagging for a wireless policy profile, use the **wgb broadcast-tagging** command.

**wgb broadcast-tagging**

---

## Command Default

None

---

## Command Modes

config-wireless-policy

---

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

## Examples

The following example shows how to enable WGB broadcast tagging for a wireless policy profile:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy profile-policy-name
Device(config-wireless-policy)# wgb broadcast-tagging
```

# wgb vlan

To configure WGB VLAN client support for a WLAN policy profile, use the **wgb vlan** command.

## wgb vlan

### Command Default

None

### Command Modes

config-wireless-policy

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to enable WGB VLAN client support for the WLAN policy profile named *wlan1-policy-profile*:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy wlan1-policy-profile
Device(config-wireless-policy)# wgb vlan
```

# whitelist acl

To configure the whitelist ACL, use the **whitelist acl** command.

**whitelist acl** { *standard\_acl\_value* | *extended\_acl\_value* | *acl\_name* }

<b>Syntax Description</b>	<i>standard_acl_value</i>	Specifies the standard access list. Range is from 1 to 199.
	<i>extended_acl_value</i>	Specifies the extended access list. Range is from 1300 to 2699.
	<i>acl_name</i>	Specifies the named access list.
<b>Command Default</b>	None	
<b>Command Modes</b>	ET-Analytics configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to enable in-active timer in the ET-Analytics configuration mode:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# et-analytics
Device(config-et-analytics)# whitelist acl
eta-whitelist
Device((config-et-analytics)# ip access-list
extended eta-whitelist
Device(config-ext-nacl)# permit udp any any eq tftp
Device(config-ext-nacl)# end
```

# wired-vlan-range

To configure wired VLANs on which mDNS service discovery should take place, use the **wired-vlan-range** command. To disable the command, use the **no** form of this command.

**wired-vlan-range** *wired-vlan-range-value*

Syntax Description	Command	Description
	<b>wired-vlan-range</b>	Configures wired VLANs on which mDNS service discovery should take place.
	<i>wired-vlan-range-value</i>	Specifies the wired VLAN range value.

**Command Default** None

**Command Modes** mDNS flex profile configuration

Command History	Release	Modification
	Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

**Usage Guidelines** None

## Example

The following example shows how to configure wired VLANs on which mDNS service discovery should take place:

```
Device(config-mdns-flex-prof)# wired-vlan-range range-value
```

## config wlan assisted-roaming

To configure assisted roaming on a WLAN, use the **config wlan assisted-roaming** command.

```
config wlan assisted-roaming { neighbor-list | dual-list | prediction } { enable | disable } wlan_id
```

### Syntax Description

<b>neighbor-list</b>	Configures an 802.11k neighbor list for a WLAN.
<b>dual-list</b>	Configures a dual band 802.11k neighbor list for a WLAN. The default is the band that the client is currently associated with.
<b>prediction</b>	Configures an assisted roaming optimization prediction for a WLAN.
<b>enable</b>	Enables the configuration on the WLAN.
<b>disable</b>	Disables the configuration on the WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512 (inclusive).

### Command Default

The 802.11k neighbor list is enabled for all WLANs.

By default, dual band list is enabled if the neighbor list feature is enabled for the WLAN.

### Command History

Release	Modification
8.3	This command was introduced.

### Usage Guidelines

When you enable the assisted roaming prediction list, a warning appears and load balancing is disabled for the WLAN, if load balancing is already enabled on the WLAN.

The following example shows how to enable an 802.11k neighbor list for a WLAN:

```
(Cisco Controller) >config wlan assisted-roaming neighbor-list enable 1
```

# wireless aaa policy

To configure a wireless AAA policy, use the **wireless aaa policy** command.

```
wireless aaa policy aaa-policy
```

<b>Syntax Description</b>	<i>aaa-policy</i> Name of the wireless AAA policy.
---------------------------	----------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Global configuration (config)
----------------------	-------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to configure a wireless AAA policy named *aaa-policy-test*

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless aaa policy aaa-policy-test
```



# wireless aaa policy

To configure a new AAA policy, use the **wireless aaa policy** command.

**wireless aaa policy** *aaa-policy-name*

---

## Syntax Description

*aaa-policy-name* AAA policy name.

---



---

## Command Default

None

---

## Command Modes

Global configuration (config)

---

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

## Examples

The following example shows how to configure a AAA policy name:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless aaa policy my-aaa-policy
```

## wireless autoqos policy-profile

To enable the **autoqos** wireless policy with an executable command, use the **autoqos** command. Use the **disable** command to disable wireless AutoQoS.

```
wireless autoqos policy-profile policy-profile-name default_policy_profile mode { clear |
enterprise-avc | fastlane | guest | voice }
```

### wireless autoqos disable

Syntax Description	Command	Description
	<b>autoqos</b>	Configures wireless Auto QoS.
	<b>mode</b>	Specifies the wireless AutoQoS mode.
	<b>enterprise-avc</b>	Enables AutoQos wireless enterprise AVC policy.
	<b>clear</b>	Clears the configured wireless policy.
	<b>fastlane</b>	Enables the AutoQos fastlane policy. This will disable and enable the 2.4GHz or 5GHz 802.11 network.
	<b>guest</b>	Enables AutoQos wireless guest policy.
	<b>voice</b>	Enables AutoQos wireless voice policy. This will disable and enable the 2.4GHz or 5GHz 802.11 network.

**Command Default** None

**Command Modes** Privilege EXEC mode

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

### Example

This example shows how to enable AutoQoS wireless enterprise policy:

```
Device# wireless autoqos policy-profile default-policy-profile mode enterprise-avc
```

## wireless broadcast vlan

To enable broadcast support on a VLAN, use the **wireless broadcast vlan** command in global configuration mode. To disable Ethernet broadcast support, use the **no** form of the command.

**wireless broadcast vlan** [*vlan-id*]  
**no wireless broadcast vlan** [*vlan-id*]

<b>Syntax Description</b>	<i>vlan-id</i> (Optional) Specifies the VLAN ID to enable broadcast support to that VLAN. The value ranges from 1 to 4095.
---------------------------	----------------------------------------------------------------------------------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Global configuration mode
----------------------	---------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

<b>Usage Guidelines</b>	Use this command in the global configuration mode only.
-------------------------	---------------------------------------------------------

This example shows how to enable broadcasting on VLAN 20:

```
Device(config)# wireless broadcast vlan 20
```

## wireless client

To configure client parameters, use the **wireless client** command in global configuration mode.

```
wireless client {association limit assoc-number interval interval | band-select {client-rssi rssi |
cycle-count count | cycle-threshold threshold | expire dual-band timeout | expire suppression timeout}
| max-user-login max-user-login | timers auth-timeout seconds | user-timeout user-timeout}
```

### Syntax Description

<b>association limit</b> <i>assoc-number</i> <b>interval</b> <i>interval</i>	Enables association request limit per access point slot at a given interval and configures the association request limit interval.  You can configure number of association request per access point slot at a given interval from one through 100.  You can configure client association request limit interval from 100 through 10000 milliseconds.
<b>band-select</b>	Configures the band select options for the client.
<b>client-rssi</b> <i>rssi</i>	Sets the client received signal strength indicator (RSSI) threshold for band select.  The minimum dBm of a client RSSI to respond to probe is between -90 and -20.
<b>cycle-count</b> <i>count</i>	Sets the band select probe cycle count.  You can configure the cycle count from 1 to 10.
<b>cycle-threshold</b> <i>threshold</i>	Sets the time threshold for a new scanning cycle.  You can configure the cycle threshold from 1 to 1000 milliseconds.
<b>expire dual-band</b> <i>timeout</i>	Sets the timeout before stopping to try to push a given client to the 5-GHz band.  You can configure the timeout from 10 to 300 seconds, and the default value is 60 seconds.
<b>expire suppression</b> <i>timeout</i>	Sets the expiration time for pruning previously known dual-band clients.  You can configure the suppression from 10 to 200 seconds, and the default timeout value is 20 seconds.
<b>max-user-login</b> <i>max-user-login</i>	Configures the maximum number of login sessions for a user.
<b>timers auth-timeout</b> <i>seconds</i>	Configures the client timers.
<b>user-timeout</b> <i>user-timeout</i>	Configures the idle client timeout.

**Command Default** No default behavior or values.

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to set the probe cycle count for band select to 8:

```
Device# configure terminal
Device(config)# wireless client band-select cycle-count 8
Device(config)# end
```

This example shows how to set the time threshold for a new scanning cycle with threshold value of 700 milliseconds:

```
Device# configure terminal
Device(config)# wireless client band-select cycle-threshold 700
Device(config)# end
```

This example shows how to suppress dual-band clients from the dual-band database after 70 seconds:

```
Device# configure terminal
Device(config)# wireless client band-select expire suppression 70
Device(config)# end
```

## wireless client mac-address

To configure the wireless client settings, use the **wireless client mac-address** command in global configuration mode.

```
wireless client mac-address mac-addr ccx {clear-reports | clear-results | default-gw-ping | dhcp-test
| dns-ping | dns-resolve hostname host-name | get-client-capability | get-manufacturer-info |
get-operating-parameters | get-profiles | log-request {roam | rsna | syslog} | send-message message-id
| stats-request measurement-duration {dot11 | security} | test-abort | test-association ssid bssid dot11
channel | test-dot1x [profile-id] bssid dot11 channel | test-profile {anyprofile-id}
```

### Syntax Description

<i>mac-addr</i>	MAC address of the client.
<b>ccx</b>	Cisco client extension (CCX).
<b>clear-reports</b>	Clears the client reporting information.
<b>clear-results</b>	Clears the test results on the controller.
<b>default-gw-ping</b>	Sends a request to the client to perform the default gateway ping test.
<b>dhcp-test</b>	Sends a request to the client to perform the DHCP test.
<b>dns-ping</b>	Sends a request to the client to perform the Domain Name System (DNS) server IP address ping test.
<b>dns-resolve hostname</b> <i>host-name</i>	Sends a request to the client to perform the Domain Name System (DNS) resolution test to the specified hostname.
<b>get-client-capability</b>	Sends a request to the client to send its capability information.
<b>get-manufacturer-info</b>	Sends a request to the client to send the manufacturer's information.
<b>get-operating-parameters</b>	Sends a request to the client to send its current operating parameters.
<b>get-profiles</b>	Sends a request to the client to send its profiles.
<b>log-request</b>	Configures a CCX log request for a specified client device.
<b>roam</b>	(Optional) Specifies the request to specify the client CCX roaming log
<b>rsna</b>	(Optional) Specifies the request to specify the client CCX RSNA log.
<b>syslog</b>	(Optional) Specifies the request to specify the client CCX system log.

---

**send-message** *message-id*

---

Sends a message to the client.

Message type that involves one of the following:

- 1—The SSID is invalid
  - 2—The network settings are invalid.
  - 3—There is a WLAN credibility mismatch.
  - 4—The user credentials are incorrect.
  - 5—Please call support.
  - 6—The problem is resolved.
  - 7—The problem has not been resolved.
  - 8—Please try again later.
  - 9—Please correct the indicated problem.
  - 10—Troubleshooting is refused by the network.
  - 11—Retrieving client reports.
  - 12—Retrieving client logs.
  - 13—Retrieval complete.
  - 14—Beginning association test.
  - 15—Beginning DHCP test.
  - 16—Beginning network connectivity test.
  - 17—Beginning DNS ping test.
  - 18—Beginning name resolution test.
  - 19—Beginning 802.1X authentication test.
  - 20—Redirecting client to a specific profile.
  - 21—Test complete.
  - 22—Test passed.
  - 23—Test failed.
  - 24—Cancel diagnostic channel operation or select a WLAN profile to resume normal operation.
  - 25—Log retrieval refused by the client.
  - 26—Client report retrieval refused by the client.
  - 27—Test request refused by the client.
  - 28—Invalid network (IP) setting.
  - 29—There is a known outage or problem with the network.
-



- 30—Scheduled maintenance period.
- 31—The WLAN security method is not correct.
- 32—The WLAN encryption method is not correct.
- 33—The WLAN authentication method is not correct.

<b>stats-request</b> <i>measurement-duration</i>	Sends a request for statistics.
<b>dot11</b>	(Optional) Specifies dot11 counters.
<b>security</b>	(Optional) Specifies security counters.
<b>test-abort</b>	Sends a request to the client to abort the current test.
<b>test-association</b> <i>ssid bssid</i> <i>dot11 channel</i>	Sends a request to the client to perform the association test.
<b>test-dot1x</b>	Sends a request to the client to perform the 802.1x test.
<i>profile-id</i>	(Optional) Test profile name.
<i>bssid</i>	Basic SSID.
<i>dot11</i>	Specifies the 802.11a, 802.11b, or 802.11g network.
<i>channel</i>	Channel number.
<b>test-profile</b>	Sends a request to the client to perform the profile redirect test.
<b>any</b>	Sends a request to the client to perform the profile redirect test.
<i>profile-id</i>	Test profile name.
	<b>Note</b> The profile ID should be from one of the client profiles for which client reporting is enabled.

**Command Default** No default behavior or values.

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** The **default-gw-ping** test does not require the client to use the diagnostic channel.

This example shows how to clear the reporting information of the client MAC address 00:1f:ca:cf:b6:60:

```
Device# configure terminal
```

**wireless client mac-address**

```
Device(config)# wireless client mac-address 00:1f:ca:cf:b6:60 ccx clear-reports  
Device(config)# end
```

# wireless config validate

To validate whether the wireless configuration is complete and consistent (all the functional profiles and tags are defined, and all the associations are complete and consistent), use the **wireless config validate** command in privileged EXEC mode.

## wireless config validate

### Syntax Description

This command has no keywords or arguments.

### Command Default

None

### Command Modes

Privileged EXEC (#)

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

### Usage Guidelines

In Cisco vEWLC, the wireless configuration is built using a collection of profiles, with each profile defining a functional block. These functional blocks are defined independently and is used to realize well-defined associations through intent based work-flows in building the wireless LAN. Such flexibility of modularizing the functional blocks requires the administrator to ensure that all associations are consistent and complete.

To ensure completeness and consistency of the wireless configuration, a configuration validation library is used to validate the configuration definitions across tables. The **wireless config validate** exec command is introduced from this release to validate the wireless configuration and report inconsistencies, if any, using contextual error message that is visible in btrace infra and on the console (if console logging is enabled). This command calls out any inconsistencies (unresolved associations) enabling you to realize a functional wireless LAN.

Use the following command to direct the output to a file: **show logging | redirect bootflash: filename** .

The following set of wireless configurations are validated:

RF tag	Site tag	Policy tag	Policy profile	Flex profile
site-tag	flex-profile	wlan profile	IPv4 ACL name	VLAN ACL
poliy-tag	ap-profile	policy profile	Fabric name	ACL-policy
rf-tag	---	---	service-policy input and output name	RF Policy (5GHz and 24GHz)
---	---	---	service-policy input and client output name	---

## Example

The following is sample output from the **wireless config validate** command

```
Device# wireless config validate
```

```
Oct 10 18:21:59.576 IST: %CONFIG_VALIDATOR_MESSAGE-5-EWLC_GEN_ERR: Chassis 1 R0/0: wncmgrd:  
Error in AP: fc99.473e.0a90 Applied site-tag : mysite definition does not exist  
Oct 10 18:21:59.576 IST: %CONFIG_VALIDATOR_MESSAGE-5-EWLC_GEN_ERR: Chassis 1 R0/0: wncmgrd:  
Error in AP: fc99.473e.0a90 Applied policy-tag : mypolicy definition does not exist  
Oct 10 18:21:59.576 IST: %CONFIG_VALIDATOR_MESSAGE-5-EWLC_GEN_ERR: Chassis 1 R0/0: wncmgrd:  
Error in AP: fc99.473e.0a90 Applied rf-tag : myrf definition does not exist
```

# wireless country

To configure one or more country codes for a device, use the **wireless country** command.

**wireless country** *country-code*

---

## Syntax Description

*country-code* Two-letter country code.

---

## Command Default

None

## Command Modes

Global configuration

---

## Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

---

## Usage Guidelines

The Cisco must be installed by a network administrator or qualified IT professional and the installer must select the proper country code. Following installation, access to the unit should be password protected by the installer to maintain compliance with regulatory requirements and to ensure proper unit functionality. See the related product guide for the most recent country codes and regulatory domains.

This example shows how to configure country code on the device to IN (India):

```
Device(config)# wireless country IN
```

# wireless exclusionlist mac address

To manually add clients to the exclusionlist, use the wireless exclusion list command. To remove the manual entry, use the no form of the command.

**wireless exclusionlist** *mac\_address* **description**

---

**Syntax Description**      **description** *value* Configures the entry description.

---



---

**Command Default**      None

---

**Command Modes**      Global Configuration

---

**Command History**      **Cisco IOS XE Gibraltar 16.10.1 Modification**

---

This command was introduced in this release.

---



---

**Usage Guidelines**      If a client was added to the exclusion list dynamically, the command to remove it is **wireless client mac-address xxxx.xxxx.xxxx deauthenticate** from enable mode.

## Example

This example shows how to manage exclusion entries:

```
Device(config)# wireless exclusion list xxxx.xxxx.xxxx
```

# wireless ipv6 ra wired

To enable the forwarding of Router Advertisement message to the wired clients, use the **wireless ipv6 ra wired** command.

**wireless ipv6 ra wired** { **nd** { **na-forward** | **ns-forward** } | **ra-wired** }

Syntax Description	
<i>nd</i>	Configures wireless IPv6 ND parameters.
<i>na-forward</i>	Enables forwarding of Neighbor Advertisement to wireless clients.
<i>ns-forward</i>	Enable forwarding of Neighbor Solicitation to wireless clients.
<i>ra</i>	Configures wireless IPv6 Router Advertisement parameters.
<i>wired</i>	Enables forwarding of Router Advertisement message to the wired clients.

**Command Default** None

**Command Modes** Global Configuration (config)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.3	This command was introduced.

## Example

The following example shows how to enable the forwarding of Router Advertisement message to the wired clients:

```
Device(config)# wireless ipv6 ra wired
```



**Warning** The **wireless ipv6 ra wired** command must be enabled only for certification purpose and not during the deployment.

# wireless load-balancing

To globally configure aggressive load balancing on the controller, use the **wireless load-balancing** command in global configuration mode.

**wireless load-balancing** {**denial** *denial-count* | **window** *client-count*}

## Syntax Description

<b>denial</b> <i>denial-count</i>	Specifies the number of association denials during load balancing.  Maximum number of association denials during load balancing is from 1 to 10 and the default value is 3.
<b>window</b> <i>client-count</i>	Specifies the aggressive load balancing client window, with the number of clients needed to trigger aggressive load balancing on a given access point.  Aggressive load balancing client window with the number of clients is from 0 to 20 and the default value is 5.

## Command Default

Disabled.

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

## Usage Guidelines

Load-balancing-enabled WLANs do not support time-sensitive applications like voice and video because of roaming delays.

When you use Cisco 7921 and 7920 Wireless IP Phones with controllers, make sure that aggressive load balancing is disabled on the voice WLANs for each controller. Otherwise, the initial roam attempt by the phone might fail, causing a disruption in the audio path.

This example shows how to configure association denials during load balancing:

```
Device# configure terminal
Device(config)# wireless load-balancing denial 5
Device(config)# end
```



# wireless macro-micro steering transition-threshold

To configure micro-macro transition thresholds, use the **wireless macro-micro steering transition-threshold** command.

**wireless macro-micro steering transition-threshold** {**balancing-window** | **client count** *number-clients* } {**macro-to-micro** | **micro-to-macro** *RSSI in dBm*}

Syntax Description		
<b>balancing-window</b>	Active instance of the configuration in Route-processor slot 0.	
<b>client</b>	Standby instance of the configuration in Route-processor slot 0.	
<i>number-clients</i>	Valid range is 0 to 65535 clients.	
<b>macro-to-micro</b>	Configures the macro to micro transition RSSI.	
<b>micro-to-macro</b>	Configures micro-macro client load balancing window.	
<i>RSSI in dBm</i>	RSSI in dBm. Valid range is -128 to 0.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration (config)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to configure balancing-window:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless macro-micro steering transition-threshold balancing-window
number-of-clients
```

# wireless macro-micro steering probe-suppression

To configure micro-macro probe suppressions, use the **wireless macro-micro steering probe-suppression** command.

**wireless macro-micro steering probe-suppression** {*aggressiveness number-of-cycles* | | *hysteresisRSSI in dBm* | **probe-auth** | **probe-only**}

## Syntax Description

<b>aggressiveness</b>	Configures probe cycles to be suppressed. The number of cycles range between 0 - 255.
<b>hysteresis</b>	Indicate show much greater the signal strength of a neighboring access point must be in order for the client to roam to it. The RSSI decibel value ranges from -6 to -3.
<b>probe-auth</b>	Enables mode to suppress probes and single auth
<b>probe-only</b>	Enables mode to suppress only probes

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

### Examples

The following example shows how to configure balancing-window:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless macro-micro steering probe-suppression aggressiveness
number-of-cycles
```

# wireless management certificate

To create a wireless management certificate details, use the **wireless management certificate** command.

**wireless management certificate ssc** { **auth-token** { **0** | **8** } *token* | **trust-hash** *hash-key* }

Syntax Description	
<b>auth-token</b>	Authentication token.
<i>token</i>	Token name.
<b>trust-hash</b>	Trusted SSC hash list.
<i>hash-key</i>	SHA1 fingerprint.
<b>0</b>	Specifies an UNENCRYPTED token.
<b>8</b>	Specifies an AES encrypted token.

**Command Default** None

**Command Modes** Global Configuration(config)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Example

The following example shows how to configure a wireless management certificate:

```
Device# configure terminal
Device(config)# wireless management certificate ssc trust-hash test
```

# wireless management interface

To create a wireless management interface, use the **wireless management interface** command.

**wireless management interface** { **GigabitEthernet** | **Loopback** | **Vlan** } *interface-number*

---

## Syntax Description

*interface-number* Interface number.

---



---

## Command Default

None

---

## Command Modes

Global Configuration(config)

---

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

## Example

The following example shows how to configure a wireless management interface:

```
Device# configure terminal
Device(config)# wireless management interface vlan vlan1
```

# wireless management trustpoint

To create a wireless management trustpoint, use the **wireless management trustpoint** command.

**wireless management trustpoint** *trustpoint-name*

---

## Syntax Description

*trustpoint-name* Trustpoint name.

---



---

## Command Default

None

---

## Command Modes

Global Configuration(config)

---

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---



---

## Usage Guidelines

Use this command only on the Cisco Catalyst 9800 Wireless Controller for Cloud platform and not on appliances as the appliances use the SUDI certificate by default without the need for this command.

## Example

The following example shows how to configure a wireless management trustpoint:

```
Device# configure terminal
Device(config)# wireless management trustpoint test
```

## wireless ewc-ap ap ap-type

To convert a single AP to CAPWAP or to embedded wireless controller, use the **wireless ewc-ap ap ap-type** command.

**wireless ewc-ap ap ap-type** *Cisco-AP-name* { **capwap** | **ewc** }

Syntax Description	ewc-ap	Configures the embedded wireless controller parameters.
	<b>ap-type</b>	Configures the AP parameter.
	<i>Cisco-AP-name</i>	Indicates the name of the Cisco AP.
	<b>capwap</b>	Changes to Capwap ap-type.
	<b>ewc</b>	Changes to the embedded wireless controller ap-type.

**Command Default** None

**Command Modes** Privileged EXEC mode

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This message was introduced.

### Example

The following example shows how to convert a single AP to a CAPWAP ap-type or a embedded wireless controller ap-type:

```
Device#wireless ewc-ap ap ap-type ap_name {capwap | ewc}
```

## wireless ewc-ap ap capwap

To specify the CAPWAP parameters for an AP, use the **wireless ewc-ap ap capwap** command.

**wireless ewc-ap ap capwap** *Primary-Controller-Name* { **A.B.C.D** | **X:X:X:X::X** }

Syntax Description		
<b>ewc-ap</b>	Configures the embedded wireless controller parameters.	
<b>capwap</b>	Configures the CAPWAP parameters.	
<i>Primary-Controller-Name</i>	Indicates the name of the controller.	
<b>A.B.C.D</b>	Indicates the IPv4 address of the primary controller.	
<b>X:X:X:X::X</b>	Indicates the IPv6 address of the primary controller.	
Command Default	None	
Command Modes	Privileged EXEC mode	
Command History	Release	Modification
	Cisco IOS XE 16.12.1	This message was introduced.

### Example

The following example shows how to specify the CAPWAP parameters for an AP:

```
Device#wireless ewc-ap ap capwap controller_name {10.1.1.1 | 9:0:0:0::1}
```

# wireless ewc-ap ap reload

To reload the embedded wireless controller AP, use the **wireless ewc-ap ap reload** command.

## wireless ewc-ap ap reload

<b>Syntax Description</b>	<b>ewc-ap</b>	Configures the embedded wireless controller parameters.
	<b>reload</b>	Reloads the embedded wireless controller AP.
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC mode	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This message was introduced.

## Example

The following example shows how to reload the embedded wireless controller AP:

```
Device#wireless ewc-ap ap reload
```



# wireless ewc-ap ap shell

To access the AP parameters on the embedded wireless controller AP shell, use the **wireless ewc-ap ap shell** command.

**wireless ewc-ap ap shell** { **chassis** { *chassis-number* | **active** | **standby** } **R0** | **username** }

Syntax Description	Parameter	Description
	<b>chassis</b>	Specifies the chassis.
	<i>chassis-number</i>	Specifies the chassis number as either 1 or 2.
	<b>active</b>	Configures the active instance in route processor slot 0.
	<b>standby</b>	Configures the standby instance in route processor slot 0.
	<b>R0</b>	Specifies the route processor in slot 0.
	<b>username</b>	Specifies the AP management username.

**Command Default** None

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

## Example

```
Device#wireless ewc-ap ap shell chassis 1 R0
```

## wireless ewc-ap ap shell username

To configure the AP management username on the embedded wireless controller AP shell, use the **wireless ewc-ap ap shell username** command.

**wireless ewc-ap ap shell username** *username* **chassis** { *chassis-number* | **active** | **standby** } **R0**

Syntax Description	Parameter	Description
	<b>chassis</b>	Specifies the chassis.
	<i>chassis-number</i>	Specifies the chassis number as either 1 or 2.
	<b>active</b>	Configures the active instance in route processor slot 0.
	<b>standby</b>	Configures the standby instance in route processor slot 0.
	<b>R0</b>	Specifies the route processor in slot 0.
	<b>username</b>	Specifies the AP management username.

**Command Default** None

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

### Example

```
Device#wireless ewc-ap ap shell username username1 chassis 1 R0
```

## wireless ewc-ap preferred-master

To select the standby controller when the network is up and running, use the **wireless ewc-ap preferred-master** command.

**wireless ewc-ap preferred-master** *AP-name*

<b>Syntax Description</b>	<b>ewc-ap</b>	Configures the embedded wireless controller parameters.
	<b>preferred-master</b>	Configures the preferred primary AP.
	<i>AP-name</i>	Indicates the name of the preferred primary AP.
<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration (config)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This message was introduced.

### Example

The following example shows how to set a preferred primary ap-type:

```
Device(config)#wireless ewc-ap preferred-master AP-name
```

# wireless ewc-ap factory-reset

To perform factory reset on the embedded wireless controller and on all the access points connected to the controller, use the **wireless ewc-ap factory-reset** command.

## wireless ewc-ap factory-reset

<b>Syntax Description</b>	<b>ewc-ap</b>	Configures the embedded wireless controller parameters
	<b>factory-reset</b>	Resets Cisco AP configuration to factory default.
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC mode	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

## Example

The following example shows how to factory-reset the embedded wireless controller network:

```
Device#wireless ewc-ap factory-reset
```

## wireless ewc-ap vrrp vrid

To configure the embedded wireless controller VRRP network identifier, use the **wireless ewc-ap vrrp vrid** command.

**wireless ewc-ap vrrp vrid***value* <1-255>

<b>Syntax Description</b>	<b>ewc-ap</b>	Configures the embedded wireless controller parameters.
	<b>vrrp</b>	Configures the preferred primary AP embedded wireless controller VRRP.
	<b>vrid</b>	Indicates the VRRP VRID. Values are from 1-255. The default value is 1.
	<i>value</i>	Indicates the VRRP VRID value.
<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration mode	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This message was introduced.

### Example

The following example shows how to configure the VRRP network identifier:

```
Device#wireless ewc-ap vrrp vrid 1
```

# wireless profile flex

To configure a wireless flex profile and enter wireless flex profile configuration mode, use the **wireless profile flex** command. To disable the feature, use the **no** form of the command.

**wireless profile flex** *custom-flex-profile*

**[no] wireless profile flex** *custom-flex-profile*

<b>Syntax Description</b>	<b>wireless profile flex</b>	Configures a wireless flex profile and enter wireless flex profile configuration mode.
	<i>custom-flex-profile</i>	Specifies the flex profile name.
<b>Command Default</b>	None	
<b>Command Modes</b>	Wireless flex profile mode	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

## Example

This example shows how the wireless flex profile is configured:

```
Device(config)#wireless profile flex custom-flex-profile
```

# wireless profile image-download default

To configure the default image download profile for AP Join Download and Predownload, use the following command:



**Note** **Default** is the only profile name that you can enter.

## wireless profile image-download default

### Syntax Description

**wireless profile** Configures the wireless profile parameters.

**image-download** Configures the EWC-AP image download parameters.

**default** Specifies the profile name - default. Default is the only profile name that you can enter.

### Command Default

None

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

### Example

```
Device# wireless profile image-download default
```

## wireless profile policy

To configure WLAN policy profile, use the **wireless profile policy** command.

**wireless profile policy** *policy-profile*

---

**Syntax Description** *policy-profile* Name of the WLAN policy profile.

---

**Command Default** The default profile name is default-policy-profile.

**Command Modes** Global configuration (config)

---

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

### Examples

The following example shows how to configure a WLAN policy profile:

```
Device(config)# wireless profile policy mywlan-profile-policy
```



# wireless profile transfer

To configure the export of trace logs on the embedded wireless controller, use the **wireless profile transfer** command. Use the **no** form of this command to negate the command or to set the command to its default.

[no] **wireless profiletransfertrace-export** *trace-export-profile-name*

<b>Syntax Description</b>	<b>trace-export</b>	Configures the trace export parameters.
	<i>trace-export-profile-name</i>	Specifies the trace export profile name.
<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

## Example

```
Device# wireless profile transfer trace-export trace-export-profile-name
```

## wireless rfid

To set the static radio-frequency identification (RFID) tag data timeout value, use the **wireless rfid** command in global configuration mode.

**wireless rfid timeout** *timeout-value*

<b>Syntax Description</b>	<b>timeout</b>	Configures the static RFID tag data timeout value.
	<i>timeout-value</i>	RFID tag data timeout value. Valid values range from 60-7200.
<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration (config)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

### Example

This example shows how to set the static RFID tag data timeout value.

```
Device(config)# wireless rfid timeout 70
```

# wireless security dot1x

To configure IEEE 802.1x global configurations, use the **wireless security dot1x** command.

```
wireless security dot1x [{eapol-key {retries retries | timeout milliseconds} | group-key interval
sec | identity-request {retries retries | timeout seconds} | radius [call-station-id] {ap-macaddress |
ap-macaddress-ssid | ipaddress | macaddress} | request {retries retries | timeout seconds} | wep key
{index 0 | index 3}}]
```

Syntax Description		
<b>eapol-key</b>		Configures eapol-key related parameters.
<b>retries</b> <i>retries</i>		(Optional) Specifies the maximum number of times (0 to 4 retries) that the controller retransmits an EAPOL (WPA) key message to a wireless client. The default value is 2.
<b>timeout</b> <i>milliseconds</i>		(Optional) Specifies the amount of time (200 to 5000 milliseconds) that the controller waits before retransmitting an EAPOL (WPA) key message to a wireless client using EAP or WPA/WPA-2 PSK. The default value is 1000 milliseconds.
<b>group-key interval</b> <i>sec</i>		Configures EAP-broadcast key renew interval time in seconds (120 to 86400 seconds).
<b>identity-request</b>		Configures EAP ID request related parameters.
<b>retries</b> <i>retries</i>		(Optional) Specifies the maximum number of times (0 to 4 retries) that the controller request the EAP ID. The default value is 2.
<b>timeout</b> <i>seconds</i>		(Optional) Specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting an EAP Identity Request message to a wireless client. The default value is 30 seconds.
<b>radius</b>		Configures radius messages.
<b>call-station-id</b>		(Optional) Configures Call-Station Id sent in radius messages.
<b>ap-macaddress</b>		Sets Call Station Id Type to the AP's MAC Address.
<b>ap-macaddress-ssid</b>		Sets Call Station Id Type to 'AP MAC address': 'SSID'.
<b>ipaddress</b>		Sets Call Station Id Type to the system's IP Address.
<b>macaddress</b>		Sets Call Station Id Type to the system's MAC Address.
<b>request</b>		Configures EAP request related parameters.

<b>retries</b> <i>retries</i>	(Optional) For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the maximum number of times (0 to 20 retries) that the controller retransmits the message to a wireless client.  The default value is 2.
<b>timeout</b> <i>seconds</i>	(Optional) For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting the message to a wireless client.  The default value is 30 seconds.
<b>wep key</b>	Configures 802.1x WEP related paramters.
<b>index 0</b>	Specifies the WEP key index value as 0
<b>index 3</b>	Specifies the WEP key index value as 3

**Command Default** Default for eapol-key-timeout: 1 second.  
Default for eapol-key-retries: 2 retries.

**Command Modes** config

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** None.

This example lists all the commands under **wireless security dot1x** .

```
Device#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#wireless security dot1x ?
  eapol-key          Configure eapol-key related parameters
  group-key          Configures EAP-broadcast key renew interval time in seconds
  identity-request   Configure EAP ID request related parameters
  radius             Configure radius messages
  request            Configure EAP request related parameters
  wep                Configure 802.1x WEP related paramters
  <cr>
```

## wireless security dot1x radius accounting mac-delimiter

To configure a MAC delimiter for called-station-ID or a calling-station-ID, use the **wireless security dot1x radius accounting mac-delimiter** command.

To remove MAC delimiter for a called-station-ID or a calling-station-ID, use the **no** form of the command.

**wireless security dot1x radius accounting mac-delimiter** { **colon** | **hyphen** | **none** | **single-hyphen** }

Syntax Description	Option	Description
	<b>colon</b>	Sets the delimiter to colon.
	<b>hyphen</b>	Sets the delimiter to hyphen.
	<b>none</b>	Disables delimiters.
	<b>single-hyphen</b>	Sets the delimiters to single hyphen.

**Command Default** None

**Command Modes** Global Configuration Mode

Command History	Release	Modification
	Cisco IOS XE 3.6.0 E	This command was introduced.

This example shows how to configure a MAC delimiter for called-station-ID or a calling-station-ID to colon:

```
Device(config)# wireless security dot1x radius accounting mac-delimiter colon
```

# wireless security dot1x radius accounting username-delimiter

To set the delimiter type, use **wireless security dot1x radius accounting username-delimiter** command, to remove the configuration, use the **no** form of this command.

**wireless security dot1x radius accounting username-delimiter** { colon | hyphen | none | single-hyphen }

Syntax Description	Option	Description
	<b>colon</b>	Sets the delimiter to colon.
	<b>hyphen</b>	Sets the delimiter to hyphen.
	<b>none</b>	Disables delimiters.
	<b>single-hyphen</b>	Sets the delimiters to single hyphen.

**Command Default** None

**Command Modes** Global Configuration Mode.

Command History	Release	Modification
	Cisco IOS XE 3.7.2 E	This command was introduced.

This example shows how to sets the delimiter to colon.

```
Device(config)# wireless security dot1x radius accounting username-delimiter colon
```

## wireless security dot1x radius callStationIdCase

To configure Call Station Id CASE send in RADIUS messages, use the **wireless security dot1x radius callStationIdCase** command.

To remove the Call Station Id CASE send in RADIUS messages, use the **no** form of the command.

**wireless security dot1x radius callStationIdCase** {**lower** | **upper**}

Syntax Description	
<b>lower</b>	Sends all Call Station Ids to RADIUS in lowercase
<b>upper</b>	Sends all Call Station Ids to RADIUS in uppercase

**Command Default** None

**Command Modes** Global Configuration Mode

Command History	Release	Modification
	Cisco IOS XE 3.6.0 E	This command was introduced.

This example shows how to configure Call Station Id CASE send in RADIUS messages in lowercase:

```
Device(config)# wireless security dot1x radius callstationIdCase lower
```

# wireless security dot1x radius mac-authentication call-station-id

To configure call station ID type for mac-authentication, use the **wireless security dot1x radius mac-authentication call-station-id** command. To remove the configuration, use the **no** form of it.

**wireless security dot1x radius mac-authentication call-station-id ap-ethmac-only | ap-ethmac-ssid | ap-group-name | ap-label-address | ap-label-address-ssid | ap-location | ap-macaddress | ap-macaddress-ssid | ap-name | ap-name-ssid | ipaddress | macaddress | vlan-id**

Syntax Description		
	<b>ap-ethmac-only</b>	Sets call station ID type to the AP Ethernet MAC address.
	<b>ap-ethmac-ssid</b>	Sets call station ID type to the format 'AP Ethernet MAC address':'SSID'.
	<b>ap-group-name</b>	Sets call station ID type to the AP Group Name.
	<b>ap-label-address</b>	Sets call station ID type to the AP MAC address on AP Label.
	<b>ap-label-address-ssid</b>	Sets call station ID type to the format 'AP Label MAC address': 'SSID'.
	<b>ap-location</b>	Sets call station ID type to the AP Location.
	<b>ap-macaddress</b>	Sets call station ID type to the AP Radio MAC Address.
	<b>ap-macaddress-ssid</b>	Sets call station ID type to the 'AP radio MAC Address':'SSID'.
	<b>ap-name</b>	Sets call station ID type to the AP name.
	<b>ap-name-ssid</b>	Sets call station ID type to the format 'AP name':'SSID'.
	<b>ipaddress</b>	Sets call station ID type to the system IP Address.
	<b>macaddress</b>	Sets call station ID type to the system MAC Address.
	<b>vlan-id</b>	Sets call station ID type to the VLAN ID.

**Command Default** None

**Command Modes** Global Configuration Mode

Command History	Release	Modification
	Cisco IOS XE 3.7.2	This command was introduced.
	E	

The example show how to set call station ID type to the AP Ethernet MAC address:

```
Device(config)# wireless security dot1x radius mac-authentication call-station-id
ap-ethmac-only
```



# wireless security dot1x radius mac-authentication mac-delimiter

To configure MAC-Authentication attributes, use the **wireless security dot1x radius mac-authentication mac-delimiter** command.

To remove MAC-Authentication attributes, use the **no** form of the command.

**wireless security dot1x radius mac-authentication mac-delimiter** { **colon** | **hyphen** | **none** | **single-hyphen** }

Syntax Description	Option	Description
	<b>colon</b>	Sets the delimiter to colon.
	<b>hyphen</b>	Sets the delimiter to hyphen.
	<b>none</b>	Disables delimiters.
	<b>single-hyphen</b>	Sets the delimiters to single hyphen.

**Command Default** None

**Command Modes** Global Configuration Mode

Command History	Release	Modification
	Cisco IOS XE 3.6.0 E	This command was introduced.

This example shows how to configure MAC-Authentication attributes to colon:

```
Device(config)# Scurity dot1x radius mac-authentication mac-delimiter colon
```

## wireless security web-auth retries

To enable web authentication retry on a particular WLAN, use the **wireless wireless security web-auth retries** command. To disable, use the **no** form of the command.

**wireless securityweb-authretries***retries*  
**nowireless securityweb-authretries**

### Syntax Description

<b>wireless security web-auth</b>	Enables web authentication on a particular WLAN.
<b>retries</b> <i>retries</i>	Specifies maximum number of web authentication request retries. The range is from 0 through 30. The default value is 3.

### Command Default

### Command Modes

config

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

### Usage Guidelines

None.

This example shows how to enable web authentication retry on a particular WLAN.

```
Device#configure terminal
Device# wireless security web-auth retries 10
```

# wireless tag policy

To configure wireless tag policy, use the **wireless tag policy** command.

**wireless tag policy** *policy-tag*

---

## Syntax Description

*policy-tag* Name of the wireless tag policy.

---

## Command Default

The default policy tag is default-policy-tag.

## Command Modes

Global configuration (config)

---

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

## Examples

The following example shows how to configure a wireless policy tag:

```
Device(config)# wireless tag policy guest-policy
```

## wireless tag site

To configure a wireless site tag, use the **wireless tag site** *site-tag* command.

**wireless tag site** *site-tag*

<b>Syntax Description</b>	<i>site-tag</i> Name of the site tag.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration (config)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

### Example

The following example shows how to configure a site tag:

```
Device(config)# wireless tag site test-site
```

# wireless wps ap-authentication threshold

To configure the alarm trigger threshold for access point neighbor authentication, use the **wireless wps ap-authentication threshold** command. To remove the access point neighbor authentication, use the no form of the command.

**wireless wps ap-authentication threshold** *value*

**no wireless wps ap-authentication threshold** *value*

<b>Syntax Description</b>	<b>threshold</b> <i>value</i> Specifies that the WMM-enabled clients are on the wireless LAN. The threshold value range is between 1 and 255. The default value is 1.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Global Configuration mode				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Amsterdam 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Amsterdam 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.				
<b>Usage Guidelines</b>	None				

## Example

The following example shows you how to configure the alarm trigger threshold for access point neighbor authentication:

```
Device(config)# wireless wps ap-authentication threshold 1
```

## wireless wps client-exclusion

To configure client exclusion policies, use the **wireless wps client-exclusion** command. To remove the client exclusion policies, use the **no** form of the command.

**wireless wps client-exclusion** {all | dot11-assoc | dot11-auth | dot1x-auth | ip-theft | web-auth}

**no wireless wps client-exclusion** {all | dot11-assoc | dot11-auth | dot1x-auth | ip-theft | web-auth}

### Syntax Description

<b>dot11-assoc</b>	Specifies that the controller excludes clients on the sixth 802.11 association attempt, after five consecutive failures.
<b>dot11-auth</b>	Specifies that the controller excludes clients on the sixth 802.11 authentication attempt, after five consecutive failures.
<b>dot1x-auth</b>	Specifies that the controller excludes clients on the sixth 802.11X authentication attempt, after five consecutive failures.
<b>ip-theft</b>	Specifies that the control excludes clients if the IP address is already assigned to another device.  For more information, see the Usage Guidelines section.
<b>web-auth</b>	Specifies that the controller excludes clients on the fourth web authentication attempt, after three consecutive failures.
<b>all</b>	Specifies that the controller excludes clients for all of the above reasons.

### Command Default

Enabled.

### Command Modes

config

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

### Usage Guidelines

In IP-theft scenarios, there are differences between the older Cisco IOS XE releases and the Cisco IOS XE Denali 16.x releases:

Older Cisco IOS XE Releases	Cisco IOS XE Denali 16.x Releases
<p>Priority wise, wired clients have higher priority over wireless clients, and DHCP IP has higher priority over static IP. The client security type is not checked; security of all client types are treated with same priority.</p> <p>If the existing binding is from a higher priority source, the new binding is ignored and an IP-theft is signaled. If the existing binding has the same source-priority as the new binding, the binding is ignored and an IP-theft is signaled. This ensures that the bindings are not toggled if two hosts send traffic using the same IP. Only the initial binding is retained in the software. If the new binding is from a higher priority source, the existing binding is replaced. This results in an IP-theft notification of existing binding and also a new binding notification.</p>	<p>There is not really a fundamental difference between wired and wireless; what matters is the trust (preflevel) of the entry, which is a function on how it was learnt (ARP, DHCP, ND, and so on) and the policy that is attached to the port. When preflevel is equal, the IP takeover is denied if the old entry is still reachable. IP takeover occurs when the update comes from a trusted port or a new entry gets IP from the DHCP server. Otherwise, you must explicitly grant it. The IP-theft is not reported if an old entry is replaced by a new and a more trusted one.</p>

This example shows how to disable clients on the 802.11 association attempt after five consecutive failures.

```
Device#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#wireless wps client-exclusion dot11-assoc
```

# wireless wps mfp ap-impersonation

To configure AP impersonation detection, use the **wireless wps mfp ap-impersonation** command. Use the **no** form of this command to disable the configuration.

**wireless wps mfp ap-impersonation**

**no wireless wps mfp ap-impersonation**

<b>Syntax Description</b>	<b>ap-impersonation</b> Configures AP impersonation detection.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Global Configuration mode	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 16.12.1	This command was introduced.
<b>Usage Guidelines</b>	None	

## Example

The following example shows you how to configure AP impersonation detection:

```
Device(config)# wireless wps mfp ap-impersonation
```



# wireless wps rogue network-assurance enable

To enable the rogue wireless service assurance (WSA) events, use the **wireless wps rogue network-assurance enable** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue network-assurance enable**

**no wireless wps rogue network-assurance enable**

<b>Syntax Description</b>	<b>network-assurance enable</b> Enables rogue WSA events.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Global Configuration mode				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Amsterdam 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Amsterdam 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.				
<b>Usage Guidelines</b>	None				

## Example

The following example shows you how to enable the rogue wireless service assurance events:

```
Device(config)# wireless wps rogue network-assurance enable
```

## wireless wps rogue ap aaa

To configure the use of AAA/local database to detect valid AP MAC addresses, use the **wireless wps rogue ap aaa** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue ap aaa**

**no wireless wps rogue ap aaa**

<b>Syntax Description</b>	<b>aaa</b> Configures the use of AAA or local database to detect valid AP MAC addresses.
---------------------------	------------------------------------------------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Global Configuration mode
----------------------	---------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

<b>Usage Guidelines</b>	None
-------------------------	------

### Example

The following example shows you how to configure the use of AAA/local database to detect valid AP MAC addresses:

```
Device(config)# wireless wps rogue ap aaa
```

## wireless wps rogue ap aaa polling-interval

To configure Rogue AP AAA validation interval, in seconds, use the **wireless wps rogue ap aaa polling-interval** command. To disable the configuration, use the no form of this command.

**wireless wps rogue ap aaa polling-interval** *60 - 86400*

**no wireless wps rogue ap aaa polling-interval** *60 - 86400*

Syntax Description	aaa	Sets the use of AAA or local database to detect valid AP MAC addresses.
	<b>polling-interval</b>	Configures the rogue AP AAA validation interval.
	<i>60 - 86400</i>	Specifies AP AAA validation interval, in seconds.

**Command Default** None

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** None

### Example

This example shows how to configure Rogue AP AAA validation interval, in seconds:

```
Device(config)# wireless wps rogue ap aaa polling-interval 120
```

## wireless wps rogue ap init-timer

To configure the init timer for rogue APs, use the **wireless wps rogue ap init-timer** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue ap init-timer**

**no wireless wps rogue ap init-timer**

<b>Syntax Description</b>	<b>init-timer</b> Configures the init timer for rogue APs.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Global Configuration mode				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Amsterdam 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Amsterdam 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.				
<b>Usage Guidelines</b>	None				

### Example

The following example shows you how to configure the init timer for rogue APs:

```
Device(config)# wireless wps rogue ap init-timer
```

# wireless wps rogue ap mac-address rldp initiate

To initiate and configure Rogue Location Discovery Protocol on rogue APs, use the **wireless wps rogue ap mac-address rldp initiate** command.

**wireless wps rogue ap mac-address** *<MAC Address>* **rldp initiate**

Syntax Description	Parameter	Description
	<b>wps</b>	Configures the WPS settings.
	<b>rogue</b>	Configures the global rogue devices.
	<b>ap mac-address</b> <i>&lt;MAC Address&gt;</i>	The MAC address of the APs.
	<b>rldp initiate</b>	Initiates RLDP on rogue APs.

**Command Default** None

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

**Usage Guidelines** None

## Example

The following example shows you how to initiate and configure Rogue Location Discovery Protocol on rogue APs:

```
Device# wireless wps rogue ap mac-address 10.1.1 rldp initiate
```

## wireless wps rogue ap notify-min-rssi

To configure the minimum RSSI notification threshold for rogue APs, use the **wireless wps rogue ap notify-min-rssi** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue ap notify-min-rssi**

**no wireless wps rogue ap notify-min-rssi**

<b>Syntax Description</b>	<b>notify-min-rssi</b> Configure the minimum RSSI notification threshold for rogue APs.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Global Configuration mode				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Amsterdam 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Amsterdam 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.				
<b>Usage Guidelines</b>	None				

### Example

The following example shows you how to configure the minimum RSSI notification threshold for rogue APs:

```
Device(config)# wireless wps rogue ap notify-min-rssi
```

# wireless wps rogue ap notify-rssi-deviation

To configure the RSSI deviation notification threshold for rogue APs, use the **wireless wps rogue ap notify-rssi-deviation** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue ap notify-rssi-deviation**

**no wireless wps rogue ap notify-rssi-deviation**

<b>Syntax Description</b>	<b>notify-rssi-deviation</b> Configures the RSSI deviation notification threshold for rogue APs.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Global Configuration mode				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Amsterdam 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Amsterdam 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.				
<b>Usage Guidelines</b>	None				

## Example

The following example shows you how to configure the RSSI deviation notification threshold for rogue APs:

```
Device(config)# wireless wps rogue ap notify-rssi-deviation
```

## wireless wps rogue ap rldp alarm-only

To set Rogue Location Discovery Protocol (RLDP) and alarm if rogue is detected, use the **wireless wps rogue ap rldp alarm-only** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue ap rldp alarm-only**

**no wireless wps rogue ap rldp alarm-only**

<b>Syntax Description</b>	<b>alarm-only</b> Sets RLDP and alarm if rogue is detected.
---------------------------	-------------------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Global Configuration mode
----------------------	---------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

<b>Usage Guidelines</b>	None
-------------------------	------

### Example

The following example shows you how to set RLDP and alarm if rogue is detected:

```
Device(config)# wireless wps rogue ap rldp alarm-only
```



# wireless wps rogue ap rldp alarm-only monitor-ap-only

To perform RLDP only on monitor APs, use the **wireless wps rogue ap rldp alarm-only monitor-ap-only** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue ap rldp alarm-only monitor-ap-only**

**no wireless wps rogue ap rldp alarm-only monitor-ap-only**

<b>Syntax Description</b>	<b>monitor-ap-only</b> Performs RLDP on monitor APs only.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Global Configuration mode				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Amsterdam 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Amsterdam 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.				
<b>Usage Guidelines</b>	None				

## Example

The following example shows you how to perform RLDP only on monitor APs,:

```
Device(config)# wireless wps rogue ap rldp alarm-only monitor-ap-only
```

## wireless wps rogue ap rldp auto-contain

To configure RLDP, alarm and auto-contain if rogue is detected, use **wirelesswps rogueaprl dp auto-contain** command. Use the **no** form of the command to disable the alarm.

**[no] wireless wps rogue ap rldp auto-contain monitor-ap-only**

<b>Syntax Description</b>	<b>monitor-ap-only</b> Perform RLDP only on monitor AP						
<b>Command Default</b>	None						
<b>Command Modes</b>	Global Configuration						
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.1</td> <td>This command was introduced.</td> </tr> <tr> <td>Cisco IOS XE 3.7.3E</td> <td>The <b>no</b> form of the command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.	Cisco IOS XE 3.7.3E	The <b>no</b> form of the command was introduced.
Release	Modification						
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.						
Cisco IOS XE 3.7.3E	The <b>no</b> form of the command was introduced.						

### Example

This example shows how to configure an alarm for a detected rogue.

```
Device# wireless wps rogue ap rldp auto-contain
```

# wireless wps rogue ap rldp retries

To configure RLDP retry times on rogue APs, use the **wireless wps rogue ap rldp retries** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue ap rldp retries**

**no wireless wps rogue ap rldp retries**

<b>Syntax Description</b>	<b>retries</b> Configures RLDP retry times on rogue APs.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Global Configuration mode				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Amsterdam 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Amsterdam 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.				
<b>Usage Guidelines</b>	None				

## Example

The following example shows you how to configure RLDP retry times on rogue APs:

```
Device(config)# wireless wps rogue ap rldp retries
```

## wireless wps rogue ap rldp schedule

To configure RLDP scheduling, use the **wireless wps rogue ap rldp schedule** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue ap rldp schedule**

**no wireless wps rogue ap rldp schedule**

<b>Syntax Description</b>	<b>schedule</b> Configures RLDP scheduling.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Global Configuration mode				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Amsterdam 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Amsterdam 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.				
<b>Usage Guidelines</b>	None				

### Example

The following example shows you how to configure RLDP scheduling:

```
Device(config)# wireless wps rogue ap rldp schedule
```

# wireless wps rogue ap rldp schedule day

To configure the day when RLDP scheduling is to be done, use the **wireless wps rogue ap rldp schedule day** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue ap rldp schedule day** { **friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday** } **start** [HH:MM:SS] **end** [HH:MM:SS]

**no wireless wps rogue ap rldp schedule day** { **friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday** } **start** [HH:MM:SS] **end** [HH:MM:SS]

<b>Syntax Description</b>	<b>day</b> { <b>friday</b>   <b>monday</b>   <b>saturday</b>   <b>sunday</b>   <b>thursday</b>   <b>tuesday</b>   <b>wednesday</b> }	Configures the day of the week when RLDP scheduling is to be done.
	<b>start</b> [HH:MM:SS]	Configures the start time for RLDP schedule for the day.
	<b>end</b> [HH:MM:SS]	Configures the end time for RLDP schedule for the day.

**Command Default** None

**Command Modes** Global Configuration mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

**Usage Guidelines** None

## Example

The following example shows you how to configure the day of the week, when RLDP scheduling is to be done:

```
Device(config)# wireless wps rogue ap rldp schedule day friday start 10:10:10 end 15:15:15
```

## wireless wps rogue ap timeout

To configure the expiry time for rogue APs, in seconds, use the **wireless wps rogue ap timeout** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue ap timeout** *240-3600*

**no wireless wps rogue ap timeout** *240-3600*

<b>Syntax Description</b>	<b>rogue ap timeout</b>	Configures the expiry time for rogue APs, in seconds.	
	<i>240-3600</i>	Specifies the number of seconds before rogue entries are flushed.	
<b>Command Default</b>	None		
<b>Command Modes</b>	Global configuration		
<b>Command History</b>	<b>Release</b>	<b>Modification</b>	
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.	
<b>Usage Guidelines</b>	None		

### Example

This example shows how to configure the expiry time for rogue APs, in seconds:

```
Device(config)# wireless wps rogue ap timeout 250
```

# wireless wps rogue auto-contain

To configure the auto contain level and to configure auto containment for monitor AP mode, use the **wireless wps rogue auto-contain** command. To disable the configuration, use the **no** form of this command.

**wireless wps rogue auto-contain** { level 1 - 4 | monitor-ap-only }

**no wireless wps rogue auto-contain** { level 1 - 4 | monitor-ap-only }

Syntax Description	Parameter	Description
	<b>auto-contain</b>	Configures auto contain for rogue devices.
	<b>level</b>	Configures auto contain levels.
	<i>1 - 4</i>	Specifies the auto containment levels.
	<b>monitor-ap-only</b>	Configures auto contain for monitor AP mode.

**Command Default** None

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** None

## Example

This example shows how to configure the auto contain level and to configure auto containment for monitor AP mode:

```
Device(config)# wireless wps rogue auto-contain level 2
```

```
Device(config)# wireless wps rogue auto-contain monitor-ap-only
```

## wireless wps rogue client aaa

To configure the use of AAA or local database to detect valid MAC addresses of rogue clients, use the **wireless wps rogue client aaa** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue client aaa**

**no wireless wps rogue client aaa**

<b>Syntax Description</b>	<b>aaa</b> Configures the use of AAA or local database to detect valid MAC addresses of rogue clients.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Global Configuration mode	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 16.12.1	This command was introduced.
<b>Usage Guidelines</b>	None	

### Example

The following example shows you how to configure the use of AAA or local database to detect valid MAC addresses of rogue clients:

```
Device(config)# wireless wps rogue client aaa
```



# wireless wps rogue client mse

To configure Mobility Services Engine (MSE) to detect valid MAC addresses of rogue clients, use the **wireless wps rogue client mse** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue client mse**

**no wireless wps rogue client mse**

<b>Syntax Description</b>	<b>mse</b> Configures the MSE to detect valid MAC addresses of rogue clients.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Global Configuration mode				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Amsterdam 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Amsterdam 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.				
<b>Usage Guidelines</b>	None				

## Example

The following example shows you how to configure Mobility Services Engine (MSE) to detect valid MAC addresses of rogue clients:

```
Device(config)# wireless wps rogue client mse
```

## wireless wps rogue client client-threshold

To configure rogue client per a rogue AP SNMP trap threshold, use the **wireless wps rogue client client-threshold** command. To disable the configuration, use the **no** form of this command.

**wireless wps rogue client client-threshold** *0 - 256*

**no wireless wps rogue client client-threshold** *0 - 256*

<b>Syntax Description</b>	<b>rogue client</b>	Configures rogue clients.
	<b>client-threshold</b>	Configures the rogue client per a rogue AP SNMP trap threshold.
	<i>0 - 256</i>	Specifies the client threshold.
<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
<b>Usage Guidelines</b>	None	

### Example

This example shows how to configure rogue client per a rogue AP SNMP trap threshold:

```
Device(config)# wireless wps rogue ap timeout 250
```

## wireless wps rogue client notify-min-rssi

To configure the minimum RSSI notification threshold for rogue clients, use the **wireless wps rogue client notify-min-rssi** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue client notify-min-rssi** *-128 - -70*

**no wireless wps rogue client notify-min-rssi** *-128 - -70*

Syntax Description		
	<b>rogue clients</b>	Configures rogue clients.
	<b>notify-min-rssi</b>	Configures the minimum RSSI notification threshold for rogue clients.
	<i>-128 - -70</i>	Specifies the RSSI threshold in decibels.

**Command Default** None

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** None

### Example

This example shows how to configure the minimum RSSI notification threshold for rogue clients:

```
Device(config)# wireless wps rogue client notify-min-rssi -125
```

## wireless wps rogue client notify-rssi-deviation

To configure the RSSI deviation notification threshold for rogue clients, use the **wireless wps rogue client notify-rssi-deviation** command. To disable the configuration, use the **no** form of this command.

**wireless wps rogue client notify-rssi-deviation** *0 - 10*

**no wireless wps rogue client notify-rssi-deviation** *0 - 10*

<b>Syntax Description</b>	<b>notify-rssi-deviation</b>	Configures the RSSI deviation notification threshold for rogue clients.
	<i>0 - 10</i>	Specifies the RSSI threshold in decibels.

**Command Default** None

**Command Modes** Global configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** None

### Example

This example shows how to configure the RSSI deviation notification threshold for rogue clients:

```
Device(config)# wireless wps rogue client notify-rssi-deviation 6
```

# wireless wps rogue rule

To configure rogue classification rule, use the **wireless wps rogue rule** command.

```
wireless wps rogue rule rule-name priority priority {classify{friendly | malicious} | condition
{client-count number | duration | encryption | infrastructure | rfssi | ssid} | default | exit | match {all |
any} | no | shutdown}
```

Syntax Description		
<b>rule</b> <i>rule-name</i>		Specifies a rule name.
<b>priority</b> <i>priority</i>		Changes the priority of a specific rule and shifts others in the list accordingly.
<b>classify</b>		Specifies the classification of a rule.
<b>friendly</b>		Classifies a rule as friendly.
<b>malicious</b>		Classifies a rule as malicious.
<b>condition</b> { <b>client-count</b> <i>number</i>   <b>duration</b>   <b>encryption</b>   <b>infrastructure</b>   <b>rfssi</b>   <b>ssid</b> }		Specifies the conditions for a rule that the rogue access point must meet. Type of the condition to be configured. The condition types are listed below: <ul style="list-style-type: none"> <li>• <b>client-count</b>—Requires that a minimum number of clients be associated to a rogue access point. The valid range is 1 to 10 (inclusive).</li> <li>• <b>duration</b>—Requires that a rogue access point be detected for a minimum period of time. The valid range is 0 to 3600 seconds (inclusive).</li> <li>• <b>encryption</b>—Requires that the advertised WLAN does not have encryption enabled.</li> <li>• <b>infrastructure</b>—Requires the SSID to be known to the controller</li> <li>• <b>rfssi</b>—Requires that a rogue access point have a minimum RSSI value. The range is from -95 to -50 dBm (inclusive).</li> <li>• <b>ssid</b>—Requires that a rogue access point have a specific SSID.</li> </ul>
<b>default</b>		Sets the command to its default settings.
<b>exit</b>		Exits the sub-mode.
<b>match</b> { <b>all</b>   <b>any</b> }		Configures matching criteria for a rule. Specifies whether a detected rogue access point must meet all or any of the conditions specified by the rule in order for the rule to be matched and the rogue access point to adopt the classification type of the rule.
<b>no</b>		Negates a command or set its defaults.
<b>shutdown</b>		Shuts down the system.

**Command Default** None.

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines**

None.

This example shows how to create a rule that can organize and display rogue access points as Friendly:

```
Device# configure terminal  
Device(config)# wireless wps rogue rule ap1 priority 1  
Device(config-rule)# classify friendly  
Device(config)# end
```

# wireless wps rogue security-level

To configure the wireless WPS rogue detection security levels, use the **wireless wps rogue security-level** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue security-level** { **critical** | **custom** | **high** | **low** }

**no wireless wps rogue security-level** { **critical** | **custom** | **high** | **low** }

Syntax Description	
<b>rogue security-level</b>	Configures the rogue detection security level.
<b>critical</b>	Specifies the rogue detection setup for highly sensitive deployments.
<b>custom</b>	Specifies the customizable security level.
<b>high</b>	Specifies the rogue detection setup for medium-scale deployments.
<b>low</b>	Specifies the basic rogue detection setup for small-scale deployments.

**Command Default** None

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** None

## Example

This example shows how to configure the wireless WPS rogue detection security levels:

```
Device(config)# wireless wps rogue security-level critical
```

## wireless-default radius server

To configure multiple radius servers, use the **wireless-default radius server** command.

```
wireless-default radius server IP key secret
```

<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration (config)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
<b>Usage Guidelines</b>	Using this utility, you can configure a maximum of ten radius servers.	

### Example

This example shows how to configure multiple radius servers:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless-default radius server 9.2.58.90 key cisco123
Device(config)# end
```



## wlan policy

To map a policy profile to a WLAN profile, use the **wlan policy** command.

**wlan** *wlan-name* **policy** *policy-name*

### Syntax Description

*wlan-name* Name of the WLAN profile.

**policy** Map a policy profile to the WLAN profile.

*policy-name* Name of the policy profile.

### Command Default

None

### Command Modes

config-policy-tag

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.





## Show Commands

---

- [show aaa dead-criteria radius](#), on page 573
- [show access-list](#), on page 575
- [show ap auth-list](#), on page 577
- [show ap auth-list ap-cert-policy](#), on page 578
- [show ap auto-rf](#), on page 579
- [show ap config](#), on page 582
- [show ap crash-file](#), on page 584
- [show ap dot11](#), on page 585
- [show ap dot11](#), on page 591
- [show ap dot11 24ghz](#), on page 592
- [show ap dot11 24ghz SI config](#), on page 593
- [show ap dot11 24ghz SI device type](#), on page 594
- [show ap dot11 5ghz](#), on page 595
- [show ap dot11 24ghz cleanair air-quality](#), on page 597
- [show ap dot11 24ghz cleanair air-quality](#), on page 598
- [show ap dot11 cleanair config](#), on page 599
- [show ap dot11 cleanair summary](#), on page 601
- [show ap dot11 dual-band summary](#), on page 602
- [show ap environment](#), on page 603
- [show ap filters active](#), on page 604
- [show ap filters all](#), on page 605
- [show ap fra](#), on page 606
- [show ap gps location](#), on page 607
- [show history channel interface dot11Radio all](#), on page 608
- [show ap link-encryption](#), on page 609
- [show ap lldp neighbors detail](#), on page 610
- [show ap lldp neighbors](#), on page 611
- [show ap name lldp neighbors detail](#), on page 612
- [show ap name lldp neighbors](#), on page 613
- [show ap master list](#), on page 614
- [show ap multicast mom \(multicast over multicast\)](#), on page 615
- [show ap name auto-rf](#), on page 616
- [show ap name ble detail](#), on page 619

- [show ap name cablemodem](#), on page 620
- [show ap name config](#), on page 621
- [show ap name config ethernet](#), on page 623
- [show ap name dot11](#), on page 624
- [show ap name environment](#), on page 625
- [show ap name gps location](#), on page 626
- [show ap name mesh neighbor detail](#), on page 627
- [show ap name wlan](#), on page 628
- [show ap profile](#), on page 630
- [show ap rf-profile name](#), on page 631
- [show ap rf-profile summary](#), on page 633
- [show ap summary](#), on page 634
- [show ap tag sources](#), on page 635
- [show ap tag summary](#), on page 636
- [show ap upgrade](#), on page 637
- [show arp](#), on page 638
- [show arp summary](#) , on page 639
- [show avc client](#), on page 640
- [show avc wlan](#), on page 641
- [show chassis](#), on page 642
- [show checkpoint](#), on page 643
- [show flexconnect office-extend diagnostics](#), on page 650
- [show flow exporter](#), on page 652
- [show flow interface](#), on page 654
- [show flow monitor](#), on page 656
- [show flow record](#), on page 658
- [show interfaces](#), on page 659
- [show install package](#), on page 663
- [show install rollback](#), on page 664
- [show install summary](#), on page 665
- [show ip](#), on page 666
- [show ip nbar protocol-id](#), on page 667
- [show ldap attributes](#), on page 668
- [show ldap server](#), on page 669
- [show license all](#), on page 670
- [show license authorization](#), on page 674
- [show license data conversion](#), on page 679
- [show license eventlog](#), on page 680
- [show license history message](#), on page 681
- [show license reservation](#), on page 682
- [show license status](#), on page 683
- [show license summary](#), on page 692
- [show license tech](#), on page 694
- [show license udi](#), on page 700
- [show license usage](#), on page 701
- [show platform software sl-infra](#), on page 704

- [show platform software tls client summary](#), on page 705
- [show platform software client detail](#), on page 706
- [show platform software tls statistics](#), on page 708
- [show platform software tls session summary](#), on page 710
- [show logging profile wireless end timestamp](#), on page 711
- [show logging profile wireless filter](#), on page 712
- [show logging profile wireless fru](#), on page 713
- [show logging profile wireless internal](#), on page 714
- [show logging profile wireless level](#), on page 715
- [show logging profile wireless module](#), on page 716
- [show logging profile wireless reverse](#), on page 717
- [show logging profile wireless start](#), on page 718
- [show logging profile wireless switch](#), on page 719
- [show logging profile wireless to-file](#), on page 720
- [show mdns-sd cache](#), on page 721
- [show mdns-sd cache detail](#), on page 722
- [show mdns-sd cache upn shared](#), on page 723
- [show mdns-sd cache upn detail](#), on page 725
- [show mdns-sd flexconnect summary](#) , on page 726
- [show mdns-sd statistics](#), on page 727
- [show mdns-sd summary](#), on page 728
- [show mdns-sd sp-sdg statistics](#), on page 729
- [show nmsp](#), on page 730
- [show nmsp cloud-services statistics](#), on page 731
- [show nmsp cloud-services summary](#), on page 732
- [show nmsp subscription group detail all](#), on page 733
- [show nmsp subscription group detail ap-list](#), on page 734
- [show nmsp subscription group detail services](#), on page 735
- [show nmsp subscription group summary](#), on page 736
- [show platform conditions](#), on page 737
- [show platform software wlavc status cp-exporter](#), on page 738
- [show platform software system all](#), on page 739
- [show platform software trace filter-binary](#), on page 740
- [show platform software trace level](#), on page 741
- [show platform software trace message](#) , on page 744
- [show platform software trace message license-manager chassis active R0](#), on page 745
- [show policy-map](#), on page 748
- [show ssh](#) , on page 753
- [show stealthwatch-cloud connection](#), on page 754
- [show stealthwatch-cloud wireless-shim](#), on page 755
- [show tech-support wireless](#), on page 756
- [show tech-support wireless ap](#), on page 758
- [show tech-support wireless client](#), on page 768
- [show tech-support wireless radio](#), on page 772
- [show tunnel eogre global-configuration](#), on page 783
- [show tunnel eogre domain detailed](#), on page 784

- [show tunnel eogre domain summary](#), on page 785
- [show tunnel eogre gateway summary](#), on page 786
- [show tunnel eogre gateway detailed](#) , on page 787
- [show tunnel eogre manager stats global](#), on page 788
- [show tunnel eogre manager stats instance](#), on page 790
- [show wireless band-select](#), on page 792
- [show wireless client](#) , on page 793
- [show wireless client mac-address](#) , on page 794
- [show wireless client mac-address \(Call Control\)](#), on page 796
- [show wireless client mac-address \(TCLAS\)](#), on page 797
- [show wireless client summary](#), on page 798
- [show wireless client timers](#), on page 799
- [show wireless country](#), on page 800
- [show wireless detail](#), on page 803
- [show wireless dot11h](#) , on page 804
- [show wireless dtls connections](#), on page 805
- [show wireless exclusionlist](#) , on page 806
- [show wireless load-balancing](#), on page 807
- [show wireless ewc-ap ap summary](#), on page 808
- [show wireless ewc-ap ap config-sync](#), on page 809
- [show wireless ewc-ap ap image predownload status](#), on page 810
- [show wireless ewc-ap country-code](#), on page 811
- [show wireless ewc-ap image-master](#), on page 812
- [show wireless ewc-ap invalid-image-master](#), on page 813
- [show wireless ewc-ap predownload](#), on page 814
- [show wireless ewc-ap redundancy summary](#), on page 815
- [show wireless ewc-ap redundancy peers](#), on page 816
- [show wireless pmk-cache](#), on page 817
- [show wireless profile flex](#) , on page 818
- [show wireless profile policy detailed](#) , on page 819
- [show wireless rfid](#), on page 820
- [show wireless summary](#), on page 821
- [show wireless tag rf](#), on page 822
- [show wireless urlfilter details](#), on page 823
- [show wireless urlfilter summary](#), on page 824
- [show wireless vlan details](#) , on page 825
- [show wireless wgb mac-address](#) , on page 826
- [show wireless wgb summary](#) , on page 827
- [show wireless wps rogue ap summary](#) , on page 828
- [show wireless wps rogue client detailed](#), on page 829
- [show wireless wps rogue client summary](#), on page 830

# show aaa dead-criteria radius

To verify the dead-server-detection information for a RADIUS server, use the **show aaa dead-criteria radius** command.

**show aaa dead-criteria radius** *ipaddr* **auth-port** *authport* **acct-port** *acctport*

<b>Syntax Description</b>	<i>ipaddr</i> IP address.				
	<i>authport</i> Authentication port.				
	<i>acctport</i> Accounting port.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Privileged EXEC (#)				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.
Release	Modification				
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.				

**Usage Guidelines** The **show aaa dead-criteria radius** *ipaddr* command displays output only if default ports are used. For non-default ports, use the **show aaa dead-criteria radius** *ipaddr* **auth-port** *authport* **acct-port** *acctport* command.

## Example

The following example shows how to see the dead-server-detection information for a RADIUS server with non-default authorization and accounting ports:

```
Device# show aaa dead-criteria radius 4.4.4.4 auth-port 4444 acct-port 3333
```

```
RADIUS: No server group specified. Using radius
RADIUS Server Dead Criteria:
=====
Server Details:
Address : 4.4.4.4
Auth Port : 4444
Acct Port : 3333
Server Group : radius
Dead Criteria Details:
Configured Retransmits : 3
Configured Timeout : 5
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Dead Detect Time : 10s
Computed Retransmit Tries: 10
Statistics Gathered Since Last Successful Transaction
=====
Max Computed Outstanding Transactions: 0
Max Computed Dead Detect Time: 0s
```

```
Max Computed Retransmits : 0
```

The following example shows how to see the dead-server-detection information for a RADIUS server using default ports:

```
Device# show aaa dead-criteria radius 9.3.13.37

RADIUS: No server group specified. Using radius
RADIUS Server Dead Criteria:
=====
Server Details:
Address : 9.3.13.37
Auth Port : 1812
Acct Port : 1813
Server Group : radius
Dead Criteria Details:
Configured Retransmits : 3
Configured Timeout : 30
Estimated Outstanding Access Transactions: 1
Estimated Outstanding Accounting Transactions: 0
Dead Detect Time : 10s
Computed Retransmit Tries: 10
Statistics Gathered Since Last Successful Transaction
=====
Max Computed Outstanding Transactions: 4
Max Computed Dead Detect Time: 48s
Max Computed Retransmits : 30
```



# show access-list

To display access control lists (ACLs) configured on the device, use the **show access-lists** command in privileged EXEC mode.

**show access-lists** [ {*namenumber* | **hardware counters** | **ipc**} ]

Syntax Description	
<i>number</i>	(Optional) ACL number. The range is 1 to 2799.
<i>name</i>	(Optional) Name of the ACL.
<b>hardware counters</b>	(Optional) Displays the access list hardware counters.
<b>ipc</b>	(Optional) Display Interprocess Communication (IPC) protocol access-list configuration download information

## Command Default

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

## Usage Guidelines

Though visible in the command-line help strings, the **rate-limit** keyword is not supported

The device supports only IP standard and extended access lists. Therefore, the allowed numbers are only 1 to 199 and 1300 to 2799.

This command also displays the MAC ACLs that are configured.

This is an example of output from the **show access-lists** command:

```
Device# show access-lists

Extended IP access list 103
  10 permit ip any any dscp af11
Extended IP access list ssm-range
  10 deny ip any 232.0.0.0 0.255.255.255
  20 permit ip any any
Extended MAC access list mac1
```

This is an example of output from the **show access-lists hardware counters** command:

```
Device# show access-lists hardware counters
L3 ACL INPUT Statistics
  All Drop:                               frame count: 0
  All Bridge Only:                         frame count: 0
  All Forwarding To CPU:                   frame count: 294674
  All Forwarded:                           frame count: 2577677
```

```
All Drop And Log:                frame count: 0
All Bridge Only And Log:         frame count: 0
All Forwarded And Log:          frame count: 0
All IPv6 Drop:                   frame count: 0
All IPv6 Bridge Only:           frame count: 0
All IPv6 Forwarding To CPU:     frame count: 0
All IPv6 Forwarded:             frame count: 102
All IPv6 Drop And Log:          frame count: 0
All IPv6 Bridge Only And Log:   frame count: 0
All IPv6 Forwarded And Log:     frame count: 0
```

## L3 ACL OUTPUT Statistics

```
All Drop:                        frame count: 0
All Bridge Only:                 frame count: 0
All Forwarding To CPU:           frame count: 0
All Forwarded:                   frame count: 266050
All Drop And Log:                frame count: 0
All Bridge Only And Log:         frame count: 0
All Forwarded And Log:           frame count: 0
All IPv6 Drop:                   frame count: 0
All IPv6 Bridge Only:           frame count: 0
All IPv6 Forwarding To CPU:     frame count: 0
All IPv6 Forwarded:             frame count: 0
All IPv6 Drop And Log:          frame count: 0
All IPv6 Bridge Only And Log:   frame count: 0
All IPv6 Forwarded And Log:     frame count: 0
```

## show ap auth-list

To see the access point authorization list, use the **show ap auth-list** command.

```
show ap auth-list [chassis {chassis-number | active | standby} R0]
```

### Syntax Description

*chassis-number* Chassis number as either 1 or 2.

**active R0** Active instance in Route-processor slot 0.

**standby R0** Standby instance in Route-processor slot 0.

### Command Default

None

### Command Modes

Privileged EXEC

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

### Examples

The following example shows how to see the access point authorization list:

```
Device# show ap auth-list
```

# show ap auth-list ap-cert-policy

To verify if the APs have been authorized by the AP certificate policy, use the **show ap auth-list ap-cert-policy**

**show ap auth-list ap-cert-policy**

<b>Syntax Description</b>	This command has no arguments.
---------------------------	--------------------------------

<b>Command Default</b>	Privileged EXEC (#)
------------------------	---------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

## Example

The following example shows how to verify if the APs have been authorized by the AP certificate policy:

```
Device# show ap auth-list ap-cert-policy
```

# show ap auto-rf

To display the auto-RF settings for a Cisco lightweight access point, use the **show ap auto-rf** command.

```
show ap auto-rf dot11 { 24ghz | 5ghz | dual-band } cisco_ap
```

Syntax Description	24ghz	Specifies the 802.11b AP.
	5ghz	Specifies the 802.11a AP.
	dual-band	Specifies dual bands.

Command Default	None
-----------------	------

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.12.1

**Usage Guidelines** The **show ap auto-rf command** output will not display neighbor AP names.

The following example shows how to display auto-RF information for an access point:

```
Device# show ap auto-rf dot11 24ghz AP1
#####
Number of Slots                : 3
AP Name                        : APA023.9FD8.EA22
MAC Address                    : 40ce.24bf.8ca0
Ethernet MAC Address          : a023.9fd8.ea22
  Slot ID                      : 0
  Radio Type                   : 802.11n - 2.4 GHz
  Current TX/RX Band           : 2.4Ghz band
  Subband Type                 : All
  Noise Information
    Noise Profile              : Passed
    Channel 1                  : -91 dBm
    Channel 2                  : -67 dBm
    Channel 3                  : -54 dBm
    Channel 4                  : -55 dBm
    Channel 5                  : -71 dBm
    Channel 6                  : -85 dBm
    Channel 7                  : -50 dBm
    Channel 8                  : -54 dBm
    Channel 9                  : -77 dBm
    Channel 10                 : -88 dBm
    Channel 11                 : -65 dBm
  Interference Information
    Interference Profile       : Failed
    Channel 1                  : -47 dBm @ 21% busy
    Channel 2                  : -45 dBm @ 2% busy
    Channel 3                  : -128 dBm @ 0% busy
    Channel 4                  : -128 dBm @ 0% busy
    Channel 5                  : -48 dBm @ 2% busy
    Channel 6                  : -45 dBm @ 2% busy
```

```

Channel 7 : -42 dBm @ 3% busy
Channel 8 : -128 dBm @ 0% busy
Channel 9 : -128 dBm @ 0% busy
Channel 10 : -39 dBm @ 3% busy
Channel 11 : -46 dBm @ 3% busy
Rogue Histogram (20)
  Channel 1 : 36
  Channel 2 : 0
  Channel 3 : 0
  Channel 4 : 1
  Channel 5 : 0
  Channel 6 : 11
  Channel 7 : 0
  Channel 8 : 1
  Channel 9 : 3
  Channel 10 : 0
  Channel 11 : 14
Load Information
  Load Profile : Failed
  Receive Utilization : 0%
  Transmit Utilization : 0%
  Channel Utilization : 98%
  Attached Clients : 0 clients
Coverage Information
  Coverage Profile : Passed
  Failed Clients : 0 clients
Client Signal Strengths
  RSSI -100 dBm : 0 clients
  RSSI -92 dBm : 0 clients
  RSSI -84 dBm : 0 clients
  RSSI -76 dBm : 0 clients
  RSSI -68 dBm : 0 clients
  RSSI -60 dBm : 0 clients
  RSSI -52 dBm : 0 clients
Client Signal to Noise Ratios
  SNR 0 dB : 0 clients
  SNR 5 dB : 0 clients
  SNR 10 dB : 0 clients
  SNR 15 dB : 0 clients
  SNR 20 dB : 0 clients
  SNR 25 dB : 0 clients
  SNR 30 dB : 0 clients
  SNR 35 dB : 0 clients
  SNR 40 dB : 0 clients
  SNR 45 dB : 0 clients
Nearby APs
  AP d0ec.3572.b9a0 slot 0 : -23 dBm on ( 11, 20 MHz) (181.22.0.22)
  AP 0c75.bdb3.9000 slot 0 : -28 dBm on ( 11, 20 MHz) (181.21.0.21)
  AP a4b2.3980.3740 slot 0 : -28 dBm on ( 1, 20 MHz) (181.21.0.21)
  AP d0ec.3576.8320 slot 0 : -33 dBm on ( 11, 20 MHz) (50.1.1.122)
  AP a0f8.49dc.9780 slot 0 : -34 dBm on ( 1, 20 MHz) (9.9.57.94)
  AP a0f8.49dc.8260 slot 0 : -34 dBm on ( 6, 20 MHz) (9.9.57.94)
  AP d0ec.3573.7c80 slot 0 : -36 dBm on ( 6, 20 MHz) (192.185.183.44)

  AP 00b0.e192.9d20 slot 0 : -36 dBm on ( 11, 20 MHz) (9.9.42.47)
  AP a4b2.397f.41c0 slot 0 : -36 dBm on ( 1, 20 MHz) (185.10.0.10)
  AP 2c5a.0fd5.b8c0 slot 0 : -36 dBm on ( 6, 20 MHz) (9.7.97.51)
  AP a488.7351.4740 slot 0 : -36 dBm on ( 11, 20 MHz) (9.7.97.51)
  AP 10b3.d5e9.c8e0 slot 0 : -36 dBm on ( 1, 20 MHz) (50.1.1.122)
  AP 0c75.bdb3.ab00 slot 0 : -37 dBm on ( 6, 20 MHz) (185.10.0.10)
  AP 68ca.e451.5120 slot 0 : -37 dBm on ( 1, 20 MHz) (9.4.155.15)
  AP a0f8.49dc.97a0 slot 0 : -37 dBm on ( 11, 20 MHz) (9.9.57.94)
  AP 188b.4501.7940 slot 0 : -38 dBm on ( 11, 20 MHz) (9.9.57.94)
  AP 002c.c88a.f8e0 slot 0 : -38 dBm on ( 11, 20 MHz) (9.9.50.55)

```

```

AP 7069.5a78.4960 slot 0           : -38 dBm on ( 11, 20 MHz) (9.7.97.51)
AP 3c41.0ea7.0880 slot 0           : -39 dBm on ( 11, 20 MHz) (185.10.0.10)
AP a0f8.49dc.93a0 slot 0           : -39 dBm on ( 6, 20 MHz) (9.9.57.94)
AP f4db.e685.7360 slot 0           : -39 dBm on ( 6, 20 MHz) (50.1.1.122)
AP 7070.8bb4.4120 slot 0           : -40 dBm on ( 11, 20 MHz) (9.9.57.94)
AP 707d.b93e.39e0 slot 0           : -40 dBm on ( 1, 20 MHz) (4.4.4.1)
AP 706d.150c.6860 slot 0           : -40 dBm on ( 11, 20 MHz) (50.1.1.122)
Radar Information
Channel Assignment Information via DCA
  Current Channel Average Energy      : -50 dBm
  Previous Channel Average Energy     : -50 dBm
  Channel Change Count                : 9
  Last Channel Change Time            : 02/14/2021 20:54:57
  Recommended Best Channel           : 1
RF Parameter Recommendations
  Power Level                         : 8
  RTS/CTS Threshold                   : 2347
  Fragmentation Threshold             : 2346
  Antenna Pattern                     : 0
Persistent Interference Devices
Class Type          Channel  DC (%)  RSSI (dBm)  Last Update Time
-----
All third party trademarks are the property of their respective owners.

```

# show ap config

To display configuration settings for all access points that join the device, use the **show ap config** command.

**show ap config** {general | slots}

Syntax Description	
<b>ethernet</b>	Displays ethernet related information for all Cisco APs.
<b>general</b>	Displays common information for all Cisco APs.
<b>slots</b>	Displays configuration information for all slots of all Cisco APs.

**Command Default** None

**Command Modes** Any command mode

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

This example shows how to display global syslog server settings:

```
Device# show ap config general
Cisco AP Name      : APA023.9FAE.E190
=====
Cisco AP Identifier      : 40ce.24f7.50e0
Country Code            : US
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-AB
AP Country Code        : US - United States
AP Regulatory Domain
  Slot 0                : -B
  Slot 1                : -B
MAC Address             : a023.9fae.e190
IP Address Configuration : DHCP
IP Address              : 9.12.33.244
IP Netmask              : 255.255.255.0
Gateway IP Address      : 9.12.33.1
Fallback IP Address Being Used :
Domain                  :
Name Server             :
CAPWAP Path MTU        : 1485
Capwap Active Window Size : 1
Telnet State           : Disabled
SSH State               : Disabled
Cisco AP Location      : default location
Site Tag Name          : default-site-tag
RF Tag Name            : default-rf-tag
Policy Tag Name        : default-policy-tag
AP join Profile        : default-ap-profile
Flex Profile           : default-flex-profile
Primary Cisco Controller Name : ewlc-doc-17.1.1
Primary Cisco Controller IP Address : 9.12.35.10
Secondary Cisco Controller Name : Doc-86
Secondary Cisco Controller IP Address : 9.12.33.10
Tertiary Cisco Controller Name : Cisco-docwlc-85
```



```
Tertiary Cisco Controller IP Address      : 9.12.35.16
Administrative State                      : Enabled
Operation State                           : Registered
NAT External IP Address                  : 9.12.33.244
AP Certificate type                       : Manufacturer Installed Certificate
AP Mode                                  : Local
AP VLAN tagging state                    : Disabled
AP VLAN tag                              : 0
.
.
.
```

## show ap crash-file

To display the list of both crash and radio core dump files generated by lightweight access points, use the **show ap crash-file** command.

**show ap crash-file***chassis chassis-number <1-2>***active standby**

Syntax Description		
<b>chassis</b>	Displays the chassis details.	
<i>chassis-number</i>	Specifies the chassis number, either 1 or 2.	
<b>active</b>	Specifies an active instance.	
<b>standby</b>	Specifies a standby instance.	
Command Default	None	
Command Modes	Any command mode	
Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

This example shows how to display the crash file generated by the access point:

```
Device# show ap crash-file
```

# show ap dot11

To view 802.11a or 802.11b configuration information, use the **show ap dot11** command.

```
show ap dot11 {24ghz | 5ghz} {channel | coverage | group | load-info | logging | media-stream | monitor
| network | profile | summary | txpower | }
```

Syntax	Description				
<b>24ghz</b>	Specifies the 2.4 GHz band.				
<b>5ghz</b>	Specifies the 5 GHz band.				
<b>channel</b>	Displays the automatic channel assignment configuration and statistics.				
<b>coverage</b>	Displays the configuration and statistics for coverage hole detection.				
<b>group</b>	Displays 802.11a or 802.11b Cisco radio RF grouping.				
<b>load-info</b>	Displays channel utilization and client count information for all Cisco APs.				
<b>logging</b>	Displays 802.11a or 802.11b RF event and performance logging.				
<b>media-stream</b>	Display 802.11a or 802.11b Media Resource Reservation Control configurations.				
<b>monitor</b>	Displays the 802.11a or 802.11b default Cisco radio monitoring.				
<b>network</b>	Displays the 802.11a or 802.11b network configuration.				
<b>profile</b>	Displays the 802.11a or 802.11b lightweight access point performance profiles.				
<b>receiver</b>	Displays the configuration and statistics of the 802.11a or 802.11b receiver.				
<b>summary</b>	Displays the 802.11a or 802.11b Cisco lightweight access point name, channel, and transmit level summary.				
<b>txpower</b>	Displays the 802.11a or 802.11b automatic transmit power assignment.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Any command mode				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.2s</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.				

This example shows how to display the automatic channel assignment configuration and statistics:

```

Device# show ap dot11 5ghz channel
Automatic Channel Assignment
  Channel Assignment Mode           : AUTO
  Channel Update Interval          : 12 Hours
  Anchor time (Hour of the day)    : 20
  Channel Update Contribution      : SNI.
  Channel Assignment Leader        : web (9.9.9.2)
  Last Run                         : 13105 seconds ago
  DCA Sensitivity Level            : MEDIUM (15 dB)
  DCA 802.11n Channel Width       : 40 Mhz
  Channel Energy Levels
    Minimum                       : unknown
    Average                       : unknown
    Maximum                       : unknown
  Channel Dwell Times
    Minimum                       : unknown
    Average                       : unknown
    Maximum                       : unknown
  802.11a 5 GHz Auto-RF Channel List
  Allowed Channel List             : 36,40,44,48,52,56,60,64,149,153,1
57,161
  Unused Channel List              : 100,104,108,112,116,132,136,140,1
65
  802.11a 4.9 GHz Auto-RF Channel List
  Allowed Channel List             :
  Unused Channel List              : 1,2,3,4,5,6,7,8,9,10,11,12,13,14,
15,16,17,18,19,20,21,22,23,24,25,26
  DCA Outdoor AP option            : Disabled

```

This example shows how to display the statistics for coverage hole detection:

```

Device# show ap dot11 5ghz coverage
Coverage Hole Detection
  802.11a Coverage Hole Detection Mode : Enabled
  802.11a Coverage Voice Packet Count  : 100 packet(s)
  802.11a Coverage Voice Packet Percentage : 50 %
  802.11a Coverage Voice RSSI Threshold : -80dBm
  802.11a Coverage Data Packet Count    : 50 packet(s)
  802.11a Coverage Data Packet Percentage : 50 %
  802.11a Coverage Data RSSI Threshold  : -80dBm
  802.11a Global coverage exception level : 25
  802.11a Global client minimum exception level : 3 clients

```

This example shows how to display Cisco radio RF group settings:

```

Device# show ap dot11 5ghz group
Radio RF Grouping

  802.11a Group Mode                : STATIC
  802.11a Group Update Interval     : 600 seconds
  802.11a Group Leader              : web (10.10.10.1)
  802.11a Group Member              : web(10.10.10.1)
                                     nb1(172.13.21.45) (*Unreachable)
  802.11a Last Run                  : 438 seconds ago

  Mobility Agents RF membership information
  -----
  No of 802.11a MA RF-members : 0

```

This example shows how to display 802.11a RF event and performance logging:

```
Device# show ap dot11 5ghz logging
RF Event and Performance Logging

Channel Update Logging           : Off
Coverage Profile Logging        : Off
Foreign Profile Logging         : Off
Load Profile Logging            : Off
Noise Profile Logging           : Off
Performance Profile Logging     : Off
TxPower Update Logging          : Off
```

This example shows how to display the 802.11a media stream configuration:

```
Device# show ap dot11 5ghz media-stream
Multicast-direct                 : Disabled
Best Effort                      : Disabled
Video Re-Direct                 : Disabled
Max Allowed Streams Per Radio    : Auto
Max Allowed Streams Per Client  : Auto
Max Video Bandwidth              : 0
Max Voice Bandwidth              : 75
Max Media Bandwidth              : 85
Min PHY Rate (Kbps)              : 6000
Max Retry Percentage             : 80
```

This example shows how to display the radio monitoring for the 802.11b network:

```
Device# show ap dot11 5ghz monitor
Default 802.11a AP monitoring

802.11a Monitor Mode              : Enabled
802.11a Monitor Mode for Mesh AP Backhaul : disabled
802.11a Monitor Channels          : Country channels
802.11a RRM Neighbor Discover Type : Transparent
802.11a AP Coverage Interval     : 180 seconds
802.11a AP Load Interval         : 60 seconds
802.11a AP Noise Interval        : 180 seconds
802.11a AP Signal Strength Interval : 60 seconds
```

This example shows how to display the global configuration and statistics of an 802.11a profile:

```
Device# show ap dot11 5ghz profile
Default 802.11a AP performance profiles
802.11a Global Interference threshold..... 10%
802.11a Global noise threshold..... -70 dBm
802.11a Global RF utilization threshold..... 80%
802.11a Global throughput threshold..... 1000000 bps
802.11a Global clients threshold..... 12 clients
802.11a Global coverage threshold..... 12 dB
802.11a Global coverage exception level..... 80%
802.11a Global client minimum exception lev..... 3 clients
```

This example shows how to display the network configuration of an 802.11a profile:

```
Device# show ap dot11 5ghz network
802.11a Network : Enabled
11nSupport : Enabled
 802.11a Low Band : Enabled
 802.11a Mid Band : Enabled
 802.11a High Band : Enabled
```

```
802.11a Operational Rates
 802.11a 6M : Mandatory
 802.11a 9M : Supported
 802.11a 12M : Mandatory
 802.11a 18M : Supported
 802.11a 24M : Mandatory
 802.11a 36M : Supported
 802.11a 48M : Supported
 802.11a 54M : Supported
802.11n MCS Settings:
MCS 0 : Supported
MCS 1 : Supported
MCS 2 : Supported
MCS 3 : Supported
MCS 4 : Supported
MCS 5 : Supported
MCS 6 : Supported
MCS 7 : Supported
MCS 8 : Supported
MCS 9 : Supported
MCS 10 : Supported
MCS 11 : Supported
MCS 12 : Supported
MCS 13 : Supported
MCS 14 : Supported
MCS 15 : Supported
MCS 16 : Supported
MCS 17 : Supported
MCS 18 : Supported
MCS 19 : Supported
MCS 20 : Supported
MCS 21 : Supported
MCS 22 : Supported
MCS 23 : Supported
802.11n Status:
A-MPDU Tx:
  Priority 0 : Enabled
  Priority 1 : Disabled
  Priority 2 : Disabled
  Priority 3 : Disabled
  Priority 4 : Enabled
  Priority 5 : Enabled
  Priority 6 : Disabled
  Priority 7 : Disabled
A-MSDU Tx:
  Priority 0 : Enabled
  Priority 1 : Enabled
  Priority 2 : Enabled
  Priority 3 : Enabled
  Priority 4 : Enabled
  Priority 5 : Enabled
  Priority 6 : Disabled
  Priority 7 : Disabled
Guard Interval : Any
Rifs Rx : Enabled
Beacon Interval : 100
CF Pollable mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 36
Default Tx Power Level : 1
DTPC Status : Enabled
```

```

Fragmentation Threshold : 2346
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
TI Threshold : 0
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type check : default-wmm
Call Admission Control (CAC) configuration
Voice AC
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size : 84000
  Voice Max-Streams : 2
  Voice Max RF Bandwidth : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode : Enabled
  Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
  SIP based CAC : Disabled
  SIP call bandwidth : 64
  SIP call bandwidth sample-size : 20
Video AC
  Video AC - Admission control (ACM) : Disabled
  Video max RF bandwidth : Infinite
  Video reserved roaming bandwidth : 0

```

This example shows how to display the global configuration and statistics of an 802.11a profile:

```

Device# show ap dot11 5ghz receiver
Default 802.11a AP performance profiles
802.11a Global Interference threshold..... 10%
802.11a Global noise threshold..... -70 dBm
802.11a Global RF utilization threshold..... 80%
802.11a Global throughput threshold..... 1000000 bps
802.11a Global clients threshold..... 12 clients
802.11a Global coverage threshold..... 12 dB
802.11a Global coverage exception level..... 80%
802.11a Global client minimum exception lev..... 3 clients

```

This example shows how to display the global configuration and statistics of an 802.11a profile:

```

Device# show ap dot11 5ghz service-policy

```

This example shows how to display a summary of the 802.11b access point settings:

```

Device# show ap dot11 5ghz summary
AP Name MAC Address Admin State Operation State Channel TxPower
-----
CJ-1240 00:21:1b:ea:36:60 ENABLED UP 161 1 ( )
CJ-1130 00:1f:ca:cf:b6:60 ENABLED UP 56* 1 (*)

```

This example shows how to display the configuration and statistics of the 802.11a transmit power cost:

```

Device# show ap dot11 5ghz txpower
Automatic Transmit Power Assignment

Transmit Power Assignment Mode : AUTO
Transmit Power Update Interval : 600 seconds
Transmit Power Threshold : -70 dBm
Transmit Power Neighbor Count : 3 APs
Min Transmit Power : -10 dBm

```

```
Max Transmit Power           : 30 dBm
Transmit Power Update Contribution : SNI.
Transmit Power Assignment Leader : web (10.10.10.1)
Last Run                     : 437 seconds ago
```

This example shows how to display the configuration and statistics of the 802.11a transmit power cost:

```
Device# show ap dot11 5ghz ccx global
802.11a Client Beacon Measurements:
    disabled
```



# show ap dot11

To display 802.11 band parameters, use the **show ap dot11** command.

```
show ap dot11 {24ghz | 5ghz} {media-stream rrc}
```

<b>Syntax Description</b>	<b>media-stream rrc</b> Displays Media Stream configurations.
<b>Command Default</b>	None
<b>Command Modes</b>	User EXEC command mode or Privileged EXEC command mode
<b>Usage Guidelines</b>	None.

The following is a sample output of the **show ap dot11 24ghz media-stream rrc** command.

```
Device#show ap dot11 24ghz media-stream rrc

Multicast-direct           : Disabled
Best Effort                 : Disabled
Video Re-Direct            : Disabled
Max Allowed Streams Per Radio : Auto
Max Allowed Streams Per Client : Auto
Max Video Bandwidth         : 0
Max Voice Bandwidth         : 75
Max Media Bandwidth         : 85
Min PHY Rate (Kbps)         : 6000
Max Retry Percentage        : 80
```

# show ap dot11 24ghz

To display the 2.4 GHz RRM parameters, use the **show ap dot11 24ghz** command.

**show ap dot11 24ghz** {**channel** | **coverage** | **group** | **logging** | **monitor** | **profile** | **summary** | **txpower**}

Syntax Description	
<b>ccx</b>	Displays the 802.11b CCX information for all Cisco APs.
<b>channel</b>	Displays the configuration and statistics of the 802.11b channel assignment.
<b>coverage</b>	Displays the configuration and statistics of the 802.11b coverage.
<b>group</b>	Displays the configuration and statistics of the 802.11b grouping.
<b>l2roam</b>	Displays 802.11b l2roam information.
<b>logging</b>	Displays the configuration and statistics of the 802.11b event logging.
<b>monitor</b>	Displays the configuration and statistics of the 802.11b monitoring.
<b>profile</b>	Displays 802.11b profiling information for all Cisco APs.
<b>receiver</b>	Displays the configuration and statistics of the 802.11b receiver.
<b>summary</b>	Displays the configuration and statistics of the 802.11b Cisco APs.
<b>txpower</b>	Displays the configuration and statistics of the 802.11b transmit power control.

**Command Default** None.

**Command Modes** Global configuration.

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

**Usage Guidelines** None.

This example shows how to display configuration and statistics of the 802.11b coverage.

```
Device#show ap dot11 24ghz coverage
```

```
Coverage Hole Detection
 802.11b Coverage Hole Detection Mode      : Enabled
 802.11b Coverage Voice Packet Count      : 100 packet(s)
 802.11b Coverage Voice Packet Percentage : 50%
 802.11b Coverage Voice RSSI Threshold    : -80 dBm
 802.11b Coverage Data Packet Count       : 50 packet(s)
 802.11b Coverage Data Packet Percentage  : 50%
 802.11b Coverage Data RSSI Threshold     : -80 dBm
 802.11b Global coverage exception level   : 25 %
 802.11b Global client minimum exception level : 3 clients
```

## show ap dot11 24ghz SI config

To see the spectrum intelligence (SI) configuration details for the 2.4-GHz band, use the **show ap dot11 24ghz SI config** command.

```
show ap dot11 24ghz SI config [chassis {chassis-number | active | standby} R0]
```

<b>Syntax Description</b>	<i>chassis-number</i> Chassis number as either 1 or 2.				
<b>active R0</b>	Active instance of the configuration in Route-processor slot 0.				
<b>standby R0</b>	Standby instance of the configuration in Route-processor slot 0.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Privileged EXEC				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.
Release	Modification				
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.				

### Examples

The following example shows how to see the SI configuration details for the 2.4-GHz band:

```
Device# show ap dot11 24ghz SI config chassis 1 R0
```

## show ap dot11 24ghz SI device type

To see the spectrum intelligence (SI) interferers of different types for the 2.4-GHz band, use the **show ap dot11 24ghz SI device type** command.

```
show ap dot11 24ghz SI device type {cont_tx | mw_oven | si_fhss} [chassis {chassis-number
| active | standby} R0]
```

### Syntax Description

<b>cont_tx</b>	SI interferers of type Continuous transmitter for the 2.4-GHz band.
<b>mw_oven</b>	SI interferers of type microwave oven for the 2.4-GHz band.
<b>si_fhss</b>	SI interferers of type Frequency Hopping Spread Spectrum for the 2.4-GHz band.
<i>chassis-number</i>	Enter the chassis number as either 1 or 2.
<b>active R0</b>	Active instance of the configuration in Route-processor slot 0.
<b>standby R0</b>	Standby instance of the configuration in Route-processor slot 0.

### Command Default

None

### Command Modes

Privileged EXEC

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

### Examples

The following example shows how to see the details of SI interferers of type microwave oven in the 2.4-GHz band:

```
Device# show ap dot11 24ghz SI device type mw_oven chassis 1 R0
```

# show ap dot11 5ghz

To display the 5GHz RRM parameters, use the **show ap dot11 5ghz** command.

**show ap dot11 5ghz** {**channel** | **coverage** | **group** | **logging** | **monitor** | **profile** | **summary** | **txpower**}

Syntax Description	
<b>ccx</b>	Displays the 802.11a CCX information for all Cisco APs.
<b>channel</b>	Displays the configuration and statistics of the 802.11a channel assignment.
<b>coverage</b>	Displays the configuration and statistics of the 802.11a coverage.
<b>group</b>	Displays the configuration and statistics of the 802.11a grouping.
<b>l2roam</b>	Displays 802.11a l2roam information.
<b>logging</b>	Displays the configuration and statistics of the 802.11a event logging.
<b>monitor</b>	Displays the configuration and statistics of the 802.11a monitoring.
<b>profile</b>	Displays 802.11a profiling information for all Cisco APs.
<b>receiver</b>	Displays the configuration and statistics of the 802.11a receiver.
<b>summary</b>	Displays the configuration and statistics of the 802.11a Cisco APs.
<b>txpower</b>	Displays the configuration and statistics of the 802.11a transmit power control.

**Command Default** None.

**Command Modes** Global configuration.

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

**Usage Guidelines** None.

This example shows configuration and statistics of 802.11a channel assignment.

```
Device#show ap dot11 5ghz channel
```

```
Automatic Channel Assignment
  Channel Assignment Mode      : AUTO
  Channel Update Interval     : 12 Hours
  Anchor time (Hour of the day) : 20
  Channel Update Contribution : SNI..
  Channel Assignment Leader    : web (9.9.9.2)
  Last Run                    : 16534 seconds ago
  DCA Sensitivity Level        : MEDIUM (15 dB)
  DCA 802.11n Channel Width    : 40 Mhz
  Channel Energy Levels
    Minimum                    : unknown
```

```
Average : unknown
Maximum : unknown
Channel Dwell Times
  Minimum : unknown
  Average : unknown
  Maximum : unknown
802.11a 5 GHz Auto-RF Channel List
Allowed Channel List : 36,40,44,48,52,56,60,64,149,153,1
                    57,161
Unused Channel List : 100,104,108,112,116,132,136,140,1
                    65
802.11a 4.9 GHz Auto-RF Channel List
Allowed Channel List :
Unused Channel List : 1,2,3,4,5,6,7,8,9,10,11,12,13,14,
                    15,16,17,18,19,20,21,22,23,24,25,26
DCA Outdoor AP option : Disabled
```

# show ap dot11 24ghz cleanair air-quality

To display the air-quality summary information and air-quality worst information for the 802.11 networks, use the **show ap dot11 cleanair** command.

```
show ap dot11 {24ghz | 5ghz | dual-band} cleanair{air-quality | config | device | summary}
```

Syntax Description		
<b>24ghz</b>	Displays the 2.4 GHz band.	
<b>5ghz</b>	Displays the 5 GHz band.	
<b>dual-band</b>	Displays 802.11 dual-band radios.	
<b>cleanair</b>	Displays cleanair configurations.	
<b>air-quality</b>	Displays the Cleanair Air-Quality (AQ) data for 2.4GHz band.	
<b>device</b>	Displays the CleanAir Interferers of device for 2.4GHz band.	
<b>config</b>	Displays CleanAir Configuration for 2.4GHz band.	
<b>summary</b>	Displays cleanair configurations for all 802.11a Cisco APs.	

**Command Default** None

**Command Modes** Any command mode

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

This example shows how to display the worst air-quality information for the 5 GHz band:

```
Device# show ap dot11 5ghz cleanair air-quality worst
```

```
AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel Avg AQ Min AQ Interferers DFS
-----
CISCO_AP3500 36      95      70      0          40
```

This example shows how to display the worst air-quality information for the 2.4 GHz band:

```
Device# show ap dot11 24ghz cleanair air-quality worst
```

```
AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel Avg AQ Min AQ Interferers DFS
-----
CISCO_AP3500 1        83      57      3          5
```

# show ap dot11 24ghz cleanair air-quality

To display the air-quality summary information and air-quality worst information for the 802.11 networks, use the **show ap dot11 cleanair air-quality** command.

**show ap dot11 {24ghz | 5ghz} cleanair air-quality {summary | worst}**

Syntax Description	Option	Description
	<b>24ghz</b>	Displays the 2.4 GHz band.
	<b>5ghz</b>	Displays the 5 GHz band.
	<b>summary</b>	Displays a summary of 802.11 radio band air-quality information.
	<b>worst</b>	Displays the worst air-quality information for 802.11 networks.

**Command Default** None

**Command Modes** Any command mode

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

This example shows how to display the worst air-quality information for the 5 GHz band:

```
Device# show ap dot11 5ghz cleanair air-quality worst
```

```
AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel Avg AQ Min AQ Interferers DFS
-----
CISCO_AP3500 36      95    70    0          40
```

This example shows how to display the worst air-quality information for the 2.4 GHz band:

```
Device# show ap dot11 24ghz cleanair air-quality worst
```

```
AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel Avg AQ Min AQ Interferers DFS
-----
CISCO_AP3500 1        83    57    3          5
```



# show ap dot11 cleanair config

To display the CleanAir configuration for the 802.11 networks, use the **show ap dot11 cleanair config** command.

**show ap dot11 {24ghz | 5ghz} cleanair config**

<b>Syntax Description</b>	<b>24ghz</b> Displays the 2.4 GHz band.				
	<b>5ghz</b> Displays the 5 GHz band.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Any command mode				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.				

This example shows how to display the CleanAir configuration for the 2.4 GHz band:

```

Device# show ap dot11 24ghz cleanair config
Clean Air Solution..... : Disabled
Air Quality Settings:
  Air Quality Reporting..... : Disabled
  Air Quality Reporting Period (min)..... : 15
  Air Quality Alarms..... : Enabled
  Air Quality Alarm Threshold..... : 10
Interference Device Settings:
  Interference Device Reporting..... : Enabled
  Bluetooth Link..... : Enabled
  Microwave Oven..... : Enabled
  802.11 FH..... : Enabled
  Bluetooth Discovery..... : Enabled
  TDD Transmitter..... : Enabled
  Jammer..... : Enabled
  Continuous Transmitter..... : Enabled
  DECT-like Phone..... : Enabled
  Video Camera..... : Enabled
  802.15.4..... : Enabled
  WiFi Inverted..... : Enabled
  WiFi Invalid Channel..... : Enabled
  SuperAG..... : Enabled
  Canopy..... : Enabled
  Microsoft Device..... : Enabled
  WiMax Mobile..... : Enabled
  WiMax Fixed..... : Enabled
Interference Device Types Triggering Alarms:
  Bluetooth Link..... : Disabled
  Microwave Oven..... : Disabled
  802.11 FH..... : Disabled
  Bluetooth Discovery..... : Disabled
  TDD Transmitter..... : Disabled
  Jammer..... : Disabled
  Continuous Transmitter..... : Disabled
  DECT-like Phone..... : Disabled
    
```

```
Video Camera..... : Disabled
802.15.4..... : Disabled
WiFi Inverted..... : Enabled
WiFi Invalid Channel..... : Enabled
SuperAG..... : Disabled
Canopy..... : Disabled
Microsoft Device..... : Disabled
WiMax Mobile..... : Disabled
WiMax Fixed..... : Disabled
Interference Device Alarms..... : Enabled
Additional Clean Air Settings:
CleanAir Event-driven RRM State..... : Disabled
CleanAir Driven RRM Sensitivity..... : LOW
CleanAir Persistent Devices state..... : Disabled
```

## show ap dot11 cleanair summary

To view CleanAir configurations for all 802.11a Cisco APs, use the **show ap dot11 cleanair summary** command.

```
show ap dot11 {24ghz | 5ghz} cleanair summary
```

<b>Syntax Description</b>	<b>24ghz</b>	Specifies the 2.4-GHz band
	<b>5ghz</b>	Specifies the 5-GHz band
	<b>cleanair summary</b>	Summary of CleanAir configurations for all 802.11a Cisco APs
<b>Command Default</b>	None	
<b>Command Modes</b>	Any command mode	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

# show ap dot11 dual-band summary

To view a brief summary of access points with dual-band radios, use the **show ap dot11 dual-band summary** command.

**show ap dot11 dual-band summary**

---

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--------------------------------------------

---

---

<b>Command Default</b>	None
------------------------	------

---

---

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

---

---

<b>Command History</b>	
------------------------	--

---

## Example

The following example shows how to view brief summary of tag names:

```
Device# show ap dot11 dual-band summary
```

# show ap environment

To see the AP environment information of all APs, use the **show ap environment** command.

**show ap environment** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

*chassis-number* Enter the chassis number as either 1 or 2.

**active R0** Active instance of the AP filters in Route-processor slot 0.

**standby R0** Standby instance of the AP filters in Route-processor slot 0.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to see the AP environment information:

```
Device# show ap environment
```

# show ap filters active

To see the details of active AP filters, use the **show ap filters active** command.

**show ap filters active** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

*chassis-number* Chassis number as either 1 or 2.

**active R0** Active instance of the active AP filters in Route-processor slot 0.

**standby R0** Standby instance of the active AP filters in Route-processor slot 0.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to see the details of the active AP filters for the active instance:

```
Device# show ap filters active chassis active R0
```

# show ap filters all

To see the details of all AP filters, use the **show ap filters all** command.

**show ap filters all** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

*chassis-number* Enter the chassis number as either 1 or 2.

**active R0** Active instance of the AP filters in Route-processor slot 0.

**standby R0** Standby instance of the AP filters in Route-processor slot 0.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to see the details of all the AP filters for the active instance:

```
Device# show ap filters all chassis active R0
```

# show ap fra

To see the flexible radio assignment (FRA) configurations in APs, use the **show ap fra** command.

**show ap fra** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

*chassis-number* Chassis number as either 1 or 2.

**active R0** Active instance in Route-processor slot 0.

**standby R0** Standby instance in Route-processor slot 0.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to see the FRA configurations in APs:

```
Device# show ap fra
```



# show ap gps location

To see the GPS location of all APs, use the **show ap gps location** command.

**show ap gps location** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

*chassis-number* Enter the chassis number as either 1 or 2.

**active R0** Active instance of the AP filters in Route-processor slot 0.

**standby R0** Standby instance of the AP filters in Route-processor slot 0.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to see the GPS location of all APs:

```
Device# show ap gps location
```

# show history channel interface dot11Radio all

To check channel change or trigger reason and history, use the **show history channel interface dot11Radio all** command.

**show history channel interface dot11Radio all**

<b>Syntax Description</b>	This command has no keywords or arguments.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC (#)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

## Examples

This example shows how to check channel change or trigger reason and history:

```
Device# show history channel interface dot11Radio all

          Timestamp Slot Client count Channel Trigger
Fri May 31 12:57:04 2019    0         0      11 RRM-DCA
Fri May 31 13:10:02 2019    0         0       1 RRM-DCA
Fri May 31 12:57:04 2019    1         0       60 Manual
Fri May 31 13:00:16 2019    1         0      149   DFS
```

## show ap link-encryption

To display the link encryption status, use the **show ap link-encryption** command.

```
show ap link-encryption [{chassis | {chassis-number | active | standby} | R0}]
```

### Syntax Description

*chassis-number* Chassis number as either 1 or 2.

**active R0** Active instance in Route-processor slot 0.

**standby R0** Standby instance in Route-processor slot 0.

### Command Default

None

### Command Modes

Any command mode

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

This example show how to display the link-encryption status:

```
Device# show Cisco IOS XE Gibraltar 16.12.2s link-encryption
```

# show ap lldp neighbors detail

To view the details of the AP Link Layer Discovery Protocol (LLDP) neighbor information on the controller, when the AP is connected to the third-party switch.

## show ap lldp neighbors detail

<b>Syntax Description</b>	This command has no arguments.	
<b>Command Default</b>	None	
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.
<b>Usage Guidelines</b>	None	

## Example

The following example shows how to view the details of AP Link Layer Discovery Protocol (LLDP) neighbor information on the controller, when the AP is connected to the third-party switch:

```
Device# show ap lldp neighbors detail
Number of neighbors: 1
AP Name           : 9130-ap1
AP Interface      : GigabitEthernet0
-----
Neighbor MAC      : c89c.1db1.1f80
Neighbor Name     : flex-ctrl-switch
System Description : Cisco IOS Software, C3750E Software (C3750E-UNIVERSALK9-M), Version
                  15.2(4)E6, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Thu 05-Apr-18 02:22 by prod_rel_team
Port ID           : Gi1/0/15
Port Description  : 9130-ap2
Chassis Alias     :
Management Addresses :
  IPv4 address    : None
  IPv6 address    : None
Capabilities      :
  Bridge
  Router
Last updated time : 12/02/2020 09:15:48
```

# show ap lldp neighbors

To view the AP Link Layer Discovery Protocol (LLDP) neighbor information on the controller, when the AP is connected to the third-party switch.

## show ap lldp neighbors

<b>Syntax Description</b>	This command has no arguments.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.
<b>Usage Guidelines</b>	None	

## Example

The following example shows how to view the AP Link Layer Discovery Protocol (LLDP) neighbor information on the controller, when the AP is connected to the third-party switch:

```
Device# show ap lldp neighbors
```

```
Capability Codes:
```

```
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device  
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
```

AP Name	AP Interface	Neighbor Name	Neighbor MAC	Port ID	Mgmt. Address	Capabilities	Last updated time
9130-ap1	GigabitEthernet0	switch	cxxx.1dxx.1fxx	Gi1/0/15	None	B R	12/02/2020 09:15:48
9117-ap1	GigabitEthernet0	switch	cxxx.1dxx.1fxx	Gi1/0/19	None	B R	12/02/2020 09:15:47

## show ap name lldp neighbors detail

To view the details of the AP Link Layer Discovery Protocol (LLDP) neighbor information on the controller, for a specific AP, when the AP is connected to the third-party switch.

**show ap name** *ap-name* **lldp neighbors detail**

<b>Syntax Description</b>	This command has no arguments.
---------------------------	--------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

<b>Usage Guidelines</b>	None
-------------------------	------

### Example

The following example shows how to view the details of the AP Link Layer Discovery Protocol (LLDP) neighbor information on the controller, for a specific AP, when the AP is connected to the third-party switch:

```
Device# show ap name 9130-ap1 lldp neighbors detail
AP Name           : 9130-ap1
AP Interface      : GigabitEthernet0
-----
Neighbor MAC      : c89c.1db1.1f80
Neighbor Name     : flex-ctrl-switch
System Description : Cisco IOS Software, C3750E Software (C3750E-UNIVERSALK9-M), Version
                  15.2(4)E6, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Thu 05-Apr-18 02:22 by prod_rel_team
Port ID           : Gi1/0/15
Port Description  : 9130-ap2
Chassis Alias     :
Management Addresses :
  IPv4 address    : None
  IPv6 address    : None
Capabilities      :
  Bridge
  Router
Last updated time : 12/02/2020 09:15:48
```

# show ap name lldp neighbors

To view the AP Link Layer Discovery Protocol (LLDP) neighbor information on the controller, for a specific AP, when the AP is connected to the third-party switch.

**show ap name** *ap-name* **lldp neighbors**

<b>Syntax Description</b>	This command has no arguments.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.
<b>Usage Guidelines</b>	None	

## Example

The following example shows how to view the AP Link Layer Discovery Protocol (LLDP) neighbor information on the controller, for a specific AP, when the AP is connected to the third-party switch:

```
Device# show ap name 9130-ap1 lldp neighbors
AP Name           : 9130-ap1
AP Interface      : GigabitEthernet0
-----
Neighbor MAC      : c89c.1db1.1f80
Neighbor Name     : flex-ctrl-switch
System Description : Cisco IOS Software, C3750E Software (C3750E-UNIVERSALK9-M), Version
                  15.2(4)E6, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Thu 05-Apr-18 02:22 02:22 by prod_rel_team
Port ID           : Gi1/0/15
Port Description  : 9130-ap2
Chassis Alias    :
Management Addresses :
  IPv4 address    : None
  IPv6 address    : None
Capabilities     :
  Bridge
  Router
Last updated time : 12/02/2020 09:15:48
```

# show ap master list

To see the AP master list, use the **show ap master list** command.

```
show ap master list[ {chassis | {chassis-number | active | standby} | R0}]
```

## Syntax Description

*chassis-number* Chassis number as either 1 or 2.

**active R0** Active instance in Route-processor slot 0.

**standby R0** Standby instance in Route-processor slot 0.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to see the AP master list:

```
Device# show ap master list
```



## show ap multicast mom (multicast over multicast)

To verify the multicast mode on the controller, use the **show ap multicast mom** command.

<b>Syntax Description</b>	This command has no keywords and arguments.
---------------------------	---------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.2	This command was introduced.

This example shows how to verify the multicast mode:

```
Device# show ap multicast mom
```

AP Name	MOM-IP	TYPE	MOM-	STATUS
SS-E-1	IPv4		Up	
SS-E-2	IPv4		Up	
9130E-r3-sw2-g1012	IPv4		Up	
9115i-r3-sw2-te1-0-38	IPv4		Up	
AP9120-r3-sw3-Gi1-0-46	IPv4		Up	
ap3800i-r2-sw1-te2-0-2	IPv4		Up	

# show ap name auto-rf

To display the auto-RF settings for a Cisco lightweight access point, use the **show ap name auto-rf** command.

```
show ap name ap-name auto-rf dot11 {24ghz | 5ghz | dual-band}
```

Syntax Description	
<i>ap-name</i>	Name of the Cisco lightweight access point.
<b>24ghz</b>	Displays the 2.4 GHz band.
<b>5ghz</b>	Displays the 5 GHz band.
<b>dual-band</b>	Displays dual band.

**Command Default** None

**Command Modes** Privileged EXEC.

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

This example shows how to display auto-RF information for an access point:

```
Device# show ap name AP01 auto-rf dot11 24ghz

Number of Slots                : 2
AP Name                        : TSIM_AP-1
MAC Address                    : 0000.2000.02f0
Slot ID                        : 0
Radio Type                     : 802.11b/g
Subband Type                   : All

Noise Information
  Noise Profile                : Failed
  Channel 1                    : 24 dBm
  Channel 2                    : 48 dBm
  Channel 3                    : 72 dBm
  Channel 4                    : 96 dBm
  Channel 5                    : 120 dBm
  Channel 6                    : -112 dBm
  Channel 7                    : -88 dBm
  Channel 8                    : -64 dBm
  Channel 9                    : -40 dBm
  Channel 10                   : -16 dBm
  Channel 11                   : 8 dBm

Interference Information
  Interference Profile         : Passed
  Channel 1                    : -128 dBm @ 0% busy
  Channel 2                    : -71 dBm @ 1% busy
  Channel 3                    : -72 dBm @ 1% busy
  Channel 4                    : -73 dBm @ 2% busy
  Channel 5                    : -74 dBm @ 3% busy
  Channel 6                    : -75 dBm @ 4% busy
  Channel 7                    : -76 dBm @ 5% busy
```

```

Channel 8 : -77 dBm @ 5% busy
Channel 9 : -78 dBm @ 6% busy
Channel 10 : -79 dBm @ 7% busy
Channel 11 : -80 dBm @ 8% busy

Rogue Histogram (20/40_ABOVE/40_BELOW)
Channel 36 : 27/ 4/ 0
Channel 40 : 13/ 0/ 0
Channel 44 : 5/ 0/ 0
Channel 48 : 6/ 0/ 1
Channel 52 : 4/ 0/ 0
Channel 56 : 5/ 0/ 0
Channel 60 : 1/ 3/ 0
Channel 64 : 3/ 0/ 0
Channel 100 : 0/ 0/ 0
Channel 104 : 0/ 0/ 0
Channel 108 : 0/ 1/ 0

Load Information
Load Profile : Passed
Receive Utilization : 10%
Transmit Utilization : 20%
Channel Utilization : 50%
Attached Clients : 0 clients

Coverage Information
Coverage Profile : Passed
Failed Clients : 0 clients

Client Signal Strengths
RSSI -100 dBm : 0 clients
RSSI -92 dBm : 0 clients
RSSI -84 dBm : 0 clients
RSSI -76 dBm : 0 clients
RSSI -68 dBm : 0 clients
RSSI -60 dBm : 0 clients
RSSI -52 dBm : 0 clients

Client Signal to Noise Ratios
SNR 0 dB : 0 clients
SNR 5 dB : 0 clients
SNR 10 dB : 0 clients
SNR 15 dB : 0 clients
SNR 20 dB : 0 clients
SNR 25 dB : 0 clients
SNR 30 dB : 0 clients
SNR 35 dB : 0 clients
SNR 40 dB : 0 clients
SNR 45 dB : 0 clients

Nearby APs
AP 0000.2000.0300 slot 0 : -68 dBm on 11 (10.10.10.1)
AP 0000.2000.0400 slot 0 : -68 dBm on 11 (10.10.10.1)
AP 0000.2000.0600 slot 0 : -68 dBm on 11 (10.10.10.1)

Radar Information

Channel Assignment Information
Current Channel Average Energy : 0 dBm
Previous Channel Average Energy : 0 dBm
Channel Change Count : 0
Last Channel Change Time : Wed Oct 17 08:13:36 2012
Recommended Best Channel : 11

```

```
RF Parameter Recommendations
  Power Level                : 1
  RTS/CTS Threshold         : 2347
  Fragmentation Threshold   : 2346
  Antenna Pattern           : 0

Persistent Interference Devices
```

# show ap name ble detail

To display BLE management details, use the **show ap name ble detail** command.

**show ap name** *ap-name* **ble detail**

---

## Syntax Description

*ap-name* Specifies the name of the AP.

---



---

## Command Default

None

---

## Command Modes

Privileged EXEC (#)

---

## Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

---



---

## Usage Guidelines

None

## Example

The following example shows how to display the BLE management details:

```
Device(config)# show ap name ap-name ble detail
```

# show ap name cablemodem

To see cable modem information of an AP, use the **show ap name *ap-name* cablemodem** command.

**show ap name *ap-name* cablemodem** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

<i>ap-name</i>	Name of the AP.
<i>chassis-number</i>	Enter the chassis number as either 1 or 2.
<b>active R0</b>	Active instance of the AP filters in Route-processor slot 0.
<b>standby R0</b>	Standby instance of the AP filters in Route-processor slot 0.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to see cable modem information of an AP:

```
Device# show ap name my-ap cablemodem
```

# show ap name config

To display common information and Ethernet VLAN tagging information for a specific Cisco lightweight access point, use the **show ap name config** command.

```
show ap name ap-name config {ethernet | general}
```

<b>Syntax Description</b>	<i>ap-name</i> Name of the Cisco lightweight access point.				
<b>ethernet</b>	Displays Ethernet tagging configuration information for an access point.				
<b>general</b>	Displays common information for an access point.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Any command mode				
<b>Command History</b>	<table border="1"> <thead> <tr> <th style="border-bottom: 1px solid black;">Release</th> <th style="border-bottom: 1px solid black;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border-bottom: 1px solid black;">Cisco IOS XE Gibraltar 16.12.1</td> <td style="border-bottom: 1px solid black;">This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.				

This example shows how to display Ethernet tagging information for an access point:

```
Device# show ap name AP01 config ethernet
```

```
VLAN Tagging Information for AP01
```

This example shows how to display common information for an access point:

```
Device# show ap name AP01 config general
```

```
Cisco AP Name                : AP01
Cisco AP Identifier          : 5
Country Code                 : US - United States
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-A
AP Country Code              : US - United States
AP Regulatory Domain         : Unconfigured
Switch Port Number          : Tel/0/1
MAC Address                  : 0000.2000.02f0
IP Address Configuration     : Static IP assigned
IP Address                   : 10.10.10.12
IP Netmask                   : 255.255.0.0
Gateway IP Address          : 10.10.10.1
Fallback IP Address Being Used : 10.10.10.12
Domain                       : Cisco
Name Server                  : 0.0.0.0
CAPWAP Path MTU              : 1485
Telnet State                  : Enabled
SSH State                     : Disabled
Cisco AP Location            : sanjose
Cisco AP Group Name          : default-group
Primary Cisco Controller Name : CAPWAP Controller
Primary Cisco Controller IP Address : 10.10.10.1
Secondary Cisco Controller Name :
Secondary Cisco Controller IP Address : Not Configured
```

## show ap name config

```

Tertiary Cisco Controller Name           :
Tertiary Cisco Controller IP Address    : Not Configured
Administrative State                     : Enabled
Operation State                         : Registered
AP Mode                                  : Local
AP Submode                              : Not Configured
Remote AP Debug                          : Disabled
Logging Trap Severity Level             : informational
Software Version                        : 7.4.0.5
Boot Version                            : 7.4.0.5
Stats Reporting Period                  : 180
LED State                                : Enabled
PoE Pre-Standard Switch                 : Disabled
PoE Power Injector MAC Address          : Disabled
Power Type/Mode                         : Power Injector/Normal Mode
Number of Slots                         : 2
AP Model                                 : 1140AG
AP Image                                 : C1140-K9W8-M
IOS Version                             :
Reset Button                            :
AP Serial Number                        : SIM1140K001
AP Certificate Type                     : Manufacture Installed
Management Frame Protection Validation  : Disabled
AP User Mode                            : Customized
AP User Name                            : cisco
AP 802.1X User Mode                    : Not Configured
AP 802.1X User Name                    : Not Configured
Cisco AP System Logging Host            : 255.255.255.255
AP Up Time                              : 15 days 16 hours 19 minutes 57
seconds
AP CAPWAP Up Time                      : 4 minutes 56 seconds
Join Date and Time                     : 10/18/2012 04:48:56
Join Taken Time                        : 15 days 16 hours 15 minutes 0
seconds
Join Priority                           : 1
Ethernet Port Duplex                   : Auto
Ethernet Port Speed                    : Auto
AP Link Latency                        : Disabled
Rogue Detection                        : Disabled
AP TCP MSS Adjust                      : Disabled
AP TCP MSS Size                        : 6146

```



# show ap name config ethernet

To see Ethernet related configuration information of an AP, use the **show ap name *ap-name* config ethernet** command.

**show ap name *ap-name* config ethernet** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

<i>ap-name</i>	Name of the AP.
<i>chassis-number</i>	Enter the chassis number as either 1 or 2.
<b>active R0</b>	Active instance of the AP filters in Route-processor slot 0.
<b>standby R0</b>	Standby instance of the AP filters in Route-processor slot 0.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to see Ethernet related configuration information of an AP:

```
Device# show ap name my-ap config ethernet
```

# show ap name dot11

To display 802.11a or 802.11b configuration information that corresponds to specific Cisco lightweight access points, use the **show ap name dot11** command.

```
show ap name ap-name dot11 {24ghz | 5ghz} {SI | airtime-fairness | call-control | cleanair radio-reset | voice}
```

Syntax Description		
	<i>ap-name</i>	Name of the Cisco lightweight access point.
	<b>24ghz</b>	Displays the 2.4 GHz band.
	<b>5ghz</b>	Displays the 5 GHz band.
	<b>SI</b>	Displays the SI configurations.
	<b>airtime-fairness</b>	Displays the stats of 24Ghz or 5Ghz airtime-fairness.
	<b>call-control</b>	Displays the call control information.
	<b>radio-reset</b>	Displays radio-reset.
	<b>slot</b>	Displays slot information.
	<b>voice</b>	Displays voice information.

**Command Default** None

**Command Modes** Any command mode

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

This example shows how to display the cleanair air-quality that is associated with the access point:

```
Device# show ap name test-ap dot11 24ghz cleanair air-quality chassis active r0
```

# show ap name environment

To see the AP environment information of an AP, use the **show ap name *ap-name* environment** command.

**show ap name *ap-name* environment** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

<i>ap-name</i>	Name of the AP.
<i>chassis-number</i>	Enter the chassis number as either 1 or 2.
<b>active R0</b>	Active instance of the AP filters in Route-processor slot 0.
<b>standby R0</b>	Standby instance of the AP filters in Route-processor slot 0.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to see the AP environment information of an AP:

```
Device# show ap name my-ap environment
```

# show ap name gps location

To see the GPS location of the AP, use the **show ap name gps location** command.

**show ap name** *ap-name* **gps location** [ {*chassis-number* | **active** | **standby**} **R0**

Syntax Description	
<i>ap-name</i>	Name of the Access Point
<b>gps</b>	See the GPS information of a Cisco AP
<b>location</b>	Shows the Mesh linktest data
<i>chassis-number</i>	Enter the chassis number as either 1 or 2.
<b>active R0</b>	Active instance of the active AP filters in Route-processor slot 0.
<b>standby R0</b>	Standby instance of the configuration in Route-processor slot 0.

**Command Default** None

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to see the GPS location of an AP:

```
Device# show ap name mesh-profile-name gps location
```

# show ap name mesh neighbor detail

To see detailed information about a neighbor of a mesh AP, use the **show ap name *ap-name* mesh neighbor detail** command.

**show ap name *ap-name* mesh neighbor detail** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description	
<i>ap-name</i>	Name of the AP.
<i>chassis-number</i>	Enter the chassis number as either 1 or 2.
<b>active R0</b>	Active instance of the AP filters in Route-processor slot 0.
<b>standby R0</b>	Standby instance of the AP filters in Route-processor slot 0.

**Command Default** None

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to see detailed information about a neighbor of a mesh AP:

```
Device# show ap name mymeshap mesh neighbor detail
```

# show ap name wlan

To display the Basic Service Set Identifier (BSSID) value for each WLAN defined on an access point and to display WLAN statistics, use the **show ap name wlan** command.

```
show ap name ap-name wlan {dot11 {24ghz | 5ghz} | statistic}
```

Syntax Description	
<i>ap-name</i>	Name of the Cisco lightweight access point.
<b>dot11</b>	Displays 802.11 parameters.
<b>24ghz</b>	Displays 802.11b network settings.
<b>5ghz</b>	Displays 802.11a network settings.
<b>statistic</b>	Displays WLAN statistics.

**Command Default** None

**Command Modes** Any command mode

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to display BSSID information of an access point in an 802.11b network:

```
Device# show ap name AP01 wlan dot11 24ghz

Site Name                : default-group
Site Description         :

WLAN ID  Interface  BSSID
-----
1        default    00:00:20:00:02:00
12       default    00:00:20:00:02:0b
```

This example shows how to display WLAN statistics for an access point:

```
Device# show ap name AP01 wlan statistic

WLAN ID : 1
WLAN Profile Name : maria-open

EAP Id Request Msg Timeouts : 0
EAP Id Request Msg Timeouts Failures : 0
EAP Request Msg Timeouts : 0
EAP Request Msg Timeouts Failures : 0
EAP Key Msg Timeouts : 0
EAP Key Msg Timeouts Failures : 0

WLAN ID : 12
WLAN Profile Name : 24
```

```
EAP Id Request Msg Timeouts          : 0
EAP Id Request Msg Timeouts Failures : 0
EAP Request Msg Timeouts              : 0
EAP Request Msg Timeouts Failures    : 0
EAP Key Msg Timeouts                  : 0
EAP Key Msg Timeouts Failures        : 0
```

# show ap profile

To see overall status of Hyperlocation for an AP profile, use the **show ap profile** command.

```
show ap profile profile-name {detailed | hyperlocation {ble-beacon | detail | summary}} [chassis
{chassis-number | active | standby} R0]
```

Syntax Description	
<i>profile-name</i>	AP profile name.
<b>detailed</b>	Shows the detailed parameters of the AP join profile.
<b>hyperlocation</b>	Shows Hyperlocation information for the AP profile.
<b>ble-beacon</b>	Show the list of configured BLE beacons for the AP profile.
<b>detail</b>	Shows detailed status of Hyperlocation for the AP profile.
<b>summary</b>	Shows overall status of Hyperlocation for the AP profile
<i>chassis-number</i>	Chassis number as either 1 or 2.
<b>active R0</b>	Active instance in Route-processor slot 0.
<b>standby R0</b>	Standby instance in Route-processor slot 0.

**Command Default** None

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to see the overall status of Hyperlocation for an AP profile:

```
Device# show ap profile my-ap-profile detailed
```



# show ap rf-profile name

To display the selected ap RF-Profile details, use the **show ap rf-profile name** command.

**show ap rf-profile name** *profile-name* **detail**

<b>Syntax Description</b>	<i>profile-name</i>	Name of the RF-Profile.
	<b>detail</b>	Show detail of selected RF Profile.
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Denali 16.3.1	This command was introduced.
<b>Usage Guidelines</b>	None	

This example shows how to display the details of the selected RF-Profile.

```

Device#show ap rf-profile name doctest detail
Description :
AP Group Names :
RF Profile Name : doctest
Band : 2.4 GHz
802.11n client only : Disabled
Transmit Power Threshold v1: -70 dBm
Min Transmit Power: -10 dBm
Max Transmit Power: 30 dBm
Operational Rates
 802.11b 1M Rate : Mandatory
 802.11b 2M Rate : Mandatory
 802.11b 5.5M Rate : Mandatory
 802.11b 11M Rate : Mandatory
 802.11b 6M Rate : Mandatory
 802.11b 9M Rate : Supported
 802.11b 12M Rate : Supported
 802.11b 18M Rate : Supported
 802.11b 24M Rate : Supported
 802.11b 36M Rate : Supported
 802.11b 48M Rate : Supported
 802.11b 54M Rate : Supported
Max Clients : 200
Wlan name                               Max Clients
-----
Trap Threshold
  Clients: 12 clients
  Interference: 10%
  Noise: -70 dBm
  Utilization: 80%
Multicast Data Rate: auto
Rx SOP Threshold : auto
Band Select

```

## show ap rf-profile name

```
Probe Response: Disabled
Cycle Count: 2 cycles
Cycle Threshold: 200 milliseconds
Expire Suppression: 20 seconds
Expire Dual Band: 60 seconds
Client RSSI: -80 dBm
Client Mid RSSI: -80 dBm
Load Balancing
Window: 5 clients
Denial: 3 count
Coverage Data
Data: -80 dBm
Voice: -80 dBm
Minimum Client Level: 3 clients
Exception Level: 25%
DCA Channel List : 1,5,9,13
DCA Foreign AP Contribution : Enabled
802.11n MCS Rates
MCS 0 : Enabled
MCS 1 : Enabled
MCS 2 : Enabled
MCS 3 : Enabled
MCS 4 : Enabled
MCS 5 : Enabled
MCS 6 : Enabled
MCS 7 : Enabled
MCS 8 : Enabled
MCS 9 : Enabled
MCS 10 : Enabled
MCS 11 : Enabled
MCS 12 : Enabled
MCS 13 : Enabled
MCS 14 : Enabled
MCS 15 : Enabled
MCS 16 : Enabled
MCS 17 : Enabled
MCS 18 : Enabled
MCS 19 : Enabled
MCS 20 : Enabled
MCS 21 : Enabled
MCS 22 : Enabled
MCS 23 : Enabled
MCS 24 : Enabled
MCS 25 : Enabled
MCS 26 : Enabled
MCS 27 : Enabled
MCS 28 : Enabled
MCS 29 : Enabled
MCS 30 : Enabled
MCS 31 : Enabled
State : Down
```

## show ap rf-profile summary

To display the ap RF-Profile summary, use the **show ap rf-profile summary** command.

**show ap rf-profile summary**

<b>Syntax Description</b>	<b>summary</b>	Show summary of RF Profiles
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Denali 16.3.1	This command was introduced.
<b>Usage Guidelines</b>	None	

This example shows how to display the ap RF-Profile summary .

```
Device#show ap rf-profile summary
Number of RF Profiles : 1
```

RF Profile Name	Band	Description	Applied	State
doctest	2.4 GHz		No	Down

# show ap summary

To display the status summary of all Cisco lightweight access points attached to the device, use the **show ap summary** command.

**show ap summary**

<b>Syntax Description</b>	This command has no keywords and arguments.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Any command mode	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
<b>Usage Guidelines</b>	Use this command to display a list that contains each lightweight access point name, number of slots, manufacturer, MAC address, location, and the device port number.	

This example shows how to display a summary of all connected access points:

```
Controller# show ap summary
```

```
Number of APs: 1
```

```
Global AP User Name: Cisco
```

```
Global AP Dot1x User Name: Not configured
```

AP Name	AP Model	Ethernet MAC	Radio MAC	State
3602a	3502I	003a.99eb.3fa8	d0c2.8267.8b00	Registered

## show ap tag sources

To see AP tag sources with priorities, use the **show ap tag sources** command.

```
show ap tag sources [chassis {chassis-number | active | standby} R0]
```

### Syntax Description

*chassis-number* Chassis number as either 1 or 2.

**active R0** Active instance of the AP filters in Route-processor slot 0.

**standby R0** Standby instance of the AP filters in Route-processor slot 0.

### Command Default

None

### Command Modes

Privileged EXEC

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

### Examples

The following example shows how to see the AP tag sources with priorities for the active instance:

```
Device# show ap tag sources chassis active R0
```

# show ap tag summary

To view brief summary of tag names, use the **show ap tag summary** command.

**show ap tag summary**

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

## Example

The following example shows how to view brief summary of tag names:

```
Device# show ap tag summary
```

# show ap upgrade

To see AP upgrade information, use the **show ap upgrade** command.

```
show ap upgrade [{name ap-upgrade-report-name | summary | chassis {chassis-number | active | standby}]
```

## Syntax Description

<b>name</b> <i>ap-upgrade-report-name</i>	Enter the name of the AP upgrade report.
<b>summary</b>	Shows a summary of AP upgrade information.
<i>chassis-number</i>	Enter the chassis number as either 1 or 2.
<b>active R0</b>	Active instance in Route-processor slot 0.
<b>standby R0</b>	Standby instance in Route-processor slot 0.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to see a summary of the AP upgrade information:

```
Device# show ap upgrade summary
```

# show arp

To view the ARP table, use the **show arp** command.

## show arp

### Syntax Description

**arp** Shows ARP table

### Command Modes

User EXEC (>)  
Privileged EXEC (#)

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

The following example shows a sample output of the command:

```
Device# show arp
Address Age (min)      Hardware Addr
 9.11.8.1             0 84:80:2D:A0:D2:E6
9.11.32.111          0 3C:77:E6:02:33:3F
```



# show arp summary

To see the ARP table summary, use the **show arp summary** command.

```
show arp summary
```

---

**Command Default**

None

---

**Command Modes**

Privileged EXEC

---

**Command History**

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

## Examples

The following example shows how to see the ARP table summary:

```
Device# show arp summary
```

# show avc client

To display information about top number of applications, use the **show avc client** command in privileged EXEC mode.

**show avc client** *client-mac* **top n application** [**aggregate** | **upstream** | **downstream**]

<b>Syntax Description</b>	<b>client</b> <i>client-mac</i> Specifies the client MAC address.				
	<b>top n application</b> Specifies the number of top "N" applications for the given client.				
<b>Command Default</b>	No default behavior or values.				
<b>Command Modes</b>	Privileged EXEC				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.				

The following is sample output from the **show avc client** command:

```
Device# sh avc client 0040.96ae.65ec top 10 application aggregate
```

Cumulative Stats:

No.	AppName	Packet-Count	Byte-Count	AvgPkt-Size	usage%
1	skinny	7343	449860	61	94
2	unknown	99	13631	137	3
3	dhcp	18	8752	486	2
4	http	18	3264	181	1
5	tftp	9	534	59	0
6	dns	2	224	112	0

Last Interval(90 seconds) Stats:

No.	AppName	Packet-Count	Byte-Count	AvgPkt-Size	usage%
1	skinny	9	540	60	100

# show avc wlan

To display information about top applications and users using the applications, use the **show avc wlan** command in privileged EXEC mode.

**show avc wlan ssid top n application** [**aggregate** | **upstream** | **downstream**]

<b>Syntax Description</b>	<b>wlan ssid</b> Specifies the Service Set Identifier (SSID) for WLAN.				
	<b>top n application</b> Specifies the number of top "N" applications.				
<b>Command Default</b>	No default behavior or values.				
<b>Command Modes</b>	Privileged EXEC				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.				

The following is sample output from the **show avc wlan** command:

Device# **show avc wlan Lobby\_WLAN top 10 application aggregate**

Cumulative Stats:

No.	AppName	Packet-Count	Byte-Count	AvgPkt-Size	usage%
1	ssl	10598677	1979525706	997	42
2	vnc	5550900	3764612847	678	14
3	http	3043131	2691327197	884	10
4	unknown	1856297	1140264956	614	4
5	video-over-http	1625019	2063335150	1269	8
6	binary-over-http	1329115	1744190344	1312	6
7	webex-meeting	1146872	540713787	471	2
8	rtp	923900	635650544	688	2
9	unknown	752341	911000213	1210	3
10	youtube	631085	706636186	1119	3

Last Interval (90 seconds) Stats:

No.	AppName	Packet-Count	Byte-Count	AvgPkt-Size	usage%
1	vnc	687093	602731844	877	68
2	video-over-http	213272	279831588	1312	31
3	ssl	6515	5029365	771	1
4	webex-meeting	3649	1722663	472	0
5	http	2634	1334355	506	0
6	unknown	1436	99412	69	0
7	google-services	722	378121	523	0
8	linkedin	655	393263	600	0
9	exchange	432	167390	387	0
10	gtalk-chat	330	17330	52	0

# show chassis

To see the chassis information, use the **show chassis** command.

```
show chassis [{1 | 2} | detail | mode | neighbors | ha-status {active | local | standby}]
```

## Syntax Description

<b>{1   2}</b>	Chassis number as 1 or 2 to see the information about the relevant chassis.
<b>detail</b>	Shows detailed information about the chassis.
<b>mode</b>	Shows information about the chassis mode.
<b>neighbors</b>	Shows information about the chassis neighbors.
<b>ha-status</b>	Option to see information about the High Availability (HA) status.
<b>active</b>	Shows HA status on the chassis that is in active state.
<b>local</b>	Shows HA status on the local .
<b>standby</b>	Shows HA status on the chassis that is in standby state.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to see the HA status on the active chassis:

```
Device# show chassis ha-status active
```

# show checkpoint

To display information about the Checkpoint Facility (CF) subsystem, use the **show checkpoint** command.

**show checkpoint** { **clients** *client-ID* <0-381> | **entities** *entity-ID* <1-7> | **statistics** **buffer-usage** }

Syntax Description	clients	Displays detailed information about checkpoint clients.
	<b>entities</b>	Displays detailed information about checkpoint entities.
	<b>statistics</b>	Displays detailed information about checkpoint statistics.
	<b>buffer-usage</b>	Displays the checkpoint statistics of clients using large number of buffers.

**Command Default** None

**Command Modes** Privileged EXEC

Command History	Release	Modification
		This command was introduced.

This example shows how to display all the CF clients.

```

Client residing in process : 8135
-----
Checkpoint client: WCM_MOBILITY
Client ID                  : 24105
Total DB inserts           : 0
Total DB updates           : 0
Total DB deletes           : 0
Total DB reads             : 0
Number of tables           : 6
Client residing in process : 8135
-----
Checkpoint client: WCM_DOT1X
Client ID                  : 24106
Total DB inserts           : 2
Total DB updates           : 1312
Total DB deletes           : 2
Total DB reads             : 0
Number of tables           : 1
Client residing in process : 8135
-----
Checkpoint client: WCM_APFROGUE
Client ID                  : 24107
Total DB inserts           : 0
Total DB updates           : 0
Total DB deletes           : 0
Total DB reads             : 0
Number of tables           : 1
Client residing in process : 8135
-----
Checkpoint client: WCM_CIDS
Client ID                  : 24110
Total DB inserts           : 0

```

## show checkpoint

```

Total DB updates      : 0
Total DB deletes     : 0
Total DB reads       : 0
Number of tables     : 0
Client residing in process : 8135
-----
Checkpoint client: WCM_NETFLOW
Client ID            : 24111
Total DB inserts     : 7
Total DB updates     : 0
Total DB deletes     : 0
Total DB reads       : 0
Number of tables     : 1
Client residing in process : 8135
-----
Checkpoint client: WCM_MCAST
Client ID            : 24112
Total DB inserts     : 0
Total DB updates     : 0
Total DB deletes     : 0
Total DB reads       : 0
Number of tables     : 1
Client residing in process : 8135
-----
Checkpoint client: wcm_comet
Client ID            : 24150
Total DB inserts     : 0
Total DB updates     : 0
Total DB deletes     : 0
Total DB reads       : 0
Number of tables     : 0
Client residing in process : 8135
-----

All iosd checkpoint clients
-----
Client Name           Client      Entity      Bundle
                    ID           ID           Mode
-----
Network RF Client     3           --           Off

Total API Messages Sent:           0
Total Transport Messages Sent:     0
Length of Sent Messages:           0
Total Blocked Messages Sent:       0
Length of Sent Blocked Messages:   0
Total Non-blocked Messages Sent:   0
Length of Sent Non-blocked Messages: 0
Total Bytes Allocated:             0
Buffers Held:                     0
Buffers Held Peak:                 0
Huge Buffers Requested:            0
Transport Frag Count:              0
Transport Frag Peak:               0
Transport Sends w/Flow Off:        0
Send Errs:                         0
Send Peer Errs:                   0
Rcv Xform Errs:                   0
Xmit Xform Errs:                   0
Incompatible Messages:             0
Client Unbundles to Process Memory: T
-----
Client Name           Client      Entity      Bundle

```

```

-----
                ID          ID          Mode
-----
SNMP CF Client          12          --          Off

Total API Messages Sent:                0
Total Transport Messages Sent:           0
Length of Sent Messages:                 0
Total Blocked Messages Sent:             0
Length of Sent Blocked Messages:         0
Total Non-blocked Messages Sent:         0
Length of Sent Non-blocked Messages:     0
Total Bytes Allocated:                  0
Buffers Held:                           0
Buffers Held Peak:                      0
Huge Buffers Requested:                 0
Transport Frag Count:                   0
Transport Frag Peak:                    0
Transport Sends w/Flow Off:             0
Send Errs:                              0
Send Peer Errs:                         0
Rcv Xform Errs:                         0
Xmit Xform Errs:                        0
Incompatible Messages:                  0
Client Unbundles to Process Memory:      T
-----

Client Name          Client      Entity      Bundle
                   ID          ID          Mode
-----
Online Diags HA          14          --          Off

Total API Messages Sent:                0
Total Transport Messages Sent:           0
Length of Sent Messages:                 0
Total Blocked Messages Sent:             0
Length of Sent Blocked Messages:         0
Total Non-blocked Messages Sent:         0
Length of Sent Non-blocked Messages:     0
Total Bytes Allocated:                  0
Buffers Held:                           0
Buffers Held Peak:                      0
Huge Buffers Requested:                 0
Transport Frag Count:                   0
Transport Frag Peak:                    0
Transport Sends w/Flow Off:             0
Send Errs:                              0
Send Peer Errs:                         0
Rcv Xform Errs:                         0
Xmit Xform Errs:                        0
Incompatible Messages:                  0
Client Unbundles to Process Memory:      T
-----

Client Name          Client      Entity      Bundle
                   ID          ID          Mode
-----
ARP                    22          --          Off

Total API Messages Sent:                0
Total Transport Messages Sent:           0
Length of Sent Messages:                 0
Total Blocked Messages Sent:             0
Length of Sent Blocked Messages:         0
Total Non-blocked Messages Sent:         0
Length of Sent Non-blocked Messages:     0
Total Bytes Allocated:                  0

```

## show checkpoint

```

Buffers Held:                                0
Buffers Held Peak:                          0
Huge Buffers Requested:                     0
Transport Frag Count:                       0
Transport Frag Peak:                        0
Transport Sends w/Flow Off:                 0
Send Errs:                                  0
Send Peer Errs:                             0
Rcv Xform Errs:                             0
Xmit Xform Errs:                             0
Incompatible Messages:                      0
Client Unbundles to Process Memory:         T
-----
Client Name          Client      Entity      Bundle
                   ID          ID          Mode
-----
Tableid CF          27          --          Off

Total API Messages Sent:                    0
Total Transport Messages Sent:              0
Length of Sent Messages:                   0
Total Blocked Messages Sent:               0
Length of Sent Blocked Messages:           0
Total Non-blocked Messages Sent:           0
Length of Sent Non-blocked Messages:       0
Total Bytes Allocated:                     0
Buffers Held:                              0
Buffers Held Peak:                         0
Huge Buffers Requested:                   0
Transport Frag Count:                     0
Transport Frag Peak:                      0
Transport Sends w/Flow Off:               0
Send Errs:                                 0
Send Peer Errs:                           0
Rcv Xform Errs:                           0
Xmit Xform Errs:                           0
Incompatible Messages:                    0
Client Unbundles to Process Memory:       T
-----
Client Name          Client      Entity      Bundle
                   ID          ID          Mode
-----
Event Manager        33          0          Off

Total API Messages Sent:                    0
Total Transport Messages Sent:              --
Length of Sent Messages:                   0
Total Blocked Messages Sent:               0
Length of Sent Blocked Messages:           0
Total Non-blocked Messages Sent:           0
Length of Sent Non-blocked Messages:       0
Total Bytes Allocated:                     0
Buffers Held:                              0
Buffers Held Peak:                         0
Huge Buffers Requested:                   0
Transport Frag Count:                     0
Transport Frag Peak:                      0
Transport Sends w/Flow Off:               0
Send Errs:                                 0
Send Peer Errs:                           0
Rcv Xform Errs:                           0
Xmit Xform Errs:                           0
Incompatible Messages:                    0
Client Unbundles to Process Memory:       T

```



```

-----
Client Name          Client      Entity      Bundle
                   ID          ID          Mode
-----
LAN-Switch Port Mana      35          0          Off

Total API Messages Sent:                0
Total Transport Messages Sent:           --
Length of Sent Messages:                 0
Total Blocked Messages Sent:             0
Length of Sent Blocked Messages:         0
Total Non-blocked Messages Sent:         0
Length of Sent Non-blocked Messages:     0
Total Bytes Allocated:                   0
Buffers Held:                             0
Buffers Held Peak:                       0
Huge Buffers Requested:                  0
Transport Frag Count:                    0
Transport Frag Peak:                     0
Transport Sends w/Flow Off:              0
Send Errs:                               0
Send Peer Errs:                          0
Rcv Xform Errs:                          0
Xmit Xform Errs:                         0
Incompatible Messages:                   0
Client Unbundles to Process Memory:      T
-----

```

```

-----
Client Name          Client      Entity      Bundle
                   ID          ID          Mode
-----
LAN-Switch PAgP/LACP      36          0          Off

Total API Messages Sent:                0
Total Transport Messages Sent:           --
Length of Sent Messages:                 0
Total Blocked Messages Sent:             0
Length of Sent Blocked Messages:         0
Total Non-blocked Messages Sent:         0
Length of Sent Non-blocked Messages:     0
Total Bytes Allocated:                   0
Buffers Held:                             0
Buffers Held Peak:                       0
Huge Buffers Requested:                  0
Transport Frag Count:                    0
Transport Frag Peak:                     0
Transport Sends w/Flow Off:              0
Send Errs:                               0
Send Peer Errs:                          0
Rcv Xform Errs:                          0
Xmit Xform Errs:                         0
Incompatible Messages:                   0
Client Unbundles to Process Memory:      T
-----

```

```

-----
Client Name          Client      Entity      Bundle
                   ID          ID          Mode
-----
LAN-Switch VLANs         39          0          Off

Total API Messages Sent:                0
Total Transport Messages Sent:           --
Length of Sent Messages:                 0
Total Blocked Messages Sent:             0
Length of Sent Blocked Messages:         0
Total Non-blocked Messages Sent:         0
-----

```

```

Length of Sent Non-blocked Messages:      0
Total Bytes Allocated:                    0
Buffers Held:                              0
Buffers Held Peak:                        0
Huge Buffers Requested:                   0
Transport Frag Count:                      0
Transport Frag Peak:                      0
Transport Sends w/Flow Off:                0
Send Errs:                                 0
Send Peer Errs:                            0
Rcv Xform Errs:                            0

```

This example shows how to display all the CF entities.

```

KATANA_DOC#show checkpoint entities
                        Check Point List of Entities

```

CHKPT on ACTIVE server.

```

-----
Entity ID      Entity Name
-----
          0      CHKPT_DEFAULT_ENTITY

Total API Messages Sent:      0
Total Messages Sent:          0
Total Sent Message Len:      0
Total Bytes Allocated:        0
Total Number of Members:     10

Member(s) of entity 0 are:
  Client ID      Client Name
-----
          168      DHCP Snooping
          167      IGMP Snooping
           41      Spanning-tree
           40      AUTH MGR CHKPT CLIEN
           39      LAN-Switch VLANs
           33      Event Manager
           35      LAN-Switch Port Mana
           36      LAN-Switch PAgP/LACP
          158      Inline Power Checkpoint

```

This example shows how to display the CF statistics.

```

KATANA_DOC#show checkpoint statistics
                        IOSd Check Point Status
CHKPT on ACTIVE server.

Number Of Msgs In Hold Q:      0
CHKPT MAX Message Size:       0
TP MAX Message Size:          65503
CHKPT Pending Msg Timer:      100 ms

FLOW_ON total:                 0
FLOW_OFF total:                 0
Current FLOW status is:        ON
Total API Messages Sent:       0
Total Messages Sent:           0
Total Sent Message Len:        0
Total Bytes Allocated:         0
Rcv Msg Q Peak:                0
Hold Msg Q Peak:               0

```

```
Buffers Held Peak:          0
Current Buffers Held:      0
Huge Buffers Requested:    0
```

# show flexconnect office-extend diagnostics

To display the results of the network diagnostics for all flexconnect OfficeExtend AP, use the **show flexconnect office-extend diagnostics** command.

## show flexconnect office-extend diagnostics

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

**Usage Guidelines** To get periodic details for latency (current, minimum, or maximum) ensure that you enable link-latency under the ap profile, as given in the following example:

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# link-latency
```

If the above configuration is not in place, you will only see the following output:

```
Summary of OfficeExtend AP Link Latency

CAPWAP Latency Heartbeat

Current: current latency (ms)
Min: minimum latency (ms)
Max: maximum latency (ms)

Link Test

Upload: DTLS Upload (Mbps)
Latency: DTLS Link Latency (ms)
Jitter: DTLS Link Jitter (ms)

AP Name Last Latency Heartbeat from AP Current Max Min Last Link Test Run Upload Latency
Jitter
-----
ap-18 Disabled - - - 12/04/20 11:08:58 16 3
0
```

## Examples

This following example shows how to display the network diagnostics information for OfficeExtend AP.

```
Device# show flexconnect office-extend diagnostics

Summary of OfficeExtend AP Link Latency

CAPWAP Latency Heartbeat

Current: current latency (ms)
```

Min: minimum latency (ms)  
 Max: maximum latency (ms)

Link Test

Upload: DTLS Upload (Mbps)  
 Latency: DTLS Link Latency (ms)  
 Jitter: DTLS Link Jitter (ms)

AP Name	Last Latency	Heartbeat from AP	Current Max	Min	Last Link Test Run	Upload Latency	Jitter
ap-18	1 minute 1 second		0	0	0 12/04/20 09:19:48	8	2

# show flow exporter

To display flow exporter status and statistics, use the **show flow exporter** command in privileged EXEC mode.

```
show flow exporter [{export-ids netflow-v9} [name] exporter-name [{statistics | templates}] | statistics | templates}]
```

## Syntax Description

<b>export-ids netflow-v9</b>	(Optional) Displays the NetFlow Version 9 export fields that can be exported and their IDs.
<b>name</b>	(Optional) Specifies the name of a flow exporter.
<i>exporter-name</i>	(Optional) Name of a flow exporter that was previously configured.
<b>statistics</b>	(Optional) Displays statistics for all flow exporters or for the specified flow exporter.
<b>templates</b>	(Optional) Displays template information for all flow exporters or for the specified flow exporter.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

The following example displays the status and statistics for all of the flow exporters configured on a device:

```
Device# show flow exporter
Flow Exporter FLOW-EXPORTER-1:
  Description:           Exports to the datacenter
  Export protocol:       NetFlow Version 9
  Transport Configuration:
    Destination IP address: 192.168.0.1
    Source IP address:     192.168.0.2
    Transport Protocol:    UDP
    Destination Port:      9995
    Source Port:           55864
    DSCP:                  0x0
    TTL:                   255
    Output Features:       Used
```

This table describes the significant fields shown in the display:

**Table 9: show flow exporter Field Descriptions**

Field	Description
Flow Exporter	The name of the flow exporter that you configured.

Field	Description
Description	The description that you configured for the exporter, or the default description User defined.
Transport Configuration	The transport configuration fields for this exporter.
Destination IP address	The IP address of the destination host.
Source IP address	The source IP address used by the exported packets.
Transport Protocol	The transport layer protocol used by the exported packets.
Destination Port	The destination UDP port to which the exported packets are sent.
Source Port	The source UDP port from which the exported packets are sent.
DSCP	The differentiated services code point (DSCP) value.
TTL	The time-to-live value.
Output Features	Specifies whether the <b>output-features</b> command, which causes the output features to be run on Flexible NetFlow export packets, has been used or not.

The following example displays the status and statistics for all of the flow exporters configured on a device:

```
Device# show flow exporter name FLOW-EXPORTER-1 statistics
Flow Exporter FLOW-EXPORTER-1:
  Packet send statistics (last cleared 2w6d ago):
    Successfully sent:          0                (0 bytes)
```

# show flow interface

To display the configuration and status for an interface, use the **show flow interface** command in privileged EXEC mode.

**show flow interface** [*type number*]

Syntax Description	
<i>type</i>	(Optional) The type of interface on which you want to display accounting configuration information.
<i>number</i>	(Optional) The number of the interface on which you want to display accounting configuration information.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

## Examples

The following example displays the accounting configuration on Ethernet interfaces 0/0 and 0/1:

```
Device# show flow interface gigabitethernet1/0/1

Interface Ethernet1/0
  monitor:          FLOW-MONITOR-1
  direction:       Output
  traffic(ip):      on
Device# show flow interface gigabitethernet1/0/2
Interface Ethernet0/0
  monitor:          FLOW-MONITOR-1
  direction:       Input
  traffic(ip):      sampler SAMPLER-2#
```

The table below describes the significant fields shown in the display.

**Table 10: show flow interface Field Descriptions**

Field	Description
Interface	The interface to which the information applies.
monitor	The name of the flow monitor that is configured on the interface.
direction:	The direction of traffic that is being monitored by the flow monitor. The possible values are: <ul style="list-style-type: none"> <li>• Input—Traffic is being received by the interface.</li> <li>• Output—Traffic is being transmitted by the interface.</li> </ul>



Field	Description
traffic(ip)	<p data-bbox="508 296 1198 323">Indicates if the flow monitor is in normal mode or sampler mode.</p> <p data-bbox="508 344 760 371">The possible values are:</p> <ul data-bbox="540 392 1515 506" style="list-style-type: none"><li data-bbox="540 392 1003 420">• on—The flow monitor is in normal mode.</li><li data-bbox="540 441 1515 506">• sampler—The flow monitor is in sampler mode (the name of the sampler will be included in the display).</li></ul>

# show flow monitor

To display the status and statistics for a flow monitor, use the **show flow monitor** command in privileged EXEC mode.

Syntax Description	name	(Optional) Specifies the name of a flow monitor.
	<i>monitor-name</i>	(Optional) Name of a flow monitor that was previously configured.
	<b>cache</b>	(Optional) Displays the contents of the cache for the flow monitor.
	<b>format</b>	(Optional) Specifies the use of one of the format options for formatting the display output.
	<b>csv</b>	(Optional) Displays the flow monitor cache contents in comma-separated variables (CSV) format.
	<b>record</b>	(Optional) Displays the flow monitor cache contents in record format.
	<b>table</b>	(Optional) Displays the flow monitor cache contents in table format.
	<b>statistics</b>	(Optional) Displays the statistics for the flow monitor.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** The **cache** keyword uses the record format by default.

The uppercase field names in the display output of the **show flowmonitor** *monitor-name* **cache** command are key fields that uses to differentiate flows. The lowercase field names in the display output of the **show flow monitor** *monitor-name* **cache** command are nonkey fields from which collects values as additional data for the cache.

## Examples

The following example displays the status for a flow monitor:

```
Device# show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:      Used for basic traffic analysis
  Flow Record:     flow-record-1
  Flow Exporter:   flow-exporter-1
                  flow-exporter-2

Cache:
  Type:            normal
  Status:          allocated
  Size:            4096 entries / 311316 bytes
  Inactive Timeout: 15 secs
  Active Timeout:  1800 secs
```

This table describes the significant fields shown in the display.

Table 11: show flow monitor monitor-name Field Descriptions

Field	Description
Flow Monitor	Name of the flow monitor that you configured.
Description	Description that you configured or the monitor, or the default description User defined.
Flow Record	Flow record assigned to the flow monitor.
Flow Exporter	Exporters that are assigned to the flow monitor.
Cache	Information about the cache for the flow monitor.
Type	Flow monitor cache type. The value is always normal, as it is the only supported cache type.
Status	Status of the flow monitor cache. The possible values are: <ul style="list-style-type: none"> <li>• allocated—The cache is allocated.</li> <li>• being deleted—The cache is being deleted.</li> <li>• not allocated—The cache is not allocated.</li> </ul>
Size	Current cache size.
Inactive Timeout	Current value for the inactive timeout in seconds.
Active Timeout	Current value for the active timeout in seconds.

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1:

This table describes the significant fields shown in the display.

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1 in a table format:

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-IPv6 (the cache contains IPv6 data) in record format:

The following example displays the status and statistics for a flow monitor:

# show flow record

To display the status and statistics for a flow record, use the **show flow record** command in privileged EXEC mode.

```
show flow record [{name] record-name}]
```

<b>Syntax Description</b>	<b>name</b> (Optional) Specifies the name of a flow record.
	<i>record-name</i> (Optional) Name of a user-defined flow record that was previously configured.
<b>Command Default</b>	None
<b>Command Modes</b>	Privileged EXEC
<b>Command History</b>	<b>Release</b>
	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1 This command was introduced.

The following example displays the status and statistics for FLOW-RECORD-1:

```
Device# show flow record FLOW-RECORD-1
flow record FLOW-RECORD-1:
  Description:      User defined
  No. of users:    0
  Total field space: 24 bytes
  Fields:
    match ipv6 destination address
    match transport source-port
    collect interface input
```

# show interfaces

To display the administrative and operational status of all interfaces or for a specified interface, use the **show interfaces** command in privileged EXEC mode.

```
show interfaces [{interface-id | vlan vlan-id}] [{accounting | capabilities [module number] | debounce
| description | etherchannel | flowcontrol | private-vlan mapping | pruning | stats | status [{err-disabled}]
| trunk}]
```

Syntax	Description
<i>interface-id</i>	(Optional) ID of the interface. Valid interfaces include physical ports (including type, stack member, module, and port number) and port channels. The port channel range is 1 to 48.
<b>vlan</b> <i>vlan-id</i>	(Optional) VLAN identification. The range is 1 to 4094.
<b>accounting</b>	(Optional) Displays accounting information on the interface, including active protocols and input and output packets and octets.  <b>Note</b> The display shows only packets processed in software; hardware-switched packets do not appear.
<b>capabilities</b>	(Optional) Displays the capabilities of all interfaces or the specified interface, including the features and options that you can configure on the interface. Though visible in the command line help, this option is not available for VLAN IDs.
<b>module</b> <i>number</i>	(Optional) Displays capabilities of all interfaces on the switch or specified stack member.  This option is not available if you entered a specific interface ID.
<b>description</b>	(Optional) Displays the administrative status and description set for an interface.
<b>etherchannel</b>	(Optional) Displays interface EtherChannel information.
<b>flowcontrol</b>	(Optional) Displays interface flow control information.
<b>private-vlan mapping</b>	(Optional) Displays private-VLAN mapping information for the VLAN switch virtual interfaces (SVIs). This keyword is not available if the switch is running the LAN base feature set.
<b>pruning</b>	(Optional) Displays trunk VTP pruning information for the interface.
<b>stats</b>	(Optional) Displays the input and output packets by switching the path for the interface.
<b>status</b>	(Optional) Displays the status of the interface. A status of unsupported in the Type field means that a non-Cisco small form-factor pluggable (SFP) module is inserted in the module slot.

<b>err-disabled</b>	(Optional) Displays interfaces in an error-disabled state.
<b>trunk</b>	(Optional) Displays interface trunk information. If you do not specify an interface, only information for active trunking ports appears.



**Note** Though visible in the command-line help strings, the **crb**, **fair-queue**, **irb**, **mac-accounting**, **precedence**, **random-detect**, **rate-limit**, and **shape** keywords are not supported.

<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

### Usage Guidelines

The **show interfaces capabilities** command with different keywords has these results:

- Use the **show interface capabilities module *number*** command to display the capabilities of all interfaces on that in the stack. If there is no with that module number in the stack, there is no output.
- Use the **show interfaces *interface-id* capabilities** to display the capabilities of the specified interface.
- Use the **show interfaces capabilities** (with no module number or interface ID) to display the capabilities of all interfaces in the stack.

This is an example of output from the **show interfaces** command for an interface on stack member 3:

```
Device#show interfaces gigabitEthernet 0
GigabitEthernet0 is up, line protocol is up
Hardware is MEWLC management port, address is 0000.5e00.0101 (bia 0000.0000.0000)
Internet address is 20.61.1.12/16
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Unknown, Unknown, media type is unknown media type
output flow-control is unsupported, input flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input 03:06:36, output 00:00:07, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast, 0 pause input
0 packets output, 0 bytes, 0 underruns
```

```

0 output errors, 0 collisions, 1 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out

```

This is an example of output from the **show interfaces *interface* description** command when the interface has been described as *Connects to Marketing* by using the **description** interface configuration command:

```

Device# show interfaces gigabitethernet1/0/2 description
Interface          Status      Protocol Description
Gi1/0/2            up          down      Connects to Marketing

```

This is an example of output from the **show interfaces *interface-id* pruning** command when pruning is enabled in the VTP domain:

```

Device# show interfaces gigabitethernet1/0/2 pruning
Port      Vlans pruned for lack of request by neighbor
Gi1/0/2   3,4

Port      Vlans traffic requested of neighbor
Gi1/0/2   1-3

```

This is an example of output from the **show interfaces stats** command for a specified VLAN interface:

```

Device# show interfaces vlan 1 stats
Switching path  Pkts In   Chars In   Pkts Out   Chars Out
  Processor    1165354  136205310  570800     91731594
  Route cache   0         0          0          0
  Total        1165354  136205310  570800     91731594

```

These are examples of output from the **show interfaces status** command for a specific interface when private VLANs are configured. Port 22 is configured as a private-VLAN host port. It is associated with primary VLAN 20 and secondary VLAN 25:

```

Device# show interfaces gigabitethernet1/0/22 status
Port      Name      Status      Vlan      Duplex      Speed      Type
Gi1/0/22          connected  20,25     a-full    a-100      10/100BaseTX

```

In this example, port 20 is configured as a private-VLAN promiscuous port. The display shows only the primary VLAN 20:

```

Device# show interfaces gigabitethernet1/0/20 status
Port      Name      Status      Vlan      Duplex      Speed      Type
Gi1/0/20          connected  20         a-full    a-100      10/100BaseTX

```

This is an example of output from the **show interfaces status err-disabled** command. It displays the status of interfaces in the error-disabled state:

```

Device# show interfaces status err-disabled
Port      Name      Status      Reason
Gi1/0/2          err-disabled  gbic-invalid
Gi2/0/3          err-disabled  dtp-flap

```

This is an example of output from the **show interfaces *interface-id* pruning** command:

```

Device# show interfaces gigabitethernet1/0/2 pruning
Port Vlans pruned for lack of request by neighbor

```

```
Device# show interfaces gigabitethernet1/0/1 trunk
Port      Mode      Encapsulation  Status      Native vlan
Gi1/0/1   on        802.1q         other       10

Port      Vlans allowed on trunk
Gi1/0/1   none

Port      Vlans allowed and active in management domain
Gi1/0/1   none

Port      Vlans in spanning tree forwarding state and not pruned
Gi1/0/1   none
```



# show install package

To view the install package details, use the **show install package** command.

**show install package**

<b>Syntax Description</b>	This command has no arguments.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration mode	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

## Example

This example shows how to view the install package details:

```
Device#show install package
```

# show install rollback

To view the package information for a rollback point, use the **show install rollback** command.

## show install rollback

<b>Syntax Description</b>	This command has no arguments.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration mode	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

## Example

This example shows how to view the package information for a rollback point:

```
Device#show install rollback
```

# show install summary

To view the install manager summary, use the **show install summary** command.

**show install summary**

<b>Syntax Description</b>	This command has no arguments.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Global configuration mode				
<b>Command History</b>	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Amsterdam 17.1.1s</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.
Release	Modification				
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.				

## Example

This example shows how to view the install summary information:

```
Device#show install summary
```

# show ip

To view the IP information, use the **show ip** command.

## Syntax Description

<b>access-lists</b>	Lists the IP access lists
<b>interface</b>	Displays the IP interface status and configuration
<b>brief</b>	Displays the brief summary of IP status and configuration
<b>route</b>	Displays the IP routing table
<b>tunnel</b>	Displays the IP tunnel information
<b>eogre</b>	Displays the EoGRE tunnel information
<b>domain</b>	Displays the EoGRE tunnel domain information
<b>forwarding-table</b>	Displays the EoGRE tunnel encapsulation and decapsulation information
<b>gateway</b>	Displays the EoGRE tunnel gateway information
<b>fabric</b>	Displays the IP fabric tunnel information
<b>summary</b>	Displays the information for all tunnels

## Command Modes

User EXEC (>)

Privileged EXEC (#)

## Command History

### Release Modification

8.1.111.0 This command was introduced.

The following example shows how to view information about the lists the IP access lists:

```
cisco-wave2-ap# show ip access-lists
```

# show ip nbar protocol-id

To see NBAR protocol classification ID, use the **show ip nbar protocol-id** command.

```
show ip nbar protocol-id name
```

<b>Syntax Description</b>	<b>protocol-id</b>	The protocol classification ID.
	<b>name</b>	Host server name
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 16.12.1	This command was introduced.

## Examples

The following example shows how to see the NBAR protocol classification ID:

```
Device# show ip nbar protocol-id name
```

# show ldap attributes

To view information about the default LDAP attribute mapping, use the **show ldap attributes** command.

## show ldap attributes

<b>Syntax Description</b>	This command has no arguments.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to view information about the default LDAP attribute mapping:

```

Device# show ldap attributes
LDAP Attribute                               Format      AAA Attribute
=====
airespaceBwDataBurstContract                Ulong      bsn-data-bandwidth-burst-contr
userPassword                                String     password
airespaceBwRealBurstContract                Ulong      bsn-realtime-bandwidth-burst-c
employeeType                                String     employee-type
airespaceServiceType                        Ulong      service-type
airespaceACLName                            String     bsn-acl-name
priv-lvl                                     Ulong      priv-lvl
memberOf                                    String DN  supplicant-group
cn                                           String     username
airespaceDSCP                               Ulong      bsn-dscp
policyTag                                    String     tag-name
airespaceQOSLevel                           Ulong      bsn-qos-level
airespace8021PType                           Ulong      bsn-8021p-type
airespaceBwRealAveContract                  Ulong      bsn-realtime-bandwidth-average
airespaceVlanInterfaceName                  String     bsn-vlan-interface-name
airespaceVapId                              Ulong      bsn-wlan-id
airespaceBwDataAveContract                  Ulong      bsn-data-bandwidth-average-con
sAMAccountName                              String     sam-account-name
meetingContactInfo                          String     contact-info
telephoneNumber                             String     telephone-number
Map: att_map_1
department                                  String DN  element-req-qos

```

# show ldap server

To view the LDAP server state information and various other counters for the server, use the **show ldap server** command.

**show ldap server**

<b>Syntax Description</b>	This command has no arguments.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to view the LDAP server state information and various other counters for the server:

```
Device# show ldap server
```

# show license all

To display all licensing information enter the **show license all** command in Privileged EXEC mode. This command displays status, authorization, UDI, and usage information, all combined.

## show license all

<b>Syntax Description</b>	This command has no keywords or arguments	
<b>Command Modes</b>	Privileged EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
	Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to display information relating to Smart Licensing Using Policy.  Command output no longer displays Smart Account and Virtual account information.

**Usage Guidelines**

**Smart Licensing Using Policy:** If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2 or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

**Smart Licensing:** If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

### Example (Smart Licensing Using Policy)

The following is sample output of the **show license all** command on a Cisco Catalyst 9800-CL Wireless Controller. Similar output is displayed on all supported Cisco Catalyst Wireless Controllers.

```
Device# show license all

Smart Licensing Status
=====

Smart Licensing is ENABLED
License Reservation is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
```



```
Version privacy: DISABLED

Transport:
  Type: Transport Off

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: Nov 01 20:31:46 2020 IST
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>

License Usage
=====

air-network-advantage (DNA_NWStack):
  Description: air-network-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-network-advantage
  Feature Description: air-network-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 20

air-dna-advantage (AIR-DNA-A):
  Description: air-dna-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-dna-advantage
  Feature Description: air-dna-advantage
```

```

Enforcement type: NOT ENFORCED
License type: Perpetual
Reservation:
  Reservation status: SPECIFIC INSTALLED
  Total reserved count: 20

```

Product Information

```

=====
UDI: PID:C9800-CL-K9,SN:93BBAH93MGS

```

HA UDI List:

```

  Active:PID:C9800-CL-K9,SN:93BBAH93MGS
  Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN

```

Agent Version

```

=====
Smart Agent for Licensing: 5.0.6_rel/47

```

License Authorizations

```

=====
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
    Status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
    Last Confirmation code: 102fc949
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
    Status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
    Last Confirmation code: ad4382fe

```

Specified license reservations:

```

Aironet DNA Advantage Term Licenses (AIR-DNA-A):
  Description: DNA Advantage for Wireless
  Total reserved count: 20
  Enforcement type: NOT ENFORCED
  Term information:
    Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      License type: TERM
      Start Date: 2020-OCT-14 UTC
      End Date: 2021-APR-12 UTC
      Term Count: 5
      Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      License type: TERM
      Start Date: 2020-JUN-18 UTC
      End Date: 2020-DEC-15 UTC
      Term Count: 5
    Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      License type: TERM
      Start Date: 2020-OCT-14 UTC
      End Date: 2021-APR-12 UTC
      Term Count: 10

```

AP Perpetual Networkstack Advantage (DNA\_NWStack):

```

  Description: AP Perpetual Network Stack entitled with DNA-A
  Total reserved count: 20
  Enforcement type: NOT ENFORCED
  Term information:
    Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      License type: TERM
      Start Date: 2020-OCT-14 UTC
      End Date: 2021-APR-12 UTC
      Term Count: 5
      Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      License type: TERM

```

```
Start Date: 2020-JUN-18 UTC
End Date: 2020-DEC-15 UTC
Term Count: 5
Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
License type: TERM
Start Date: 2020-OCT-14 UTC
End Date: 2021-APR-12 UTC
Term Count: 10
```

Purchased Licenses:

No Purchase Information Available

# show license authorization

To display authorization-related information for (export-controlled and enforced) licenses, enter the **show license authorization** command in privileged EXEC mode.

## show license authorization

<b>Syntax Description</b>	This command has no keywords or arguments
---------------------------	-------------------------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.3.2a	This command was introduced.

<b>Usage Guidelines</b>	<p>Only export-controlled or enforced licenses require authorization before use.</p> <p>While there are no export-controlled or enforced licenses on Cisco Catalyst Wireless Controllers, you can use this command to display migrated SLR authorization codes.</p>
-------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### Examples

See [Table 12: show license authorization Field Descriptions, on page 675](#) for information about fields shown in the display.

See [show license authorization Displaying Migrated Authorization Code, on page 677](#) for sample output.

Table 12: show license authorization Field Descriptions

Field	Description
Overall Status	<p>Header for UDI information for all product instances in the set-up, the type of authorization that is installed, and configuration errors, if any.</p> <p>In a High Availability set-up, all UDIs in the set-up are listed.</p>
Active: Status:	<p>The active product instance UDI, followed by the status of the authorization code installation for this UDI.</p> <p>If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.</p>
Standby: Status:	<p>The standby product instance UDI, followed by the status of the authorization code installation for this UDI.</p> <p>If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.</p>
Member: Status:	<p>The member product instance UDI, followed by the status of the authorization code installation for this UDI.</p> <p>If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.</p>
ERROR:	<p>Configuration errors or discrepancies in the High Availability set-up, if any.</p>

Field	Description
Authorizations	<p>Header for detailed license authorization information. All licenses, their enforcement types, and validity durations are displayed. Errors are displayed for each product instance if its authorization or mode does not match what is installed on the active.</p> <p>This section is displayed only if the product instance is using a license with an authorization code.</p>
()	License name and a shortened form of the license name.
Description	License description.
Total available count:	<p>Total count of licenses that are available to consume.</p> <p>This includes licenses of all durations (perpetual and subscription), including expired subscription licenses, for all the product instances in a High Availability setup.</p>
Enforcement type	<p>Enforcement type for the license. This may be one of the following:</p> <ul style="list-style-type: none"> <li>• Enforced</li> <li>• Not enforced</li> <li>• Export-Controlled</li> </ul>
Term information:	

Field	Description	
		<p>Header providing license duration information. The following fields maybe included under this header:</p> <ul style="list-style-type: none"> <li>• Active: The active product instance UDI, followed by the status of the authorization code installation for this UDI.</li> <li>• Authorization type: Type of authorization code installed and date of installation. The type can be: SLAC, UNIVERSAL, SPECIFIED, PAK, RTU.</li> <li>• Start Date: Displays validity start date if the license is for a specific term or time period.</li> <li>• Start Date: Displays validity end date if the license is for a specific term or time period.</li> <li>• Term Count: License count.</li> <li>• Subscription ID: Displays ID if the license is for a specific term or time period.</li> <li>• License type: License duration. This can be: SUBSCRIPTION or PERPETUAL.</li> <li>• Standby: The standby product instance UDI, followed by the status of the authorization code installation for this UDI.</li> <li>• Member: The member product instance UDI, followed by the status of the authorization code installation for this UDI.</li> </ul> <p>For more information about the duration or term of a license's validity, see &lt;link tbd&gt;.</p>
Purchased Licenses	Header for license purchase information.	
	Active:	The active product instance and its the UDI.
	Count:	License count.
	Description:	License description.
	License type:	License duration. This can be: SUBSCRIPTION or PERPETUAL.
	Standby:	The standby product instance UDI.
	Member:	The member product instance UDI.

### show license authorization Displaying Migrated Authorization Code

The following is sample output of the **show license authorization** command on a Cisco Catalyst 9800-CL Wireless Controller. The `Last Confirmation code:` shows that SLR authorization code is available after migration. Similar output is displayed on all supported Cisco Catalyst Wireless Controllers.

## show license authorization

```

Device# show license authorization
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
    Status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
    Last Confirmation code: 102fc949
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
    Status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
    Last Confirmation code: ad4382fe

Specified license reservations:
  Aironet DNA Advantage Term Licenses (AIR-DNA-A):
    Description: DNA Advantage for Wireless
    Total reserved count: 20
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
        Start Date: 2020-OCT-14 UTC
        End Date: 2021-APR-12 UTC
        Term Count: 5
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
        Start Date: 2020-JUN-18 UTC
        End Date: 2020-DEC-15 UTC
        Term Count: 5
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
        Start Date: 2020-OCT-14 UTC
        End Date: 2021-APR-12 UTC
        Term Count: 10
  AP Perpetual Networkstack Advantage (DNA_NWStack):
    Description: AP Perpetual Network Stack entitled with DNA-A
    Total reserved count: 20
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
        Start Date: 2020-OCT-14 UTC
        End Date: 2021-APR-12 UTC
        Term Count: 5
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
        Start Date: 2020-JUN-18 UTC
        End Date: 2020-DEC-15 UTC
        Term Count: 5
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
        Start Date: 2020-OCT-14 UTC
        End Date: 2021-APR-12 UTC
        Term Count: 10

Purchased Licenses:
  No Purchase Information Available

```



# show license data conversion

To display license data conversion information, enter the **show license data** command in privileged EXEC mode.

**show license data conversion**

---

<b>Syntax Description</b>	This command has no keywords or arguments
---------------------------	-------------------------------------------

---

<b>Command Modes</b>	Privileged EXEC (Device#)
----------------------	---------------------------

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
	Cisco IOS XE Amsterdam 17.3.2a	This command continues to be available with the introduction of Smart Licensing Using Policy.

---

<b>Usage Guidelines</b>	Although visible on the CLI, this command is not applicable to Cisco Catalyst Wireless Controllers.
-------------------------	-----------------------------------------------------------------------------------------------------

# show license eventlog

To display event logs relating to Smart Licensing Using Policy, enter the **show license eventlog** command in privileged EXEC mode.

**show license eventlog** [ *days* ]

## Syntax Description

*days* Enter the number of days for which you want to display event logs. The valid value range is from 0 to 2147483647.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	Additional events were added with the introduction of Smart Licensing Using Policy: <ul style="list-style-type: none"> <li>• Installation and removal of a policy</li> <li>• Request, installation and removal of an authorization code.</li> <li>• Installation and removal of a trust code.</li> <li>• Addition of authorization source information for license usage.</li> </ul>

## Usage Guidelines

**Smart Licensing Using Policy:** If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

**Smart Licensing:** If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

## show license history message

To display communication history between the product instance and CSSM or CSLU (as the case may be), enter the **show license history message** command in privileged EXEC mode. The output of this command is used by the technical support team, for troubleshooting.

**show license history message**

---

**Syntax Description**

This command has no keywords or arguments.

---

**Command Modes**

Privileged EXEC

---

**Command History**

Release	Modification
Cisco IOS XE Amsterdam 17.3.2a	This command was introduced.

---

**Usage Guidelines**

When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: **show license tech support**, **show license history message**, and the **show platform software sl-infra** privileged EXEC commands.

# show license reservation

To display license reservation information, enter the **show license reservation** command in privileged EXEC mode.

## show license reservation

<b>Syntax Description</b>	This command has no keywords or arguments
---------------------------	-------------------------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
	Cisco IOS XE Amsterdam 17.3.2a	This command continues to be available with the introduction of Smart Licensing Using Policy.

<b>Usage Guidelines</b>	The command continues to be available on the CLI and corresponding output is displayed, but with the introduction of Smart Licensing Using Policy, the notion of reservation is not longer applicable. Use the <b>show license all</b> command in privileged EXEC mode, to display <i>migrated</i> SLR licenses instead (the SLR authorization code is migrated to Smart Licensing Using Policy).
-------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

# show license status

To display information about licensing settings such as data privacy, policy, transport, usage reporting and trust codes, enter the **show license status** command in privileged EXEC mode.

**show license status**

<b>Syntax Description</b>	This command has no keywords or arguments	
<b>Command Modes</b>	Privileged EXEC (Device#)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
	Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy. This includes <code>Trust code installed:</code> , <code>Policy in use</code> , <code>Policy name:</code> , reporting requirements as in the policy ( <code>Attributes:</code> ), and fields related to usage reporting.  Command output no longer displays Smart Account and Virtual account information.
<b>Usage Guidelines</b>	<b>Smart Licensing Using Policy:</b> If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.	
	<b>Smart Licensing:</b> If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.	
<b>Examples</b>		
See <a href="#">Table 13: show license status Field Descriptions for Smart Licensing Using Policy</a> , on page 684 for information about fields shown in the display.		
<a href="#">show license status with Cisco Default Policy (Smart Licensing Using Policy)</a> , on page 689		
<a href="#">show license status with Custom Policy (Smart Licensing Using Policy)</a> , on page 690		

Table 13: show license status Field Descriptions for Smart Licensing Using Policy

Field	Description	
Utility	Header for utility settings that are configured on the product instance.	
	Status:	Status
	Utility report:	Last attempt:
	Customer Information:	The following fields are displayed: <ul style="list-style-type: none"> <li>• Id:</li> <li>• Name:</li> <li>• Street</li> <li>• City:</li> <li>• State:</li> <li>• Country:</li> <li>• Postal Code:</li> </ul>
Smart Licensing Using Policy:	Header for policy settings on the product instance.	
	Status:	Indicates if Smart Licensing Using Policy is enabled. Smart Licensing Using Policy is supported starting from Cisco IOS XE Amsterdam 17.3.2 and is always enabled on supported software images.
Data Privacy:	Header for privacy settings that are configured on the product instance.	
	Sending Hostname:	A <i>yes</i> or <i>no</i> value which shows if the hostname is sent in usage reports.
	Callhome hostname privacy:	Indicates if the Call Home feature is configured as the mode of transport for reporting. If configured, one of these values is displayed: <ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DISABLED</li> </ul>
	Smart Licensing hostname privacy:	One of these values is displayed: <ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DISABLED</li> </ul>
	Version privacy:	One of these values is displayed: <ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DISABLED</li> </ul>

Field		Description
Transport:		Header for transport settings that are configured on the product instance.
	Type:	Mode of transport that is in use.  Additional fields are displayed for certain transport modes. For example, if transport type is set to CSLU, the CSLU address is also displayed.

Field	Description
Policy:	Header for policy information that is applicable to the product instance.
Policy in use:	Policy that is applied  This can be one of the following: Cisco default, Product default, Permanent License Reservation, Specific License Reservation, PAK license, Installed on <date>, Controller.
Policy name:	Name of the policy
Reporting ACK required:	A <i>yes</i> or <i>no</i> value which specifies if the report for this product instance requires CSSM acknowledgement (ACK) or not. The default policy is always set to “yes”.
Unenforced/Non-Export Perpetual Attributes	Displays policy values for perpetual licenses. <ul style="list-style-type: none"> <li>• First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name.</li> <li>• Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name.</li> <li>• Report on change (days): he maximum amount of time available to send a report in case of a change in license usage, followed by policy name</li> </ul>
Unenforced/Non-Export Subscription Attributes	Displays policy values for subscription licenses. <ul style="list-style-type: none"> <li>• First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name.</li> <li>• Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name.</li> <li>• Report on change (days): he maximum amount of time available to send a report in case of a change in license usage, followed by policy name</li> </ul>
Enforced (Perpetual/Subscription) License Attributes	



Field		Description
		<p>Displays policy values for enforced licenses.</p> <ul style="list-style-type: none"> <li>• First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name.</li> <li>• Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name.</li> <li>• Report on change (days): The maximum amount of time available to send a report in case of a change in license usage, followed by policy name</li> </ul>
	Export (Perpetual/Subscription) License Attributes	<p>Displays policy values for export-controlled licenses.</p> <ul style="list-style-type: none"> <li>• First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name.</li> <li>• Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name.</li> <li>• Report on change (days): The maximum amount of time available to send a report in case of a change in license usage, followed by policy name</li> </ul>
Miscellaneous	Header for custom ID.	
	Custom Id:	ID

Field	Description
Usage Reporting:	Header for usage reporting (RUM reports) information.
Last ACK received:	Date and time of last ACK received, in the local time zone.
Next ACK deadline:	Date and time for next ACK. If the policy states that an ACK is not required then this field displays <code>none</code> .  <b>Note</b> If an ACK is required and is not received by this deadline, a syslog is displayed.
Reporting Interval:	Reporting interval in days  The value displayed here depends on what you configure in the <b>license smart usage interval</b> <code>interval_in_days</code> and the policy value. For more information, see the corresponding Syntax Description: <a href="#">license smart (global config)</a> , on page 336.
Next ACK push check:	Date and time when the product instance will submit the next polling request for an ACK. Date and time are in the local time zone.  This applies only to product instance- initiated communication to CSSM or CSLU. If the reporting interval is zero, or if no ACK polling is pending, then this field displays <code>none</code> .
Next report push:	Date and time when the product instance will send the next RUM report. Date and time are in the local time zone. If the reporting interval is zero, or if there are no pending RUM reports, then this field displays <code>none</code> .
Last report push:	Date and time for when the product instance sent the last RUM report. Date and time are in the local time zone.
Last report file write:	Date and time for when the product instance last saved an offline RUM report. Date and time are in the local time zone.
Last report pull:	Date and time for when usage reporting information was retrieved using data models. Date and time are in the local time zone.

Field	Description
Trust Code Installed:	Header for trust code-related information. Displays date and time if trust code is installed. Date and time are in the local time zone. If a trust code is not installed, then this field displays <code>none</code> .
Active:	Active product instance. In a High Availability set-up, the the UDIs of all product instances in the set-up, along with corresponding trust code installation dates and times are displayed.
Standby:	Standby product instance.
Member:	Member product instance

**show license status with Cisco Default Policy (Smart Licensing Using Policy)**

The following is sample output of the **show license status** command; a default is policy applied here.

```
Device# show license status

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
```

```

    Report on change (days): 0 (CISCO default)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>

```

### show license status with Custom Policy (Smart Licensing Using Policy)

The following is sample output of the **show license status** command; a custom policy applied here.

```

Device# show license status
Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured

Policy:
  Policy in use: Installed On Nov 02 05:09:31 2020 IST
  Policy name: SLE Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 60 (Customer Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)

Miscellaneous:
  Custom Id: <empty>

```

```
Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
         INSTALLED on Nov 02 05:09:31 2020 IST
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
         INSTALLED on Nov 02 05:09:31 2020 IST
```

# show license summary

To display a brief summary of license usage, which includes information about licenses being used, the count, and status, enter the **show license summary** command in privileged EXEC mode.

## show license summary

<b>Syntax Description</b>	This command has no keywords or arguments
---------------------------	-------------------------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
	Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to reflect valid license status for Smart Licensing Using Policy. Valid license statuses include: <code>IN USE</code> , <code>NOT IN USE</code> , <code>NOT AUTHORIZED</code> .  Command output was also updated to remove registration and authorization information.  Command output no longer displays Smart Account and Virtual account information.

<b>Usage Guidelines</b>	<p><b>Smart Licensing Using Policy:</b> If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.</p>
-------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The licenses on Cisco Catalyst Wireless Controllers are never `NOT AUTHORIZED`, because none of the available licenses are export-controlled or enforced (Only these licenses require authorization before use).

**Smart Licensing:** If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

### Examples

See [Table 14: show license summary Field Descriptions, on page 692](#) for information about fields shown in the display.

[show license summary: IN USE \(Smart Licensing Using Policy\), on page 693](#)

[show license summary: NOT IN USE \(Smart Licensing Using Policy\), on page 693](#)

**Table 14: show license summary Field Descriptions**

Field	Description
License	Name of the licenses in use
Entitlement Tag	Short name for license
Count	License count

Field	Description
Status	<p>License status can be one of the following</p> <ul style="list-style-type: none"> <li>• In-Use: Valid license, and in-use.</li> <li>• Not In-Use</li> <li>• Not Authorized: Means that the license requires installation of SLAC before use.</li> </ul>

**show license summary: IN USE (Smart Licensing Using Policy)**

The following is sample output of the **show license summary** command where all licenses are in-use.

Device# **show license summary**

```
License Usage:
License           Entitlement Tag           Count Status
-----
air-network-essentials (DNA_NWSTACK_E)           1 IN USE
air-dna-essentials   (AIR-DNA-E)               1 IN USE
```

**show license summary: NOT IN USE (Smart Licensing Using Policy)**

The following is sample output of the **show license summary** command, where none of the APs have joined the controller. Current consumption (Count) is therefore zero, and the `Status` field shows that the licenses are NOT IN USE:

Device# **show license summary**

```
Device#show license summary
License Reservation is ENABLED
```

```
License Usage:
License           Entitlement Tag           Count Status
-----
Aironet DNA Advantag... (AIR-DNA-A)           0 NOT IN USE
AP Perpetual Network... (DNA_NWStack)         0 NOT IN USE
```

# show license tech

To display licensing information to help the technical support team to solve a problem, enter the **show license tech** command in privileged EXEC mode. The output for this command includes outputs of several other **show license** commands and more.

```
show license tech { data { conversion } | eventlog [{ days }] | reservation | support }
```

## Syntax Description

<b>data { conversion }</b>	Displays license data conversion information.
<b>eventlog [{ days }]</b>	Displays event logs related to Smart Licensing Using Policy. For <i>days</i> , enter the number of days for which you want to display event logs. The valid value range is from 0 to 2147483647.
<b>reservation</b>	Displays license reservation information.
<b>support</b>	Displays licensing information that helps the technical support team to debug a problem.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy.

## Usage Guidelines

**Smart Licensing Using Policy:** If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: **show license tech support**, **show license history message**, and the **show platform software sl-infra all** privileged EXEC commands.

**Smart Licensing:** If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing (whether smart licensing is enabled, all associated licensing certificates, compliance status, and so on).

### Example (Smart Licensing Using Policy)

The following is sample output from the **show license tech support** command.

```
Device# show license tech support
Smart Licensing Tech Support info
Smart Licensing Status
=====
Smart Licensing is ENABLED
```



```
License Reservation is ENABLED

Registration:
  Status: REGISTERED - SPECIFIC LICENSE RESERVATION
  Export-Controlled Functionality: ALLOWED
  Initial Registration: SUCCEEDED on Nov 02 03:16:01 2020 IST

License Authorization:
  Status: AUTHORIZED - RESERVED on Nov 02 03:16:01 2020 IST

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license

Evaluation Period:
  Evaluation Mode: Not In Use
  Evaluation Period Remaining: 89 days, 23 hours, 42 minutes, 47 seconds

License Usage
=====
Handle: 1
  License: AP Perpetual Networkstack Advantage
  Entitlement tag:
  regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896
  Description: AP Perpetual Network Stack entitled with DNA-A
  Count: 1
  Version: 1.0
  Status: AUTHORIZED(3)
  Status time: Nov 02 03:16:01 2020 IST
  Request Time: Nov 02 02:55:34 2020 IST
  Export status: NOT RESTRICTED
  Soft Enforced: True

Handle: 2
  License: Aironet DNA Advantage Term Licenses
  Entitlement tag: regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790

  Description: DNA Advantage for Wireless
  Count: 1
  Version: 1.0
  Status: AUTHORIZED(3)
  Status time: Nov 02 03:16:01 2020 IST
  Request Time: Nov 02 02:55:34 2020 IST
  Export status: NOT RESTRICTED
  Soft Enforced: True

Product Information
=====
UDI: PID:C9800-CL-K9,SN:93BBAH93MGS

HA UDI List:
```

```

Active:PID:C9800-CL-K9,SN:93BBAH93MGS
Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN

Agent Version
=====
Smart Agent for Licensing: 4.8.7_rel/52

Upcoming Scheduled Jobs
=====
Current time: Nov 02 03:17:23 2020 IST
Daily: Nov 03 02:47:04 2020 IST (23 hours, 29 minutes, 41 seconds remaining)
Certificate Renewal: Not Available
Certificate Expiration Check: Not Available
Authorization Renewal: Not Available
Authorization Expiration Check: Not Available
Init Flag Check: Not Available
Evaluation Expiration Check: Not Available
Ack Expiration Check: Not Available
Evaluation Expiration Warning: Not Available
IdCert Expiration Warning: Not Available
Reservation request in progress warning: Not Available
Reservation configuration mismatch between nodes in HA mode: Nov 09 03:16:30 2020 IST (6
days, 23 hours, 59 minutes, 7 seconds remaining)
Endpoint Report Request: Not Available

License Certificates
=====
Production Cert: True
Not registered. No certificates installed

HA Info
=====
RP Role: Active
Chassis Role: Active
Behavior Role: Active
RMF: True
CF: True
CF State: Stateless
Message Flow Allowed: False

Reservation Info
=====
License reservation: ENABLED

Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
  Reservation status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
  Export-Controlled Functionality: ALLOWED
  Request code: <none>
  Last return code: <none>
  Last Confirmation code: 102fc949
  Reservation authorization code:
  <title></title><tag>tagid=2019-06-cisco-DNAAdv,10_e2457-3d-408d-fd-265885</tag><startDate>2020-12-14
  UTC</startDate><endDate>2021-Apr-12
  UTC</endDate><licenseType>TERM</licenseType><displayName>Aironet DNA Advantage Term
  Licenses</displayName><tagDescription>DNA Advantage for
  <title></title><tag>tagid=2019-06-cisco-DNAAdv,10_e2457-3d-408d-fd-265885</tag><startDate>2020-12-14
  UTC</startDate><endDate>2020-Dec-15
  UTC</endDate><licenseType>TERM</licenseType><displayName>Aironet DNA Advantage Term
  Licenses</displayName><tagDescription>DNA Advantage for
  <title></title><tag>tagid=2019-06-cisco-DNAAdv,10_e2457-3d-408d-fd-265885</tag><startDate>2020-12-14
  UTC</startDate><endDate>2021-Apr-12
  UTC</endDate><licenseType>TERM</licenseType><displayName>AP Perpetual Networkstack
  Advantage</displayName><tagDescription>AP Perpetual Network Stack entitled with

```

```

DNA/ta<description>subscriptionID/subscriptionID/entitled/entitled-tagpid2178666cniscsDNA_NWStack_10_e2457-3a5-4388f0-d2658096/tag-count5/ent-startDate2020-In-8
UTC/</startDate><endDate>2020-Dec-15
UTC/</endDate><licenseType>TERM/</licenseType><displayName>AP Perpetual Networkstack
Advantage/</displayName><tagDescription>AP Perpetual Network Stack entitled with
DNA/ta<description>subscriptionID/subscriptionID/entitled/entitled-tagpid2178666cniscsAIR-DNA_10_e3387-3a0-41a-39581a079/tag-count10/ent-startDate2020-Oct-14
UTC/</startDate><endDate>2021-Apr-12
UTC/</endDate><licenseType>TERM/</licenseType><displayName>Aironet DNA Advantage Term
Licenses/</displayName><tagDescription>DNA Advantage for
Wireless/</tagDescription>

Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
Reservation status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
Export-Controlled Functionality: ALLOWED
Request code: <none>
Last return code: <none>
Last Confirmation code: ad4382fe
Reservation authorization code:

Aironet DNA Advantage Term Licenses (AIR-DNA-A):
Description: DNA Advantage for Wireless
Total reserved count: 20
Term information:
Active: PID:C9800-CL-K9,SN:93BBAH93MGS
License type: TERM
Start Date: 2020-OCT-14 UTC
End Date: 2021-APR-12 UTC
Term Count: 5
Subscription ID: <none>
License type: TERM
Start Date: 2020-JUN-18 UTC
End Date: 2020-DEC-15 UTC
Term Count: 5
Subscription ID: <none>
Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
License type: TERM
Start Date: 2020-OCT-14 UTC
End Date: 2021-APR-12 UTC
Term Count: 10
Subscription ID: <none>
AP Perpetual Networkstack Advantage (DNA_NWStack):
Description: AP Perpetual Network Stack entitled with DNA-A
Total reserved count: 20
Term information:
Active: PID:C9800-CL-K9,SN:93BBAH93MGS
License type: TERM
Start Date: 2020-OCT-14 UTC
End Date: 2021-APR-12 UTC
Term Count: 5
Subscription ID: <none>
License type: TERM
Start Date: 2020-JUN-18 UTC
End Date: 2020-DEC-15 UTC
Term Count: 5
Subscription ID: <none>
Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
License type: TERM
Start Date: 2020-OCT-14 UTC
End Date: 2021-APR-12 UTC

```

```

Term Count: 10
Subscription ID: <none>

```

## Other Info

```

=====

```

```

Software ID: regid.2018-05.com.cisco.WLC_9500C,1.0_85665885-b865-4e32-8184-5510412fcb54
Agent State: authorized
TS enable: True
Transport: Smart
  Default URL: https://smartreceiver.cisco.com/licservice/license
Locale: en_US.UTF-8
Debug flags: 0x7
Privacy Send Hostname: True
Privacy Send IP: True
Build type:: Production
sizeof(char) : 1
sizeof(int) : 4
sizeof(long) : 4
sizeof(char *) : 8
sizeof(time_t) : 4
sizeof(size_t) : 8
Endian: Big
Write Erase Occurred: False
XOS version: 0.12.0.0
Config Persist Received: False
Message Version: 1.3
connect_info.name: <empty>
connect_info.version: <empty>
connect_info.additional: <empty>
connect_info.prod: False
connect_info.capabilities: <empty>
agent.capabilities: UTILITY, DLC, AppHA, MULTITIER, EXPORT_2, OK_TRY_AGAIN
SmartAgentClientWaitForServer: 2000
SmartAgentCmReTrySend: True
SmartAgentClientIsUnified: True
SmartAgentCmClient: True
SmartAgentClientName: UnifiedClient
builtInEncryption: True
enableOnInit: True
routingReadyByEvent: True
systemInitByEvent: True
SmartAgentFederalLicense: True
SmartAgent_Crypto_Exit_CB: 0x55B353357A20
SmartAgent_Crypto_Start_CB: 0x55B353357A10
SmartAgentMultiTenant: False
attr365DayEvalSyslog: True
checkPointWriteOnly: False
SmartAgentDelayCertValidation: False
enableByDefault: False
conversionAutomatic: True
conversionAllowed: False
storageEncryptDisable: False
storageLoadUnencryptedDisable: False
TSPluginDisable: False
bypassUDICheck: False
loggingAddTStamp: False
loggingAddTid: True
platformOverrideEvent: UnknownPlatformEvent
WaitForHaRole: False
standbyIsHot: True
chkPtType: 2
delayCommInit: False
roleByEvent: True
maxTraceLength: 150

```

```
traceAlwaysOn: True
debugFlags: 0
Event log max size: 5120 KB
Event log current size: 21 KB

Platform Provided Mapping Table
=====
<empty>
```

# show license udi

To display Unique Device Identifier (UDI) information for a product instance, enter the **show license udi** command in privileged EXEC mode. In a High Availability set-up, the output displays UDI information for all connected product instances.

## show license udi

<b>Syntax Description</b>	This command has no keywords or arguments	
<b>Command Modes</b>	Privileged EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
	Cisco IOS XE Amsterdam 17.3.2a	This command continues to be available with the introduction of Smart Licensing Using Policy.

**Usage Guidelines** **Smart Licensing Using Policy:** If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

**Smart Licensing:** If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

## Examples

[show license udi with Standalone Product Instance, on page 700](#)

[show license udi with Active and Standby, on page 700](#)

### show license udi with Standalone Product Instance

The following is sample output from the **show license udi** command on a standalone product instance.

```
Device# show license udi
UDI: PID:C9800-L-F-K9,SN:FCW2323W016
```

### show license udi with Active and Standby

The following is sample output from the **show license udi** command in a High Availability set-up where an active and a standby product instances exist. UDI information is displayed for both.

```
Device# show license udi
UDI: PID:C9800-CL-K9,SN:93BBAH93MGS
HA UDI List:
  Active:PID:C9800-CL-K9,SN:93BBAH93MGS
  Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN
```

# show license usage

To display license usage information such as status, a count of licenses being used, and enforcement type, enter the **show license usage** command in privileged EXEC mode.

**show license usage**

<b>Syntax Description</b>	This command has no keywords or arguments
---------------------------	-------------------------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.3.2	This command was introduced.
	Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy. This includes the <code>Status</code> , <code>Enforcement type</code> fields.  Command output was also updated to remove reservation related information, authorization status information, and export status information.

<b>Usage Guidelines</b>	<b>Smart Licensing Using Policy:</b> If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.
-------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Smart Licensing:** If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

## Examples

See [Table 15: show license usage Field Descriptions, on page 701](#) for information about fields shown in the display.

[show license usage with unenforced licenses \(Smart Licensing Using Policy\), on page 702](#)

[show license usage with unenforced SLR licenses \(Smart Licensing Using Policy\), on page 703](#)

**Table 15: show license usage Field Descriptions**

Field	Description
License Authorization: Status:	Displays overall authorization status.
():	Name of the license as in CSSM.  If this license is one that requires an authorization code, the name of the license comes from the code.

Field	Description
Description	Description of the license as in CSSM.
Count	License count. If the license is not in-use, the count is reflected as zero.
Version	Version.
Status	License status can be one of the following <ul style="list-style-type: none"> <li>• In-Use: Valid license, and in-use.</li> <li>• Not In-Use</li> <li>• Not Authorized: Means that the license requires installation of SLAC before use. For more information, see</li> </ul>
Export Status:	Indicates if this license is export-controlled or not. Accordingly, one of the following statuses is displayed: <ul style="list-style-type: none"> <li>• RESTRICTED - ALLOWED</li> <li>• RESTRICTED - NOT ALLOWED</li> <li>• NOT RESTRICTED</li> </ul>
Feature name	Name of the feature that uses this license.
Feature Description:	Description of the feature that uses this license.
Utility Subscription id:	ID Not applicable, because the corresponding configuration option is not supported.
Enforcement type	Enforcement type status for the license. This may be one of the following: <ul style="list-style-type: none"> <li>• ENFORCED</li> <li>• NOT ENFORCED</li> <li>• EXPORT RESTRICTED - ALLOWED</li> <li>• EXPORT RESTRICTED - NOT ALLOWED</li> </ul> For more information about enforcement types, see <link tbd>

### show license usage with unenforced licenses (Smart Licensing Using Policy)

The following is sample output of the **show license usage** command. Unenforced licenses are in-use here.



```
Device# show license usage

License Authorization:
  Status: Not Applicable

air-network-essentials (DNA_NWSTACK_E):
  Description: air-network-essentials
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-network-essentials
  Feature Description: air-network-essentials
  Enforcement type: NOT ENFORCED
  License type: Perpetual

air-dna-essentials (AIR-DNA-E):
  Description: air-dna-essentials
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-dna-essentials
  Feature Description: air-dna-essentials
  Enforcement type: NOT ENFORCED
  License type: Perpetual
```

### show license usage with unenforced SLR licenses (Smart Licensing Using Policy)

The following is sample output of the **show license usage** command. Migrated SLR licenses are in-use here:

```
Device# show license usage

air-network-advantage (DNA_NWStack):
  Description: air-network-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-network-advantage
  Feature Description: air-network-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 20

air-dna-advantage (AIR-DNA-A):
  Description: air-dna-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-dna-advantage
  Feature Description: air-dna-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 20
```

## show platform software sl-infra

To display troubleshooting information and for debugging, enter the **show platform software sl-infra** command in privileged EXEC mode. The output of this command is used by the technical support team, for troubleshooting and debugging.

**show platform software sl-infra** { **all** | **current** | **debug** | **stored** }

Syntax Description	
<b>all</b>	Displays current, debugging, and stored information.
<b>current</b>	Displays current license-related information.
<b>debug</b>	Enables debugging
<b>stored</b>	Displays information that is stored on the product instance.

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	Cisco IOS XE Amsterdam 17.3.2a	This command was introduced.

Usage Guidelines	When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: <b>show license tech support</b> , <b>show license history message</b> , and the <b>show platform software sl-infra all</b> privileged EXEC commands.
------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

# show platform software tls client summary

To view the TLS client summary details, use the **show platform software tls client summary** command.

**show platform software tls client summary**

---

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--------------------------------------------

---

---

<b>Command Modes</b>	Global configuration
----------------------	----------------------

---

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

---

---

**Examples** This example shows how to view the TLS client summary details:

```
Device # show platform software tls client summary
```

Name	ID	Gateway	Port	Auth	Trustpoint	DPD Time	Rekey Time	Retry Time
-----								
fqdn	0		8443	PSK	N/A	60	300	20

# show platform software client detail

To display a summary of TLS client session detail, session statistics, tunnel statistics, and DNS counters, use the **show platform software client detail** command.

## show platform software client detail

### Syntax Description

This command has no keywords or arguments.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

### Examples

This example shows how to view the TLS client summary details:

```

Device # show platform software client detail

TLS Client          : Session Detail
Session Name       : fqdn
FQDN resolved IP   : 10.194.234.149
ID                 : 0
Created            : 04/20/21 00:36:42
Updated            : 04/22/21 05:56:03
State              : Up (Rekey)
Up Time            : 04/21/21 20:30:21 ( 9 hours 25 minutes 45 seconds )
Down Time          : 04/21/21 20:30:01
Rekey Time         : 04/22/21 05:55:51 ( 15 seconds )

TLS Session Statistics

Up Notifications   : 3
Down Notifications : 2
Rekey Notifications : 636
DP State Updates   : 0
DPD Cleanups       : 0

Packets From      Packets To  Packet Errors To  Bytes From      Bytes To
-----
BinOS              80           0
IOSd                0           0                0                0

TLS Client         0           0                0                0

TLS Tunnel Statistics
Type              Tx Packets      Rx Packets
-----
Total             0                80
CSTP Ctrl        3836            3836
CSTP Data        80                0

Type              Requests        Responses
-----

```

```
CSTP Cfg          639          639
CSTP DPD          3197         3197

Invalid CSTP Rx           : 0
Injected Packet Success  : 0
Injected Packet Failed   : 0
Consumed Packets         : 0

TLS Tunnel DNS Counters
DNS Resolve Request Success Count : 641
DNS Resolve Request Failure Count  : 0
DNS Resolve Success Count          : 639
DNS Resolve Failure Count          : 2
```

# show platform software tls statistics

To view the TLS client global statistic details, use the **show platform software tls statistics** command.

## show platform software tls statistics

---

**Syntax Description** This command has no keywords or arguments.

---

**Command Modes** Global configuration

---

**Command History**

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

---

**Examples** This example shows how to view the TLS client summary details:

```
Device # show platform software tls statistics

TLS Client - Global Statistics
Session Statistics
Up/Down           : 5/2
Rekeys            : 636
DP Updates        : 0
DPD Cleanups      : 0

Packets From      Packets To      Packet Errors To  Bytes From      Bytes To
-----
BinOS              85                0                  0                0
IOSd 0             0                  0                  0                0
TLS Client 0       0                  0                  0                0

Tunnel Statistics
SSL Handshake Init/Done : 641/641
TCP Connection Req/Done : 641/641

Tunnel Packets
Rx/Tx                : 85/0
Injected / Failed    : 0/0
Consumed              : 0

CSTP Packets
Control Rx/Tx        : 3839 / 3839
Data Rx/Tx           : 0 / 85
Config Req/Resp      : 641 / 641
DPD Req/Resp         : 3198 / 3198
Invalid Rx           : 0

FQDN Counters
Req/Resp/Success     : 0/0/0

NAT Counters
Transalte In/Out     : 0/0
Ignore In/Out        : 0/0
Failed                : 0
Invalid              : 0
```

```
No Entry          : 0
Unsupported       : 0
```

## Internal Counters

Type	Allocated	Freed
EV	1299	1295
Tunnel	5	4
Conn	643	642
Sess	3	2

## Config Message Related Counters

Type	Success	Failed
Create	3	0
Delete	2	0

# show platform software tls session summary

To view the tls client session summary, use the **show platform software tls session summary** command.

**show platform software tls session summary**

## Syntax Description

This command has no keywords or arguments.

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

## Examples

This example shows how to view the TLS client summary details:

```
Device # show platform software tls session summary
```

```
TLS Client - Session Summary
```

Name	ID	Created	State	Since	Elapsed
fqdn	0	04/20/21 00:36:42	Up	04/21/21 20:30:21	9 hours 26 minutes 44 seconds



# show logging profile wireless end timestamp

To specify log filtering end location timestamp for filtering, use the **show logging profile wireless end timestamp** command.

**show logging profile wireless end timestamp** *time-stamp*

<b>Syntax Description</b>	<i>time-stamp</i> Time to end the filtering. For example, 2017/02/10 14:41:50.849.
---------------------------	------------------------------------------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

<b>Usage Guidelines</b>	Ensure that you enable internal keyword using the <b>show logging profile wireless internal</b> command to get the trace output.
-------------------------	----------------------------------------------------------------------------------------------------------------------------------

## Example

The following example shows how to specify log filtering end location timestamp for filtering:

```
Device# show logging profile wireless end timestamp 2017/02/10 14:41:50.849
```

# show logging profile wireless filter

To specify filter for logs, use the **show logging profile wireless filter** command.

**show logging profile wireless filter** { **ipv4** | **mac** | **string** | **uuid** }

Syntax Description	
<b>ipv4</b>	Selects logs with specific IP address app context.
<b>mac</b>	Selects logs with specific MAC app context.
<b>string</b>	Selects logs with specific string app context.
<b>uuid</b>	Selects logs with specific Universally Unique Identifier (UUID) app context.

**Command Default** None

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

**Usage Guidelines** Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

## Example

The following example shows how to specify filter for logs:

```
Device# show logging profile wireless filter ipv4 10.10.11.1
```

## show logging profile wireless fru

To specify field-replaceable unit (FRU) specific commands, use the **show logging profile wireless fru** command.

```
show logging profile wireless fru {0 {reverse | to-file}| chassis} {0 {reverse | to-file} | chassis}
```

### Syntax Description

<b>0</b>	SPA-Inter-Processor slot 0.
<b>reverse</b>	Shows logs in reverse chronological order.
<b>to-file</b>	Decodes files stored in disk and write output to file.
<b>chassis</b>	Chassis name.

### Command Default

None

### Command Modes

Privileged EXEC (#)

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

### Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

### Example

The following example shows how to specify FRU specific commands:

```
Device# show logging profile wireless fru 0
```

# show logging profile wireless internal

To select all the logs, use the **show logging profile wireless internal** command.

## show logging profile wireless internal

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

<b>Usage Guidelines</b>	Ensure that you enable <b>internal</b> keyword using the <b>show logging profile wireless internal</b> command to get the trace output.
-------------------------	-----------------------------------------------------------------------------------------------------------------------------------------

Without the **internal** keyword, only customer curated logs are displayed.

### Example

The following example shows how to display all the logs:

```
Device# show logging profile wireless internal
```

# show logging profile wireless level

To select logs above a specific level, use the **show logging profile wireless level** command.

```
show logging profile wireless level { debug | emergency | error | info | noise | notice | verbose | warning
}
```

Syntax Description	Option	Description
	<b>debug</b>	Selects debug messages.
	<b>emergency</b>	Selects emergency possible messages.
	<b>error</b>	Selects error messages.
	<b>info</b>	Selects informational messages.
	<b>noise</b>	Selects maximum possible messages.
	<b>notice</b>	Selects notice messages.
	<b>verbose</b>	Selects verbose debug messages.
	<b>warning</b>	Selects warning messages.

**Command Default** None

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

**Usage Guidelines** Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

## Example

The following example shows how to select logs above a specific level:

```
Device# show logging profile wireless level info
```

# show logging profile wireless module

To select logs for specific modules, use the **show logging profile wireless module** command.

**show logging profile wireless module** *module-name*

<b>Syntax Description</b>	<i>module-name</i> A comma or space separated list of module names. For example, dbal, tdllib or "dbal tdllib".				
<b>Command Default</b>	None				
<b>Command Modes</b>	Privileged EXEC (#)				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.				
<b>Usage Guidelines</b>	<p>Ensure that you enable <b>internal</b> keyword using the <b>show logging profile wireless internal</b> command to get the trace output.</p> <p>Without the <b>internal</b> keyword, only customer curated logs are displayed.</p>				

## Example

The following example shows how to select logs for specific modules:

```
Device# show logging profile wireless module dbal
```

# show logging profile wireless reverse

To view logs in reverse chronological order, use the **show logging profile wireless reverse** command.

**show logging profile wireless reverse**

---

**Syntax Description**

This command has no keywords or arguments.

---

---

**Command Default**

None

---

---

**Command Modes**

Privileged EXEC (#)

---

---

**Command History**

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

---

---

**Usage Guidelines**

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

**Example**

The following example shows how to view logs in reverse chronological order:

```
Device# show logging profile wireless reverse
```

# show logging profile wireless start

To specify log filtering start location, use the **show logging profile wireless start** command.

**show logging profile wireless start** { **marker** *marker* | **timestamp** *time-stamp* }

## Syntax Description

**marker** The marker to start filtering from. It must match with previously set marker.

**timestamp** The timestamp for filtering. for example, "2017/02/10 14:41:50.849".

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

## Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

## Example

The following example shows how to specify log filtering start location:

```
Device# show logging profile wireless start timestamp 2017/02/10 14:41:50.849
```



# show logging profile wireless switch

To specify the switch to look for logs, use the **show logging profile wireless switch** command.

**show logging profile wireless switch** { *switch-num* | **active** | **standby** }

## Syntax Description

<b>active</b>	Selects the active instance.
<b>standby</b>	Selects the standby instance.

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

## Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

## Example

The following example shows how to specify the number to look for logs:

```
Device# show logging profile wireless switch active
```

# show logging profile wireless to-file

To decode files stored in disk and write the output to a file, use the **show logging profile wireless to-file** command.

**show logging profile wireless to-file** *output-file-name*

---

<b>Syntax Description</b>	<i>output-file-name</i> Output file name. File with this name will be created in the flash memory.
---------------------------	----------------------------------------------------------------------------------------------------

---

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

---

<b>Usage Guidelines</b>	Ensure that you enable <b>internal</b> keyword using the <b>show logging profile wireless internal</b> command to get the trace output.
-------------------------	-----------------------------------------------------------------------------------------------------------------------------------------

Without the **internal** keyword, only customer curated logs are displayed.

## Example

The following example shows how to decode files stored in disk and write the output to a file:

```
Device# show logging profile wireless to-file testfile
```

# show mdns-sd cache

To view mDNS cache details, use the **show mdns-sd cache** command.

```
show mdns-sd cache { ap-mac mac-address (H.H.H) | client-mac client-mac-address (H.H.H) |
detail | glan-id <1 - 5> | location-group <0 - 4096> | mdns-ap mdns-ap mac address (H.H.H)
| rlan-id <1 - 128> | statistics | type { A-AAAA | PTR | SRV | TXT } | udn
{ <1 - 4294967295> | shared } | wired | wlan-id <0 - 4096> }
```

## Syntax Description

<b>ap-mac</b> <i>mac-address (H.H.H)</i>	Specifies the AP Ethernet MAC address.
<b>client-mac</b> <i>client-mac-address (H.H.H)</i>	Specifies the client MAC address.
<b>detail</b>	Specifies the cache in detail.
<b>location-group</b> <i>&lt;0 - 4096&gt;</i>	Specifies the location group. The value range is from 0 to 4096.
<b>mdns-ap</b> <i>mdns-ap mac address (H.H.H)</i>	Specifies the cache learnt from a specific mDNS AP.
<b>rlan-id</b> <i>&lt;1 - 128&gt;</i>	Specifies the remote LAN ID. The value range is from 1 - 128.
<b>statistics</b>	Specifies the mDNS cache statistics.
<b>type</b>	Specifies the mDNS record type. The record types are, A-AAAA, PTR, SRV, and TXT.
<b>udn</b> <i>&lt;1 - 4294967295&gt;</i>	Specifies the UDN ID. The value range is from 1 to 4294967295.
<b>shared</b>	Specifies the UDN shared services.
<b>wired</b>	Specifies the mDNS services from wired clients.
<b>wlan-id</b> <i>&lt;0 - 4096&gt;</i>	Specifies the WLAN ID. The value range is from 1 to 4096.

## Command Default

None

## Command Modes

Privileged EXEC mode

## Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

## Usage Guidelines

None

## Example

The following example shows how to view the mDNS cache details:

```
Device# show mdns-sd cache
```

# show mdns-sd cache detail

To view the multicast DNS (mDNS) cache details, use the **show mdns-sd cache detail** command.

## show mdns-sd cache detail

<b>Syntax Description</b>	This command has no keywords or arguments.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC (#)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

## Example

The following is sample output from the **show mdns-sd cache detail** command:

```
Device# show mdns-sd cache detail
```

```
Name: _printer._tcp.local
Type: PTR
TTL: 4500
VLAN: 21
Client MAC: ace2.d3bc.047e
Remaining-Time: 4383
mDNS Service Policy: default-mdns-service-policy
Rdata: HP OfficeJet Pro 8720 [BC047E] (2)._printer._tcp.local
```

# show mdns-sd cache upn shared

To view the multicast DNS (mDNS) cache user personal network shared services details, use the **show mdns-sd cache upn shared** command.

## show mdns-sd cache upn shared

<b>Syntax Description</b>	This command has no keywords or arguments.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC (#)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

### Example

The following is sample output from the **show mdns-sd cache upn shared** command that displays the mDNS cache UPN shared services details:

```
Device# show mdns-sd cache upn shared
----- PTR Records -----
RECORD-NAME                                TTL      TYPE      ID      CLIENT-MAC
RR-RECORD-DATA
-----
9.1.1.7.5.D.E.F.F.F.6.C.7.E.2.1.0.0.0.0.0.0 4500     WLAN      2       10e7.c6d5.7119
HP10E7C6D57119-2860.local
_services._dns-sd._udp.local                4500     WLAN      2       10e7.c6d5.7119
_ipps._tcp.local                             4500     WLAN      2       10e7.c6d5.7119
_universal._sub._ipps._tcp.local             4500     WLAN      2       10e7.c6d5.7119
HP DeskJet 5000 series [D57119] (3127)._ipps._tcp._
_print._sub._ipps._tcp.local                 4500     WLAN      2       10e7.c6d5.7119
HP DeskJet 5000 series [D57119] (3127)._ipps._tcp._
_ePCL._sub._ipps._tcp.local                  4500     WLAN      2       10e7.c6d5.7119
HP DeskJet 5000 series [D57119] (3127)._ipps._tcp._
_ipps._tcp.local                             4500     WLAN      2       10e7.c6d5.7119
HP DeskJet 5000 series [D57119] (3127)._ipps._tcp._
_services._dns-sd._udp.local                 4500     WLAN      2       10e7.c6d5.7119
_ipp._tcp.local                              4500     WLAN      2       10e7.c6d5.7119
_universal._sub._ipp._tcp.local              4500     WLAN      2       10e7.c6d5.7119
HP DeskJet 5000 series [D57119] (3127)._ipp._tcp.l
_print._sub._ipp._tcp.local                   4500     WLAN      2       10e7.c6d5.7119
HP DeskJet 5000 series [D57119] (3127)._ipp._tcp.l
_ePCL._sub._ipp._tcp.local                    4500     WLAN      2       10e7.c6d5.7119
HP DeskJet 5000 series [D57119] (3127)._ipp._tcp.l
.
.
.
----- SRV Records -----
RECORD-NAME                                TTL      TYPE      ID      CLIENT-MAC
```

## show mdns-sd cache upn shared

## RR-RECORD-DATA

HP DeskJet 5000 series [D57119] (3127)._ipp._	4500	WLAN	2	10e7.c6d5.7119	0
0 631 HP10E7C6D57119-2860.local					
HP DeskJet 5000 series [D57119] (3127)._http.	4500	WLAN	2	10e7.c6d5.7119	0
0 80 HP10E7C6D57119-2860.local					
HP DeskJet 5000 series [D57119] (3127)._ipps.	4500	WLAN	2	10e7.c6d5.7119	0
0 631 HP10E7C6D57119-2860.local					
HP DeskJet 5000 series [D57119] (3127)._uscan	4500	WLAN	2	10e7.c6d5.7119	0
0 8080 HP10E7C6D57119-2860.local					
HP DeskJet 5000 series [D57119] (3127)._prive	4500	WLAN	2	10e7.c6d5.7119	0
0 80 HP10E7C6D57119-2860.local					
HP DeskJet 5000 series [D57119] (3127)._uscan	4500	WLAN	2	10e7.c6d5.7119	0
0 443 HP10E7C6D57119-2860.local					
HP DeskJet 5000 series [D57119] (3127)._scann	4500	WLAN	2	10e7.c6d5.7119	0
0 8080 HP10E7C6D57119-2860.local					
HP DeskJet 5000 series [D57119] (3127)._pdl-d	4500	WLAN	2	10e7.c6d5.7119	0
0 9100 HP10E7C6D57119-2860.local					

## ----- A/AAAA Records

RECORD-NAME	TTL	TYPE	ID	CLIENT-MAC
RR-RECORD-DATA				
HP10E7C6D57119-2860.local	4500	WLAN	2	10e7.c6d5.7119
8.16.16.99				

## ----- TXT Records

RECORD-NAME	TTL	TYPE	ID	CLIENT-MAC
RR-RECORD-DATA				
HP DeskJet 5000 series [D57119] (3127)._ipp._	4500	WLAN	2	10e7.c6d5.7119
[502]'txtvers=1'adminurl=http://HP10E7C6D57119-28				
HP DeskJet 5000 series [D57119] (3127)._http.	4500	WLAN	2	10e7.c6d5.7119
[1]'				
HP DeskJet 5000 series [D57119] (3127)._ipps.	4500	WLAN	2	10e7.c6d5.7119
[502]'txtvers=1'adminurl=http://HP10E7C6D57119-28				
HP DeskJet 5000 series [D57119] (3127)._uscan	4500	WLAN	2	10e7.c6d5.7119
[280]'txtvers=1'adminurl=http://HP10E7C6D57119-28				
HP DeskJet 5000 series [D57119] (3127)._prive	4500	WLAN	2	10e7.c6d5.7119
[124]'txtvers=1'ty=HP DeskJet 5000 series [D57119				
HP DeskJet 5000 series [D57119] (3127)._uscan	4500	WLAN	2	10e7.c6d5.7119
[280]'txtvers=1'adminurl=http://HP10E7C6D57119-28				
HP DeskJet 5000 series [D57119] (3127)._scann	4500	WLAN	2	10e7.c6d5.7119
[177]'txtvers=1'adminurl=http://HP10E7C6D57119-28				
HP DeskJet 5000 series [D57119] (3127)._pdl-d	4500	WLAN	2	10e7.c6d5.7119
[211]'txtvers=1'rp='priority=40'UUID=9fe36149-9				

# show mdns-sd cache upn detail

To view the multicast DNS (mDNS) cache user personal network identifier details, use the **show mdns-sd cache upn detail** command.

## show mdns-sd cache upn *upn-id* detail

<b>Syntax Description</b>	<i>upn-id</i> User personal network identifier.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Privileged EXEC (#)				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Amsterdam 17.1.1s</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.
Release	Modification				
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.				

## Example

The following is sample output from the **show mdns-sd cache upn detail** command that displays the mDNS cache UPN identifier details:

```
Device# show mdns-sd cache upn 777 detail

Name: _services._dns-sd._udp.local
Type: PTR
TTL: 4500
WLAN: 2
WLAN Name: mdns-psk
VLAN: 16
Client MAC: f4f9.51e2.a6a6
AP Ethernet MAC: 002a.1087.d68a
Remaining-Time: 4486
Site-Tag: default-site-tag
mDNS Service Policy: madhu-mDNS-Policy
Overriding mDNS Service Policy: NO
UPN-ID: 7777
UPN-Status: Enabled
Rdata: _airplay._tcp.local
```

# show mdns-sd flexconnect summary

To view the summary of the mDNS flexconnect sites, use the **show mdns-sd flexconnect summary** command.

## show mdns-sd flexconnect summary

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC mode
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

<b>Usage Guidelines</b>	None
-------------------------	------

### Example

The following example shows how to view the summary of mDNS flexconnect sites:

```
Device# show mdns-sd flexconnect summary
```



## show mdns-sd statistics

To view the mDNS statistics, use the **show mdns-sd statistics** command.

```
show mdns-sd statistics { debug | flexconnect | rlan-id <1 - 128> wired | wlan-id <1 - 4096>
}
```

Syntax Description	Parameter	Description
	<b>debug</b>	Specifies the mDNS debug statistics.
	<b>flexconnect</b>	Specifies the mDNS flexconnect statistics.
	<b>rlan-id</b> <1 - 128>	Specifies the remote LAN (RLAN) ID. The value range is from 1 to 128.
	<b>wired</b>	Specifies the mDNS wired statistics.
	<b>wlan-id</b> <1 - 4096>	Specifies the WLAN ID. The value range is from 1 to 4096.

**Command Default** None

**Command Modes** Privileged EXEC mode

Command History	Release	Modification
	Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

**Usage Guidelines** None

### Example

The following example shows how to view the mDNS statistics:

```
Device# show mdns-sd statistics
```

## show mdns-sd summary

To view the summary of mDNS service discovery configuration, use the **show mdns-sd summary** command.

**show mdns-sd summary**

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC mode
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

<b>Usage Guidelines</b>	None
-------------------------	------

### Example

The following example shows how to view the summary of mDNS service discovery configuration:

```
Device# show mdns-sd summary
```

## show mdns-sd sp-sdg statistics

To verify the Service-Peer SDG communication statistics, use the **show mdns-sd sp-sdg statistics** command.

**show mdns-sd sp-sdg statistics**

<b>Syntax Description</b>	This command has no keywords or arguments.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

The following example shows how to verify the Service-Peer SDG communication statistics:

```
Device# show mdns-sd sp-sdg statistics
                        One min, 5 mins, 1 hour
Average Input rate (pps) :    0,          0,    0
Average Output rate (pps) :    0,          0,    0
Messages sent:
Query : 0
ANY query : 0
Advertisements : 0
Advertisement Withdraw : 0
Interface down : 0
Vlan down : 0
Service-peer ID change : 0
Service-peer cache clear : 0
Resync response : 0
Keep-Alive : 1
Messages received:
Query response : 0
ANY Query response : 0
Cache-sync : 0
Get service-instance : 0
Keep-Alive response : 1
```

# show nmosp

To display the Network Mobility Services Protocol (NMSP) configuration settings, use the **show nmosp** command.

```
show nmosp {attachment | {suppress interfaces} | capability | notification interval | statistics
{connection | summary} | status | subscription detail [ip-addr ] | summary}
```

## Syntax Description

<b>attachment suppress interfaces</b>	Displays attachment suppress interfaces.
<b>capability</b>	Displays NMSP capabilities.
<b>notification interval</b>	Displays the NMSP notification interval.
<b>statistics connection</b>	Displays all connection-specific counters.
<b>statistics summary</b>	Displays the NMSP counters.
<b>status</b>	Displays status of active NMSP connections.
<b>subscription detail ip-addr</b>	The details are only for the NMSP services subscribed to by a specific IP address.
<b>subscription summary</b>	Displays details for all of the NMSP services to which the controller is subscribed. The details are only for the NMSP services subscribed to by a specific IP address.

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

The following is sample output from the **show nmosp notification interval** command:

```
Device# show nmosp notification interval
NMSP Notification Intervals
-----

RSSI Interval:
  Client           : 2 sec
  RFID             : 2 sec
  Rogue AP         : 2 sec
  Rogue Client     : 2 sec
Attachment Interval : 30 sec
Location Interval  : 30 sec
```

## show nmosp cloud-services statistics

To see NMSP cloud-service statistics, use the **show nmosp cloud-services statistics** command.

```
show nmosp cloud-services statistics [chassis {chassis-number | active | standby} R0]
```

### Syntax Description

*chassis-number* Chassis number as either 1 or 2.

**active R0** Active instance of the active NMSP cloud services in Route-processor slot 0.

**standby R0** Standby instance of the active NMSP cloud services in Route-processor slot 0.

### Command Default

None

### Command Modes

Privileged EXEC

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

### Examples

This example shows how to see NMSP cloud-service statistics:

```
Device# show nmosp cloud-services statistics
```

# show nmosp cloud-services summary

To see a summary of information about NMSP cloud-services, use the **show nmosp cloud-services summary** command.

**show nmosp cloud-services summary** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description	
<i>chassis-number</i>	Chassis number as either 1 or 2.
<b>active R0</b>	Active instance of the NMSP cloud services in Route-processor slot 0.
<b>standby R0</b>	Standby instance of the active NMSP cloud services in Route-processor slot 0.

**Command Default** None

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

This example shows how to see NMSP cloud-service summary information:

```
Device# show nmosp cloud-services summary
```

# show nmsp subscription group detail all

To display the mobility services group subscription details of all CMX connections, use the **show nmsp subscription group detail all** command.

**show nmsp subscription group detail all**

<b>Syntax Description</b>	This command has no keywords or arguments.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Privileged EXEC (#)				
<b>Command History</b>	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Gibraltar 16.10.1</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.				

## Example

The following example shows how to display the mobility services group subscription details of all CMX connections:

```
Device# show nmsp subscription group detail all
```

# show nmsp subscription group detail ap-list

To display the AP MAC list subscribed for a group by a CMX connection, use the **show nmsp subscription group detail ap-list** command.

**show nmsp subscription group detail ap-list** *group-name cmx-IP-address*

<b>Syntax Description</b>	<i>group-name</i> CMX AP group name.				
	<i>cmx-IP-address</i> CMX IP address.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Privileged EXEC (#)				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.				

## Example

The following example shows how to verify the AP MAC list subscribed for a group by a CMX connection.

```
Device# show nmsp subscription group detail ap-list Group1 127.0.0.1

CMX IP address: 127.0.0.1
CMX Group name: Group1
CMX Group AP MACs:
: 00:00:00:00:70:02 00:00:00:00:66:02 00:99:00:00:00:02 00:00:00:bb:00:02
  00:00:00:00:55:02 00:00:00:00:50:02 00:33:00:00:00:02 00:d0:00:00:00:02
  00:10:00:10:00:02 00:00:00:06:00:02 00:00:00:02:00:02 00:00:00:00:40:02
  00:00:00:99:00:02 00:00:00:00:a0:02 00:00:77:00:00:02 00:22:00:00:00:02
  00:00:00:00:00:92 00:00:00:00:00:82 00:00:00:00:03:02 aa:00:00:00:00:02
  00:00:00:50:00:42 00:00:0d:00:00:02 00:00:00:00:00:32 00:00:00:cc:00:02
  00:00:00:88:00:02 20:00:00:00:00:02 10:00:00:00:00:02 01:00:00:00:00:02
  00:00:00:00:00:02 00:00:00:00:00:01 00:00:00:00:00:00
```



# show nmsp subscription group detail services

To display the services subscribed for a group by a CMX connection, use the **show nmsp subscription group detail services** command.

**show nmsp subscription group detail services** *group-name cmx-IP-address*

## Syntax Description

<i>group-name</i>	CMX AP group name.
<i>cmx-IP-address</i>	CMX IP address.

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

## Example

The following example shows how to verify the services subscribed for a group by a CMX connection.

```
Device# show nmsp subscription group detail services Group1 127.0.0.1

CMX IP address: 127.0.0.1
CMX Group name: Group1
CMX Group filtered services:
Service          Subservice
-----
RSSI              Mobile Station,
Spectrum
Info
Statistics
```

# show nmsp subscription group summary

To display the mobility services group subscription summary of all CMX connections, use the **show nmsp subscription group summary** command.

## show nmsp subscription group summary

<b>Syntax Description</b>	This command has no keywords or arguments.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC (#)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

## Example

The following example shows how to verify the mobility services group subscription summary of all CMX connections.

```
Device# show nmsp subscription group summary
CMX IP address: 127.0.0.1
Groups subscribed by this CMX server:
Group name: Group1
```

# show platform conditions

To see information about conditional debugs, use the **show platform conditions** command.

**show platform conditions**

---

**Command Default**

None

---

**Command Modes**

Privileged EXEC

---

**Command History**

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

## Examples

The following example shows how to see information about conditional debugs:

```
Device# show platform conditions
```

# show platform software wlavc status cp-exporter

To view the wireless AVC information from the control place exporter, use the **show platform software wlavc status cp-exporter** command.

**show platform software wlavc status cp-exporter**

<b>Syntax Description</b>	<b>wlavc</b>	Displays the wireless AVC information.
	<b>status</b>	Displays information about the AVC status.
	<b>cp-exporter</b>	Collects information from the Control Plane exporter.
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC (#) mode	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

## Example

This example shows how to display the wireless AVC information from the control place exporter:

```
show platform software wlavc status cp-exporter
AVC FNF Exporter status
IP: 10.10.1.1
connection statistics
Sent bytes : 5672
Sent packets : 569
Received records : 564
Socket statistics
New sockets : 3
Closed sockets : 0
Library statistics AVC
cache errors : 0
Unexpected Flow Monitor ID : 0
Socket creation error : 0
Sent records : 240
Received packets : 800
```

# show platform software system all

To check status of the current virtual machine and look for performance issues due to inadequate resources (or other issues with the hosting environment), use the **set platform software system all** command in privileged EXEC mode.

## show platform software system all

### Syntax Description

This command has no keywords or arguments.

### Command Modes

Privileged EXEC (#)

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

### Examples

This example shows how to check status of the current virtual machine and its resources:

```
Device# show platform software system all

Processor Details
=====
Number of Processors : 6
Processor : 1 - 6
vendor_id : GenuineIntel
cpu MHz : 2593.750
cache size : 35840 KB
Crypto Supported : Yes
model name : Intel(R) Xeon(R) CPU E5-2690 v4 @ 2.60GHz

Memory Details
=====
Physical Memory : 16363904KB

VNIC Details
=====
Name      Mac Address      Status Platform MTU
GigabitEthernet1 000c.2964.7126  UP 1500
GigabitEthernet2 000c.2964.7130  UP 1500

Hypervisor Details
=====
Hypervisor: VMWARE
Manufacturer: VMware, Inc.
Product Name: VMware Virtual Platform
Serial Number: VMware-56 4d e5 0a a7 dd 27 2b-0e 2f 36 6e 0f 64 71 26
UUID: 564DE50A-A7DD-272B-0E2F-366E0F647126
image_variant :

Boot Details
=====
Boot mode: BIOS
Bootloader version: 1.1
```

# show platform software trace filter-binary

To display the most recent trace information for a specific module, use the **show platform software trace filter-binary** command in privileged EXEC or user EXEC mode.

**show platform software trace filter-binary***modules* [**context** *mac-address*]

<b>Syntax Description</b>	<b>context</b> <i>mac-address</i>	Represents the context used to filter. Additionally, you can filter based on module names and trace levels. The context keyword accepts either a MAC address or any other argument based on which a trace is tagged.
---------------------------	-----------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>Command Modes</b>	User EXEC (>) Privileged EXEC (#)
----------------------	--------------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

<b>Usage Guidelines</b>	This command collates and sorts all the logs present in the <code>/tmp/.../</code> across all the processes relevant to the module. The trace logs of all the processes relevant to the specified module are printed to the console. This command also generates a file named <code>collated_log_{system time}</code> with the same content, in the <code>/crashinfo/tracelogs</code> directory.
-------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>Examples</b>	This example shows how to display the trace information for a wireless module:
-----------------	--------------------------------------------------------------------------------

```
Device# show platform software trace filter-binary wireless
```

## show platform software trace level

To view the trace levels for all the modules under a specific process, use the **show platform software trace level** command in privileged EXEC or user EXEC mode.

Syntax Description	<i>process</i>	Process whose tracing level is being set. Options include:
		<ul style="list-style-type: none"> <li>• <b>chassis-manager</b>—The Chassis Manager process.</li> <li>• <b>cli-agent</b>—The CLI Agent process.</li> <li>• <b>cmm</b>—The CMM process.</li> <li>• <b>dbm</b>—The Database Manager process.</li> <li>• <b>emd</b>—The Environmental Monitoring process.</li> <li>• <b>fed</b>—The Forwarding Engine Driver process.</li> <li>• <b>forwarding-manager</b>—The Forwarding Manager process.</li> <li>• <b>geo</b>—The Geo Manager process.</li> <li>• <b>host-manager</b>—The Host Manager process.</li> <li>• <b>interface-manager</b>—The Interface Manager process.</li> <li>• <b>iomd</b>—The Input/Output Module daemon (IOMd) process.</li> <li>• <b>ios</b>—The IOS process.</li> <li>• <b>license-manager</b>—The License Manager process.</li> <li>• <b>logger</b>—The Logging Manager process.</li> <li>• <b>platform-mgr</b>—The Platform Manager process.</li> <li>• <b>pluggable-services</b>—The Pluggable Services process.</li> <li>• <b>replication-mgr</b>—The Replication Manager process.</li> <li>• <b>shell-manager</b>—The Shell Manager process.</li> <li>• <b>sif</b>—The Stack Interface (SIF) Manager process.</li> <li>• <b>smd</b>—The Session Manager process.</li> <li>• <b>stack-mgr</b>—The Stack Manager process.</li> <li>• <b>table-manager</b>—The Table Manager Server.</li> <li>• <b>thread-test</b>—The Multithread Manager process.</li> <li>• <b>virt-manager</b>—The Virtualization Manager process.</li> <li>• <b>wireless</b>—The wireless controller module process.</li> </ul>

<i>slot</i>	<p>Hardware slot where the process for which the trace level is set, is running. Options include:</p> <ul style="list-style-type: none"> <li>• <i>number</i>—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2.</li> <li>• <i>SIP-slot / SPA-bay</i>—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2.</li> <li>• <b>F0</b>—The Embedded Service Processor in slot 0.</li> <li>• <b>F1</b>—The Embedded Service Processor in slot 1.</li> <li>• <b>FP active</b>—The active Embedded Service Processor.</li> <li>• <b>R0</b>—The route processor in slot 0.</li> <li>• <b>RP active</b>—The active route processor.</li> <li>• <b>switch &lt;number&gt;</b> —The switch, with its number specified.</li> <li>• <b>switch active</b>—The active switch.</li> <li>• <b>switch standby</b>—The standby switch. <ul style="list-style-type: none"> <li>• <i>number</i>—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2.</li> <li>• <i>SIP-slot / SPA-bay</i>—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2.</li> <li>• <b>F0</b>—The Embedded Service Processor in slot 0.</li> <li>• <b>FP active</b>—The active Embedded Service Processor.</li> <li>• <b>R0</b>—The route processor in slot 0.</li> <li>• <b>RP active</b>—The active route processor.</li> </ul> </li> </ul>
-------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Command Modes**

User EXEC (&gt;)

Privileged EXEC (#)

**Command History**

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Examples**

This example shows how to view the trace level:

```
Device# show platform software trace level dbm chassis active R0
```



Module Name	Trace Level
-----	-----
binos	Notice
binos/brand	Notice
bipc	Notice
btrace	Notice
bump_ptr_alloc	Notice
cdllib	Notice
chasfs	Notice
dbal	Informational
dbm	Debug
evlib	Notice
evutil	Notice
file_alloc	Notice
green-be	Notice
ios-avl	Notice
klib	Debug
services	Notice
sw_wdog	Notice
syshw	Notice
tcl_cdlcore_message	Notice
tcl_dbal_root_message	Notice
tcl_dbal_root_type	Notice

## show platform software trace message

To display the trace messages for a process, use the **set platform software trace** command in privileged EXEC or user EXEC mode.

**show platform software trace message** *process* **chassis**{<1-2> | **active** | **standby**} **R0**

### Command Modes

User EXEC (>)

Privileged EXEC (#)

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

### Examples

This example shows how to display the trace messages for the Stack Manager and the Forwarding Engine Driver processes:

```
Device# show platform software trace message stack_mgr switch active R0
10/30 09:42:48.767 [btrace] [8974]: (note): Successfully registered module [97] [uiutil]
10/30 09:42:48.762 [btrace] [8974]: (note): Successfully registered module [98]
[tdl_cdlcore_message]
10/29 13:28:19.023 [stack_mgr] [8974]: (note): Examining peer state
10/29 13:28:19.023 [stack_mgr] [8974]: (note): no switch eligible for standby election
presently
10/29 13:28:19.022 [stack_mgr] [8974]: (note): Posting event
stack_fsm_event_wait_standby_elect_timer_expired, curstate stack_fsm_state_active_ready
10/29 13:28:19.022 [stack_mgr] [8974]: (note): Timer HDL - STACK_WAIT_STANDBY_ELECT_TIMER
expired
10/29 13:26:46.584 [btrace] [8974]: (note): Successfully registered module [99]
[tdl_ui_message]
10/29 13:26:46.582 [bipc] [8974]: (note): Pending connection to server 10.129.1.0
10/29 13:26:36.582 [evutil] [8974]: (ERR): Connection attempt for sman-ui-serv (uipeer
uplink to slot 1) failed, invoking disconnect
10/29 13:26:36.582 [evutil] [8974]: (ERR): Asynchronous connect failed for [uipeer uplink
to slot 1] (fd == -1)
10/29 13:26:36.581 [bipc] [8974]: (note): Pending connection to server 10.129.1.0
10/29 13:26:26.581 [evutil] [8974]: (ERR): Connection attempt for sman-ui-serv (uipeer
uplink to slot 1) failed, invoking disconnect
```

# show platform software trace message license-manager chassis active R0

To display the trace message for license-manager process of active route processor, use the **show platform software trace message license-manager chassis active R0** command in privileged EXEC mode.

```
show platform software trace message license-manager chassis {chassis-number
| active | standby}R0reverse
```

This command has no arguments or keywords.

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

## Example

This example shows how to display the trace messages for the Forwarding Engine Driver processes:

```
Device# show platform software trace message license-manager chassis active R0
.....
2018/06/25 07:16:53.121 {lman_R0-0}{1}: [btrace] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Decode of the file /tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy completed in 35
msecs
/tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy: DECODE(50:50:0:7)
2018/06/25 07:16:53.088 {lman_R0-0}{1}: [btrace] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Decode of file [/tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy] returned [0]
2018/06/25 06:53:20.421 {lman_R0-0}{1}: [btrace] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Decode of the file /tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy completed in 34
msecs
2018/06/25 06:53:20.389 {lman_R0-0}{1}: [btrace] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Decode of file [/tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy] returned [0]
2018/06/20 07:55:10.540 {lman_R0-0}{1}: [trccfg] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Processing all-modules
2018/06/20 07:55:10.540 {lman_R0-0}{1}: [trccfg] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Empty trace conf file
2018/06/20 07:54:46.453 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Constructing domain iosd_lmrp for RP/0/0 to RP/0/0
2018/06/20 07:54:46.453 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Received registration msg from [IOS]
2018/06/20 07:54:46.449 {lman_R0-0}{1}: [bipc] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Received a connection from client for path /tmp/rp/lipc/license_mgr_socket
2018/06/20 07:54:45.557 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:44.556 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:43.556 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:42.555 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:41.554 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
```

## show platform software trace message license-manager chassis active R0

```

2018/06/20 07:54:40.553 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:39.553 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:38.552 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:37.551 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:36.550 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:35.550 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:34.549 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:33.548 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:32.547 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:31.547 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:30.547 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:30.537 {lman_R0-0}{1}: [bipc] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Pending connection to server 10.0.1.0
2018/06/20 07:54:29.546 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:28.545 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:27.545 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:26.544 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:25.543 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:24.542 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:23.542 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:22.541 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:21.540 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:20.633 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note): Peer
attach: from location R0:0 is successful
2018/06/20 07:54:20.633 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note): Not
setting domain for cmand
2018/06/20 07:54:20.625 {lman_R0-0}{1}: [bipc] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Received a connection from client for path /tmp/rp/lipc/lman_lic_serv_socket
2018/06/20 07:54:20.624 {lman_R0-0}{1}: [tdllib] [21231]: UUID: 0, ra: 0, TID: 0 (note):
epoch file read /tmp/tldresolve/epoch_dir//2018_06_20_07_54_2413.epoch
2018/06/20 07:54:20.624 {lman_R0-0}{1}: [tdllib] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Detect newly epoch file generated: new epoch:
/tmp/tldresolve/epoch_dir//2018_06_20_07_54_2413.epoch
2018/06/20 07:54:20.624 {lman_R0-0}{1}: [tdllib] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Flag tdlh stale epoch for all tdl handles
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Chasfs Watch on rp/0/0/rtu_licensing for platform to create RTU properties
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note): The
chassis product id: 'ISR4461/K9'
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note): The
chassis serial number: 'FDO2213A0GL'
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [bcrdu] [21231]: UUID: 0, ra: 0, TID: 0 (note):
CRDU
/tmp/sw/mount/isr4400v2-mono-universalk9.BLD_V169_THROTTLE_LATEST_20180618_044856_V16_9_0_163.SSA.pkg/usr/binos/bin/lman

```

```
proc path is /tmp/patch/CRDU/BPROC_LM_RP/
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [bcrdu] [21231]: UUID: 0, ra: 0, TID: 0 (note):
CRDU
/tmp/sw/mount/isr4400v2-mono-universalk9.ELD_V169_THROTTLE_LATEST_20180618_044856_V16_9_0_163.SSA.pkg/usr/binos/bin/lman
procstr is BPROC_LM_RP
2018/06/20 07:54:20.533 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note): No
licensing objects present in chasfs to delete
2018/06/20 07:54:20.533 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Deleting any existing licensing chasfs objects under [rp/0/0/licensing]
2018/06/20 07:54:20.532 {lman_R0-0}{1}: [syshw] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): syshw
build device: could not add register 7 dev:
/sys/bus/platform/devices/cpld/reg_rp_sku_register (No such file or directory) due to No
such file or directory
2018/06/20 07:54:20.532 {lman_R0-0}{1}: [syshw] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): syshw
build device: could not add register 5 dev: /sys/bus/platform/devices/cpld/phys_slot_number
(No such file or directory) due to No such file or directory

Total messages : 49
```

# show policy-map

To display quality of service (QoS) policy maps, which define classification criteria for incoming traffic, use the **show policy-map** command in EXEC mode.

```
show policy-map [{policy-map-name | interface interface-id}]
```

```
show policy-map interface {Auto-template | Capwap | GigabitEthernet | GroupVI |
InternalInterface | Loopback | Lspvif | Null | Port-channel | TenGigabitEthernet | Tunnel
| Vlan | brief | class | input | output
```

```
show policy-map interface {ap name ap_name | client mac mac_address | radio type {24ghz |
5ghz} ap name ap_name | ssid name ssid_name {ap name ap_name | radio type {24ghz | 5ghz}
ap name ap_name}}
```

Syntax Description		
	<i>policy-map-name</i>	(Optional) Name of the policy-map.
	<b>interface</b> <i>interface-id</i>	(Optional) Displays the statistics and the configurations of the input and output policies that are attached to the interface.
	<b>ap name</b> <i>ap_name</i>	Displays SSID policy configuration of an access point.
	<b>client mac</b> <i>mac_address</i>	Displays information about the policies for all the client targets.
	<b>radio type</b> {24ghz   5ghz}	Displays policy configuration of the access point in the specified radio type.
	<b>ssid name</b> <i>ssid_name</i>	Displays policy configuration of an SSID.

Command Modes	
	User EXEC
	Privileged EXEC

Command History	Release	Modification
		This command was introduced.

Usage Guidelines	
	Policy maps can include policers that specify the bandwidth limitations and the action to take if the limits are exceeded.



**Note** Though visible in the command-line help string, the **control-plane**, **session**, and **type** keywords are not supported, and the statistics shown in the display should be ignored.

To display classification counters for ternary content addressable memory (TCAM) (marking or policing) based policies, enter the interface ID. Classification counters have the following restrictions:

- Classification counters are supported only on wired ports (in the ingress and egress directions).
- Classification counters count packets instead of bytes.
- Only QoS configurations with marking or policing trigger the classification counter.
- As long as there is policing or marking action in the policy, the class-default will have classification counters.
- Classification counters are not port based. The counters are shared across targets sharing the same policy map. This means that the classification counter aggregates all packets belonging to the same class of the same policy which attach to different interfaces.

This is an example of output from the **show policy-map interface** command, where classification counters are displayed:

```
Device# show policy-map interface gigabitEthernet1/0/1

GigabitEthernet1/0/1

Service-policy input: AutoQos-4.0-CiscoPhone-Input-Policy

Class-map: AutoQos-4.0-Voip-Data-CiscoPhone-Class (match-any)
  0 packets
  Match: cos 5
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp ef
  police:
    cir 128000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Voip-Signal-CiscoPhone-Class (match-any)
  0 packets
  Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs3
  police:
    cir 32000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps
```

```

Class-map: AutoQos-4.0-Default-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Default
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp default

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps

Service-policy output: AutoQos-4.0-Output-Policy

queue stats for all priority classes:
  Queueing
  priority level 1

  (total drops) 0
  (bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  0 packets
  Match: dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match: dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

```



```
(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match: dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match: dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 4%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match: dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 1%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match: dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
```

```
5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 25%
queue-buffers ratio 25
```

# show ssh

To see the SSH connection status, use the **show ssh** command.

```
show ssh {connection-number | {vtty connection-number } }
```

---

**Syntax Description**

*connection-number* SSH connection number. Valid range is 0 to 530.

---

---

**Command Default**

None

---

**Command Modes**

Privileged EXEC

---

---

**Command History**

<b>Release</b>	<b>Modification</b>
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

## Examples

The following example shows how to see the SSH connection status:

```
Device# show ssh connection-number
```

# show stealthwatch-cloud connection

To view the connection details of Stealthwatch Cloud, use the **show stealthwatch-cloud connection** command.

## show stealthwatch-cloud connection

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC mode
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.4.1	This command was introduced.

<b>Usage Guidelines</b>	None
-------------------------	------

### Example

The following example shows how to view the connection details of Stealthwatch Cloud:

```
Device# show stealthwatch-cloud connection
```

# show stealthwatch-cloud wireless-shim

To view the wireless-shim details of Stealthwatch Cloud, use the **show stealthwatch-cloud wireless-shim** command.

## show stealthwatch-cloud wireless-shim

---

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--------------------------------------------

---

---

<b>Command Default</b>	None
------------------------	------

---

---

<b>Command Modes</b>	Privileged EXEC mode
----------------------	----------------------

---

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Bengaluru 17.4.1	This command was introduced.

---

---

<b>Usage Guidelines</b>	None
-------------------------	------

---

### Example

The following example shows how to view the wireless-shim details of Stealthwatch Cloud:

```
Device# show stealthwatch-cloud wireless-shim
```

# show tech-support wireless

To display Cisco wireless LAN controller variables frequently requested by Cisco Technical Assistance Center (TAC), use the **show tech-support wireless** command in privileged EXEC mode.

## show tech-support wireless

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

The following is sample output from the **show tech-support wireless** command:

```
Device# show tech-support wireless
*** show ap capwap timers ***

Cisco AP CAPWAP timers

AP Discovery timer      : 10
AP Heart Beat timeout  : 30
Primary Discovery timer : 120
Primed Join timeout    : 0
Fast Heartbeat         : Disabled
Fast Heartbeat timeout : 1
*** show ap capwap retransmit ***
Global control packet retransmit interval : 3
Global control packet retransmit count : 5

AP Name                                Retransmit Interval      Retransmit Count
-----
TSIM_AP-2                              3                          5
TSIM_AP-3                              3                          5
*** show ap dot11 24ghz cleanair air-quality summary ***

AQ = Air Quality
DFS = Dynamic Frequency Selection

*** show ap dot11 24ghz cleanair air-quality worst ***

AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel  Avg AQ  Min AQ  Interferers  DFS
-----
              0         0       0       0             0       No

*** show ap dot11 24ghz cleanair config ***

Clean Air Solution..... : Disabled
Air Quality Settings:
  Air Quality Reporting..... : Disabled
  Air Quality Reporting Period (min)..... : 15
```

```

Air Quality Alarms..... : Enabled
Air Quality Alarm Threshold..... : 10
Interference Device Settings:
  Interference Device Reporting..... : Enabled
    Bluetooth Link..... : Enabled
    Microwave Oven..... : Enabled
    802.11 FH..... : Enabled
    Bluetooth Discovery..... : Enabled
    TDD Transmitter..... : Enabled
    Jammer..... : Enabled
    Continuous Transmitter..... : Enabled
    DECT-like Phone..... : Enabled
    Video Camera..... : Enabled
    802.15.4..... : Enabled
    WiFi Inverted..... : Enabled
    WiFi Invalid Channel..... : Enabled
    SuperAG..... : Enabled
    Canopy..... : Enabled
    Microsoft Device..... : Enabled
    WiMax Mobile..... : Enabled
    WiMax Fixed..... : Enabled
  Interference Device Types Triggering Alarms:
    Bluetooth Link..... : Disabled
    Microwave Oven..... : Disabled
    802.11 FH..... : Disabled
    Bluetooth Discovery..... : Disabled
    TDD Transmitter..... : Disabled
    Jammer..... : Disabled
    Continuous Transmitter..... : Disabled
    DECT-like Phone..... : Disabled
    Video Camera..... : Disabled
    802.15.4..... : Disabled
    WiFi Inverted..... : Enabled
    WiFi Invalid Channel..... : Enabled
    SuperAG..... : Disabled
    Canopy..... : Disabled
    Microsoft Device..... : Disabled
    WiMax Mobile..... : Disabled
    WiMax Fixed..... : Disabled
  Interference Device Alarms..... : Enabled
Additional Clean Air Settings:
  CleanAir Event-driven RRM State..... : Disabled
  CleanAir Driven RRM Sensitivity..... : LOW
  CleanAir Persistent Devices state..... : Disabled

```

# show tech-support wireless ap

To display specific information about the Cisco APs variables frequently requested by Cisco Technical Assistance Center (TAC), use the **show tech-support wireless ap** command in privileged EXEC mode.

## show tech-support wireless ap

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

**Usage Guidelines** The output of the following commands are displayed as part of **show tech-support wireless ap** command:

- show ap session termination statistics
- show ap status
- show ap tag summary
- show platform software bssid chassis active F0 statistics
- show platform software bssid chassis active R0 statistics
- show platform software capwap chassis active F0 statistics
- show platform software capwap chassis active R0 statistics
- show platform software dtls chassis active F0 statistics
- show platform software dtls chassis active R0 statistics
- show platform software radio chassis active F0 statistics
- show platform software radio chassis active R0 statistics

### Example

The following is sample output from the **show tech-support wireless ap** command

```
Device# show tech-support wireless ap
----- show platform software dtls chassis active R0 statistics -----

DTLS Counters      (Success/Failure)
-----
Create              0/0
```



```
Delete                0/0
```

```
Switch 1:
OM Create             0/0
OM Delete             0/0
Ack Nack Notify      0/0
```

```
----- show platform software radio chassis active R0 statistics
-----
```

```
Switch 1:
NACK Notify          0/0
  Create Failure      0
  Delete Failure      0
```

```
----- show platform software bssid chassis active R0 statistics
-----
```

```
Switch 1:
NACK Notify          0/0
  Create Failure      0
  Delete Failure      0
```

```
----- show platform software capwap chassis active R0 statistics
-----
```

```
Capwap Counters      (Success/Failure)
-----
```

```
Create                0/0
Delete                0/0
Modify                0/0
```

```
Switch 1:
OM Create             0/0
OM Delete             0/0
ACK-NACK Notify      0/0
  Tunnel State        0/0
  Tunnel Create        0/0
  Tunnel Modify        0/0
  Tunnel Delete        0/0
```

```
----- show platform software dtls chassis active F0 statistics -----
```

```
DTLS Counters        (Success/Failure)
-----
```

```
Create                0/0
Delete                0/0
HW Create             0/0
HW Modify             0/0
HW Delete             0/0
Create Ack            0/0
Modify Ack            0/0
Delete Ack            0/0
Ack Ack Notify        0/0
```

```

Ack Nack Notify          0/0
Nack Notify              0/0
HA Seq GET               665/0
HA Seq SET               0/0
HA Seq Crypto GET       0/0
HA Seq Crypto SET       0/0
HA Seq Crypto Callback  0/0

HA Seq last Responded   0
HA Seq Pending          0
HA Seq Outstanding cb   0

```

```

----- show platform software radio chassis active F0 statistics
-----

```

```

Radio Counters      (Success/Failure)
-----
Create              0/0
Delete              0/0
HW Create           0/0
HW Modify           0/0
HW Delete           0/0
Create Ack          0/0
Modify Ack          0/0
Delete Ack          0/0
Nack Notify         0/0

```

```

----- show platform software bssid chassis active F0 statistics
-----

```

```

Bssid Counters      (Success/Failure)
-----
Create              0/0
Delete              0/0
HW Create           0/0
HW Modify           0/0
HW Delete           0/0
Create Ack          0/0
Modify Ack          0/0
Delete Ack          0/0
Nack Notify         0/0

```

```

----- show platform software capwap chassis active F0 statistics
-----

```

```

Capwap Counters      (Success/Failure)
-----
Create              0/0
Delete              0/0
HW Create           0/0
HW Modify           0/0
HW Delete           0/0
Create Ack          0/0
Modify Ack          0/0
Delete Ack          0/0
Ack Ack Notify     0/0
Ack Nack Notify    0/0
Nack Notify         0/0

```

```

----- show ap auto-rf dot11 24ghz -----

----- show ap auto-rf dot11 5ghz -----

----- show ap capwap retransmit -----

----- show ap config dot11 dual-band summary -----

----- show ap config general -----

----- show ap dot11 24ghz channel -----

Leader Automatic Channel Assignment
Channel Assignment Mode           : AUTO
Channel Update Interval          : 600 seconds
Anchor time (Hour of the day)    : 0
Channel Update Contribution
  Noise                           : Enable
  Interference                     : Enable
  Load                             : Disable
  Device Aware                     : Disable
CleanAir Event-driven RRM option : Disabled
Channel Assignment Leader        : ewlc-doc (9.12.32.10)
Last Run                          : 25 seconds ago

DCA Sensitivity Level             : MEDIUM : 10 dB
DCA Minimum Energy Limit         : -95 dBm
Channel Energy Levels
  Minimum                          : unknown
  Average                          : unknown
  Maximum                          : -128 dBm
Channel Dwell Times
  Minimum                          : unknown
  Average                          : unknown

----- show ap dot11 24ghz group -----

Radio RF Grouping

802.11b Group Mode                : AUTO
802.11b Group Update Interval    : 600 seconds
802.11b Group Leader             : ewlc-doc (9.12.32.10)
802.11b Last Run                 : 26 seconds ago

RF Group Members

Controller name                   Controller IP

```

```
-----
ewlc-doc                               9.12.32.10
```

```
----- show ap dot11 24ghz load-info -----
```

```
----- show ap dot11 24ghz monitor -----
```

```
Default 802.11b AP monitoring
 802.11b Monitor Mode           : Enabled
 802.11b Monitor Channels       : Country channels
 802.11b RRM Neighbor Discover Type : Transparent
 802.11b AP Coverage Interval   : 180 seconds
 802.11b AP Load Interval      : 60 seconds
 802.11b AP Noise Interval      : 180 seconds
 802.11b AP Signal Strength Interval : 60 seconds
 802.11b NDP RSSI Normalization  : Enabled
```

```
----- show ap dot11 24ghz network -----
```

```
802.11b Network           : Enabled
11gSupport                : Enabled
11nSupport                : Enabled
802.11b/g Operational Rates
 802.11b 1M               : Mandatory
 802.11b 2M               : Mandatory
 802.11b 5.5M            : Mandatory
 802.11b 11M             : Mandatory
 802.11g 6M              : Supported
 802.11g 9M              : Supported
 802.11g 12M             : Supported
 802.11g 18M            : Supported
 802.11g 24M            : Supported
 802.11g 36M            : Supported
 802.11g 48M            : Supported
 802.11g 54M            : Supported
802.11n MCS Settings:
MCS 0 : Supported
MCS 1 : Supported
MCS 2 : Supported
MCS 3 : Supported
```

```
----- show ap dot11 24ghz profile -----
```

```
Default 802.11b AP performance profiles
 802.11b Global Interference threshold : 10 %
 802.11b Global noise threshold       : -70 dBm
 802.11b Global RF utilization threshold : 80 %
 802.11b Global throughput threshold  : 1000000 bps
 802.11b Global clients threshold     : 12 clients
```

```
----- show ap dot11 24ghz summary -----
```

```
----- show ap dot11 24ghz txpower -----
```

Automatic Transmit Power Assignment

```

Transmit Power Assignment Mode      : AUTO
Transmit Power Update Interval      : 600 seconds
Transmit Power Threshold             : -70 dBm
Transmit Power Neighbor Count       : 3 APs
Min Transmit Power                   : -10 dBm
Max Transmit Power                   : 30 dBm
Update Contribution
  Noise                               : Enable
  Interference                         : Enable
  Load                                : Disable
  Device Aware                         : Disable
Transmit Power Assignment Leader     : ewlc-doc (9.12.32.10)
Last Run                              : 27 seconds ago

```

```
----- show ap dot11 5ghz channel -----
```

Leader Automatic Channel Assignment

```

Channel Assignment Mode              : AUTO
Channel Update Interval              : 600 seconds
Anchor time (Hour of the day)       : 0
Channel Update Contribution
  Noise                               : Enable
  Interference                         : Enable
  Load                                : Disable
  Device Aware                         : Disable
CleanAir Event-driven RRM option    : Disabled
Channel Assignment Leader            : ewlc-doc (9.12.32.10)
Last Run                              : 27 seconds ago

DCA Sensitivity Level                : MEDIUM : 15 dB
DCA 802.11n/ac Channel Width        : 20 MHz
DCA Minimum Energy Limit             : -95 dBm
Channel Energy Levels
  Minimum                             : unknown
  Average                              : unknown
  Maximum                              : -128 dBm
Channel Dwell Times
  Minimum                              : unknown

```

```
----- show ap dot11 5ghz group -----
```

Radio RF Grouping

```

802.11a Group Mode                   : AUTO
802.11a Group Update Interval       : 600 seconds
802.11a Group Leader                 : ewlc-doc (9.12.32.10)
802.11a Last Run                     : 28 seconds ago

```

RF Group Members

```

Controller name                      Controller IP

```

```
-----
ewlc-doc                               9.12.32.10
```

```
----- show ap dot11 5ghz load-info -----
```

```
----- show ap dot11 5ghz monitor -----
```

```
Default 802.11a AP monitoring
 802.11a Monitor Mode           : Enabled
 802.11a Monitor Channels       : Country channels
 802.11a RRM Neighbor Discover Type : Transparent
 802.11a AP Coverage Interval   : 180 seconds
 802.11a AP Load Interval       : 60 seconds
 802.11a AP Noise Interval      : 180 seconds
 802.11a AP Signal Strength Interval : 60 seconds
 802.11a NDP RSSI Normalization  : Enabled
```

```
----- show ap dot11 5ghz network -----
```

```
802.11a Network                 : Enabled
11nSupport                      : Enabled
 802.11a Low Band               : Enabled
 802.11a Mid Band               : Enabled
 802.11a High Band              : Enabled
802.11a Operational Rates
 802.11a 6M                    : Mandatory
 802.11a 9M                    : Supported
 802.11a 12M                   : Mandatory
 802.11a 18M                   : Supported
 802.11a 24M                   : Mandatory
 802.11a 36M                   : Supported
 802.11a 48M                   : Supported
 802.11a 54M                   : Supported
802.11n MCS Settings:
MCS 0 : Supported
MCS 1 : Supported
MCS 2 : Supported
MCS 3 : Supported
MCS 4 : Supported
MCS 5 : Supported
```

```
----- show ap dot11 5ghz profile -----
```

```
Default 802.11a AP performance profiles

 802.11a Global Interference threshold : 10 %
 802.11a Global noise threshold       : -70 dBm
 802.11a Global RF utilization threshold : 80 %
 802.11a Global throughput threshold  : 1000000 bps
 802.11a Global clients threshold     : 12 clients
```

```
----- show ap dot11 5ghz summary -----
```

----- show ap dot11 5ghz txpower -----

Automatic Transmit Power Assignment

```

Transmit Power Assignment Mode      : AUTO
Transmit Power Update Interval      : 600 seconds
Transmit Power Threshold             : -70 dBm
Transmit Power Neighbor Count       : 3 APs
Min Transmit Power                   : -10 dBm
Max Transmit Power                   : 30 dBm
Update Contribution
  Noise                               : Enable
  Interference                         : Enable
  Load                                : Disable
  Device Aware                         : Disable
Transmit Power Assignment Leader     : ewlc-doc (9.12.32.10)
Last Run                             : 28 seconds ago
    
```

----- show ap image -----

----- show wireless stats ap join summary -----

Number of APs: 0

Base MAC	Ethernet MAC	AP Name	IP Address	Status
Last Failure Type	Last Disconnect Reason			

----- show ap rf-profile summary -----

Number of RF-profiles: 6

RF Profile Name	Band	Description	State
Low_Client_Density_rf_5gh	5 GHz	pre configured Low Client Density rf	Up
High_Client_Density_rf_5gh	5 GHz	pre configured High Client Density r	Up
Low_Client_Density_rf_24gh	2.4 GHz	pre configured Low Client Density rf	Up
High_Client_Density_rf_24gh	2.4 GHz	pre configured High Client Density r	Up
Typical_Client_Density_rf_5gh	5 GHz	pre configured Typical Density rfpro	Up
Typical_Client_Density_rf_24gh	2.4 GHz	pre configured Typical Client Densit	Up

----- show ap slots -----

----- show ap summary -----

Number of APs: 0

```
----- show ap uptime -----
```

```
Number of APs: 0
```

```
----- show ap tag summary -----
```

```
Number of APs: 0
```

```
----- show ap status -----
```

```
----- show ap cdp neighbors -----
```

```
Number of neighbors: 0
```

```
----- show ap ap-join-profile summary -----
```

```
Number of AP Profiles: 1
```

AP Profile Name	Description
default-ap-profile	default ap profile

```
----- show ap link-encryption -----
```

```
----- show wireless stats ap session termination -----
```

```
----- show wireless loadbalance ap affinity wncd 0 -----
```

```
----- show wireless loadbalance ap affinity wncd 1 -----
```

```
----- show wireless loadbalance ap affinity wncd 2 -----
```

```
----- show wireless loadbalance ap affinity wncd 3 -----
```

```
----- show wireless loadbalance ap affinity wncd 4 -----
```

```
----- show wireless loadbalance ap affinity wncd 5 -----
```



```
----- show wireless loadbalance ap affinity wncd 6 -----
```

```
----- show wireless loadbalance ap affinity wncd 7 -----
```

# show tech-support wireless client

To print the data related to all clients or a particular client, use the **show tech-support wireless client** command in privileged EXEC mode.

## show tech-support wireless client

<b>Syntax Description</b>	<b>mac-address</b> Client MAC address.
---------------------------	----------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

**Usage Guidelines** The output of the following commands are displayed as part of **show tech-support wireless client** command:

- show platform software wireless-client chassis active F0 statistics
- show platform software wireless-client chassis active R0 statistics
- show wireless client calls active
- show wireless client calls rejected
- show wireless client client-statistics summary
- show wireless client device summary
- show wireless client mac <mac-addr> details
- show wireless client probing
- show wireless client sleeping-client
- show wireless client statistic
- show wireless client steering
- show wireless client summary
- show wireless exclusionlist
- show wireless pmk-cache

### Example

The following is sample output from the **show tech-support wireless client** command

```

Device# show tech-support wireless client

----- show wireless stats client summary -----

Number of Local Clients : 0

MAC Address      AP Name                WLAN UpTime(secs) Rx Pkts Tx Pkts RSSI SNR
  Data Retries
-----

----- show wireless client summary -----

Number of Local Clients: 0

Number of Excluded Clients: 0

----- show wireless client device summary -----

----- show wireless client steering -----

Client Steering Configuration Information
Macro to micro transition threshold      : -55 dBm
Micro to Macro transition threshold      : -65 dBm
Micro-Macro transition minimum client count : 3
Micro-Macro transition client balancing window : 3
Probe suppression mode                   : Disabled
Probe suppression validity window        : 100 s
Probe suppression aggregate window       : 200 ms
Probe suppression transition aggressiveness : 3
Probe suppression hysteresis             : -6 dBm

WLAN Configuration Information

----- show wireless client calls active -----

----- show wireless client calls rejected -----

----- show wireless client sleeping-client -----

Total number of sleeping-client entries: 0

----- show wireless client probing -----

----- show wireless client ap dot11 24ghz -----

```

```
----- show wireless client ap dot11 5ghz -----
```

```
----- show wireless pmk-cache -----
```

Number of PMK caches in total : 0

Type	Station	Entry Lifetime	VLAN Override	IP Override
Audit-Session-Id				

```
----- show wireless exclusionlist -----
```

```
----- show wireless country configured -----
```

```
Configured Country..... US - United States
Configured Country Codes
      US - United States          802.11a Indoor/ 802.11b Indoor/ 802.11g Indoor
```

```
----- show wireless tag rf summary -----
```

Number of RF Tags: 1

RF tag name	Description
default-rf-tag	default RF tag

```
----- show platform software wireless-client chassis active R0 statistics -----
```

Client Counters	(Success/Failure)
Create	0/0
Delete	0/0
Modify	0/0

```
Switch 1:
OM Create          0/0
OM Delete          0/0
NACK Notify        0/0
  Create Failure   0
  Modify Failure   0
  Delete Failure   0
```

```
----- show platform software wireless-client chassis active F0 statistics
```

```
-----  
Client Counters      (Success/Failure)  
-----  
Create                0/0  
Delete                0/0  
HW Create             0/0  
HW Modify             0/0  
HW Delete             0/0  
Create Ack            0/0  
Modify Ack            0/0  
Delete Ack            0/0  
NACK Notify           0/0
```

# show tech-support wireless radio

To print the data related to the radio, use the **show tech-support wireless radio** command in privileged EXEC mode.

## show tech-support wireless radio

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

**Usage Guidelines** The output of the following commands are displayed as part of **show tech-support wireless radio** command:

- show ap auto-rf dot11 24ghz
- show ap auto-rf dot11 5ghz
- show ap config dot11 dual-band summary
- show ap config general
- show ap dot11 24ghz channel
- show ap dot11 24ghz coverage
- show ap dot11 24ghz group
- show ap dot11 24ghz high-density
- show ap dot11 24ghz load-info
- show ap dot11 24ghz monitor
- show ap dot11 24ghz network
- show ap dot11 24ghz summary
- show ap dot11 24ghz txpower
- show ap dot11 5ghz channel
- show ap dot11 5ghz coverage
- show ap dot11 5ghz group
- show ap dot11 5ghz high-density
- show ap dot11 5ghz load-info

- show ap dot11 5ghz monitor
- show ap dot11 5ghz network
- show ap dot11 5ghz summary
- show ap dot11 5ghz txpower
- show ap fra
- show ap rf-profile name Rf1 detail
- show ap rf-profile summary
- show ap summary
- show wireless band-select

### Example

The following is sample output from the **show tech-support wireless radio** command

```
Device# show tech-support wireless radio
----- show ap summary -----

Number of APs: 0

----- show ap dot11 24ghz summary -----

----- show ap dot11 5ghz summary -----

----- show ap config dot11 dual-band summary -----

----- show ap dot11 24ghz channel -----

Leader Automatic Channel Assignment
Channel Assignment Mode           : AUTO
Channel Update Interval          : 600 seconds
Anchor time (Hour of the day)    : 0
Channel Update Contribution
  Noise                           : Enable
  Interference                     : Enable
  Load                             : Disable
  Device Aware                     : Disable
CleanAir Event-driven RRM option : Disabled
Channel Assignment Leader        : ewlc-doc (9.12.32.10)
Last Run                          : 550 seconds ago

DCA Sensitivity Level             : MEDIUM : 10 dB
DCA Minimum Energy Limit         : -95 dBm
Channel Energy Levels
```

```

Minimum                               : unknown
Average                               : unknown
Maximum                               : -128 dBm
Channel Dwell Times
  Minimum                             : unknown
  Average                             : unknown
  Maximum                             : unknown
802.11b 2.4 GHz Auto-RF Channel List
  Allowed Channel List                 : 1,6,11
  Unused Channel List                  : 2,3,4,5,7,8,9,10

```

```
----- show ap dot11 5ghz channel -----
```

```

Leader Automatic Channel Assignment
Channel Assignment Mode                 : AUTO
Channel Update Interval                : 600 seconds
Anchor time (Hour of the day)          : 0
Channel Update Contribution
  Noise                                : Enable
  Interference                         : Enable
  Load                                : Disable
  Device Aware                         : Disable
CleanAir Event-driven RRM option       : Disabled
Channel Assignment Leader               : ewlc-doc (9.12.32.10)
Last Run                               : 552 seconds ago

DCA Sensitivity Level                   : MEDIUM : 15 dB
DCA 802.11n/ac Channel Width           : 20 MHz
DCA Minimum Energy Limit                : -95 dBm
Channel Energy Levels
  Minimum                             : unknown
  Average                             : unknown
  Maximum                             : -128 dBm
Channel Dwell Times
  Minimum                             : unknown
  Average                             : unknown
  Maximum                             : unknown
802.11a 5 GHz Auto-RF Channel List
  Allowed Channel List                 :
36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140,144,149,153,157,161
  Unused Channel List                  : 165

```

```
----- show ap dot11 24ghz coverage -----
```

```

Coverage Hole Detection
802.11b Coverage Hole Detection Mode   : Enabled
802.11b Coverage Voice Packet Count    : 100 packet(s)
802.11b Coverage Voice Packet Percentage : 50%
802.11b Coverage Voice RSSI Threshold  : -80 dBm
802.11b Coverage Data Packet Count     : 50 packet(s)
802.11b Coverage Data Packet Percentage : 50%
802.11b Coverage Data RSSI Threshold   : -80 dBm
802.11b Global coverage exception level : 25 %
802.11b Global client minimum exception level : 3 clients

```

```
----- show ap dot11 5ghz coverage -----
```

```
Coverage Hole Detection
```



```

802.11a Coverage Hole Detection Mode      : Enabled
802.11a Coverage Voice Packet Count     : 100 packet(s)
802.11a Coverage Voice Packet Percentage : 50 %
802.11a Coverage Voice RSSI Threshold   : -80dBm
802.11a Coverage Data Packet Count     : 50 packet(s)
802.11a Coverage Data Packet Percentage : 50 %
802.11a Coverage Data RSSI Threshold    : -80dBm
802.11a Global coverage exception level  : 25 %
802.11a Global client minimum exception level : 3 clients

```

```
----- show ap dot11 24ghz group -----
```

Radio RF Grouping

```

802.11b Group Mode          : AUTO
802.11b Group Update Interval : 600 seconds
802.11b Group Leader       : ewlc-doc (9.12.32.10)
802.11b Last Run           : 553 seconds ago

```

RF Group Members

Controller name	Controller IP
-----	-----
ewlc-doc	9.12.32.10

```
----- show ap dot11 5ghz group -----
```

Radio RF Grouping

```

802.11a Group Mode          : AUTO
802.11a Group Update Interval : 600 seconds
802.11a Group Leader       : ewlc-doc (9.12.32.10)
802.11a Last Run           : 553 seconds ago

```

RF Group Members

Controller name	Controller IP
-----	-----
ewlc-doc	9.12.32.10

```
----- show ap dot11 24ghz high-density -----
```

```
----- show ap dot11 5ghz high-density -----
```

```
----- show ap dot11 5ghz load-info -----
```

```
----- show ap dot11 24ghz load-info -----
```

```
----- show ap dot11 24ghz profile -----
```

```
Default 802.11b AP performance profiles
 802.11b Global Interference threshold      : 10 %
 802.11b Global noise threshold            : -70 dBm
 802.11b Global RF utilization threshold    : 80 %
 802.11b Global throughput threshold       : 1000000 bps
 802.11b Global clients threshold         : 12 clients
```

```
----- show ap dot11 5ghz profile -----
```

```
Default 802.11a AP performance profiles

 802.11a Global Interference threshold      : 10 %
 802.11a Global noise threshold            : -70 dBm
 802.11a Global RF utilization threshold    : 80 %
 802.11a Global throughput threshold       : 1000000 bps
 802.11a Global clients threshold         : 12 clients
```

```
----- show ap dot11 24ghz monitor -----
```

```
Default 802.11b AP monitoring
 802.11b Monitor Mode                      : Enabled
 802.11b Monitor Channels                  : Country channels
 802.11b RRM Neighbor Discover Type        : Transparent
 802.11b AP Coverage Interval              : 180 seconds
 802.11b AP Load Interval                  : 60 seconds
 802.11b AP Noise Interval                 : 180 seconds
 802.11b AP Signal Strength Interval       : 60 seconds
 802.11b NDP RSSI Normalization            : Enabled
```

```
----- show ap dot11 5ghz monitor -----
```

```
Default 802.11a AP monitoring
 802.11a Monitor Mode                      : Enabled
 802.11a Monitor Channels                  : Country channels
 802.11a RRM Neighbor Discover Type        : Transparent
 802.11a AP Coverage Interval              : 180 seconds
 802.11a AP Load Interval                  : 60 seconds
 802.11a AP Noise Interval                 : 180 seconds
 802.11a AP Signal Strength Interval       : 60 seconds
 802.11a NDP RSSI Normalization            : Enabled
```

```
----- show ap dot11 24ghz network -----
```

```
802.11b Network                          : Enabled
11gSupport                                : Enabled
11nSupport                                 : Enabled
802.11b/g Operational Rates
 802.11b 1M                               : Mandatory
```

```

802.11b 2M                : Mandatory
802.11b 5.5M             : Mandatory
802.11b 11M              : Mandatory
802.11g 6M               : Supported
802.11g 9M               : Supported
802.11g 12M              : Supported
802.11g 18M              : Supported
802.11g 24M              : Supported
802.11g 36M              : Supported
802.11g 48M              : Supported
802.11g 54M              : Supported
802.11n MCS Settings:
MCS 0 : Supported
MCS 1 : Supported
MCS 2 : Supported
MCS 3 : Supported
MCS 4 : Supported
MCS 5 : Supported
MCS 6 : Supported
MCS 7 : Supported
MCS 8 : Supported
MCS 9 : Supported
MCS 10 : Supported
MCS 11 : Supported
MCS 12 : Supported
MCS 13 : Supported
MCS 14 : Supported
MCS 15 : Supported
MCS 16 : Supported
MCS 17 : Supported
MCS 18 : Supported
MCS 19 : Supported
MCS 20 : Supported
MCS 21 : Supported
MCS 22 : Supported
MCS 23 : Supported
MCS 24 : Supported
MCS 25 : Supported
MCS 26 : Supported
MCS 27 : Supported
MCS 28 : Supported
MCS 29 : Supported
MCS 30 : Supported
MCS 31 : Supported
802.11n Status:
A-MPDU Tx:
  Priority 0                : Enabled
  Priority 1                : Disabled
  Priority 2                : Disabled
  Priority 3                : Disabled
  Priority 4                : Enabled
  Priority 5                : Enabled
  Priority 6                : Disabled
  Priority 7                : Disabled
  Aggregation scheduler    : Enabled
  Realtime timeout         : 10
A-MSDU Tx:
  Priority 0                : Enable
  Priority 1                : Enable
  Priority 2                : Enable
  Priority 3                : Enable
  Priority 4                : Enable
  Priority 5                : Enable
  Priority 6                : Disable

```

## show tech-support wireless radio

```

Priority 7 : Disable
Guard Interval : Any
Rifs Rx : Enabled
Beacon Interval : 100
CF Pollable mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 1
Default Tx Power Level : 1
DTPC Status : Enabled
Call Admission Limit :
G711 CU Quantum :
ED Threshold : -50
Fragmentation Threshold : 2346
RSSI Low Check : Disabled
RSSI Threshold : -127 dbm
PBCC Mandatory : unknown
Pico-Cell-V2 Status : unknown
RTS Threshold : 2347
Short Preamble Mandatory : Enabled
Short Retry Limit : 7
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type check : default-wmm
Call Admission Control (CAC) configuration
Voice AC
Voice AC - Admission control (ACM) : Disabled
Voice Stream-Size : 84000
Voice Max-Streams : 2
Voice Max RF Bandwidth : 75
Voice Reserved Roaming Bandwidth : 6
Voice Load-Based CAC mode : Enabled
Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
SIP based CAC : Disabled
SIP call bandwidth : 64
SIP call bandwidth sample-size : 20
Maximum Number of Clients per AP Radio : 200

```

```
----- show ap dot11 5ghz network -----
```

```

802.11a Network : Enabled
11nSupport : Enabled
802.11a Low Band : Enabled
802.11a Mid Band : Enabled
802.11a High Band : Enabled
802.11a Operational Rates
802.11a 6M : Mandatory
802.11a 9M : Supported
802.11a 12M : Mandatory
802.11a 18M : Supported
802.11a 24M : Mandatory
802.11a 36M : Supported
802.11a 48M : Supported
802.11a 54M : Supported
802.11n MCS Settings:
MCS 0 : Supported
MCS 1 : Supported
MCS 2 : Supported

```

```

MCS 3 : Supported
MCS 4 : Supported
MCS 5 : Supported
MCS 6 : Supported
MCS 7 : Supported
MCS 8 : Supported
MCS 9 : Supported
MCS 10 : Supported
MCS 11 : Supported
MCS 12 : Supported
MCS 13 : Supported
MCS 14 : Supported
MCS 15 : Supported
MCS 16 : Supported
MCS 17 : Supported
MCS 18 : Supported
MCS 19 : Supported
MCS 20 : Supported
MCS 21 : Supported
MCS 22 : Supported
MCS 23 : Supported
MCS 24 : Supported
MCS 25 : Supported
MCS 26 : Supported
MCS 27 : Supported
MCS 28 : Supported
MCS 29 : Supported
MCS 30 : Supported
MCS 31 : Supported
802.11n Status:
A-MPDU Tx:
  Priority 0 : Enabled
  Priority 1 : Disabled
  Priority 2 : Disabled
  Priority 3 : Disabled
  Priority 4 : Enabled
  Priority 5 : Enabled
  Priority 6 : Disabled
  Priority 7 : Disabled
  Aggregation scheduler : Enabled
  Realtime timeout : 10
A-MSDU Tx:
  Priority 0 : Enable
  Priority 1 : Enable
  Priority 2 : Enable
  Priority 3 : Enable
  Priority 4 : Enable
  Priority 5 : Enable
  Priority 6 : Disable
  Priority 7 : Disable
  Guard Interval : Any
Rifs Rx : Enabled
802.11ac : Enabled
  Frame burst : Automatic
802.11ac MCS Settings:
Beacon Interval : 100
CF Pollable mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 36
Default Tx Power Level : 1
DTPC Status : Enabled
Fragmentation Threshold : 2346

```

## show tech-support wireless radio

```

RSSI Low Check                : Disabled
RSSI Threshold                 : -127 dbm
Pico-Cell-V2 Status           : unknown
TI Threshold                   :
Legacy Tx Beamforming setting  : Disabled
Traffic Stream Metrics Status  : Disabled
Expedited BW Request Status    : Disabled
EDCA profile type check       : default-wmm
Call Admission Control (CAC) configuration
Voice AC
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size                : 84000
  Voice Max-Streams                : 2
  Voice Max RF Bandwidth           : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode        : Enabled
  Voice tspec inactivity timeout   : Enabled
CAC SIP-Voice configuration
  SIP based CAC                    : Disabled
  SIP call bandwidth               : 64
  SIP call bandwidth sample-size   : 20
Maximum Number of Clients per AP Radio : 200

```

```
----- show ap dot11 24ghz txpower -----
```

## Automatic Transmit Power Assignment

```

Transmit Power Assignment Mode      : AUTO
Transmit Power Update Interval      : 600 seconds
Transmit Power Threshold             : -70 dBm
Transmit Power Neighbor Count       : 3 APs
Min Transmit Power                  : -10 dBm
Max Transmit Power                   : 30 dBm
Update Contribution
  Noise                              : Enable
  Interference                       : Enable
  Load                               : Disable
  Device Aware                       : Disable
Transmit Power Assignment Leader     : ewlc-doc (9.12.32.10)
Last Run                             : 558 seconds ago

```

```
----- show ap dot11 5ghz txpower -----
```

## Automatic Transmit Power Assignment

```

Transmit Power Assignment Mode      : AUTO
Transmit Power Update Interval      : 600 seconds
Transmit Power Threshold             : -70 dBm
Transmit Power Neighbor Count       : 3 APs
Min Transmit Power                  : -10 dBm
Max Transmit Power                   : 30 dBm
Update Contribution
  Noise                              : Enable
  Interference                       : Enable
  Load                               : Disable
  Device Aware                       : Disable
Transmit Power Assignment Leader     : ewlc-doc (9.12.32.10)
Last Run                             : 558 seconds ago

```

----- show ap auto-rf dot11 5ghz -----

----- show ap auto-rf dot11 24ghz -----

----- show ap config general -----

----- show ap dot11 5ghz optimized-roaming -----

802.11a OptimizedRoaming

```

Mode                               : Disabled
Reporting Interval                 : 90 seconds
Rate Threshold                     : Disabled
Hysteresis                         : 6 db
    
```

----- show ap rf-profile summary -----

Number of RF-profiles: 6

RF Profile Name	Band	Description	State
Low_Client_Density_rf_5gh	5 GHz	pre configured Low Client Density rf	Up
High_Client_Density_rf_5gh	5 GHz	pre configured High Client Density r	Up
Low_Client_Density_rf_24gh	2.4 GHz	pre configured Low Client Density rf	Up
High_Client_Density_rf_24gh	2.4 GHz	pre configured High Client Density r	Up
Typical_Client_Density_rf_5gh	5 GHz	pre configured Typical Density rfpro	Up
Typical_Client_Density_rf_24gh	2.4 GHz	pre configured Typical Client Densit	Up

----- show ap fra -----

```

FRA State                           : Disabled
FRA Sensitivity                      : medium (95%)
FRA Interval                         : 1 Hour(s)
  Last Run                           : 2299 seconds ago
  Last Run time                       : 0 seconds
    
```

AP Name	MAC Address	Slot ID	Current-Band	COF %	Suggested Mode
---------	-------------	---------	--------------	-------	----------------

COF : Coverage Overlap Factor

----- show wireless band-select -----

```

Band Select Probe Response          : per WLAN enabling
Cycle Count                         : 2
Cycle Threshold (millisec)         : 200
Age Out Suppression (sec)          : 20
Age Out Dual Band (sec)             : 60
Client RSSI (dBm)                  : -80
Client Mid RSSI (dBm)              : -80
    
```

```
----- show wireless country configure -----
```

```
Configured Country..... US - United States
Configured Country Codes
    US - United States          802.11a Indoor/ 802.11b Indoor/ 802.11g Indoor
```

```
----- show wireless tag rf summary -----
```

```
Number of RF Tags: 1
```

RF tag name	Description
default-rf-tag	default RF tag

```
----- show ap tag summary -----
```

```
Number of APs: 0
```

```
----- show ap status -----
```

```
----- show ap uptime -----
```

```
Number of APs: 0
```



# show tunnel eogre global-configuration

To display the Ethernet over GRE (EoGRE) global configuration, use the **show tunnel eogre global-configuration** command.

**show tunnel eogre global-configuration**

<b>Syntax Description</b>	This command has no keywords or arguments.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Privileged EXEC (#)				
<b>Command History</b>	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Gibraltar 16.11.1</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE Gibraltar 16.11.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.				

## Example

This example shows how to display the EoGRE global configuration:

```
Device# show tunnel eogre global-configuration

Heartbeat interval      : 60
Max Heartbeat skip count : 3
Source Interface        : (none)
```

# show tunnel eogre domain detailed

To display the detailed information of the Ethernet over GRE (EoGRE) tunnel domain, use the **show tunnel eogre domain detailed** command.

**show tunnel eogre domain detailed** *domain-name*

<b>Syntax Description</b>	<i>domain-name</i>	EoGRE domain name.
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC (#)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

## Example

This example shows how to display the detailed information of the EoGRE tunnel domain:

```
Device# show tunnel eogre domain detailed eogre_domain
```

```
Domain Name      : eogre_domain
Primary GW       : Tunnel1
Secondary GW     : Tunnel2
Active GW        : Tunnel1
Redundancy       : Non-Revertive
```

## show tunnel eogre domain summary

To display the summary information of the Ethernet over GRE (EoGRE) tunnel domain, use the **show tunnel eogre domain summary** command.

**show tunnel eogre domain summary**

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

### Example

This example shows how to display the summary information of the EoGRE tunnel domain:

```
Device# show tunnel eogre domain summary
```

Domain Name	Primary GW	Secondary GW	Active GW	Redundancy
domain1	Tunnel1	Tunnel2	Tunnel1	Non-Revertive
eogre_domain	Tunnel1	Tunnel2	Tunnel1	Non-Revertive

# show tunnel eogre gateway summary

To display the summary information of the Ethernet over GRE (EoGRE) tunnel gateway, use the **show tunnel eogre gateway summary** command.

## show tunnel eogre gateway summary

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

## Example

This example shows how to display the summary information of the EoGRE tunnel gateway:

```
Device# show tunnel eogre gateway summary
```

Name	Type	Address	AdminState	State	Clients
Tunnel1	IPv4	9.51.1.11	Up	Up	0
Tunnel2	IPv4	9.51.1.12	Up	Down	0
Tunnel10	IPv6	fd09:9:8:21::90	Down	Down	0
Tunnel11	IPv4	9.51.1.11	Up	Up	0
Tunnel12	IPv6	fd09:9:8:21::90	Up	Down	0
Tunnel100	IPv4	9.51.1.100	Up	Down	0

# show tunnel eogre gateway detailed

To display the detailed information of the Ethernet over GRE (EoGRE) tunnel domain, use the **show tunnel eogre gateway detailed** command.

**show tunnel eogre gateway detailed** *gateway-name*

<b>Syntax Description</b>	<i>gateway-name</i> EoGRE gateway name.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Privileged EXEC (#)				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.11.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.11.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.				

## Example

This example shows how to display the detailed information of the EoGRE tunnel gateway:

```
Device# show tunnel eogre domain detailed Tunnell
```

```
Gateway : Tunnell
Mode    : IPv4
IP      : 9.51.1.11
Source  : Vlan51 / 9.51.1.1
State   : Up
SLA ID  : 56
MTU     : 1480
Up Time: 4 minutes 45 seconds

Clients
  Total Number of Wireless Clients      : 0
Traffic
  Total Number of Received Packets     : 0
  Total Number of Received Bytes       : 0
  Total Number of Transmitted Packets  : 0
  Total Number of Transmitted Bytes    : 0
Keepalives
  Total Number of Lost Keepalives      : 0
  Total Number of Received Keepalives  : 5
  Total Number of Transmitted Keepalives: 5
Windows
  Transmitted Keepalives in last window : 2
  Received Keepalives in last window   : 2
```

# show tunnel eogre manager stats global

To display the global tunnel manager statistics, use the **show tunnel eogre manager stats global** command.

## show tunnel eogre manager stats global

<b>Syntax Description</b>	This command has no keywords or arguments.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC (#)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

### Example

This example shows how to display the global tunnel manager statistics:

```
Device# show tunnel eogre manager stats global

Tunnel Global Statistics
Last Updated                : 02/18/2019 23:50:35
EoGRE Objects
  Gateways                  : 6
  Domains                   : 2

EoGRE Flex Objects
  AP Gateways               : 2
  AP Domains                : 1
  AP Gateways HA inconsistencies : 0
  AP Domains HA inconsistencies : 0

Config events
  IOS Tunnel updates        : 806
  IOS Domain updates        : 88
  Global updates            : 48
  Tunnel Profile updates    : 120
  Tunnel Rule updates       : 16
  AAA proxy key updates     : 0

AP events
  Flex AP Join              : 1
  Flex AP Leave             : 0
  Local AP Join             : 0
  Local AP leave            : 0
  Tunnel status (rx)       : 4
  Domain status (rx)       : 1
  IAPP stats msg (rx)      : 3
  Client count (rx)        : 6
  VAP Payload msg (tx)     : 4
  Domain config (tx)       : 1
  Global config (tx)       : 1
  Client delete (tx)       : 1
```

```

Client delete per domain (tx) : 3
DHCP option 82 (tx) : 4

Client events
Add-mobile : 2
Run-State : 3
Delete : 1
Cleanup : 0
Join : 2
Plumb : 0
Join Errors : 0
HandOff : 0
MsPayload : 2
FT Recover : 0
Zombie GW counter increase : 0
Zombie GW counter decrease : 0
Tunnel Profile reset : 88
Client deauth : 0
HA reconciliation : 0

Client Join Events
Generic Error : 0
MSPayload Fail : 0
Invalid VLAN : 0
Invalid Domain : 0
No GWs in Domain : 0
Domain Shut : 0
Invalid GWs : 0
GWs Down : 0
Rule Match Error : 0
AAA-override : 0
Flex No Active GW : 0
Open Auth join attempt : 2
Dotlx join attempt : 2
Mobility join attempt : 0
Tunnel Profile not valid : 2
Tunnel Profile valid : 2
No rule match : 0
Rule match : 2
AAA proxy : 0
AAA proxy accounting : 0
AAA eogre attributes : 0
Has aaa override : 0
Error in handoff payload : 0
Handoff AAA override : 0
Handoff no AAA override : 0
Handoff payload received : 0
Handoff payload sent : 0

SNMP Traps
Client : 0
Tunnel : 2
Domain : 0

IPC
IOSd TX messages : 0

Zombie Client
Entries : 0

```

# show tunnel eogre manager stats instance

To display the tunnel manager statistics for a specific WNCd instance, use the **show tunnel eogre manager stats instance** command.

**show tunnel eogre manager stats instance** *instance-number*

<b>Syntax Description</b>	<i>instance-number</i> WNCd instance number.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Privileged EXEC (#)				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.11.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.11.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.				

## Example

This example shows how to display the tunnel manager statistics for a specific WNCd instance:

```
Device# show tunnel eogre manager stats instance 0

Tunnel Manager statistics for process instance : 0
Last Updated                               : 02/18/2019 23:50:35
EoGRE Objects
  Gateways                                  : 6
  Domains                                    : 2

EoGRE Flex Objects
  AP Gateways                               : 2
  AP Domains                                 : 1
  AP Gateways HA inconsistencies            : 0
  AP Domains HA inconsistencies            : 0

Config events
  IOS Tunnel updates                        : 102
  IOS Domain updates                        : 11
  Global updates                            : 6
  Tunnel Profile updates                    : 15
  Tunnel Rule updates                       : 2
  AAA proxy key updates                     : 0

AP events
  Flex AP Join                              : 1
  Flex AP Leave                             : 0
  Local AP Join                             : 0
  Local AP leave                            : 0
  Tunnel status (rx)                       : 4
  Domain status (rx)                       : 1
  IAPP stats msg (rx)                      : 3
  Client count (rx)                        : 6
  VAP Payload msg (tx)                     : 4
```



```

Domain config (tx)           : 1
Global config (tx)          : 1
Client delete (tx)           : 1
Client delete per domain (tx) : 3
DHCP option 82 (tx)         : 4

Client events
Add-mobile                   : 2
Run-State                    : 3
Delete                       : 1
Cleanup                      : 0
Join                         : 2
Plumb                        : 0
Join Errors                  : 0
HandOff                      : 0
MsPayload                    : 2
FT Recover                   : 0
Zombie GW counter increase  : 0
Zombie GW counter decrease  : 0
Tunnel Profile reset        : 11
Client deauth                : 0
HA reconciliation            : 0

Client Join Events
Generic Error                : 0
MSPayload Fail               : 0
Invalid VLAN                 : 0
Invalid Domain               : 0
No GWs in Domain             : 0
Domain Shut                  : 0
Invalid GWs                  : 0
GWs Down                     : 0
Rule Match Error             : 0
AAA-override                 : 0
Flex No Active GW            : 0
Open Auth join attempt       : 2
Dot1x join attempt           : 2
Mobility join attempt        : 0
Tunnel Profile not valid     : 2
Tunnel Profile valid         : 2
No rule match                : 0
Rule match                   : 2
AAA proxy                    : 0
AAA proxy accounting         : 0
AAA eogre attributes         : 0
Has aaa override             : 0
Error in handoff payload     : 0
Handoff AAA override         : 0
Handoff no AAA override      : 0
Handoff payload received     : 0
Handoff payload sent         : 0

SNMP Traps
Client                       : 0
Tunnel                       : 2
Domain                       : 0

IPC
IOSd TX messages             : 0

Zombie Client
Entries                       : 0

```

# show wireless band-select

To display the status of the band-select configuration, use the **show wireless band-select** command in privileged EXEC mode.

**show wireless band-select**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--------------------------------------------

<b>Command Default</b>	No default behavior or values.
------------------------	--------------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

The following is sample output from the **show wireless band-select** command:

```
Device# show wireless band-select
Band Select Probe Response      : per WLAN enabling
Cycle Count                     : 2
Cycle Threshold (millisec)     : 200
Age Out Suppression (sec)      : 20
Age Out Dual Band (sec)        : 60
Client RSSI (dBm)              : 80
```

# show wireless client

To see the summary of the classified devices, use the **show wireless client** command.

```
show wireless client device {cache | count | summary } | {steering}[{chassis{chassis-number | active | standby }}]R0
```

Syntax Description	device	Shows classified devices.
	<b>steering</b>	Wireless client steering information
	<b>cache</b>	Shows the cached classified device summary.
	<b>count</b>	Shows the wireless device count.
	<b>summary</b>	Shows the active classified device summary.
	<i>chassis-number</i>	Chassis number. Valid range is 1–2.
	<b>active</b>	Active instance.
	<b>standby</b>	Standby instance.
	<b>R0</b>	Route-Processor slot 0.

**Command Default** None

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to see the summary of the classified devices:

```
Device# show wireless client device summary
```

# show wireless client mac-address

To view detailed information of a client using its mac-address, use the **show wireless client mac-address detail** command.

**show wireless client mac-address *mac-address* detail** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description	
<i>mac-address</i>	Client MAC address.
<i>chassis-number</i>	Chassis number. Valid range is 1–2.
<b>active</b>	Active instance.
<b>standby</b>	Standby instance.
<b>R0</b>	Route-Processor slot 0.

**Command Default** None

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

**Usage Guidelines** The Client Scan Reports section in the output of the **show wireless client mac-address detail** is populated only for the following Apple devices:

- Any iPhone 7 and running iOS 11.0 or higher
- Any iPad after iPad Pro (1st gen, 12.9-inch, 2015) and running iOS 11.0 or higher

Other client devices, even if it supports 802.11k or is Wi-Fi Agile Multiband (MBO) certified, are not currently supported to populate the Client Scan Reports section.

Client ACLs shown under **show wireless client mac-address <mac address> detail** are ACLs applied on the client in Flexconnect local authentication case with MAB+Web authentication WLAN with AAA override enabled. This is applicable only for Express Wi-Fi by Facebook Policy on Controller. For more information about Facebook policy, see [Express Wi-Fi by Facebook](#).

From Cisco IOS XE Amsterdam 17.3.1 onwards, the controller retains client session for 10 seconds. This feature is applicable for clients in the RUN state and is supported on central authentication with local and flex mode.

In idle state, 10 sec represents idle state timeout and 09 sec represent remaining time out of 10 sec. An example is given below:

```
Idle state timeout : 10 sec (Remaining time: 09 sec)
```

### Examples

The following example shows how to see detailed client information using its MAC address:

```
Device# show wireless client mac-address 98-XX-7B-XX-EF-XX detail
```

## show wireless client mac-address (Call Control)

To view call control information related to clients, use the **show wireless client mac-address** command in privileged EXEC mode.

**show wireless client mac-address** *mac-address* **call-control call-info**

<b>Syntax Description</b>	<i>mac-address</i>	The client MAC address.
	<b>call-control call-info</b>	Displays the call control and IP-related information about a client.
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
		This command was introduced.

This example shows how to display call control and IP-related information about a client:

```
Device# show wireless client mac-address 30e4.db41.6157 call-control call-info
Client MAC Address      : 30E4DB416157

Call 1 Statistics

Uplink IP Address      : 209.165.200.225
Downlink IP Address    : 209.165.200.226
Uplink Port            : 29052
Downlink Port          : 27538
Call ID                : c40acb4d-3b3b0.3d27da1e-356bed03
Called Party           : sip:1011
Calling Party          : sip:1012
Priority                : 6
Call On Hold           : false
Call Duration          : 30

Call 2 Statistics

No Active Call
```

## show wireless client mac-address (TCLAS)

To view information about TCLAS and user priority, use the **show wireless client mac-address** command in privileged EXEC mode.

**show wireless client mac-address** *mac-address* **tclas**

### Syntax Description

<i>mac-address</i>	The client MAC address.
<b>tclas</b>	Displays TCLAS and user priority-related information about a client.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to display the TCLAS and user priority-related information about a client:

```
Device# show wireless client mac-address 30e4.db41.6157 tclas
MAC Address      UP TID Mask Source IP Addr  Dest IP Addr  SrcPort DstPort Proto
-----
30e4.db41.6157   4  4  95 167838052      2164326668    5060    5060    6
30e4.db41.6157   6  1  31 0              2164326668    0       27538   17
```

# show wireless client summary

To display a summary of active clients associated with the controller, use the **show wireless client summary** command in privileged EXEC mode.

**show wireless client summary**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

**Usage Guidelines** The following is sample output from the **show wireless client summary** command:  
Use the **show wireless exclusionlist** command to display clients on the exclusion list.

```
Device# show wireless client summary
Number of Local Clients : 1
```

MAC Address	AP Name	WLAN State	Protocol
0000.1515.000f	AP-2	1 UP	11a



## show wireless client timers

To display 802.11 system timers, use the **show wireless client timers** command in privileged EXEC mode.

**show wireless client timers**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** No default behavior or values.

---

**Command Modes** Privileged EXEC

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

---

The following is sample output from the **show wireless client timers** command:

```
Device# show wireless client timers
Authentication Response Timeout (seconds)      : 10
```



The following is sample output from the **show wireless country configured** command:

```
Device# show wireless country configured
Configured Country.....: US - United States
Configured Country Codes
    US - United States : 802.11a Indoor,Outdoor/ 802.11b / 802.11g
```

The following is sample output from the **show wireless country supported tx-power** command:

```
Device# show wireless country supported tx-power
KEY: ##      = Tx Power in dBm.
     ##*     = Channel supports radar detection .
     .       = Channel is not legal in this country.
     (-)     = Regulatory Domains allowed by this country.
     (-,-)   = (indoor, outdoor) regulatory Domains allowed by this country.
-----:+++++-----:
      802.11bg      :
      Channels      :                1 1 1 1 1
                   : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
-----:+++++-----:
(-CE , -CE ) AE  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) AL  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A  , -AR ) AR  : 27 27 27 27 27 27 27 27 27 27 27 27 27 27 .
(-E  , -E  ) AT  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A  , -NA ) AU  : 27 27 27 27 27 27 27 27 27 27 27 27 27 27 .
(-E  , -   ) BA  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) BE  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) BG  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -   ) BH  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A  , -A  ) BO  : 27 27 27 27 27 27 27 27 27 27 27 27 27 27 .
(-A  , -AR ) BR  : 27 27 27 27 27 27 27 27 27 27 27 27 27 27 .
(-E  , -   ) BY  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A  , -ABN ) CA  : 27 27 27 27 27 27 27 27 27 27 27 27 27 27 .
(-A  , -ABN ) CA2 : 27 27 27 27 27 27 27 27 27 27 27 27 27 27 .
(-E  , -E  ) CH  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-AER , -AR ) CL  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) CM  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-CE  , -CE ) CN  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A  , -AR ) CO  : 27 27 27 27 27 27 27 27 27 27 27 27 27 27 .
(-A  , -AB  ) CR  : 27 27 27 27 27 27 27 27 27 27 27 27 27 27 .
(-E  , -E  ) CY  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) CZ  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) DE  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) DK  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A  , -ABN ) DO  : 27 27 27 27 27 27 27 27 27 27 27 27 27 27 .
(-E  , -   ) DZ  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A  , -AB  ) EC  : 27 27 27 27 27 27 27 27 27 27 27 27 27 27 .
(-E  , -E  ) EE  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) EG  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) ES  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) FI  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) FR  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) GB  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) GI  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) GR  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A  , -NA ) HK  : 27 27 27 27 27 27 27 27 27 27 27 27 27 27 .
(-E  , -   ) HR  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) HU  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -ER ) ID  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) IE  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-EI  , -IE ) IL  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
```

## show wireless country

```

(-I , -I ) ILO : . . . . 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -AN ) IN : 27 27 27 27 27 27 27 27 27 27 27 . . .
(-E , -E ) IQ : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) IS : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) IT : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-JPU , -JPU ) J2 : 23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-JPU , -JPU ) J3 : 23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-JPQU , -PQ ) J4 : 23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-E , - ) JO : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-JPU , -JPU ) JP : 23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-ACE , -ACEK) KE : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) KN : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-ACE , -ACEK) KR : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) KW : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) KZ : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) LB : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) LI : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , ) LK : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) LT : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) LU : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) LV : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) MC : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) ME : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) MK : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , ) MO : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) MT : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -NA ) MX : 27 27 27 27 27 27 27 27 27 27 27 . . .
(-ACE , -AEC ) MY : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) NL : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) NO : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -NA ) NZ : 27 27 27 27 27 27 27 27 27 27 27 . . .
(-E , -E ) OM : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -AR ) PA : 27 27 27 27 27 27 27 27 27 27 27 . . .
(-A , -AR ) PE : 27 27 27 27 27 27 27 27 27 27 27 . . .
(-A , -ABN ) PH : 27 27 27 27 27 27 27 27 27 27 27 . . .
(-A , -ABN ) PH2 : 27 27 27 27 27 27 27 27 27 27 27 . . .
(-E , -E ) PK : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) PL : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -A ) PR : 27 27 27 27 27 27 27 27 27 27 27 . . .
(-E , -E ) PT : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -A ) PY : 27 27 27 27 27 27 27 27 27 27 27 . . .
(-E , -E ) QA : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) RO : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) RS : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-AER , -ER ) RU : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-AE , -AE ) SA : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) SE : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -SE ) SG : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) SI : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) SK : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -ER ) TH : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) TN : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-EI , -E ) TR : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -ANT ) TW : 27 27 27 27 27 27 27 27 27 27 27 . . .
(-E , -E ) UA : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -AB ) US : 27 27 27 27 27 27 27 27 27 27 27 . . .
(-A , -AB ) US2 : 27 27 27 27 27 27 27 27 27 27 27 . . .
(-A , -AB ) USL : 27 27 27 27 27 27 27 27 27 27 27 . . .
(-A , - ) USX : 27 27 27 27 27 27 27 27 27 27 27 . . .
(-A , -A ) UY : 27 27 27 27 27 27 27 27 27 27 27 . . .
(-A , -AR ) VE : 27 27 27 27 27 27 27 27 27 27 27 . . .
(-E , -E ) VN : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) ZA : 20 20 20 20 20 20 20 20 20 20 20 20 20 .

```

# show wireless detail

To display the details of the wireless parameters configured, use the **show wireless detail** command in privileged EXEC mode.

**show wireless detail**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** No default behavior or values.

---

**Command Modes** Privileged EXEC

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

---

---

**Usage Guidelines** The following parameters are displayed:

- The wireless user idle timeout
- The controller configured RF group name
- Fast SSID change

The following is sample output from the **show wireless detail** command:

```
Device# show wireless detail
User Timeout           : 300
RF network              : default
Fast SSID              : Disabled
```

# show wireless dot11h

To see 802.11h configuration details, use the **show wireless dot11h** command.

**show wireless dot11h** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

*chassis-number* Chassis number. Valid range is 1–2.

**active** Active instance.

**standby** Standby instance.

**R0** Route-Processor slot 0.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to see the 802.11h configuration details:

```
Device# show wireless dot11h
```

# show wireless dtls connections

To display the Datagram Transport Layer Security (DTLS) server status, use the **show wireless dtls connections** command in privileged EXEC mode.

**show wireless dtls connections**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

The following is sample output from the **show wireless dtls connections** command:

```
Device# show wireless dtls connections
AP Name          Local Port  Peer IP    Peer Port  Ciphersuite
-----
AP-2             Capwap_Ctrl 10.0.0.16  52346     TLS_RSA_WITH_AES_128_CBC_SHA
AP-3             Capwap_Ctrl 10.0.0.17  52347     TLS_RSA_WITH_AES_128_CBC_SHA
```

# show wireless exclusionlist

To see the wireless exclusion list, use the **show wireless exclusionlist** command.

**show wireless exclusionlist** [{**client mac-address** *client-mac-addr* **detail** }] [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description	
<i>client-mac-addr</i>	SI interferers of type microwave oven for the 2.4-GHz band.
<i>chassis-number</i>	Enter the chassis number as either 1 or 2.
<b>active R0</b>	Active instance of the configuration in Route-processor slot 0.
<b>standby R0</b>	Standby instance of the configuration in Route-processor slot 0.

**Command Default** None

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to see the wireless exclusion list:

```
Device# show wireless exclusionlist
```



# show wireless load-balancing

To display the status of the load-balancing feature, use the **show wireless load-balancing** command in privileged EXEC mode.

**show wireless load-balancing**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--------------------------------------------

<b>Command Default</b>	No default behavior or values.
------------------------	--------------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

The following is sample output from the **show wireless load-balancing** command:

```
> show wireless load-balancing
Aggressive Load Balancing.....: per WLAN enabling
Aggressive Load Balancing Window (clients).....: 5
Aggressive Load Balancing Denial Count.....: 3

Statistics
Total Denied Count (clients).....: 0
Total Denial Sent (messages).....: 0
Exceeded Denial Max Limit Count (times).....: 0
None 5G Candidate Count (times).....: 0
None 2.4G Candidate Count (times).....: 0
```

# show wireless ewc-ap ap summary

To view the embedded wireless controller AP summary, use the **show wireless ewc-ap ap summary** command.

**show wireless ewc-ap ap summary** [**chassis** {*chassis\_number* | **active** | **standby**} {**R0**}]

Syntax	Description
<b>ewc-ap</b>	Configures the embedded wireless controller parameters.
<b>ap summary</b>	Displays the embedded wireless controller AP, AP summary.
<b>chassis</b>	Indicates the details of the chassis.
<i>chassis-number</i>	Indicates the chassis number, which is either 1 or 2..
<b>R0</b>	Indicates Route Processor slot 0.
<b>Active</b>	Indicates the active operational mode of the AP chassis.
<b>Standby</b>	Indicates the standby operational mode of the AP chassis.

**Command Default** None

**Command Modes** Privileged EXEC mode

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

## Example

The following example shows how to view the embedded wireless controller, AP summary:

```
Device#show wireless ewc-ap ap summary
```

## show wireless ewc-ap ap config-sync

To view the embedded wireless controller AP configuration synchronization information or summary, use the **show wireless ewc-ap ap config-sync** command.

```
show wireless ewc-ap ap config-sync summary [ chassis {chassis_number | active | standby} {R0}]
```

<b>Syntax Description</b>	<b>config-sync</b> Configures the embedded wireless controller parameters.
---------------------------	----------------------------------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC mode
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

### Example

The following example shows how to view the embedded wireless controller AP configuration synchronization information or summary:

```
Device#show wireless ewc-ap ap config-sync summary
```

# show wireless ewc-ap ap image predownload status

To view the AP image predownload statistics, use the **show wireless ewc-ap ap image predownload status** command.

**show wireless ewc-ap ap image predownload status**

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC mode
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

<b>Usage Guidelines</b>	None
-------------------------	------

## Example

The following example shows how to view the AP image predownload statistics:

```
Device#show wireless ewc-ap ap image predownload status
```

## show wireless ewc-ap country-code

To view the default country codes and the supported country codes of the embedded wireless controller AP, use the **show wireless ewc-ap country-code** command.

```
show wireless ewc-ap country-code [ chassis { chassis_number | active | standby } { R0 } ]
```

<b>Syntax Description</b>	<b>country-code</b> Indicates the default country codes and the supported country codes.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Privileged EXEC mode				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.2s</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.				

### Example

The following example shows how to view the default and supported country codes of embedded wireless controller AP:

```
Device#show wireless ewc-ap country-codes
```

# show wireless ewc-ap image-master

To view the image maser information, use the **show wireless ewc-ap image-master** command.

**show wireless ewc-ap image-master** [**chassis** {*chassis\_number* | **active** | **standby**} {**R0**}]

<b>Syntax Description</b>	<b>image-master</b> Indicates the image master information.
---------------------------	-------------------------------------------------------------

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Privileged EXEC mode
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

## Example

The following example shows how to view the image master information:

```
Device#show wireless ewc-ap image-master
```

## show wireless ewc-ap invalid-image-master

To view the details of the invalid image master, use the **show wireless ewc-ap invalid-image-master** command.

**show wireless ewc-ap invalid-image-master** [**chassis** {*chassis\_number* | **active** | **standby**} {**R0**}]

<b>Syntax Description</b>	<b>invalid-image-master</b> Indicates the invalid image master information.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Privileged EXEC mode				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.2s</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.				

### Example

The following example shows how to view the invalid image master information:

```
Device#show wireless ewc-ap invalid-image-master
```

# show wireless ewc-ap predownload

To view the image predownload information, use the **show wireless ewc-ap predownload** command.

```
show wireless ewc-ap predownload { count | status } [ chassis { chassis_number | active | standby }
{ R0 } ]
```

<b>Syntax Description</b>	<b>predownload</b> Indicates the image predownload information.				
	<b>count</b> Indicates the image predownload count.				
	<b>status</b> Indicates the image predownload status.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Privileged EXEC mode				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.12.2s</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.				

## Example

The following example shows how to view the image predownload count and status:

```
Device#show wireless ewc-ap predownload
```



## show wireless ewc-ap redundancy summary

To view the HA redundancy summary, use the **show wireless ewc-ap redundancy summary** command.

**show wireless ewc-ap redundancy summary** [**chassis** {*chassis\_number* | **active** | **standby**} {**R0**}]

Syntax Description	
<b>redundancy</b>	Indicates the HA redundancy information.
<b>summary</b>	Indicates the summary of HA redundancy.

**Command Default** None

**Command Modes** Privileged EXEC mode

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

### Example

The following example shows how to view the default and supported country codes of embedded wireless controller AP:

```
Device#show wireless ewc-ap redundancy summary
```

# show wireless ewc-ap redundancy peers

To view the HA redundancy peers, use the **show wireless ewc-ap redundancy peers** command.

**show wireless ewc-ap redundancy peers** [**chassis** {*chassis\_number* | **active** | **standby**} {**R0**}]

Syntax Description	
<b>redundancy</b>	Indicates the HA redundancy information.
<b>peers</b>	Indicates the peers of HA redundancy.

**Command Default** None

**Command Modes** Privileged EXEC mode

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

## Example

The following example shows how to view the default and supported country codes of embedded wireless controller AP:

```
Device#show wireless ewc-ap redundancy peers
```

# show wireless pmk-cache

To display information about the pairwise master key (PMK) cache, use the **show wireless pmk-cache** command in privileged EXEC mode.

```
show wireless pmk-cache[mac-address mac-addr]
```

<b>Syntax Description</b>	<b>mac-address <i>mac-addr</i></b> (Optional) Information about a single entry in the PMK cache.				
<b>Command Default</b>	No default behavior or values.				
<b>Command Modes</b>	Privileged EXEC				
<b>Command History</b>	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Gibraltar 16.12.1</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
Release	Modification				
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.				

The following is sample output from the **show wireless pmk-cache mac-address** command:

```
Device# show wireless pmk-cache mac-address H.H.H  
Number of PMK caches in total : 0
```

# show wireless profile flex

To see the flex parameters of an wireless profile, use the **show wireless profile flex** command.

```
show wireless profile flex { detailed flex-profile-name chassis {chassis-number | active | standby } R0
} | summary chassis {chassis-number | active | standby} R0}
```

Syntax Description		
<b>detailed</b>	Shows the flex-profile detailed parameters	
<b>summary</b>	Show the flex-profile summary.	
<i>chassis-number</i>	Chassis number. Valid range is 1–2.	
<b>active</b>	Active instance.	
<b>standby</b>	Standby instance.	
<b>R0</b>	Route-Processor slot 0.	

**Command Default** None

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

## Examples

The following example shows how to see the flex parameter's summary of the wireless profile:

```
Device# show wireless profile flex summary
```

## show wireless profile policy detailed

To display the wireless policy profile details, use the **show wireless profile policy detailed** command.

**show wireless profile policy detailed** *policy-profile-name*

<b>Syntax Description</b>	This command has no keywords or arguments.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Privilege EXEC (#)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

### Example

This example displays the wireless policy profile details:

```
Device#show wireless profile policy detailed policy-profile-name
```

# show wireless rfid

To display RFID tag information, use the **show wireless rfid** command in privileged EXEC mode.

**show wireless rfid** { **client** | **detail** *rfid-mac-address* | **stats** | **summary** }

Syntax Description		
<b>client</b>	Displays the summary of RFID tags that are clients.	
<b>detail</b>	Displays information about a particular RFID tag.	
<b>stats</b>	Displays RFID statistics.	
<b>summary</b>	Displays summary information for all known RFID tags.	
<i>rfid-mac-address</i>	RFID MAC address.	

**Command Default** None

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

## Example

This example shows how to view RFID information:

```
Device# show wireless rfid summary
```

```
Total RFID entries: : 16
Total Unique RFID entries : 16
RFID ID VENDOR Closet AP RSSI Time Since Last Heard
0012.b80a.c791 Cisco 7069.5a63.0520 -31 1 minute 40 seconds ago
0012.b80a.c953 Cisco 7069.5a63.0460 -33 2 minutes 15 seconds ago
0012.b80b.806c Cisco 7069.5a63.0260 -45 22 seconds ago
0012.b80d.e9f9 Cisco 7069.5a63.0460 -38 2 minutes 37 seconds ago
0012.b80d.ea03 Cisco 7069.5a63.0520 -43 2 minutes 38 seconds ago
0012.b80d.ea6b Cisco 7069.5a63.0460 -39 2 minutes 35 seconds ago
0012.b80d.ebe8 Cisco 7069.5a63.0520 -43 1 minute 31 seconds ago
0012.b80d.ebeb Cisco 7069.5a63.0520 -43 2 minutes 37 seconds ago
0012.b80d.ec48 Cisco 7069.5a63.0460 -42 2 minutes 16 seconds ago
0012.b80d.ec55 Cisco 7069.5a63.0520 -41 1 second ago
```

# show wireless summary

To display the number of access points, radios and wireless clients known to the controller, use the **show wireless summary** command in privileged EXEC mode.

**show wireless summary**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

The following is sample output from the **show wireless summary** command:

```
Device# show wireless summary

Access Point Summary

              Total    Up    Down
-----
802.11a/n      2     2     0
802.11b/g/n    2     2     0
All APs        2     2     0

Client Summary

Current Clients : 1
Excluded Clients: 0
Disabled Clients: 0
```

# show wireless tag rf

To display the details of wireless RF tag, use the **show wireless tag rf** command.

**show wireless tag rf** { **summary** | **detailed** } *rf-tag-name*

Syntax Description	
<b>summary</b>	Displays the summary of all RF tags.
<b>detailed</b>	Displays details of an RF tag.
<i>rf-tag-name</i>	RF tag name.

**Command Default** None

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

## Example

The following example shows the sample output of **show wireless tag rf summary** command:

```
Device# show wireless tag rf summary
```

```
Number of RF Tags: 1
```

```
RF tag name           Description
-----
default-rf-tag       default RF tag
```



# show wireless urlfilter details

To view the details of a specified wireless URL filter, use the **show wireless urlfilter details** command.

**show wireless urlfilter details** *list-name*

<b>Syntax Description</b>	This command has no arguments.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to view the details of a specified wireless URL filter:

```
Device# show wireless urlfilter details urllist_flex_preauth
List Name..... : urllist_flex_preauth
Filter ID..... : : 1
Filter Type..... : PRE-AUTH
Action..... : PERMIT
Redirect server ipv4..... : 8.8.8.8
Redirect server ipv6..... : 2001:0300:0008:0000:0000:0000:0000:0081
Configured List of URLs
  URL..... : url1.dns.com
```

## show wireless urlfilter summary

To view the summary of all wireless URL filters, use the **show wireless urlfilter summary** command.

**show wireless urlfilter summary**

<b>Syntax Description</b>	This command has no arguments.	
<b>Command Default</b>	None	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to view the summary of all wireless URL filters:

```
Device# show wireless urlfilter summary
Black-list      - DENY
White-list      - PERMIT
Filter-Type     - Specific to Local Mode

URL-List              ID  Filter-Type  Action  Redirect-ipv4  Redirect-ipv6
-----
urllist_flex_preauth    1   PRE-AUTH    PERMIT    8.8.8.8
2001:0300:0008:0000:0000:0000:0000:0081
```

# show wireless vlan details

To see the VLAN details, use the **show wireless vlan details** command.

```
show wireless vlan details [chassis {chassis-number | active | standby} R0]
```

---

**Command Default**      None

---

**Command Modes**      Privileged EXEC

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

## Examples

The following example shows how to see the VLAN details:

```
Device# show wireless vlan details chassis active r0
```

# show wireless wgb mac-address

To view all the clients of the wireless workgroup bridge (WGB) using its MAC address, use the **show wireless wgb mac-address** command.

**show wireless wgb mac-address** *mac-address* **detail**

<b>Syntax Description</b>	<i>mac-address</i> MAC address of the WGB.				
	<b>detail</b> View clients of the wireless WGB.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Privileged EXEC				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.
Release	Modification				
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.				

## Examples

The following example shows how to see the clients of the wireless WGB:

```
Device# show wireless wgb mac-address 98-C7-7B-09-EF-ED detail
```

# show wireless wgb summary

To see the active workgroup bridges (WGB), use the **show wireless wgb summary** command.

**show wireless wgb summary**

---

**Command Default** None

---

**Command Modes** Privileged EXEC

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

---

## Examples

The following example shows how to see the active workgroup bridges (WGB):

```
Device# show wireless wgb summary
```

## show wireless wps rogue ap summary

To display a list of all rogue access points detected by the device, use the **show wireless wps rogue ap summary** command.

**show wireless wps rogue ap summary**

**Command Default** None.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

**Usage Guidelines** None.

This example shows how to display a list of all rogue access points detected by the device:

```
Device# show wireless wps rogue ap summary
Rogue Location Discovery Protocol      : Disabled
Rogue on wire Auto-Contain            : Disabled
Rogue using our SSID Auto-Contain     : Disabled
Valid client on rogue AP Auto-Contain : Disabled
Rogue AP timeout                      : 1200
Rogue Detection Report Interval       : 10
Rogue AP minimum RSSI                 : -128
Rogue AP minimum transient time       : 0
```

Number of rogue APs detected : 624

MAC Address	Classification	# APs	# Clients	Last Heard
0018.e78d.250a	Unclassified	1	0	Thu Jul 25 05:04:01 2013
0019.0705.d5bc	Unclassified	1	0	Thu Jul 25 05:16:26 2013
0019.0705.d5bd	Unclassified	1	0	Thu Jul 25 05:10:28 2013
0019.0705.d5bf	Unclassified	1	0	Thu Jul 25 05:16:26 2013

# show wireless wps rogue client detailed

To view the detailed information of a specific rogue client, use the **show wireless wps rogue client detailed** *client-mac* command.

**show wireless wps rogue client detailed** *client-mac*

<b>Syntax Description</b>	<i>client-mac</i> MAC address of the rogue client.
---------------------------	----------------------------------------------------

<b>Command Default</b>	None.
------------------------	-------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

<b>Usage Guidelines</b>	None.
-------------------------	-------

This example shows how to display the detailed information for a specific rogue client:

```
Device# show wireless wps rogue client detail 0024.d7f1.2558
Rogue BSSID                : 64d8.146f.379f
Rogue Radio Type           : 802.11n - 5GHz
State                       : Alert
First Time Rogue was Reported : Wed Aug  7 12:51:43 2013
Last Time Rogue was Reported  : Wed Aug  7 12:51:43 2013
Reported by
  AP 2
  MAC Address                : 3cce.7309.0370
  Name                       : AP3502-talwar-ccie
  Radio Type                  : 802.11a
  RSSI                       : -42 dBm
  SNR                        : 47 dB
  Channel                     : 52
  Last reported by this AP    : Wed Aug  7 12:51:43 2013
```

# show wireless wps rogue client summary

To display summary of WPS rogue clients, use the **show wireless wps rogue client summary** command.

**show wireless wps rogue client summary**

---

**Command Default**      None

---

**Command Modes**      Privileged EXEC

---

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

---



---

## Usage Guidelines

### Example

The following displays the output of the **show wireless wps rogue client summary** command:

```
Device# show wireless wps rogue client summary
Validate rogue clients against AAA : Disabled
Validate rogue clients against MSE : Enabled
Number of rogue clients detected : 0
```





## INDEX

[no] ap remote-lan shutdown command [167](#)

### A

- aaa accounting update periodic interval-in-minutes [14](#)
- aaa authentication login command [16](#)
- aaa authorization credential download default command [21](#)
- aaa group server ldap command [22](#)
- aaa group server radius command [23](#)
- aaa local authentication default authorization [24](#)
- aaa-override command [31](#)
- aaa-policy [32](#)
- aaa-realm enable [33](#)
- access-list [35](#)
- access-list acl-ace-limit [37](#)
- accounting-list command [38](#)
- acl-policy [39](#)
- allow at-least 5 at-most 10 [44](#)
- ap auth-list ap-policy [50](#)
- ap capwap retransmit [51](#)
- ap capwap timers [52](#)
- ap cdp [188](#)
- ap country [54](#)
- ap dot11 [55](#)
- ap dot11 24ghz cleanair command [57, 62](#)
- ap dot11 24ghz dot11g [58](#)
- ap dot11 24ghz rate [59](#)
- ap dot11 24ghz rrm [66](#)
- ap dot11 24ghz rrm coverage command [105](#)
- ap dot11 24ghz rrm tpc command [113](#)
- ap dot11 24ghz rx-sop threshold [67](#)
- ap dot11 24ghz shutdown [68](#)
- ap dot11 5ghz channelswitch quiet [69](#)
- ap dot11 5ghz cleanair [70](#)
- ap dot11 5ghz cleanair command [71](#)
- ap dot11 5ghz power-constraint [72](#)
- ap dot11 5ghz rate [73](#)
- ap dot11 5ghz rrm channel device command [75](#)
- ap dot11 5ghz rrm command [99](#)
- ap dot11 5ghz rrm txpower command [114, 115](#)
- ap dot11 5ghz rx-sop threshold [76](#)
- ap dot11 5ghz shutdown [77](#)
- ap dot11 5ghz smart-dfs [78](#)
- ap dot11 beaconperiod [79](#)
- ap dot11 cac media-stream [80](#)
- ap dot11 cac voice [84](#)
- ap dot11 cleanair [87](#)
- ap dot11 cleanair device [88](#)
- ap dot11 dot11n [89](#)
- ap dot11 dtpc [92](#)
- ap dot11 dual-band cleanair [133](#)
- ap dot11 edcs-parameters [94](#)
- ap dot11 multimedia [83](#)
- ap dot11 rrm channel cleanair-event [61](#)
- ap dot11 rrm channel command [64, 65, 74, 102](#)
- ap dot11 rrm channel dca [103](#)
- ap dot11 rrm group-member [107](#)
- ap dot11 rrm group-mode [108](#)
- ap dot11 rrm logging [109](#)
- ap dot11 rrm monitor [111](#)
- ap dot11 rrm ndp-type [112](#)
- ap filter [116](#)
- ap fra [117](#)
- ap name [154](#)
- ap name clear-personal-ssid [121](#)
- ap name country [123](#)
- ap name crash-file [124](#)
- ap name dot11 rrm profile [135](#)
- ap name image [137](#)
- ap name led [142](#)
- ap name location [144](#)
- ap name monitor-mode dot11b [148](#)
- ap name name [149](#)
- ap name priority [151](#)
- ap name reset [152](#)
- ap name reset-button [153](#)
- ap name shutdown [159](#)
- ap name slot [155](#)
- ap name static-ip [158](#)
- ap name-regex [164](#)
- ap profile [165](#)
- ap remote-lan profile-name command [166](#)
- ap remote-lan-policy policy-name command [168](#)
- ap tag-source-priority [169](#)
- ap tag-sources revalidate [170](#)
- assisted-roaming command [172](#)
- avg-packet-size packetsize [173](#)

**C**

captive-portal-bypass command [180](#)  
 capwap backup [182](#)  
 class command [196](#)  
 class-map command [199](#)  
 classify [198](#)  
 clear platform condition all [204](#)  
 client association limit command [208](#)  
 client-l2-vnid [211](#)  
 commands [486](#)  
     configuration [486](#)  
         username [486](#)  
 convergence [212](#)  
 custom-page login device [226](#)

**D**

default command [227](#)  
 description command [230](#)  
 destination command [231](#)  
 device-tracking binding vlan [233](#)  
 dhcp-tlv-caching command [234](#)  
 dnscrypt command [235](#)  
 dot11 5ghz reporting-interval [238](#)

**E**

eap profile [242](#)  
 exclusionlist command [243](#)

**F**

fallback-radio-shut [245](#)  
 flex [246](#)

**I**

idle-timeout [261](#)  
 inactive-timeout command [263](#)  
 interface vlan command [276](#)  
 ip access-group command [277](#)  
 ip access-list extended [278](#)  
 ip domain-name [285](#)  
 ip flow monitor command [286](#)  
 ip flow-export destination command [287](#)  
 ip verify source command [303](#)  
 ipv4 dhcp [305](#)  
 ipv4 flow monitor [306](#)  
 ipv4 flow monitor output [307](#)  
 ipv6 flow monitor input [308](#)  
 ipv6 flow monitor output [309](#)  
 ipv6 nd managed-config-flag command [322](#)  
 ipv6 nd ra throttler attach-policy [324](#)  
 ipv6 traffic-filter command [328](#)

**L**

local-auth ap eap-fast [353](#)  
 local-site [354](#)  
 location notify-threshold command [356](#)

**M**

mac-filtering [359](#)  
 match (access-map configuration) command [372](#)  
 match (class-map configuration) command [374](#)  
 match any [362](#)  
 match non-client-nrt command [364](#)  
 match protocol command [365](#)  
 match user-role [370](#)  
 match wlan user-priority command [377](#)  
 max-bandwidth [378](#)  
 method fast [384](#)  
 mgmtuser username [385](#)

**N**

nac command [387](#)  
 nas-id option2 [388](#)  
 network [389](#)  
 nmsp cloud-services enable [390](#)  
 nmsp cloud-services http-proxy [391](#)  
 nmsp cloud-services server token [392](#)  
 nmsp cloud-services server url [393](#)  
 nmsp notification interval command [394](#)

**O**

option command [397](#)

**P**

parameter-map type subscriber attribute-to-service [399](#)  
 peer-blocking command [401](#)  
 police command [403](#)  
 policy [402](#)  
 policy-map command [406, 408](#)  
 port [410](#)  
 priority priority-value [411](#)

**Q**

qos video [413](#)

**R**

radius server command [414](#)  
 range [419](#)  
 record wireless avc basic [420](#)  
 redirect [421](#)

redirect portal [422](#)  
 remote-lan command [423](#)  
 request platform software trace archive [424](#)  
 rrc-evaluation [426](#)

## S

security [427](#)  
 security dot1x authentication-list [428](#)  
 security static-wep-key [433](#)  
 security web-auth command [434](#)  
 service-policy command [442](#)  
 service-policy qos [443](#)  
 service-template command [444](#)  
 session-timeout command [447](#)  
 set command [448](#)  
 set platform software trace [740](#)  
 show ap [637](#)  
 show ap auth-list [577](#)  
 show ap config general [582](#)  
 show ap crash-file [584](#)  
 show ap dot11 [599](#)  
 show ap dot11 24 ghz cleanair air-quality [597, 598](#)  
 show ap dot11 24ghz cleanair device type command [592](#)  
 show ap dot11 24ghz command [591](#)  
 show ap dot11 24ghz SI config [593](#)  
 show ap dot11 24ghz SI device type [594](#)  
 show ap dot11 5ghz [585, 595](#)  
 show ap dot11 cleanair summary [601](#)  
 show ap environment [603](#)  
 show ap filter all [605](#)  
 show ap filters active [604](#)  
 show ap fra [606](#)  
 show ap gps location [607](#)  
 show ap link-encryption [609](#)  
 show ap master list [614](#)  
 show ap name [620, 623, 625, 626, 627](#)  
 show ap name auto-rf [616](#)  
 show ap name config [621](#)  
 show ap name dot11 [624](#)  
 show ap name wlan [628](#)  
 show ap multicast mom [615](#)  
 show ap profile [630](#)  
 show ap summary [634](#)  
 show ap tag sources [635](#)  
 show arp [638](#)  
 show arp summary [639](#)  
 show avc client command [640](#)  
 show avc wlan command [641](#)  
 show chassis [642](#)  
 show flow exporter command [652](#)  
 show flow record command [658](#)  
 show interfaces command [659](#)  
 show ip [666](#)  
 show ldap attributes command [668](#)

show ldap server command [669](#)  
 show nmsp cloud-services statistics [731](#)  
 show nmsp cloud-services summary [732](#)  
 show nmsp command [730](#)  
 show platform condition [737](#)  
 show platform software system all [739](#)  
 show platform software trace level [741](#)  
 show policy-map command [748](#)  
 show ssh [753](#)  
 show tech-support wireless command [756](#)  
 show wireless band-select command [792](#)  
 show wireless client [793](#)  
 show wireless client mac-address [794](#)  
 show wireless client mac-address command [796, 797](#)  
 show wireless client timers command [799](#)  
 show wireless country command [800](#)  
 show wireless detail command [803](#)  
 show wireless dot11h [804](#)  
 show wireless dtls connections command [805](#)  
 show wireless exclusionlist [806](#)  
 show wireless load-balancing command [807](#)  
 show wireless pmk-cache command [817](#)  
 show wireless profile flex [818](#)  
 show wireless summary command [821](#)  
 show wireless urlfilter details command [823](#)  
 show wireless urlfilter summary command [824](#)  
 show wireless vlan details [825](#)  
 show wireless wgb mac-address [826](#)  
 show wireless wgb summary [827](#)  
 show wireless wps rogue ap command [828](#)  
 show wireless wps rogue client detailed command [829](#)

## T

tag rf [473](#)  
 tag site site-tag [474](#)

## U

udp-timeout command [480](#)  
 umbrella-param-map command [481](#)

## V

violation [488](#)

## W

wgb broadcast-tagging [489](#)  
 wgb vlan [490](#)  
 whitelist acl command [491](#)  
 wireless aaa policy [494, 495](#)  
 wireless broadcast vlan command [497](#)  
 wireless client command [498](#)  
 wireless client mac-address command [500](#)

- wireless country [507](#)
- wireless load-balancing command [510](#)
- wireless macro-micro steering probe-suppression [512](#)
- wireless macro-micro steering transition-threshold [511](#)
- wireless profile policy [526](#)
- wireless security dot1x command [529](#)
- wireless security web-auth retries command [536](#)
- wireless tag policy [537](#)
- wireless wps client-exclusion command [540](#)
- wireless wps rogue rule command [563](#)
- wireless-default radius server command [566](#)
- wlan wlan1 policy policy1 [567](#)